Mötesbok: Tekniska nämnden (2026-09-24)

Tekniska nämnden

Datum: 2026-09-24

Plats: Kommunstyrelsens sammanträdesrum

Kommentar:

Dagordning

Beslutsärende

UMEÅ KOMMUN

Tjänsteskrivelse
2026-09-04

Tekniska nämnden

Diarienr: TN-2026/00011

Fastställande av dagordning och fråga om jäv september

Förslag till beslut
Tekniska nämnden beslutar

att fastställa sammanträdets dagordning.

att till protokollet notera att ingen person är jävig.

Ärendebeskrivning
Tekniska nämndens föredragningslista finns som bilaga och eventuella ändringar noteras. En jävig person får varken delta i handläggningen av ärendet eller vara närvarande vid nämndens behandling av ärendet.

Beslutsunderlag
Föredragningslista. Bilaga.

UMEÅ KOMMUN

Kallelse/Föredragningslista

Tekniska nämnden

Tid: Torsdagen den 24 september 2026 kl. 10:00

Plats: Kommunstyrelsens sammanträdesrum

Beslutsärende			
1	Fastställande av dagordning och fråga om jäv september	10.00	
2	Verksamhetsuppföljning T2 2026	10.05	Karin Isaksson/ Marucs Bystedt
3	Teknisk ramjustering gällande postdistribution och Väven	10.25	Marcus Bystedt
4	Beslut av riskbedömning och fortsatt användning av Microsoft	10.35	Mattias Wallmark
5	Remiss AI-styrning: Policy för AI och Riktlinje för AI-användning	11.10	Hannes Fries
6	Yttrande Motion 11/2026: Umeå kommun behöver styra sin AI innan implementering	11.25	Mattias Wallmark/ Hannes Fries
7	Begäran om omfördelning inom beslutad investeringsram	11.45	Mattias Wallmark
8	Yttrande Remiss informationssäkerhetspolicy och riktlinje informationssäkerhet	13.00	Rowena Jalkanen
9	Yttrande Remiss om ändrade villkor gällande BK4 i Trafikverkets föreskrifter om bärighetsklasser TRV 2026/92928	13.10	Jonas Sörlén
10	Yttrande Remiss av förslag till ändring i bestämmelserna om texthöjd och bård för varningsskyltar	13.20	Jonas Sörlén
11	Yttrande Remittering av promemoria: Vägval för framtiden: Justeringar av vägmärken i vägmärkesförordningen (2007:90)	13.30	Fredrik Öhrner
12	Aktuellt från förvaltningen september	13.40	Karin Isaksson
13	Kurser och konferenser september	14.30	
14	Delegationsbeslut och anmälningsärenden september		

UMEÅ KOMMUN

Tjänsteskrivelse
2026-09-01

Tekniska nämnden

Diarienr: TN-2026/00007

Verksamhetsuppföljning T2 september 2026

Förslag till beslut
Tekniska nämnden beslutar

att godkänna verksamhetsuppföljningen för januari – augusti (T2) 2026.

att godkänna uppföljningen av nämndens internkontrollplan för januari – augusti (T2) 2026.

att den interna styrningen och kontrollen är tillräcklig.

att godkänna Rapport fr Tekniska nämnden till KS för perioden jan – aug 2026.

att anse ärendet direktjusterat.

Ärendebeskrivning
Verksamhetsuppföljning för januari – augusti har tagits fram för nämndens verksamheter och en uppföljning av internkontrollplanen för samma period är gjord.

Beslutsunderlag
Tekniska nämndens delårsrapport T2 2026. Bilaga.
KS-2025-0187 Tekniska nämndens rapport till KS för perioden jan - aug 2026. Bilaga.
Uppföljning Tekniska nämndens riskanalys och internkontrollplan T2 2026. Bilaga.

Beredningsansvariga
Marcus Bystedt
Christina Ingmanson
Karin Isaksson
Verksamhetschefer

Beslutet ska skickas till
KSdiarium, KSrapportering, Marcus Bystedt, Karin Isaksson
Märk med KS-2025/0187

Riskanalys

Nämnd: Tekniska nämnden
Upprättad: 2025-11-03

Internkontrollplan 2026

Tekniska nämnden
2025-11-03

Steg 1 - Riskinventering ska nämnden vara direkt delaktig i			Steg 2 - Riskvärdering ska nämnden vara direkt delaktig i				Steg 3 - Nämndsansvarig chef tar fram förslag som beslutas av nämnd					
Kontrollområde	Identifierad risk	Nr	Sannolikhet	Konsekvens	Risk-värde	Rekommenderad riskhantering	Nr.	Inriktning för riskhantering från nämnd	Åtgärd	Status	Ansvarig	Återrapporteras
Samhällssäkerhet	Extremväder och naturolyckor Extremväder eller naturolyckor kan göra gator och vägar oframkomliga, orsaka omfattande skador på kommunens fastigheter och anläggningar samt påverka nämndens möjlighet att utföra sitt uppdrag och/eller påverka medborgarnas vardag samt egendom negativt.	R1	Sannolik	Allvarlig	16	Minimera risk	R1	Minimera risk	**Aktiviteter:** Genomföra en kommunövergripande klimatanalys med hjälp av SMHI, samt framtagande av åtgärdsplan utifrån denna. Ras- och skredriskundersökning längs strandpromenaden. Testa och utveckla nya lösningar för klimatanpassningar och dagvatten (Tvårån, Djupbäcken och centrala Umeå) **Löpande kontrollåtgärder:** Kontinuerlig uppdatering av beredskapsplanen i samarbete med den rekryterade klimatanpassningsstrategen för att minimera riskerna och stärka samhällets motståndskraft.		Teknisk direktör	*T3*
Samhällssäkerhet	Civil beredskap. Det finns en risk att nämnden har otillräckliga resurser och kompetens för att hantera sina nytilldelade ansvarsområden inom civil beredskap. Detta kan försvåra effektiv krishantering, samverkan med andra aktörer samt långsiktig planering för att upprätthålla samhällsviktig verksamhet vid störningar eller kriser.	R2	Sannolik	Allvarlig	16	Minimera risk	R2	Minimera risk	**Aktiviteter:** Skapa förutsättningar för tilldelade ansvarsområden. Fortbildning av förvaltningen Kris- och säkerhetsforum. Framtagande av informationsmaterial för förvaltningen. Översyn och säkerställande av relevanta kommunikationakanaler. Kontinuitetsplanera. **Löpande kontrollåtgärder:** Regelbunden (tertialvis) uppföljning i nämnd.	Förvaltningens Kris- och säkerhetsforum har genomgått utbildningar och planerar för övningar. Arbete med beredskapsuppdragen pågår.	Teknisk direktör	*T1, T2, T3*
Samhällssäkerhet	Cybersäkerhet Det finns en risk att otillräcklig cybersäkerhet leder till ökade incidenter, vilket kan påverka verksamhetens kontinuitet, informationssäkerhet och tillgång till samhällsviktiga funktioner negativt.	R3	Möjlig	Allvarlig	12	Minimera risk	R3	Minimera risk	**Aktiviteter:** Vidareutveckla vår förmåga och styrning inom cybersäkerhet. **Löpande kontrollåtgärder:** Granskning av IT-säkerhetspolicys och rutiner, inklusive incidenthantering och backup. Löpande uppföljning av inträffade IT-incidenter och lärdomar från dessa. Regelbunden kontroll av åtkomsthantering, behörigheter och användning av säker autentisering. Utvärdering av tekniska skyddsåtgärder, såsom brandväggar, antivirus och kryptering. Samverkan med IT-säkerhetsfunktioner och externa experter vid behov.	Upphandling av ett Security Operations Center pågår.	Verksamhetschef DoIT	*T2,T3*
Samhällssäkerhet	Säkerhetslösningar Det finns en risk att nämnden inte hinner identifiera, prioritera och implementera nödvändiga säkerhetslösningar i takt med samhällsutvecklingen och förändrade krav. Detta kan leda till brister i samhällssäkerheten, exempelvis genom otillräckliga lås- och tillträdessystem som möjliggör obehörig åtkomst till fastigheter.	R4	Möjlig	Allvarlig	12	Minimera risk	R4	Minimera risk	**Aktiviteter:** Inventering och riskbedömning av befintliga lås- och tillträdessystem i kommunens fastigheter. Granskning av rutiner för tillträdesrättigheter, inklusive hantering av nycklar, passerkort och digitala behörigheter. **Löpande kontrollåtgärder:** Regelbunden omvärldsbevakning av nya säkerhetskrav och tekniska lösningar inom samhällssäkerhet.	Ett förvaltnings-övergripande arbete är under uppstart.	Teknisk direktör	*T2, T3*
Klimat/Miljö	Risk att Umeå kommuns miljömål ej nås.	R5	Sannolik	Kännbar	12	Minimera risk	R5	Minimera risk	**Löpande kontrollåtgärder:** Regelbunden uppföljning av miljömålens status och indikatorer i nämndens verksamhetsområden. Granskning av miljökrav i upphandlingar, projekt och drift. Regelbunden kontroll av energianvändning, avfallshantering och utsläpp från kommunens fastigheter och anläggningar. Samverkan med miljöstrategiska funktioner inom kommunen.	Arbete pågår löpande. Förvaltningen har ett Miljöforum där dessa frågor tas om hand och som samverkar med andra funktioner inom kommunen.	Teknisk direktör	*T2, T3*
Bristande takkonstruktion fastigheter	Om dokumenterade brister i takkonstruktioner inte åtgärdas finns risk för skador på fastigheter, med potentiella konsekvenser för både säkerhet och drift. Bristande underhåll eller otillräcklig kontroll kan förvärra risken.	R6	Möjlig	Allvarlig	12	Minimera risk	R6	Minimera risk	**Aktivitetер:** En åtgärdsplan för förstärkning eller renovering av utsatta konstruktioner finns framtagen och arbete med åtgärder fortsätter under 2026.	Risken bedöms reducerad efter genomförda åtgärder i enlighet med handlingsplan. Fastighet har en god kontroll över takens konstruktioner.	Fastighetschef	*T1, T2, T3*

Styrning/Ekonomi	Anläggningars standard. Det finns en risk att kommunens anläggningar får försämrad standard till följd av bristande underhåll och otillräckliga resurser. Detta kan påverka funktion, säkerhet och långsiktig kostnadseffektivitet negativt.	R7	Möjlig	Kännbar	9	Reducera risk	R7	Reducera risk	**Löpande kontrollåtgärder:** Regelbunden granskning av underhållsplaner och faktisk genomförandegrad. Regelbunden uppföljning av budgeterade medel för drift och underhåll i relation till behov. Årlig inventering av anläggningars skick och prioritering av åtgärder utifrån risk och påverkan. Kontroll av avvikelser mellan planerat och utfört underhåll. Samverkan med ekonomifunktioner för att säkerställa långsiktig finansiering.	Arbetet följer plan med löpande uppföljning av underhåll, budget, avvikelser och finansiering.	Ekonomichef, Fastighetschef	*T2, T3*
Styrning/Ekonomi	Upphandling och avtalsuppföljning. Det finns en risk att brister i upphandling och avtalsuppföljning leder till att tjänster eller leveranser uttörs med låg kvalitet, försenas eller medför ökade kostnader. Detta kan påverka nämndens verksamhet, ekonomi och förtroende negativt.	R8	Möjlig	Kännbar	9	Reducera risk	R8	Reducera risk	**Aktiviteter:** Fortsatt genomförande av framtagen handlingsplan med föreslagna åtgärder. (2025) **Löpande kontrollåtgärder:** Regelbunden granskning av upphandlingsprocesser och efterlevnad av gällande regelverk. Regelbunden uppföljning av avtalens innehåll och leverantörers prestationer mot avtalade krav. Riskbedömning vid större upphandlingar eller strategiska avtal. Samverkan med upphandlingsbyrån för kompetensstöd och kvalitetssäkring.	Arbetet pågår tillsammans med upphandlingsenheten och en ny delegationsordning ska uppdateras under året.	Ekonomichef	*T2, T3*
Kriminalitet och otillåten påverkan	Det finns en risk att organisationen saknar tillräckliga kunskaper, rutiner och skydd för att förebygga och hantera brottslighet eller otillbörlig påverkan. Detta kan utsätta verksamheten för ekonomiska risker likväl risker som påverkar integritet, tillit och förmåga att fatta självständiga beslut.	R9	Möjlig	Kännbar	9	Reducera risk	R9	Reducera risk	**Aktiviteter:** I samverkan med Upphandlingsbyrån: Genomgång av rutiner för incidentrapportering och hantering av otillåten påverkan. Utbildning av medarbetare i att identifiera och agera vid försök till otillbörlig påverkan eller brott. **Löpande kontrollåtgärder:** Samverkan med säkerhetsfunktioner och rättsvårdande myndigheter vid misstanke om brott eller påverkan.		Teknisk direktör	*T3*
Demografi	Det finns en risk att förändringar i befolkningens åldersstruktur medför ökade krav på snabb omställning av kommunens ytor och lokaler. Om nämnden inte hinner anpassa verksamhetsmiljöer i takt med demografiska förändringar kan det påverka tillgänglighet, funktion och kvalitet i samhällsservicen.	R10	Möjlig	Lindrig	6	Reducera risk	R10	Reducera risk	**Löpande kontrollåtgärder:** Analys av demografiska trender och prognoser i samverkan med planeringsfunktioner. Granskning av lokalbehovsplanering utifrån olika åldersgrupper (t.ex. äldreomsorg, förskola, fritidsverksamhet). Regelbunden uppföljning av flexibilitet i lokalutnyttjande, inklusive möjligheter till omställning eller delning av ytor. Regelbunden kontroll av investeringsplaner i relation till befolkningsutveckling. Löpande samverkan med andra nämnder och aktörer för att identifiera behov och synergier.		Teknisk direktör	*T3*
Regelverk och teknikanpassning	Det finns en risk att hög komplexitet i regelverk och krav kring teknikens användning försvårar införandet av digitala lösningar inom nämndens verksamhet. Detta kan påverka säkerhet, effektivitet och verksamhetens smidighet negativt, särskilt om regelverken inte är anpassade till ny teknik	R11	Möjlig	Lindrig	6	Reducera risk	R11	Reducera risk	**Aktiviteter:** Inventering av juridiska hinder kopplade till teknik- och systemanvändning inom nämndens ansvarsområden. **Löpande kontrollåtgärder:** Regelbunden granskning av efterlevnad av relevanta regelverk, exempelvis GDPR, offentlighetsprincipen och upphandlingslagstiftning. Samverkan med juridisk kompetens vid införande av ny teknik eller digitala lösningar. Kontroll av att tekniska lösningar är förenliga med krav på informationssäkerhet och integritet.		Verksamhetschef DoIT	*T3*
		R12			0		R12					
		R13			0		R13					
		R14			0		R14					
		R15			0		R15					
		R16			0		R16					
		R17			0		R17					

Tekniska nämnden
Delårsrapport T2 2026

Dokumentansvarig: Teknik- och fastighetsförvaltningen
Fastställd av: Tekniska nämnden, XXXX-XX-XX
Version: 0.0
Dokumentdatum: 2026-09-01
Reviderad: 2026-xx-xx

Innehållsförteckning

UMEÅ KOMMUN

Viktiga händelser under andra tertialet

Tekniska direktören har ordet

Karin Isaksson, teknisk direktör.

Den milda vintern har medfört lägre kostnader för snöröjning av både tak och vägar än budgeterat, vilket delvis har kompenserat för de ökade kostnaderna inom färdtjänsten till följd av det tillfälliga avtal som tecknades efter entreprenörens konkurs.

Planeringsarbetet inför kommande mandatperiod har fortsatt under perioden. Planeringsdirektiven tydliggör behovet av att möta framtida utmaningar kopplade till befolkningstillväxt, investeringsbehov, lokalförsörjning, klimatanpassning och ett förändrat omvärldsläge. Förvaltningen arbetar vidare med att skapa långsiktiga förutsättningar för en hållbar utveckling av kommunens verksamheter och infrastruktur.

För att stärka organisationens förmåga att möta framtidens krav har beslut fattats om att inrätta en stabsfunktion. Syftet är att skapa bättre förutsättningar för förvaltningens chefer, möjliggöra ett mer närvarande ledarskap samt minska sårbarheten genom en mer robust organisation. Förändringen förväntas även stärka utvecklingskapaciteten och bidra till en organisation som i högre grad harmoniserar med kommunens övriga förvaltningar.
Arbetet med samhällssäkerhet och civil beredskap har fortsatt att vara prioriterat. Inom måltidsservice pågår insatser för att stärka beredskapsförmågan, bland annat genom projektet Måltidsservice Beredskapsstöd. Inom konceptet Öva enkelt har flera kök påbörjat utbildning och övning med alternativ tillagningsutrustning som ska kunna användas vid störningar eller krissituationer.
Under perioden har även implementeringen av kommunens riktlinje för upphandling och inköp påbörjats. Arbetet syftar till att säkerställa att upphandlingar och inköp genomförs i enlighet med kommunfullmäktiges policy och att kommunens resurser används på ett effektivt, hållbart och affärsmässigt sätt.

Digitalisering och informationssäkerhet är fortsatt viktiga fokusområden. Antalet försök till angrepp mot kommunens IT-infrastruktur är fortsatt högt, vilket ställer krav på ett aktivt och systematiskt säkerhetsarbete. Parallellt pågår arbete med juridiska bedömningar av Microsofts tjänster för att säkerställa att kommunens användning uppfyller gällande krav och regelverk.

Karin Isaksson

Karin Isaksson, teknisk direktör

UMEÅ KOMMUN

Verksamhetsrapport

UMEÅ KOMMUN

Underlag för verksamhetsrapport

Bedömning och motivering uppfyllnad av grunduppdrag

Verksamheten bedömer enligt bedömningskriterium (t.h.) uppfyllnad av sitt grunduppdrag samt lämnar en kortfattad beskrivning över vad som ligger till grund för bedömningen.

Verksamhetens utveckling och väsentliga händelser

Kortfattad beskrivning hur verksamheten har utvecklats under perioden samt väsentliga händelser som påverkat utveckling eller resultat. Tabeller, grafer eller diagram som nyttjas redovisas över tid (trend) samt kompletteras med en kvalitativ analys.

Status prioriterade aktiviteter

Verksamheten redovisar status över prioriterade aktiviteter samt tilldelade tilläggsuppdrag.

Bedömnings-kriterium	Definition	Symbol
I hög grad uppfyllt	Verksamheten har under perioden verkställt sitt grunduppdrag helt eller i hög omfattning i enlighet med planeringsdirektivet, nämndens verksamhetsplan och givna förutsättningar.	
I viss grad uppfyllt	Verksamheten har under perioden verkställt delar av sitt grunduppdrag, men behöver vidta åtgärder inom vissa områden	
Ej uppfyllt	Verksamheten har under perioden inte alls eller i liten omfattning uppfyllt sitt grunduppdrag.	

UMEÅ KOMMUN

Status tilläggsuppdrag

Uppdrag	
Tilläggsuppdrag 2025:1 Kommunfullmäktige ger alla nämnder i uppdrag att genomföra en analys av konsekvenser utifrån förändrade demografiska förutsättningar. Arbetet ska säkerställa att kommunen inte åtar sig kostnader som inte kan bäras över tid, samt ske i enlighet med av fullmäktige fastställd riktlinje för god ekonomisk hushållning. Förslag på förändring av principiell karaktär ska tillställas fullmäktige.	Samtliga verksamheter inom Tekniska nämnden arbetar med sina respektive analyser.
Tilläggsuppdrag 2023:1 Kommunfullmäktige ger kommunstyrelsen och nämnderna i uppdrag att öka omställningen av nämndernas verksamheter för att klara grunduppdraget i takt med att personalbristen ökar.	Omställningsarbetet inom verksamheten hanteras löpande. Fokus är att säkerställa grunduppdraget genom anpassade arbetssätt och effektiv resursanvändning.
Tilläggsuppdrag 2023:2 Kommunfullmäktige ger kommunstyrelsen och nämnderna i uppdrag att öka samarbetet och ansvarstagandet över förvaltnings- och nämndgränser.	Löpande arbete pågår för att öka samarbetet och ansvarstagandet över förvaltningsgränser.
Tilläggsuppdrag 2021:8 Kommunfullmäktige ger kommunstyrelsen i uppdrag att tillsammans med kommunens nämnder och bolag undersöka risken för att skattemedel, som bekostar verksamheter inom välfärdssektorn, även med annan utförare än kommunen, används på ett felaktigt sätt och/eller i kriminellt syfte, till exempel för att finansiera organiserad brottslighet, samt att ta fram förslag på åtgärder för att förebygga och förhindra detta.	Arbete pågår tillsammans med bl a Upphandlingsenheten för att utveckla metoder för att minska risken att skattemedel finansierar organiserad brottslighet.

Digital omställning & IT

Bedömning och motivering

Under året har vi hittills levererat de tjänster som ligger inom vårt uppdrag. I mätningar så väl som i dialoger i styrgrupper, verksamhetsdialoger och liknande får vi övervägande positiv återkoppling och i det fall negativa synpunkter sker det ofta på ett konstruktivt sätt.

Befintliga och nya e-tjänster och automationsrobotar sparar tid i kommunens verksamheter.
Arbetet med att utveckla kommunens förmågor inom data och AI har god progress och är uppskattat.

Utifrån de förutsättningar vi har för att utföra vårt uppdrag är den samlade bedömningen att vi uppfyller det i hög grad

BEDÖMNING

UMEÅ KOMMUN

Digital omställning & IT

Verksamhetens utveckling och väsentliga händelser

Under årets två första tertial har stort fokus legat på den fortsatta organisationsutvecklingen inom DoIT. Arbetet med att forma och stabilisera team samt produktdomäner har intensifierats. I dag finns cirka 15 team med olika uppdrag och förutsättningar. För att skapa tydligare riktning, bättre samordning och stärkt verksamhetsnytta införs nu ett nytt arbetssätt där teamen samlas i produktdomäner. För att ge teamen bättre stöd och riktning har vi påbörjat ett gediget arbete med en verksamhetsmålbild och färdplan att nå önskade lägen. Vi har också initierat en utökning av enhetschefer så att de ska kunna stötta medarbetarnas omställning i vår egen verksamhetsutveckling.

DoIT har också under inledningen av året mottagit erbjudande från SKR och initiativet Handslag för digitalisering om att ansluta till GSIM. En analys pågår av hur kommunen kan och bör engagera sig i detta arbete. GSIM* bedöms vara ett viktigt förutsättningsskapande initiativ som ligger i linje med regeringens nationella digitaliseringsstrategi och kan stärka kommunens förmåga till samverkan och effektiv digital utveckling.

Vidare pågår uppstart av Umeås deltagande i det regionala initiativet AI Västerbotten. Arbetet innebär samverkan med bland annat Skellefteå och övriga kommuner i regionen kring gemensam AI-plattform, juridiska frågor, kompetensutveckling och utbildningsinsatser. Initiativet bedöms skapa goda förutsättningar för ett mer strukturerat och ansvarsfullt införande av AI i kommunal verksamhet.

DoIT har bidragit med kompetens i samband med hanteringen av visselblåsarfunktionen och har levererat en krypterad inbox för att säkerställa att en trygg kanal finns även efter att avtalet med den tidigare leverantören hävts.

För att stötta omsorgsverksamheterna har vi lagt en stor mängd arbetstid med egen personal och med konsultstöd för att bidra till ett så bra upphandlingsunderlag som möjligt utifrån angivna tidsramar.

BEDÖMNING

UMEÅ KOMMUN

*GSIM = grundläggande förutsättningar för ett samlat invånarmöte

Status prioriterade aktiviteter

Plan för digital omställning – data som strategisk tillgång	
Kommunens planering och beslutsfattande stärks genom ökad användning av dataunderlag.	
• Öka antalet unika användare på app.powerbi.com med 50%. • Användarnöjdhet för analysverktyg framtagna i Power BI överskrider 85%. • Ytterligare 6 kommungemensamma datamängder är tillgängliggjorda för analys eller AI-tillämpningar.	Bra framdrift hittills, 1001 aktiva användare, vilket är en ökning med 80%. 47 kommungemensamma datamängder är tillgängliggjorda för analys eller AI-tillämpningar.
Plan för digital omställning – robust och säker digitalisering: Cybersäkerhet	
En gemensam målbild för behörighetshantering i kommunen är framtagen.	
Målarkitektur för teknisk plattform inom behörighetshantering är framtagen och beslutad. • Ta fram en gemensam informationsmodell för behörighetshantering för de fyra vanligast rekryterade befattningarna. • Minst 85 % av användare är nöjda med prototypen för gränssnittet för ansvarig chef.	Arbete pågår. Teknisk målarkitektur på övergripande nivå är framtagen, och tillhörande icke-funktionella krav är under revision.
Plan för digital omställning – robust och säker digitalisering: Cybersäkerhet	
Driftprocesser säkras genom automatisering av driftsättning, underhåll och övervakning.	
• De tio mest tidskrävande manuella processerna är kartlagda. • Minst fem av de kartlagda processerna är automatiserade. • Samtlig central infrastruktur är dokumenterad och tillgänglig vid kris.	Ej påbörjad, Tidförskjuten p.g.a. andra prioriteringar.
Plan för digital omställning – effektivare styrning och samordning	
Förtydliga ansvar och mandat inom verksamhetsutveckling och omställning med stöd av digitalisering.	
• Initiera och driva utredning och tydliggöra roll- och ansvarsfördelningen för digital omställning för att vid behov föreslå revideringar i reglementen och ägardirektiv.	Arbete för att föreslå revideringar i reglementen är pågående och sker tillsammans med Stadsledningskontoret.
• Utreda och föreslå principer för finansiering och prioritering för att möjliggöra att medel nyttjas effektivt och till det som skapar önskat värde med syfte att strukturer kan etableras för det långsiktiga och kommunövergripande digitaliseringsarbetet, inklusive nödvändiga styrdokument.	Mycket stor aktivitet med många beroenden för förankring samt arbete med så väl politiker som kommunens tjänstepersonledning.

Status prioriterade aktiviteter

Plan för digital omställning – bättre användning av kommunens resurser

Minska tekniskt strul och öka trygghet hos kommunens anställda genom systematisk förändringshantering och incidenthantering.

• Implementera en första version av en kommunövergripande incidentprocess. • Inför en verksamhetsövergripande förändringslogg enligt ITIL (infomation technology infrastructure library). • Rätt systemstöd för kommunövergripande incidentprocess implementerat. • Minska antalet IT-beställningar som kräver komplettering från användare med 50 %.	Arbete med processer och systemstöd pågår. Målsättningen att minska antalet IT-beställningar som kräver komplettering från användare med 50% har redan uppnåtts.

Plan för digital omställning – effektivare styrning och samordning

Förstärka styrning av digitalisering genom rätt underlag och principer.

• Sju stödjande arkitekturprinciper inom digitaliseringsområdet är framtagna. • Dokumentera beroenden mellan processer och system för kommunens tolv mest samhällsviktiga tjänster. • Modell för styrning av digitalisering är framtagen och presenterad i SDF.	Underlag till principer för arkitektur inom ramen för digitalisering har påbörjats inför analys och prioritering av vilka principer som genomförs först. Dokumentation av beroenden har påbörjats inom området personal- och lönesystem men har prioriterats om för att möta omsorgsverksamhetens systemflora, med anledning av kommande upphandling.

Plan för digital omställning – kunskaper, förståelse och färdigheter

Stärka Umeå kommuns förmåga att snabbt omsätta digitaliseringens möjligheter.

• Genomföra minst tre pilotinitiativ som inte tar längre tid än ett kvartal, med nya digitala lösningar kopplade till något av de strategiska områdena i Plan för digital omställning. • 80 % av deltagare i pilotinitiativen upplever att de fått tillräcklig kompetens för att förstå, omsätta och utvärdera de digitala lösningarna. • Identifiera och dokumentera minst fem framgångsfaktorer för snabb omställning i samverkan med verksamheterna.	Hittills är två pilotinitiativ genomförda.

UMEÅ KOMMUN

Fastighet

Bedömning och motivering

Verksamhetens uppdrag är att säkerställa att kommunens lokalbehov tillgodoses, att fastighetsbeståndet förvaltas, driftas och underhålls på ett kostnadseffektivt sätt samt att investerings- och underhållsprojekt genomförs med hög kvalitet. Under perioden har uppdraget genomförts med hög måluppfyllelse, och verksamheten bedöms ha levererat enligt plan.

De gynnsamma väderförhållandena under våren har medfört ett lågt behov av snöröjning och sandning, vilket har skapat goda förutsättningar för att uppdragen har kunnat genomföras i hög grad enligt plan.

BEDÖMNING

UMEÅ KOMMUN

Fastighet

Verksamhetens utveckling och väsentliga händelser

Året har präglats av en lägre nederbördsmängd än normalt, vilket har minskat behovet av snöhantering och takskottning och därmed medfört lägre kostnader. Arbetet med att analysera fastigheternas takkonstruktioners bärighet har slutförts och en handlingsplan har tagits fram för det fortsatta arbetet.

Under perioden har stort fokus lagts på lokalförsörjnings- och investeringsplanering som underlag för budgetarbetet. Planeringen har anpassats utifrån förändrade demografiska förutsättningar och en lägre befolkningsutveckling än tidigare prognosticerat.

Flera större bygg- och investeringsprojekt pågår under året. Utbyggnaden av Vasaskolan fortsätter med två nya flyglar samtidigt som Rosa huset byggs om till skolkök. Byggnationen av Östra brandstationen har påbörjats och arbetet med en ny skola i Stöcke inleds under året. Den nya skolbyggnaden vid Hedlundaskolan har färdigställts. Parallellt fortsätter satsningarna på utbyggnad av skolkök och skolrestaurang samt renovering och modernisering av den befintliga skolmiljön.

Införandet av det nya fastighetssystemet fortskrider enligt plan, men har krävt betydande personella resurser under perioden. I nära samverkan med DOIT och Datadriven kommun har arbetet med en automatiserad verksamhetsuppföljning i huvudsak färdigställts. Uppföljningen bygger på data från bland annat fastighets- och ekonomisystemen och visualiseras i Power BI, vilket ger verksamheten förbättrade möjligheter till analys, uppföljning och styrning.

Arbetet med att uppdatera och återställa kommunens skyddsrum fortsätter. Inventeringar och analyser visar att flera anläggningar är i behov av omfattande åtgärder för att återställa funktion och uppfylla gällande krav, vilket innebär betydande investeringsbehov under kommande år.

BEDÖMNING

UMEÅ KOMMUN

Status prioriterade aktiviteter

Införande av fastighetssystemet Pythagoras

Fortsatt införande av det nya fastighetssystemet, med planerad driftsättning i juni. Systemet omfattar funktionalitet för FMS[1], PMS[2], CRM[3] och BI[4], och ersätter tidigare systemstöd. Projektet är omfattande och resurskrävande, och innebär en betydande förändring för medarbetarna. Aktiviteten inkluderar utbildning och kompetensutveckling för att stödja införandet.	Nästa del att implementera är ärendeprocessen som startar igång i början av september

Utfasning av lysrörsbelysning enligt EU-direktiv

I linje med EU:s förbud mot vissa lysrör fortsätter arbetet med att byta ut äldre belysning inom våra fastigheter. Aktiviteten bidrar till minskad energiförbrukning, ökad driftssäkerhet och efterlevnad av miljölagstiftning, inklusive ekodesignförordningen 2019/2020 och RoHS-direktivet[5].	Arbetet är i fas med liggande planering, har varit vissa utmaningar att få tillträde utanför lovperioder. Viktigt att medel avsätts årsvis.

Säkerhetskrav lås och passage nu och för framtiden

Med utgångspunkt i identifierade säkerhetsrisker initieras ett projekt för att definiera och implementera lämpliga säkerhetskrav för lås- och passagesystem i kommunala lokaler. Arbetet sker i samverkan med berörda förvaltningar och syftar till att minska risken för obehörigt tillträde och stärka skyddet av verksamhetskritiska miljöer.	En skrivelse är framtagen för beslut om fortsatt inriktningsbeslut En arbetsgrupp finns uppstartat med löpande möten och agenda för att arbeta med löpande förbättringar.

Bevaka införandet av EU:s nya direktiv om byggnaders energiprestanda (EPBD)

Fastighet bevakar utvecklingen av EU:s direktiv om byggnaders energiprestanda, EPBD[6] , vars syfte är att alla nya byggnader inom EU ska vara nollutsläppsbyggnader senast 2030. Direktivet innebär bland annat skärpta krav på energieffektivitet, omfattande livscykelbaserade klimatberäkningar och uppgradering av befintliga byggnader sett ur energi- och klimatsynpunkt. Fastighet arbetar med integrering av EPBD samt förbereder verksamheten inför att direktivet blir svensk lag under 2026.	Genomförandet av EU:s energiprestandadirektiv (EPBD) har fortsatt under 2026. Flera regeländringar har beslutats, bland annat energiklass A0 och skärpta krav på laddinfrastruktur och cykelparkering. Nya föreskrifter inom energiområdet väntas under hösten. Fastighet deltar i remissarbetet och följer den fortsatta utvecklingen av direktivet.

Status tilläggsuppdrag

Uppdrag	
Tilläggsuppdrag 2025:2 Kommunfullmäktige ger tekniska nämnden i uppdrag att som en konsekvens av förändrade demografiska förutsättningar säkerställa ett fortsatt effektivt lokalnyttjande, inklusive att tillse att frigjorda lokaler så långt det är möjligt nyttjas till verksamheter med ökade behov av lokaler, i syfte att hålla nere kommunens lokalkostnader och minska investeringsbehovet i nya lokaler. Förändrade investeringsbehov ska lyftas inom ramen för ordinarie planeringsprocess.	Det pågår dialoger med övriga nämnder avseende deras analyser av tilläggsuppdrag 2025:1 inför TNs tilläggsuppdrag 2025:2.
Tilläggsuppdrag 2025:3 Kommunfullmäktige ger tekniska nämnden och individ- och familjenämnden i uppdrag att analysera behovet och utreda förutsättningarna för annan boendeform.	Arbetet med rapporten är uppstartad.
Tilläggsuppdrag 2025:4 Kommunfullmäktige ger kommunstyrelsen, gymnasie- och vuxenutbildningsnämnden, samt tekniska nämnden i uppdrag att i dialog med berörda verksamheter och externa parter ta fram förslag på samverkan kring och samnyttjande av anläggningar för djurhållning.	Förslag är framtaget.
Tilläggsuppdrag 2025:5 Kommunfullmäktige ger tekniska nämnden och gymnasie- och vuxenutbildningsnämnden i uppdrag att analysera behovet och utreda förutsättningarna för idrottshall för Vasaskolan, samt att gymnasie- och vuxenutbildningen ges i uppdrag att se över framtida programstrukturen på kommunens gymnasieskolor.	Arbete pågår med att analysera behovet och utreda förutsättningarna.
Tilläggsuppdrag 2025:6 Kommunfullmäktige ger kommunstyrelsen, fritidsnämnden, gymnasie- och vuxenutbildningsnämnden och tekniska nämnden i uppdrag att i dialog med berörda verksamheter och föreningslivet utreda förutsättningarna för att utveckla idrottsanläggningarna Gammlia Arena, Visionite Arena och Nolia Arena ur ett tillväxtperspektiv.	Det finns en styrgrupp och en arbetsgrupp samt sammanhållande projektledare från Näringsliv. Utredning pågår.

Gator och parker

Bedömning och motivering

Nivåerna på de kvalitetsfaktorer som ligger till grund för bedömningen är i Årsrapporten för 2025 fortsatt höga i jämförelse med tidigare år eller rikssnitt. Detta kombinerat med att genomförande kraften av investeringsprojekten ökade kraftigt 2025 samt att andel under året uppstartade projekt ligger på 64%, gör att bedömningen är att Gator och parker uppfyller grunduppdraget i hög grad.

Verksamhetens utveckling och väsentliga händelser

Den ovanligt milda vintern har medfört lägre driftkostnader för vinterväghållningen än budgeterat. Samtidigt har verksamheten belastats av ökade kostnader inom färdtjänsten efter att den tidigare entreprenören försattes i konkurs och ett tillfälligt avtal behövde tecknas. Det tillfälliga avtalet innebär en betydande kostnadsökning jämfört med tidigare avtal. Ett arbete har genomförts med upphandlingsunderlag för ett nytt långsiktigt färdtjänstavtal som nu är ute för anbudsförfrågan.

Under halvåret har två projektledare tillträtt för projekten Smart och robust dagvattenhantering i subarktiskt klimat och E-NORM, vilket möjliggör fortsatt genomförande av projekten enligt plan. Projekten syftar till att utveckla kommunens förmåga att möta framtida klimat- och hållbarhetsutmaningar genom innovativa lösningar för dagvattenhantering respektive utsläppsfria bygg- och anläggningsentreprenader. Båda projekten är viktiga för Umeås långsiktiga arbete med att hantera komplexa samhällsutmaningar och stärka kommunens hållbara utveckling. Inom stadsmiljöområdet har planteringsurnor som konstruerats av elever vid Dragonskolan placerats ut längs väg 503.

Satsningen bidrar både till en attraktivare stadsmiljö och till att synliggöra samverkan mellan kommunen och skolan. Årets sommarblomsplanteringar har temat Sagoväsen, vilket har bidragit till att skapa färgstarka och uppskattade miljöer för invånare och besökare.

BEDÖMNING

UMEÅ KOMMUN

Status prioriterade aktiviteter

Skapa utrymme för utveckling	
Satsning på att öka den digitala kompetensen genom deltagande i AI-klivet.	Båda projekten är genomförda med gott resultat.
Delta i arbetet kring Datadriven kommun våren 2026.	Kompetensen i verksamheten har ökat och intresset för att arbeta med datadrivna beslutsunderlag har ökat
Klimatanpassning	
Genomföra en kommunövergripande klimatanalys med hjälp av SMHI.	Klimatanalysen är genomförd och presenterad.
Framtagande av åtgärdsplan utifrån den genomförda klimatanalysen.	Arbete pågår.
Genomföra fortsatta ras- och skredriskundersökningar längs strandpromenaden, bl.a. stabilitetsundersökning, Skeppsbron.	Arbete pågår.
Testa och utveckla nya lösningar för klimatanpassningar och dagvatten, fokus på Tvärån och Djupbäcken samt centrala Umeå.	Arbete pågår.

Status tilläggsuppdrag

Uppdrag	Resurs
TN-uppdrag 2025:1 I arbetet med stadsdelsdialoger lyfta in Holmsund/Hörnefors/Sävar som tätorter att varvas in vart tredje år och därmed att se över prioriteringsordningen för Stadsdelsdialogerna. Detta för att stärka tätorternas attraktivitet samt stimulera föreningslivet och medborgare att vara med än mer i utvecklingsarbetet. Dessutom bör dessa tätorter vid exempelvis evenemang som Höstljus eller motsvarande få ta del av någon installation.	Arbetet med stadsdelssatsningarna fortgår enligt nämndens fastställda plan. Under första halvan av 2026 har vi påbörjat genomförandet av åtgärder i Obbola, Umedalen/Backen och Hörnefors. Medborgardialoger har under försommaren genomförts i Holmsund och på Västerslätt/Rödäng.

Måltidsservice

Bedömning och motivering

Under året har vi levererat goda och hälsosamma måltider. Vi har med stabil ekonomi och bra strukturförutsättningar att fokusera på grunduppdraget att laga goda, hälsosamma och klimatsmarta måltider vilket bidrar till god folkhälsa.

Verksamhetens utveckling och väsentliga händelser

Under perioden har vi tillsammans med Säkerhet vidareutvecklat och arbetet igenom vår kontinuitetsplan. Vi har nu övergripande riskbedömt tillagningskök, mottagningskök och enportionsmatskök. Dessa kommer vi framöver använda som grund för att riskbedöma alla våra 121 kök. Arbetet med beredskap har även fortsatt med bland annat utbildningar och utredning av användning av ved eller gasol för alternativ tillagning.

Mot inriktningsmålet klimat pågår arbetet ständigt mot mer klimatsmarta måltider. Nya svenska vegetariska proteinkällor testas och delar eller hela måltider byts ut succesivt. Vårt Måltidskoncept är uppdaterat enligt nya riktlinjer från Livsmedelsverket. En film har tagits fram där vi visar upp vad och varför vi serverar den mat vi gör med målet är att få vårdnadshavare att kostnadsfritt äta i våra restauranger en gång per termin.

Den digitaliserade verksamhetsuppföljningen används och underlättar uppföljningen på alla nivåer i verksamheten. Vi kan i rapporten övergripande följa resultat för alla våra nyckeltal, produktionsmått, mål och uppdrag. Ett exempel visas nedan. Här ser vi hur kostnaderna skiljer sig mellan olika typer av kök. Förskolor är dyrast, i rapporten kan vi filtrera och få ut mer detaljerade siffror. Rapporten är ett bra beslutsunderlag.

BEDÖMNING

UMEÅ KOMMUN

Status prioriterade aktiviteter

Förmågehöjning beredskap

Utöka omställningslager till två veckor och ha en påbörjad plan för lokalt och centralt beredskapslager. Öva för att öka tillagningskapacitet utan kritiska resurser.	Ett koncept kallat Öva enkelt är påbörjat med små övningar i alla kök två ggr per termin. Större utbildning/övning är genomfört med fokus på att använda den alternativa utrustning vi köpt in.

Ny livsmedelsstrategi 2.0

Samarbete med LRF och producenter för ökad robusthet i livsmedelskedjan. Omvärldsbevaka inför kommande upphandling.	Dialogmöten med grossister inbokade. Möte med LRF har genomförts.

Nya rekommendationer från livsmedelsverket

Anpassa Måltidskoncept och menyer mot nya rekommendationer från Livsmedelsverket.	Måltidskoncept och menyer är uppdaterat enligt nya riktlinjer.

Städ- och verksamhetsservice

Bedömning och motivering
Under det första halvåret har Städ- och verksamhetsservice levererat en stabil och väl fungerande lokalvård i kommunens verksamheter. Arbetet med att möta Miljö- och hälsoskydds kravbild har fortsatt enligt framtagen handlingsplan och bidrar till en successivt förbättrad städkvalitet. Detta avspeglas i förbättrade resultat vid interna kvalitetstillsyner samt i ett väl fungerande och konstruktivt samarbete med Miljö- och hälsoskydds.

På alla kommunens förskolor har det nu genomförts en intern kvalitetskontroll. Under hösten kommer fokus bli att få alla förskolor godkända samt besöka alla grund- och gymnasieskolor. Vid uppföljningsmöten har Miljö- och hälsoskydd uttryckt att de ser positiva effekter av de förändringar som genomförts utifrån den tidigare framtagna handlingsplanen för kvalitetsförbättring.

De interna kvalitetskontrollerna visar en positiv utveckling, där en allt större andel objekt uppnår godkänt resultat. Det visar att verksamhetens långsiktiga kvalitetsarbete ger önskad effekt och skapar förutsättningar för en mer likvärdig och hållbar lokalvård.

Sammantaget bedöms verksamheten utvecklas i en positiv riktning och lever upp till sitt grunduppdrag – att med omtanke och kvalitet utföra lokalvård och service i kommunens lokaler för att skapa rena, trivsamma och hållbara miljöer, med ett gott bemötande för Umeå kommuns medborgare.

BEDÖMNING

UMEÅ KOMMUN

Städ- och verksamhetsservice

Verksamhetens utveckling och väsentliga händelser

Verksamheten har under året utvecklats enligt plan med tydligt fokus på verksamhetsmålen. Särskild prioritet har lagts på bemanningsfrågor, upphandling av ett digitalt städledningssystem samt genomförandet av handlingsplanen för förbättrad kvalitet. Därutöver har Städservice moderniserat sitt intranät och fortsatt arbetet med att utveckla och tydliggöra rutiner.

Arbetet med kvalitetskontroller inom förskola och skola har intensifierats och antalet genomförda kontroller ökar successivt. Målsättningen är att samtliga enheter ska ha granskats före årets slut. Samtidigt syns en positiv utveckling där allt fler verksamheter uppnår godkända resultat enligt den nordiska branschstandarden Insta 800.

Dialogen med miljö- och hälsoskyddsverksamheten har stärkts, vilket har bidragit till en ökad samsyn kring krav och arbetssätt. Detta har skapat bättre förutsättningar för städverksamheten att vidareutveckla rutiner och processer samtidigt som tillsynsverksamheten kan genomföras i en anpassad takt. Det löpande utbildningsarbetet i samverkan med fastighetsverksamheten har också gett resultat och bidragit till att flera äldre tillsynsärenden kunnat avslutas.

Framåt är fortsatt samverkan med miljö- och hälsoskyddsverksamheten viktig för att säkerställa en långsiktigt hållbar utveckling. Regelbundna avstämningar planeras därför att genomföras under året. Parallellt fortsätter arbetet tillsammans med utbildningsverksamheten för att tydliggöra ansvarsfördelningen inom identifierade gråzoner. Arbetet kan leda till behov av justeringar av nuvarande servicenivåer, vilket i så fall kommer att lyftas till tekniska nämnden för vidare hantering.

BEDÖMNING

UMEÅ KOMMUN

Status prioriterade aktiviteter

Digitaliserat städledningssystem

Digitalt städledningssystem skall upphandlas och påbörja implementeras under 2026 med avsikt att vara helt i drift i slutet av 2027.	Avsikten är att inom kort annonsera upphandlingen.

Förbättra bemanningsplaneringen

Verksamheten ska under 2026 fortsätta utveckla bemanningsplaneringen, i syfte att öka kontinuitet och kvalitet i verksamheten.	Ett planeringssystem tar inom kort i drift, detta bedöms successivt minska beroendet av timvikarier, öka kontinuiteten och skapa en mer flexibel och långsiktigt hållbar bemanning över tid.

Enhetliga arbetssätt och städmetoder

Utvärdera befintliga städmetoder och utveckla en plan för implementering av gemensamma, standardiserade arbetssätt och städmetoder.	Arbetet har påbörjats och bedöms vara ett långsiktigt utvecklingsarbete som kommer att genomföras successivt

Förbättrad städkvalitet

Under 2026 ska verksamheten, utifrån handlingsplanen Ökad städkvalitet 2.0, fortsätta implementera de delar av planen som ännu inte genomförts. Arbetet syftar till att säkerställa en fortsatt höjning av kvalitet, effektivitet och enhetlighet i verksamheten.	Arbetet fortskrider i enlighet med fastställd handlingsplan, där åtgärder genomförs strukturerat och successivt.

Civil beredskap

Förvaltningen arbetar aktivt med att tydliggöra det uppdrag som tilldelades under våren. Inom vissa områden behövs en resursförstärkning i form av ökad bemanning, vilket planeras åtgärdas under hösten.

Förvaltningens säkerhets- och krisforum arbetar aktiv med att höja kunskapen inom civil beredskap i förvaltningen. Ett utbildningspaket har tagits fram och erfarenhetsutbyten med kommuner som kommit långt i sitt arbete finns inplanerat.

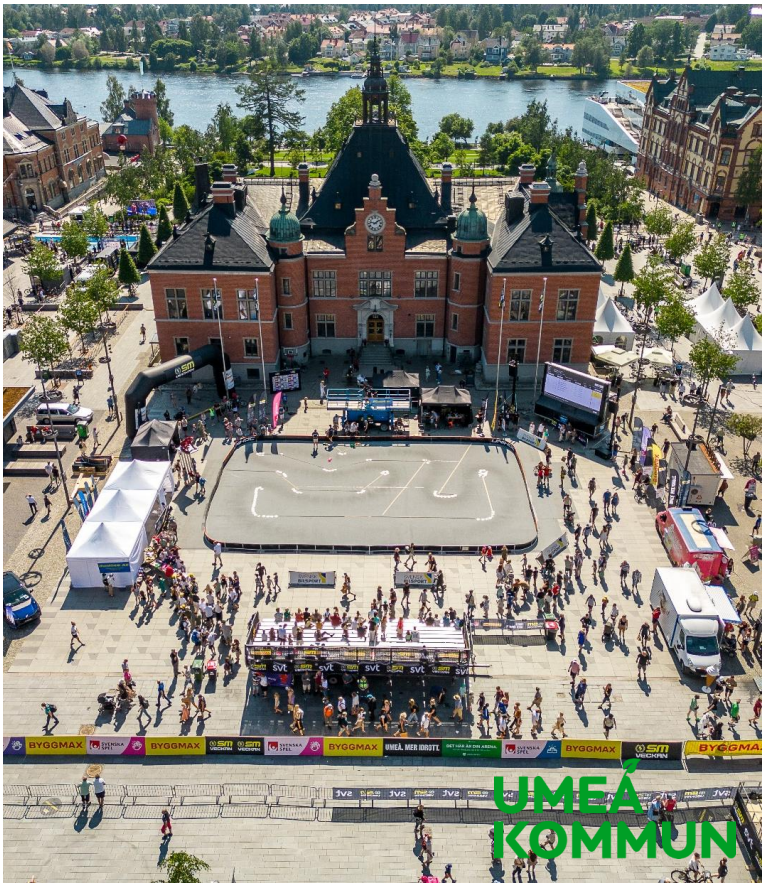
Tekniska nämnden ansvarar för	Lägesrapport T2, 2026
Uppbyggnad och drift av fast installerad samt mobil reservkraft	Arbete pågår med förmågehöjning
Lagerhållning och vid behov tillagning samt distribution av reservlivsmedel	Arbete pågår med förmågehöjning.
Lagerhållning och vid behov distribution av reservdrivmedel	Arbete pågår med resursförstärkning samt tydliggörande av uppdrag.
Lagerhållning och vid behov distribution av förbrukningsmaterial/reservdelar för att tillgodose behov i prioriterad samhällsviktig verksamhet vid samhällsstörning, kris eller krig.	Arbete pågår med resursförstärkning samt tydliggörande av uppdrag.

Inriktningsmål

Inriktningsmål 1

Umeås tillväxt ska klaras med social, ekologisk, kulturell och ekonomisk hållbarhet med visionen om 200 000 medborgare år 2050

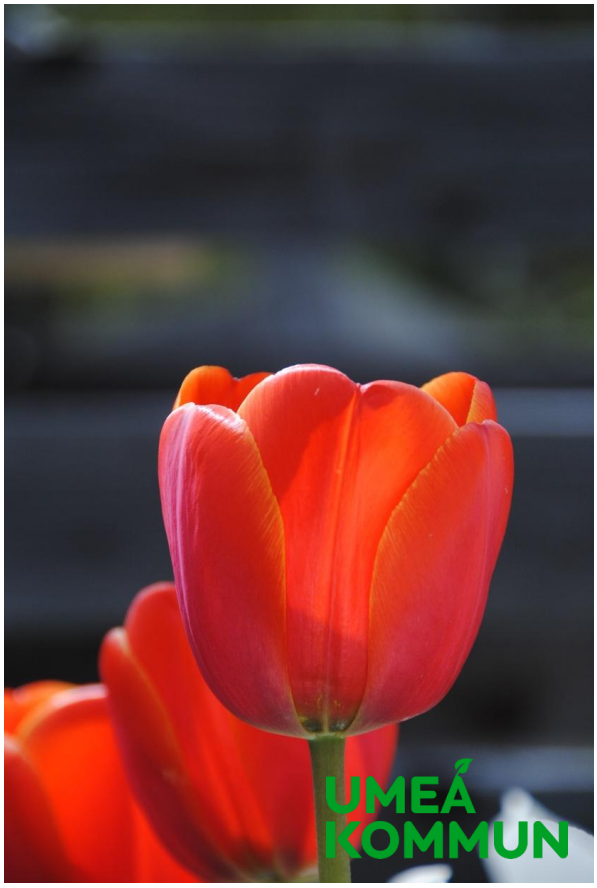
Arbetet inom Teknik- och fastighetsförvaltningen stärker Umeås attraktivitet för investeringar, kompetens och etableringar. Utmärkelsen Årets samhällsbygge, satsningen på en eldriven hjullastare och beviljade stöd från Tillväxtverket och Myndigheten för samhällsskydd och beredskap bidrar till hållbar tillväxt, innovation och en mer robust kommun.



Inriktningsmål 1

Uppföljning prioriterade aktiviteter

Uppdrag/aktivitet	Status/kommentar
Fokus på effektiv och säker implementering av IT och digitaliseringslösningar för att bidra till kommunens tillväxt och omställning.	DoIT har pågående aktiviteter för att realisera kommunens Plan för digital omställning vilket inkluderar bland annat samarbetsformer med kommunens förvaltningar och förutsättnings-skapande teknikutveckling. Det pågår också en översyn av IT- och digitaliseringsstyrningen för att utreda behov av förändrat reglemente och kompletterande policys och riktlinjer med syfte att stärka kommunens förmåga till omställning med IT.
Fokus på genomförande av investeringar	Ett arbete görs med översyn av processer för att kunna presentera fler mogna projekt i ett tidigare stadie.



Inriktningsmål 2

Umeå ska växa hållbart utan några utsatta områden

Arbetet bedrivs fortsatt i enlighet med tidigare fastställda styrdokument och inom ramen för nämndens grunduppdrag. En viktig utgångspunkt är att bidra till social hållbarhet. Genom planering, drift och underhåll av det offentliga rummet skapas trygga, säkra och inkluderande utemiljöer för alla. Insatser inom bland annat belysning, parker och naturområden stärker den sociala tryggheten, främjar möten och delaktighet samt bidrar till jämlika livsmiljöer i hela kommunen.

Inriktningsmål 2

Uppföljning prioriterade aktiviteter

Uppdrag/aktivitet	Status/kommentar
Stadsdelssatsningar, fortsätta arbetet enligt av nämnden fastställd plan.	Stadsdelsdialoger har genomförts i kommun- och stadsdelarna Holmsund och Rödäng/Västerslätt. Planering pågår för genomförandet av trygghetsvandringar i dessa områden under hösten.
Stadsdelslyft Ålidhem	Socionomstråket nedanför fotbollsplanen har i sommar omvandlats till en sommargata. Platsen har utvecklats i samarbete med elever från Ålidhemsskolan och studenter från Arkitekthögskolan. Det har placerats ut sitt- och umgängesmöbler i trä, blomsterurnor samt färgglad markmålning för att undersöka platsens potential som social mötesplats. Syftet med den tillfälliga platsbildningen har varit att utforska om platsen kan användas för möten och utevistelse med målet att öka kvaliteten och variationen i Ålidhems utemiljö samt för prioritering av gående och cyklister i trafiken.
TN-uppdrag 2025:1	Arbetet med stadsdelssatsningarna fortgår enligt nämndens fastställda plan. Under första halvan av 2026 har vi påbörjat genomförandet av åtgärder i Obbola, Umedalen/Backen och Hörnefors. Medborgardialoger har under försommaren genomförts i Holmsund och på Västerslätt/Rödäng.

UMEÅ KOMMUN

Inriktningsmål 3

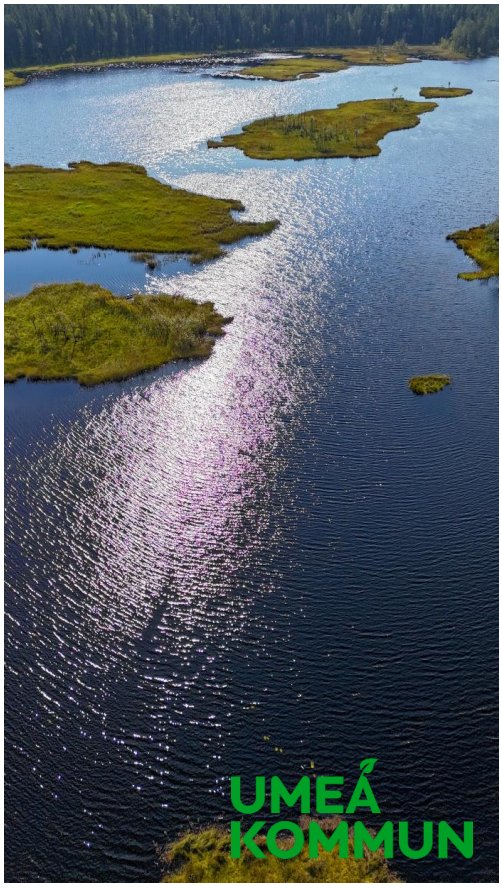
Umeå kommun ska skapa förutsättningar för kvinnor och män att ha samma makt att forma samhället såväl som sina liv

Teknik och fastighet bidrar till kommunens jämställdhetsmål genom att skapa trygga, tillgängliga och inkluderande fysiska miljöer som kan användas på lika villkor av kvinnor och män. Genom ett jämlikt samhällsbyggande, hållbara mobilitetslösningar och välskötta offentliga rum stärks möjligheterna för alla att delta i samhällslivet och forma sina egna liv. Verksamheten bidrar även internt genom arbetssätt som ökar delaktighet och inflytande.

Inriktningsmål 3

Uppföljning prioriterade aktiviteter

Uppdrag/aktivitet	Status/kommentar
Öka medborgardelaktigheten	Det är andra året dialogerna i samband med Stadsdelssatsningarna hålls på försommaren. Det har varit positivt att vara ute den ljusa årstiden. Upplevelsen är att det är lättare att få kontakt med medborgarna och fler tar sig tid att stanna och prata med oss. Elevenkäter är skickade till högstadieskola även i år.
Utveckla tryggare mötesplatser	På Västra Esplanaden har mer grönska, bänkar och en ny lekplats tillförts för att skapa en mer attraktiv och trivsam miljö. På Bölesholmarna har en ny paviljong öppnat och bidrar med sociala och rekreativa värden samtidigt som den ökar tryggheten genom att locka fler besökare till området. I Obbola genomförs belysningsåtgärder vid Ängen, bland annat vid lekplatsen, pulkabacken och fotbollsplanen. Insatserna stärker tryggheten och möjliggör fler aktiviteter under årets mörkare perioder.



Inriktningsmål 4

Umeå ska vara klimatneutralt till 2040

Under perioden har teknik- och fastighetsförvaltningen fortsatt arbetet med omställning och insatser inom inriktningsmålets fokusområden: klimat, energi, cirkulär ekonomi och hållbara transporter. Under året pågår flera utvecklings- och testprojekt för att minska förvaltningens klimatpåverkan och skapa underlag för framtida arbetssätt.

Flera aktiviteter kommer att utvärderas senare under året och bidrar till förvaltningens långsiktiga arbete mot klimatneutralitet och måluppfyllelse. Insatserna syftar bland annat till att stärka kunskap, engagemang och medvetna val hos både medarbetare och invånare. Genom exempelvis utbildningsinsatser, kommunikation och praktiska åtgärder skapas förutsättningar för en hållbar omställning som bidrar till Umeå kommuns inriktningsmål.

Inriktningsmål 4

Uppföljning prioriterade aktiviteter

Uppdrag/aktivitet	Status/kommentar
Transporter	
Testa elektrisk hjullastare i verksamhet.	Elektrisk traktor i egen drift har testats av Gator och parker under sex månader med start under vintern 2026. Elektriska arbetsmaskiner blir allt vanligare och det finns flera fördelar, exempelvis färre partiklar från avgaser, lägre klimatpåverkan i drift, minskat buller och förbättrad arbetsmiljö för föraren. Under testets gång har Gator och parker provat eltraktorn vid plogning och efterarbeten samt vid sopning av grus med gott resultat.
Hållbart resande under byggtiden i ett gatuombyggnadsprojekt genom MM.	Under T2 fortsätter arbetet med Mobility management i pilotprojektet Norra Obbolavägen. Fokus ligger på att genomföra de åtgärder som tagits fram under T1 för att underlätta hållbara transportval under byggskedet. Under hösten genomförs en testresenärsaktivitet riktad till boende och förbipasserande i området, där cirka 100 periodkort erbjuds under en testperiod. Hastighetsdisplayer sätts upp i bostadsområdet och arbetet med att testa det nya digitala informationsverktyget BUKO fortsätter. Erfarenheter från aktiviteterna kommer att följas upp och användas i det fortsatta arbetet med Mobility management i gatuombyggnadsprojekt.
Bygg och anläggning	
Upphandla ett byggprojekt med utsläppsfri byggarbetsplats	Fastighet testar att genomföra projektet Malmen 27 med utsläppsfri byggarbetsplats, arbetet pågår.
Klimatberäkna ett anläggningsprojekt	Gator och parker klimatberäknar Renmarkstorget och Fastighet klimatberäknar utemiljön på Älvan 1, båda pågår och resultat förväntas under hösten.

UMEÅ KOMMUN

Inriktningsmål 4

Uppföljning prioriterade aktiviteter

Uppdrag/aktivitet	Status/kommentar
Energi (el och fjärrvärme)	
Anordna ett energiutbildningstillfälle för Fastighets drifttekniker	Utbildning inom energi har genomförts under april. Fler utbildningar planeras till hösten 2026.
Testa digitalt verktyg för visualisering av byggnaders energiprestanda	Envista testas just nu på fastighetsbeståndet för att visualisera byggnadernas energiprestanda. Utvärderas senare under 2026.
Testa effekthantering och beteendecoaching i storkök	Awareify, effekthantering och beteendecoachning, testas just nu i sex stycken olika storkök och kommer att utvärderas senare under 2026.
Cirkulär ekonomi	
Utöka möjligheten att sortera kartong och plast för Städs verksamhetsavfall genom inköp av avfallskärl	Utökning av möjligheten att sortera kartong och plast från Städs verksamhetsavfall har genomförts på aktuella städobjekt.
Lansera digitalt återbruks-verktyg för teknik- och fastighetsförvaltningens medarbetare	Appen "Återbruksportalen" är lanserad och används av teknik- och fastighetsförvaltningens medarbetare för att öka cirkularitet av förvaltningens produkter. Användandet av appen har kommit i gång bra. Nästa steg är att automatisera sammanställning av statistik för produkter som återbrukas via Återbruksportalen. Hittills under 2026 motsvarar förvaltningens besparingar genom återbruk ca 2,9 miljoner kronor och ca 35 tusen ton kg CO_2e. Digital omställning och IT jobbar kontinuerligt med att förlängs livslängd på digitala enheter.
Förlänga livslängd på digitala enheter genom aktiv hantering och återbruk	Digital omställning och IT jobbar kontinuerligt med att förlängs livslängd på digitala enheter. DoIT har övergått från egen regi till att återbruka utrustning via ram-avtalspart.
Övergripande insatser	
Genomföra en hållbarhetsutbildning för Måltidsservices medarbetare	Hållbarhetsutbildning för Måltidsservices medarbetare hålls under hösten 2026.
Skapa en film för vårdnadshavare om hållbarhetsarbete kring livsmedel	Film för vårdnadshavare är framtagen.
Genomföra en temadag med lokala varor/livsmedel	Regnbåge från Kalix har funnits på menyn under våren samt är planerad till en gång varje månad inom äldreomsorgen under året. Måltidsservice undersöker fler alternativ för temadag med lokala varor/livsmedel

Rapporter

Personuppgiftsincidenter

Förvaltningens arbete med dataskydd och informationssäkerhet bedöms överlag fungera tillfredsställande. De återkommande årliga utbildningarna samt de insatser som genomförs både centralt och lokalt bidrar till att personuppgiftskoordinatorerna har goda förutsättningar att utföra sina uppdrag på ett effektivt sätt.

De fyra incidenter som inträffade under perioden avsåg felaktigt skickade e-postmeddelanden innehållande personuppgifter samt borttappade passerkort. Samtliga incidenter bedöms ha varit orsakade av den mänskliga faktorn och har hanterats i enlighet med gällande rutiner.

År	Antal incidenter	Antal anmälda vidare
2018	3	1
2019	6	0
2020	9	1
2021	9	1
2022	3	1
2023	12	0
2024	10	0
2025	10	0
2026, T1	3	0
2026, T2	4	0

Tabellen visar antal incidenter per år.

Personalrapport

Måluppfyllelse personalpolitiska mål

Personalpolitiska mål	Bedömning av nämndens arbete med personalpolitiska mål
Mål 5: Umeå kommun ska klara kompetensförsörjningen genom att vara en attraktiv arbetsgivare och spegla mångfalden i samhället.	Enligt plan
Mål 6: Umeå kommun ska ha ledarskap som ges och ger förutsättningar för goda resultat, där riktvärdet för antalet medarbetare per chef inte är fler än 30.	Enligt plan
Mål 7: Umeå kommuns sjukfrånvaro ska minska genom fokus på friskfaktorer och jämställda arbetsförhållanden.	Enligt plan

Tabellen visar bedömning av nämndens arbete med de personalpolitiska målen med bedömningskriterierna; Enligt plan/ Mer arbete krävs.

Resultatmått	Målvärde 2025	Utfall jan–augusti 2026			Utfall jan–augusti 2025		
		kvinnor	Män	totalt	kvinnor	män	totalt
Sjukfrånvaro, totalt i procent av anställdas sammanlagda ordinarie arbetstid	6,0	6,6	3,8	5,4	7,3	4,6	6,1
Andel långtidsfriska (%)	65	58	68	63	56	64	60
Andel heltidsanställda (%)	96	95	98	96	95	98	97

Tabellen visar utfall i procent för resultatmåtten; Sjukfrånvaro, Långtidsfriska, Heltidsanställda.

Kompetensförsörjning och attraktiv arbetsgivare

Den årliga lönekartläggningen har genomförts inom Umeå kommun och förvaltningen Teknik och fastighet. Resultatet visar att lönerna inom förvaltningen är jämställda mellan kvinnor och män, både utifrån löneläge och arbetsvärdering. I arbetsvärderingen ingår bland annat arbetets krav, utbildningsnivå och marknadspåverkan.

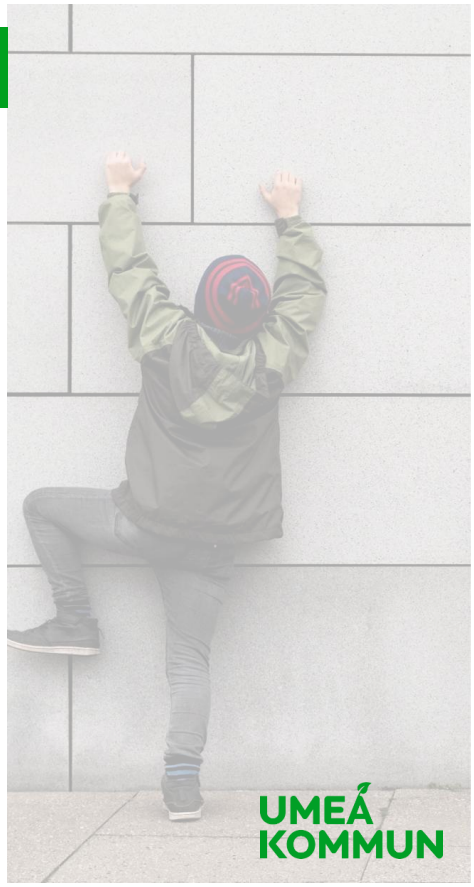
Lönekartläggningen genomförs i syfte att upptäcka, åtgärda och förebygga osakliga löneskillnader mellan kvinnor och män i enlighet med diskrimineringslagen. Inom Teknik och fastighet finns cirka 70 olika befattningar som har jämförts med varandra samt med övriga befattningar inom Umeå kommun. Att vi kan visa på jämställda och rättvisa löner är en viktig faktor, inte minst för arbetsgivarvarumärket. Det bidrar också till att stärka kommunens och förvaltningens attraktivitet som arbetsgivare

Under perioden har det nuvarande lärplattformen Learning Management Systemet (LMS) utvärderats utifrån hela Umeå kommuns behov. Utvärderingen visar att systemet bör avvecklas och ersättas med ett liknande system som redan används Infocaption Kunskapsbanken. Förändringen bedöms ge en mer effektiv budgetanvändning och bättre möta verksamhetens behov.

HR-enheten Teknik och fastighet har genomfört en workshop för chefer inom Fastighet med fokus på dialog och erfarenhetsutbyte inom kompetensförsörjning. Dialogerna berörde karriär, utveckling, arbetsgivarvarumärke samt resultat- och utvecklingssamtal.

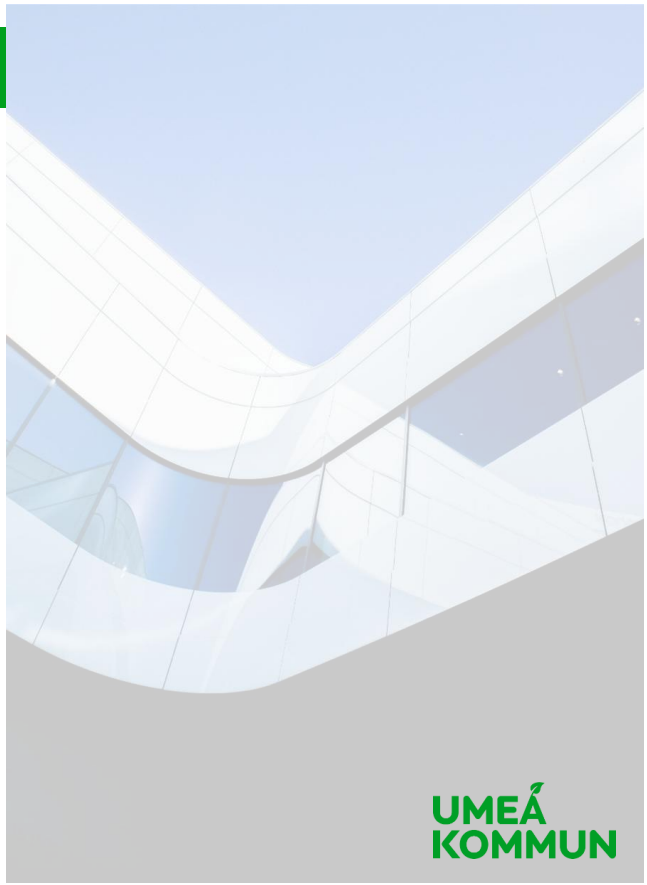
Workshopen kopplades till verksamhetens kompetensförsörjningsplan och syftade till att stärka det strategiska arbetet med att utveckla, behålla och attrahera kompetens.

En omvärldsbevakning genomfördes för att få en bild av fastighetsbranschen, dess utveckling och de behov som finns inom området.



Ledarskap

Fokusområdet för ledarskapet inom Teknik och fastighet är chefers förutsättningar och synliggöra samt tillvarata lärande i arbetsvardagen. Under april samlades Ledarforum i Medlefors i Skellefteå för nätverkande och erfarenhetsutbyte inom förvaltningen. När cheferna har rätt förutsättningar att leda blir vardagen bättre för alla som arbetar inom förvaltningen.



Friskfaktorer

I maj genomfördes en workshop med Teknik och fastighets nya skyddsombud och nya chefer på har genomförts. Workshopen handlade om roller och ansvar, arbetsmiljöns regler och vikten med att göra riskbedömningar.

Nu har arbetet i projektet SAMBA (Samverkansmodell för att behålla arbetskraft) resulterat i tio prototyper på nya och effektiva samverkansformer med målet att behålla arbetskraft på arbetsmarknaden, sex från hösten 2025 och fyra under vårterminen 2026. Prototyperna kommer finnas med i det fortsatta arbetet under hösten där planen är att djupdyka i förutsättningar, möjligheter och behov i de egna deltagande organisationers rehabprocesser, bla inom Teknik och fastighet, för att fånga upp tidiga signaler och möjliggöra och etablera tidiga insatser.

Som en del av implementeringen av arbetet med säkerhetskultur har förvaltningens arbetsmiljöingenjör genomgått utbildning i MTO (Människa, Teknik och Organisation). MTO-metodiken ger stöd för att identifiera såväl riskfaktorer som friskfaktorer och bidrar till ett mer systematiskt arbetsmiljöarbete. Kompetenshöjningen utgör en grund för det fortsatta arbetet med att utveckla en stark säkerhetskultur och en hållbar arbetsmiljö inom verksamheten.

Ekonomirapport

Nämndens budgetavvikelse jan-aug 2026: 35,2 mnkr

Nämndens resultat per aug är ett överskott på 52,7 mnkr jämfört med budget fördelat per verksamhet enligt tabell. Resultatet är ca -4,0 mnkr lägre än föregående rapport och jämfört med resultatet samma period föregående år, 8,3 mnkr, så är resultatet cirka 40 mnkr bättre. Det som skiljer mellan åren är i huvudsak att vintern är mer kostnadsmässigt gynnsam, samt att resultatet för fastighet, måltidsservice, städ samt gemensamt är bättre jämfört med 2025 medan resultatet för DoIT är sämre.

För gator och parker har året börjat med väldigt låga kostnader för vintern vilket återspeglas i resultatet. För färdtjänst är det ett underskott för perioden kopplat till ny entreprenad pga konkurs som kommer medföra stora kostnader för året.

Resultatet för fastighet är ett överskott för perioden. Låga kostnader för snöröjning lyfter resultatet samt överskott inom exempelvis hyresintäkter medan mediakostnaderna har ett underskott för perioden, främst på grund av fjärrvärmekostnader.

Verksamhet	Utfall augusti 2026	Utfall augusti 2025
Gator och parker	24,1	8,6
Fastighet	18,0	-9,5
DoIT	-2,2	5,2
Måltidsservice	2,8	4,5
Städ-och verksamhetsservice	1,0	-2,1
Gemensamt	4,9	1,5
Totalt, mnkr	**48,6**	**8,3**

Måltidsservice har ett överskott för perioden kopplat till livsmedel, men planerade inköp av ekologiska och närproducerade livsmedel kommer minska det överskottet under året.

Inom DoIT och Städ- och verksamhetsservice är det överskott på personalkostnader efter semesterperioden samt att det finns budget för ett nytt verksmanhetssystem som inte nyttjats.

Inom gemensamt är det ett överskott beroende på bidrag från livsmedelsverket kopplat till civil beredskap, kostnader kommer under året.

UMEÅ KOMMUN

Prognos per augusti 2026: 7,0 mnkr

Prognosen för perioden visar ett förväntat överskott på 7,0 mnkr mot budget.

Vintern har totalt sett varit kostnadsmässigt fördelaktig inledningsvis för året både inom gator och parker och fastighet, men kommande kostnadsökningar inom främst färdtjänst drar ner resultatet under resterande del av året. För DoIT drar kostnader för cybersäkerhet och lagstiftning ner resultatet, och för städ innebär personalkostnader högre än budget ett underskott. Måltidsservice har ett överskott inledningsvis, där kommer satsningar på ekologiskt och närproducerat minska det överskottet under året men verksamheten räknar med att gå 1 mnkr plus. Under gemensamt är det överskott för perioden främst då statsbidrag kopplat till civil beredskap har betalats ut, där är planen att nyttja de medel som finns innan årets slut.

I övrigt mindre avvikelser för verksamheterna.

Verksamhet	Prognos 2026	Prognos 2026	Prognos 2026	Resultat
	Maj	Juni	Juli	2025
Gator och parker	-5,0	0,0	2,0	9,8
Fastighet	13,0	13,0	11,0	-14,1
DoIT	-3,0	-3,0	-5,0	-2,1
Måltidsservice	1,0	1,0	1,0	5,3
Städ & verksamhet	-2,0	-2,0	-2,0	-5,3
Gemensamt	0,0	0,0	0,0	-2,9
Totalt, mnkr	**4,0**	**9,0**	**7,0**	**-9,3**

Under nuvarande förutsättningar är det väldigt svårt att göra en säker prognos, dock är det mer sannolikt med ett större överskott mot budget än prognosen, därför ska prognosen bedömas med en osäkerhet på + 20 och -10 mnkr. Nämnden påverkas till stor del av yttre faktorer som prisökningar och väder, som inte går att styra. Avvikelser mot budget hanteras genom att anpassa volym, ambition eller servicenivå där så är möjligt.

UMEÅ KOMMUN

Fastighet

Periodresultat 18,0 mnkr

Skötsel/tillsyn redovisar ett överskott för perioden som uppgår till 12,6 mnkr. Den främsta orsaken till överskottet beror på att vinterkostnaderna varit låga dvs låga kostnader för snöröjning. Högre externa hyresintäkter beror bla på att GVN har lämnat över lägenheter till Fastighet from 2026 samt på en engångsintäkt på 6,6 mnkr från en extern hyresgäst som lämnat ett hyresavtal i förtid. För perioden redovisas ett överskott på 10,2 mnkr. Personalkostnaderna redovisar ett överskott på 3,4 mnkr vilket förklaras av bl.a. vakanser. Energikostnaderna redovisar ett underskott som uppgår till -3,7 mnkr och beror främst på höga kostnader för värmeförbrukning. Högre externa hyreskostnader beror bl.a. på att GVN lämnat över lägenheter till Fastighet from 2026. För perioden redovisas ett underskott på -3,6 mnkr. Övriga kostnader slutar sammantaget med ett underskott på -0,9 mnkr

Specifikation vinterkostnader, tkr	Periodbudget	Periodutfall	Periodavvikelse	Årsprognos
Skötsel/tillsyn	**-52 540**	**-39 960**	**12 581**	**12 500**
varav snöröjning mm	*-32 656*	*-20 182*	*12 474*	
Media	**-84 994**	**-88 741**	**-3 747**	**-5 500**
varav elkostnader	*-38 694*	*-38 287*	*407*	
varav värmekostnader	*-35 034*	*-38 976*	*-3 942*	
varav vattenkostnader	*-11 266*	*-11 478*	*-213*	
Skador	**-6 667**	**-6 276**	**391**	**0**
varav vinterskador		*-410*	-410	

Varav takskottning, tkr	tom 2026-08	2025	2024	2023
Takskottning (utfall)	-2,4	-5 243,7	-2 828,6	-9 935,0

Tabell: Specificering kostnader kopplade till vintern

Fastighet

Prognos 11 mnkr

Skötsel/tillsyn bedöms redovisa ett överskott som uppgår till 12,5 mnkr. Överskottet beror uteslutande på låga snöröjningskostnader. De externa hyresintäkterna bedöms i slutet av året att redovisa ett överskott som uppgår till 9,0 mnkr och som beror på övertagande av lägenheter från GVN samt på en engångsintäkt på 6,6 mnkr från en extern hyresgäst som lämnat ett hyresavtal i förtid. Personalkostnaderna bedöms i slutet av året att redovisa ett överskott på 3,0 mnkr som beror på vakanser och ökat antal tjänster med tidskrivning. Däremot bedöms energikostnaderna att sluta med ett underskott som kommer att uppgå till -5,5 mnkr. Underskottet beror främst på höga kostnader för värmeförbrukning. Högre externa hyreskostnader beror bla på att GVN lämnat över lägenheter till Fastighet from 2026 samt på höga engångskostnader på förhyrda lokaler och bostäder. Vid årets slut beräknas underskottet uppgå till -4,0 mnkr. Det planerade underhållet bedöms vid årets slut att redovisa ett underskott som uppgår till -5,0 mnkr. Övriga poster bedöms sammantaget att visa ett överskott på 1,0 mnkr.

Gator och parker

Periodresultat 24,1 mnkr

Gator och vägar (32,9 mnkr) Året inleddes med väldigt mild vinter. Parker (0,2 mnkr). Ett litet överskott för parker hittills för året. Färdtjänst (-9,8 mnkr). På grund av konkurs har en direktupphandling gjorts vilket medför ökade kostnader.

Prognos 2,0 mnkr

Årsprognosen på 2 mnkr är fördelat på gator och vägar (22 mnkr), parker (0 mnkr) och färdtjänst (-20 mnkr). Det finns en risk att beläggningsavtalet blir dyrare p.g.a. högre drivmedelspriser som kommer av världsläget.

Digital omställning och IT

Periodresultat –2,2 mnkr

Intäkterna avviker med 0,7 mnkr. Personalkostnaderna avviker för perioden med 2,8 mnkr beroende på sjukfrånvaro, VAB, föräldraledigheter, samt tjänstledighet. Ökade licens- och konsultkostnader på sammanlagt -5,9 mnkr. Konsulter nyttjas bla för att täcka upp där ordinarie personal saknas och konsulter som arbetar med omsorgsprojektet och Public 360. Det finns även mindre avvikelse på -0,1 mnkr som består av näthyra, IT och digitalutrustning samt förbrukningsmaterial. I övrigt mindre avvikelser på 0,3 mnkr.

Prognos -5,0 mnkr

En liten avvikelse på uppskattningsvis 0,5 mnkr för ökad försäljning för helåret. Personalkostnaderna ser i dagsläget ut att avvika med 3,0 mnkr mot lagd årsbudget. Flertalet rekryteringar pågår. Konsulter används där egen personal saknas. För efterlevnaden av den nya cybersäkerhetslagen kommer behovet av konsulter och licenser överstiga årsbudget med sammanlagt -8,5 mnkr enligt de bedömningar som kan göras i dagsläget. Arbete pågår med att identifiera åtgärder för att minska avvikelsen. Övriga poster förväntas hålla budget.

Måltidsservice

Periodresultat 2,8 mnkr

Den positiva avvikelsen beror på minskade livsmedelskostnader (2,8 mnkr) och minskade personalkostnader (0,5 mnkr) samt övriga kostnader (-0,5 mnkr) positiva avvikelsen beror på minskade livsmedelskostnader (3,9 mnkr) och minskade personalkostnader (0,6 mnkr).

Prognos 1 mnkr

Kostnaderna för livsmedel förväntas öka under året på grund av inköp av ekologiska & närproducerade artiklar och successivt minska det inledande resultatet. Överskottet är kopplat till rabatterade priser på årslistan hos leverantörer.

Städ och verksamhetsservice

Periodresultat 1,0 mnkr

Personalkostnaderna ligger efter semesterperioden på 0,2 mnkr i överskott. Intäkterna visar ett litet överskott med 0,2 mnkr bestående av bidrag och försäljning. Högre kostnader för förbrukningsmaterial, -0,3mnkr beroende på både prisökningar samt ökat behov. Återhållsamhet med nyttjandet av externt städ ger 0,1 mnkr. Upphandling av ett nytt städsystem finns budgeterat men inga kostnader, därav budgetavvikelse på ca 0,8 mnkr.

Prognos -2,0 mnkr

Intäkterna ser ut att följa lagd budget medan personalkostnaderna mest troligt kommer att avvika med -1,5 mnkr vid årets slut, främst beroende på behov av vikarier. Kostnader för förbrukningsmaterial kommer uppskattningsvis generera en avvikelse med ca -0,5 mnkr, där prisökningar, avtal samt ett fortsatt stort behov är orsakerna.

För att minska den negativa avvikelsen planerar verksamheten att minska nyttjandet av externt städ samt att minska nyttjandet av vikarier där det är möjligt.

Gemensamt

Periodresultat 4,9 mnkr

Gemensamma kostnader och kostnader för ledning och politik redovisas här, samt kostnader för beredskap. Överskottet beror till största del på bidrag från livsmedelsverket kopplat till civil beredskap, kostnader kommer under året. Därutöver mindre överskott kopplat till personal och övrigt.

Prognos 0,0 mnkr

Prognosen är satt till 0 mnkr. Kostnader för civil beredskap kommer under året och planen är fortsatt att nyttja de medel som finns budgeterat, likaså för förvaltningsgemensamma kostnader.

Investeringar

Investeringsutfall jan-augusti 2026: -652,9 mnkr

Tekniska nämndens investeringsbudget uppgår per april till -955,0 mnkr varav -652,9 mnkr nyttjats, vilket ger ett överskott på 302,1 mnkr. Överskottet beror till största del på tidsförskjutningar.

Prognosen för året är -1 226,9,0 mnkr, 286,9 mnkr under budget. Dock finns alltid en risk att det blir tillkommande tidsförskjutningar eller förseningar gällande fastighetsinvesteringar vilket i så fall förändrar prognosen.

(mnkr med en decimal)	Budget 31 augusti 2026	Utfall 31 augusti 2026	Budget-avvikelse 31 augusti 2026	Utfall helår 2025	Budget helår 2026	Prognos helår 2026	Årsprognos budgetavvikelse 2026
Fastighet	-674,2	-496,5	117,7	-665,1	-1 092,7	-879,6	213,1
Gator och parker	-208,3	-113,7	94,6	-526,4	-312,5	-265,5	56,0
IT	-53,9	-39,0	14,9	-59,1	-80,8	-77,7	3,1
Övrigt	-18,6	-3,7	14,9	-12,5	-27,8	-13,1	14,7
Summa	**-955,0**	**-652,9**	**302,1**	**-1 263,1**	**-1 513,8**	**-1 226,9**	**286,9**

Tabell: Nämndens investeringar

Fastighet investeringar

Fastighets totala investeringsbudget för 2026 uppgår till -1 092,7 mnkr och prognosen för året är satt till -879,6 mnkr, dvs ett överskott på 213,1 mnkr. Orsaker till överskottet är att flera projekt inte har startat än, pausats eller har en förskjuten tidsplan, även om flera projekt har en tidigarelagd tidsplan också. Genomförandegrad med nuvarande prognos är ca 80 procent.

(mnkr med en decimal)	Budget 31 aug 2026	Utfall 31 aug 2026	Budget-avvikelse 31 aug 2026	Utfall helår 2025	Budget helår 2026	Prognos helår 2026	Årsprognos budgetavvikelse 2026
Vasaskolan gymn elevökn	-118,7	-89,9	-28,8	-62,1	-151,5	-141,0	10,5
Brandstation Umeå Östra	-41,5	-38,3	3,2	-6,5	-97,4	-66,0	31,4
Hedlundaskolan ny- & ombyggn F-6	-42,5	-45,0	-2,5	-32,8	-52,4	-59,6	-7,1
Rödängs skola utbyggnad en parallell F-6	-4,0	-0,9	3,1	-0,2	-50,0	-2,0	48,0
Grisbackaskolan matsal	-34,7	-27,6	7,1	-46,0	-45,5	-36,8	8,6
Daglig verksamhet	-16,9	-16,9	0,0	-3,3	-39,4	-41,0	-1,6
Kulturskola	-20,7	-10,6	10,0	-9,3	-37,1	-34,3	2,8
Gruppboende 2024 1, Prydnadsbusken 2 plan	-24,2	-26,9	-2,6	0,0	-30,6	-34,0	-3,4
Förstärkt serviceboende Malmen 27 2 plan	-14,5	-7,9	6,6	-3,6	-29,2	-20,0	9,2
Innertavle ersätt en byggnad för åk 4-5	-16,7	-8,1	8,6	-10,9	-26,5	-15,0	11,5
Summa	**-344,3**	**-272,0**	**62,3**	**-174,8**	**-559,7**	**-449,7**	**110,0**

Tabell: Fastighets 10 största investeringar

Om- och tillbyggnaden av **Vasaskolan**, som i framtiden kommer att benämnas **Vasagymnasiet**, pågår för att möta ett ökade elevantal. Projektet omfattar bland annat tillbyggnad av två flyglar, ombyggnad av Vasaskolan och Rosa huset. I de norra och södra flyglarna pågår byggnadsarbeten, installationsarbeten för el, ventilation och VS. I södra flygeln påbörjas dessutom montering av skärmtegel under september. I Rosa huset pågår gjutning av mellanbjälklag samtidigt som stommen till tillbyggnaden monteras. Under oktober och november planeras installationsarbetena att påbörjas även där. I Vasaskolan pågår fönsterbyten med nya fönsterbrädor av sten och justering av ventilation. Prognosen för projektet för 2026 uppgår till -141,0 mnkr och projektets bedömda slutkostnad uppgår till -265,7 mnkr. Detta innebär en avvikelse mot budget om 10,5 mnkr för år 2026 och totalt 90,0 mnkr för hela projektet. En bidragande orsak till den positiva budgetavvikelsen är att den tidigare planerade idrottshallen har utgått ur projektet. Projektet har påverkats av tidsmässiga förskjutningar till följd av omfattande asbestsanering och hantering av sulfidjord i Rosa huset. Förutsatt att inga ytterligare hinder uppstår bedöms slutbesiktning kunna genomföras i mars 2027 för Vasaskolan och flyglar och i början av juni 2027 för Rosa huset.

Nya **brandstation Umeå östra** på Tomtebo Strand är inne i entreprenadskedet och just nu arbetar man med yttertaket av byggnaden och räknar med att ha ett tätt klimatskal i slutet av september. Entreprenaden är planerad att färdigställas i slutet av november 2027. Budgeten för 2026 är -97,4 mnkr och prognosen är på -66,0 mnkr. Den totala prognosen i projektet ser ut att hamna under budget med god marginal. Anbudet låg under de kalkyler som tagits fram under planeringsskedet. Kalkylerna baserades på nyckeltal från andra nyligt byggda brandstationer i landet och projektet ser ut att markant landa under kostnaden för andra nyligt byggda brandstationer.

Illustration Brandstation Umeå östra

UMEÅ KOMMUN

På **Hedlundaskolan** blev den nya byggnaden färdigställd i november 2025 med godkänd slutbesiktning och verksamheten flyttade in och startade upp i lokalerna i januari 2026. Nu befinner sig projektet i sin andra fas där renovering och utbyggnad av befintliga byggnader är i full gång. Det har dykt upp mer asbest än planerat vilket har resulterat i extra kostnader och tid samt att entreprenadindex har stigit mer än planerat. Tidplanen för entreprenaden är förlängd med en vecka jämfört med avtalad tid, men verksamhetsstart är fortsatt planerad till vårterminen 2027. Prognosen för 2026 är -59,6 mnkr och budget är -52,4 mnkr, dvs 7,1 mnkr över budget för året och prognosen för hela projektet ser ut att hamna strax över totala budgeten. De största osäkerheterna just nu är utvecklingen av index samt några fåtal, men stora tillkommande arbeten, där ansvarsfrågan för kostnaderna är under utredning.

Rödängs skola utbyggnad en parallell F-6 är i programskede där planlösning utformas tillsammans med verksamheten. Programskedet har tagit längre tid och därför har projektet förskjutits i tid. Projektet har minskats jämfört med ursprunglig plan och det gör att den totala prognosen understiger budgeten. Budgeten för 2026 är -50,0 mnkr och prognosen visar på -2,0 mnkr.

Utbyggnaden av kök och matsal på **Grisbackaskolan** för att möta det ökade elevantalet befinner sig i slutet av första huvuddelen som är själva tillbyggnaden och slutbesiktning utfördes i juni 2026 och verksamheten har flyttat in. Efter det fortsätter ombyggnad av befintliga matsalen, ombyggnad av skolgård och rivning av paviljong och de arbetena kommer att bli klara under höst/vinter 2026. Budgeten för året är på -45,5 mnkr och prognosen visar på -36,8 mnkr. Slutprognosen för hela projektet ser ut att kunna hållas. Under hösten pågår ombyggnation av by02 och den kommer stå klar för slutbesiktning i december 2026. Även markarbete på skolgården pågår och kommer stå klar för slutbesiktning i september 2026. Allt arbete ligger i fas.

Nybyggnaden av hus på Magistervägen på **Sofiehem 5:2 för daglig verksamhet** inom IFN är nu i inne i slutfasen av arbetet med stommen. De sista gjutningarna på betongstommen är utförda och nu pågår arbete med yttertak och utfackningsväggar. Byggnaden kommer ha ett tätt klimatskal i slutet av september. Entreprenaden har kommit i gång som den ska och entreprenören har för avsikt att färdigställa entreprenaden till årsskiftet 2027/2028, ca 5 månader innan kontraktstiden löper ut. Prognosen för 2026 ligger på -41,0 mnkr och budget -39,4 mnkr. Den ackumulerade budgeten i projektet ser ut att kunna hållas med stor marginal, vilket bland annat beror på låga anbud med anledning av hård konkurrens om jobben.

Projektet med **Kulturskola** består egentligen av två byggprojekt i två olika fastigheter, Nanna 5 vid Vasagymnasiet och Hamnmagasinet på Stormen 1. Projektet på Nanna 5 är klart och verksamheten har flyttat in under sommaren 2026. Det här projektet har en delbudget på -16,5 mnkr och en prognos på -15,0 mnkr. Projektet blev försenat med ca 5 veckor på grund av komplicerade avväxlingar som behövde omprojekteras och utföras då det var brister i K-relationsritningar. Projektet på Hamnmagasinet på Stormen 1 är ute på upphandling, första upphandlingen avbröts då samtliga anbudslämnare blev diskvalificerade. Planen är att komma i gång med byggskedet under oktober månad. Det här projektet har en delbudget på -30,0 mnkr och har just nu en total prognos på -34,0 mnkr tills anbuden är öppnade. Projekteringsskedet förlängdes med 4 veckor på grund av svåra akustiklösningar kring en stor del av bottenvåningen och utmaningar kring ventilationen. Tidplanen är att nya Hamnmagasinet ska vara i klart för inflyttning under sen vår 2027.

Projektet med **Gruppboende 2024, 1 Prydnadsbusken 2 plan** är i byggskede och byggnaden förväntas vara klar i december 2026. Budgeten för året är på 30,6 mnkr och prognosen visar på att -34,0 mnkr. Den totala budgeten på 46,0 mnkr ser ut att hållas.

Projektet för **förstärkt serviceboende Malmen 27 2 plan** är upphandlad och tilldelad entreprenör och själva byggnationen har startat i maj 2026. Projektet fortlöper enligt tidplan. Prognosen för året är uppdaterat utefter entreprenörens betalplan och är korrigerad till -20,0 mnkr och budget är på -29,2 mnkr. Den totala prognosen för projektet kommer att rymmas inom den totala budgeten på -46,0 mnkr och tidplanen ser ut att hållas.

Projektet med **Innertavle skola ersätt en byggnad för åk 4-5** upphandlades i våras för själva byggnaden. Tilldelningen överklagades av en entreprenör och förvaltningsrätten har under vecka 34 avslagit överklagan. Plattan på marken är dock på plats. Planen var att byggnaden skulle vara klar att tas i bruk till höstterminen 2027. Denna tidplan kommer inte att hålla på grund av överklagan på tilldelningsbeslutet. Ny tidplan kommer tas fram tillsammans med entreprenör då de har rätt till tidsförlängning enligt gällande villkor i upphandlingen. Budget för 2026 uppgår till -26,5 mnkr och prognosen till -15,0 mnkr. Projektet fick en utökad budget med -14,0 mnkr till totalt -54,0 mnkr i vårens budgetbeslut. Den totala prognosen ser ut att hållas inom nya budgeten.

UMEÅ KOMMUN

Gator och parker investeringar

Utfallet för Gator och parker är per augusti -113,7 mnkr, 94,6 mnkr lägre än budget. För året prognostiseras att -256,5 mnkr kommer att nyttjas, vilket är ett överskott på 56 mnkr.

Renmarkstorget, ombyggnationen av torget blir något senarelagt då dagvattenanläggningen under torget måste åtgärdas först. Ombyggnationen börjar projekteras under 2027. Prognos för helår är ett överskott på 36,2 mnkr.

Norrbyskär, kraftiga fördyrningar pga. bristfälliga handlingar från konsult som har medfört förseningar och ökade kostnader genom bland annat att en tillfällig kaj har behövt byggas. Skadeståndsprocess gentemot konsult är inledd..

Stadsutveckling innanför ringen, första åtgärder genomförda, ombyggnation av cykelstället vid Västra Esplanaden har påbörjats för att tillföra mer grönska samt lekmöjligheter i stadsmiljö. Prognos för helår är ett överskott på 18,2 mnkr. Större åtgärder kommer genomföras under kommande år.

(mnkr med en decimal)	Budget 31 aug 2026	Utfall 31 aug 2026	Budget-avvikelse 31 aug 2026	Utfall helår 2025	Budget helår 2026	Prognos helår 2026	Årsprognos budgetavvikelse 2026
Renmarkstorget	-29,3	-4,8	24,4	-9,5	-43,9	-7,7	36,2
Norrbyskär	-21,3	-40,8	-19,5	-4,8	-32,0	-56,0	-24,1
Stadsutveckling innanför ringen	-17,5	-2,7	14,8	-3,1	-26,2	-8,1	18,2
Tvärån klimatanpassning	-16,5	-0,1	16,4	-0,2	-24,8	-0,2	24,6
Kungsgatan	-9,8	-4,0	5,7	-1,4	-14,6	-7,0	7,7
Norra Obbolavägen	-7,7	-5,6	2,1	1,4	-11,6	-6,1	5,5
Planskildhet Holmsund Järnvägspassage	-6,3	-0,0	6,3	-0,2	-9,5	-1,5	8,0
Djupbäcken klimatanpassning	-13,7	-0,4	13,2	-4,5	-20,5	-7,5	13,0
Framkomlighetshöjande kollektivtrafik	-4,6	-3,6	1,0	-1,8	-6,9	-3,9	3,0
Cykelparkering Umeå Ö & Umeå C	-4,0	-0,1	3,9	0,0	-6,0	-6,0	0,0
Övriga	-77,7	-52,1	25,6	-502,3	-116,5	-152,7	-36,1
Summa	**-208,3**	**-113,7**	**94,6**	**-526,4**	**-312,5**	**-256,5**	**56,0**

Tabell: Gator och parkers 10 största investeringar

Tvärån klimatanpassning, prognos för helår är ett överskott på 24,6 mnkr. Mindre åtgärder utförs under året medan större åtgärder fortfarande utreds.

Djupbäcken klimatanpassning, framtagande av systemhandling pågår och färdigställs i januari 2027. Under tiden systemhandlingen pågår genomförs åtgärder vid Sandaparken och Sandbackadammen, där medfinansiering har beviljats av Myndigheten för civilt försvar. Prognos för helår är ett överskott på 13,0 mnkr.

Kungsgatan, projektering pågår och planerad byggstart är oktober/november 2026. Prognos för helår är ett överskott på 7,7 mnkr. Projektet fortsätter under 2027 och förväntas färdigställas under 2029.

Norra Obbolavägen, projektet löper på och förväntas vara färdigt hösten 2028. Prognos för helår är ett överskott på 5,5 mnkr.

Planskildhet Holmsund Järnvägspassage (tidigare Järnvägspassage Holmsund), handlingar färdiga för upphandling av konsult, avtal med Trafikverket är framtaget och underskrivet. Projektering påbörjas under hösten och pågår till och med våren 2027. Prognos för helår är ett överskott på 8,0 mnkr.

Framkomlighetshöjande kollektivtrafik, utredningar genomförda på Ersboda som resulterat i en åtgärdsplan för kommande år. Största fokus under 2026 är slutförandet av Västra Kyrkogatan som blir klar under hösten. Prognos för helår är ett överskott på 3,0 mnkr.

Cykelparkering Umeå Ö och Umeå C, bygglovsansökan är beviljar och projektet hoppas kunna färdigställas under 2026. Prognos för helår är ett resultat på 0,0 mnkr.

Möjlig framtida utformning av Västra Esplanaden.

DoIT och övrigt

För perioden har DoIT ett utfall på -39 mnkr, vilket är 14,9 mnkr lägre än budget. Årsprognosen ett överskott på ca 3,1 mnkr, investeringar i IT-utrustning bedöms bli ca 15 mnkr lägre än budget medan investeringar i servrar, ink inköp till ITKN, bedöms bli ca -11,9 mnkr över budget. Dock osäkert om inköp för ca -7,4 mnkr hinner göras innan årets slut.

Under övrigt ingår städ- och verksamhetsservice, måltidsservice och civil beredskap. Här finns ett överskott för perioden på ca 14,9 mnkr och en årsprognos på ca 14,7 mnkr över budget. Det är främst inom civil beredskap som överskottet bedöms uppstå då inte alla medel hinner förbrukas i år.


UMEÅ
KOMMUN

Tekniska nämndens rapport till KS, januari–augusti 2026

Verksamhetsuppföljning

Nämndens grunduppdrag

	Bedömning januari-augusti 2026	Prognos för januari-december 2026
Uppdelning av nämndens grunduppdrag med bedömning per verksamhet		
Digital omställning och IT	I hög grad uppfyllt	I hög grad uppfyllt
Fastighet	I hög grad uppfyllt	I hög grad uppfyllt
Gator och parker	I hög grad uppfyllt	I hög grad uppfyllt
Måltidsservice	I hög grad uppfyllt	I hög grad uppfyllt
Städ och verksamhetsservice	I hög grad uppfyllt	I hög grad uppfyllt

Bedömning och motivering

Nämndens verksamheter har under perioden levererat de tjänster som ligger inom dess uppdrag.

Planeringsarbetet inför kommande mandatperiod har fortsatt under perioden. Planeringsdirektiven tydliggör behovet av att möta framtida utmaningar kopplade till befolkningstillväxt, investeringsbehov, lokalförsörjning, klimatanpassning och ett förändrat omvärldsläge. Förvaltningen arbetar vidare med att skapa långsiktiga förutsättningar för en hållbar utveckling av kommunens verksamheter och infrastruktur.

För att stärka organisationens förmåga att möta framtidens krav har beslut fattats om att inrätta en stabsfunktion. Syftet är att skapa bättre förutsättningar för förvaltningens chefer, möjliggöra ett mer närvarande ledarskap samt minska sårbarheten genom en mer robust organisation. Förändringen förväntas även stärka utvecklingskapaciteten och bidra till en organisation som i högre grad harmoniserar med kommunens övriga förvaltningar.

Digital omställning och IT

Under året har vi hittills levererat de tjänster som ligger inom vårt uppdrag. I mätningar så väl som i dialoger i styrgrupper, verksamhetsdialoger och liknande får vi övervägande positiv återkoppling och i det fall negativa synpunkter sker det ofta på ett konstruktivt sätt.

Befintliga och nya e-tjänster och automationsrobotar sparar tid i kommunens verksamheter.

Arbetet med att utveckla kommunens förmågor inom data och AI har god progress och är uppskattat.

Utifrån de förutsättningar vi har för att utföra vårt uppdrag är den samlade bedömningen att vi uppfyller det i hög grad.

Fastighet

Verksamhetens uppdrag är att säkerställa att kommunens lokalbehov tillgodoses, att fastighetsbeståndet förvaltas, driftas och underhålls på ett kostnadseffektivt sätt samt att investerings- och underhållsprojekt genomförs med hög kvalitet. Under perioden har uppdraget genomförts med hög måluppfyllelse, och verksamheten bedöms ha levererat enligt plan.

De gynnsamma väderförhållandena under våren har medfört ett lågt behov av snöröjning och sandning, vilket har skapat goda förutsättningar för att uppdragen har kunnat genomföras i hög grad enligt plan.

Gator och parker

Nivåerna på de kvalitetsfaktorer som ligger till grund för bedömningen är i Årsrapporten för 2025 fortsatt höga i jämförelse med tidigare år eller rikssnitt. Detta kombinerat med att genomförande kraften av investeringsprojekten ökade kraftigt 2025 samt att andel under året uppstartade projekt ligger på 64%, gör att bedömningen är att Gator och parker uppfyller grunduppdraget i hög grad.

Måltidsservice

Under året har vi levererat goda och hälsosamma måltider. Vi har med stabil ekonomi och bra strukturförutsättningar att fokusera på grunduppdraget att laga goda, hälsosamma och klimatsmarta måltider vilket bidrar till god folkhälsa.

Städ och verksamhetsservice

Under det första halvåret har Städ- och verksamhetsservice levererat en stabil och väl fungerande lokalvård i kommunens verksamheter. Arbetet med att möta Miljö- och hälsoskydds kravbild har fortsatt enligt framtagen handlingsplan och bidrar till en successivt förbättrad städkvalitet. Detta avspeglas i förbättrade resultat vid interna kvalitetstillsyner samt i ett väl fungerande och konstruktivt samarbete med Miljö- och hälsoskydd.

På alla kommunens förskolor har det nu genomförts en intern kvalitetskontroll. Under hösten kommer fokus bli att få alla förskolor godkända samt besöka alla grund- och gymnasieskolor. Vid uppföljningsmöten har Miljö- och hälsoskydd uttryckt att de ser positiva effekter av de förändringar som genomförts utifrån den tidigare framtagna handlingsplanen för kvalitetsförbättring.

De interna kvalitetskontrollerna visar en positiv utveckling, där en allt större andel objekt uppnår godkänt resultat. Det visar att verksamhetens långsiktiga kvalitetsarbete ger önskad effekt och skapar förutsättningar för en mer likvärdig och hållbar lokalvård.

Sammantaget bedöms verksamheten utvecklas i en positiv riktning och lever upp till sitt grunduppdrag – att med omtanke och kvalitet utföra lokalvård och service i kommunens lokaler för att skapa rena, trivsamma och hållbara miljöer, med ett gott bemötande för Umeå kommuns medborgare.

Verksamhetens utveckling och väsentliga händelser

Digital omställning och IT

Under årets två första tertial har stort fokus legat på den fortsatta organisationsutvecklingen inom DoIT. Arbetet med att forma och stabilisera team samt produktdomäner har intensifierats. I dag finns cirka 15 team med olika uppdrag och förutsättningar. För att skapa tydligare riktning, bättre samordning och stärkt verksamhetsnytta införs nu ett nytt arbetssätt där teamen samlas i produktdomäner. För att ge teamen bättre stöd och riktning har vi påbörjat ett gediget arbete med en verksamhetsmålbild och färdplan att nå önskade lägen. Vi har också initierat en utökning av enhetschefer så att de ska kunna stötta medarbetarnas omställning i vår egen verksamhetsutveckling.

DoIT har också under inledningen av året mottagit erbjudande från SKR och initiativet Handslag för digitalisering om att ansluta till GSIM*. En analys pågår av hur kommunen kan och bör engagera sig i detta arbete. GSIM bedöms vara ett viktigt förutsättningsskapande initiativ som ligger i linje med regeringens nationella digitaliseringsstrategi och kan stärka kommunens förmåga till samverkan och effektiv digital utveckling.

Vidare pågår uppstart av Umeås deltagande i det regionala initiativet AI Västerbotten. Arbetet innebär samverkan med bland annat Skellefteå och övriga kommuner i regionen kring gemensam AI-plattform, juridiska frågor, kompetensutveckling och utbildningsinsatser. Initiativet bedöms skapa goda förutsättningar för ett mer strukturerat och ansvarsfullt införande av AI i kommunal verksamhet.

*GSIM = grundläggande förutsättningar för ett samlat invånarmöte

DoIT har bidragit med kompetens i samband med hanteringen av visselblåsarfunktionen och har levererat en krypterad inbox för att säkerställa att en trygg kanal finns även efter att avtalet med den tidigare leverantören hävts.

För att stötta omsorgsverksamheterna har vi lagt en stor mängd arbetstid med egen personal och med konsultstöd för att bidra till ett så bra upphandlingsunderlag som möjligt utifrån angivna tidsramar.

Fastighet

Året har präglats av en lägre nederbördsmängd än normalt, vilket har minskat behovet av snöhantering och takskottning och därmed medfört lägre kostnader. Arbetet med att analysera fastigheternas takkonstruktioners bärighet har slutförts och en handlingsplan har tagits fram för det fortsatta arbetet.

Under perioden har stort fokus lagts på lokalförsörjnings- och investeringsplanering som underlag för budgetarbetet. Planeringen har anpassats utifrån förändrade demografiska förutsättningar och en lägre befolkningsutveckling än tidigare prognosticerat.

Flera större bygg- och investeringsprojekt pågår under året. Utbyggnaden av Vasaskolan fortsätter med två nya flyglar samtidigt som Rosa huset byggs om till skolkök. Byggnationen av Östra brandstationen har påbörjats och arbetet med en ny skola i Stöcke inleds under året. Den nya skolbyggnaden vid Hedlundaskolan har färdigställts. Parallellt fortsätter satsningarna på utbyggnad av skolkök och skolrestaurang samt renovering och modernisering av den befintliga skolmiljön.

Införandet av det nya fastighetssystemet fortskrider enligt plan, men har krävt betydande personella resurser under perioden. I nära samverkan med DOIT och Datadriven kommun har arbetet med en automatiserad verksamhetsuppföljning i huvudsak färdigställts. Uppföljningen bygger på data från bland annat fastighets- och ekonomisystemen och visualiseras i Power BI, vilket ger verksamheten förbättrade möjligheter till analys, uppföljning och styrning.

Arbetet med att uppdatera och återställa kommunens skyddsrum fortsätter. Inventeringar och analyser visar att flera anläggningar är i behov av omfattande åtgärder för att återställa funktion och uppfylla gällande krav, vilket innebär betydande investeringsbehov under kommande år.

Gator och parker

Den ovanligt milda vintern har medfört lägre driftkostnader för vinterväghållningen än budgeterat. Samtidigt har verksamheten belastats av ökade kostnader inom färdtjänsten

efter att den tidigare entreprenören försattes i konkurs och ett tillfälligt avtal behövde tecknas. Det tillfälliga avtalet innebär en betydande kostnadsökning jämfört med tidigare avtal. Ett arbete har genomförts med upphandlingsunderlag för ett nytt långsiktigt färdtjänstavtal som nu är ute för anbudsförfrågan.

Under halvåret har två projektledare tillträtt för projekten Smart och robust dagvattenhantering i subarktiskt klimat och E-NORM, vilket möjliggör fortsatt genomförande av projekten enligt plan.

Projekten syftar till att utveckla kommunens förmåga att möta framtida klimat- och hållbarhetsutmaningar genom innovativa lösningar för dagvattenhantering respektive utsläppsfria bygg- och anläggningsentreprenader. Båda projekten är viktiga för Umeås långsiktiga arbete med att hantera komplexa samhällsutmaningar och stärka kommunens hållbara utveckling.

Inom stadsmiljöområdet har planteringsurnor som konstruerats av elever vid Dragonskolan placerats ut längs väg 503.

Satsningen bidrar både till en attraktivare stadsmiljö och till att synliggöra samverkan mellan kommunen och skolan. Årets sommarblomsplanteringar har temat Sagoväsen, vilket har bidragit till att skapa färgstarka och uppskattade miljöer för invånare och besökare.

Måltidsservice

Under perioden har vi tillsammans med Säkerhet vidareutvecklat och arbetet igenom vår kontinuitetsplan. Vi har nu övergripande riskbedömt tillagningskök, mottagningskök och enportionsmatskök. Dessa kommer vi framöver använda som grund för att riskbedöma alla våra 121 kök. Arbetet med beredskap har även fortsatt med bland annat utbildningar och utredning av användning av ved eller gasol för alternativ tillagning.

Mot inriktningsmålet klimat pågår arbetet ständigt mot mer klimatsmarta måltider. Nya svenska vegetariska proteinkällor testas och delar eller hela måltider byts ut succesivt. Vårt Måltidskoncept är uppdaterat enligt nya riktlinjer från Livsmedelsverket. En film har tagits fram där vi visar upp vad och varför vi serverar den mat vi gör med målet är att få vårdnadshavare att kostnadsfritt äta i våra restauranger en gång per termin.

Den digitaliserade verksamhetsuppföljningen används och underlättar uppföljningen på alla nivåer i verksamheten. Vi kan i rapporten övergripande följa resultat för alla våra nyckeltal, produktionsmått, mål och uppdrag. Ett exempel visas nedan. Här ser vi hur kostnaderna skiljer sig mellan olika typer av kök. Förskolor är dyrast, i rapporten kan vi filtrera och få ut mer detaljerade siffror. Rapporten är ett bra beslutsunderlag.

Städ och verksamhetsservice

Verksamheten har under året utvecklats enligt plan med tydligt fokus på verksamhetsmålen. Särskild prioritet har lagts på bemanningsfrågor, upphandling av ett digitalt städledningssystem samt genomförandet av handlingsplanen för förbättrad kvalitet. Därutöver har Städservice moderniserat sitt intranät och fortsatt arbetet med att utveckla och tydliggöra rutiner.

Arbetet med kvalitetskontroller inom förskola och skola har intensifierats och antalet genomförda kontroller ökar successivt. Målsättningen är att samtliga enheter ska ha granskats före årets slut. Samtidigt syns en positiv utveckling där allt fler verksamheter uppnår godkända resultat enligt den nordiska branschstandarden Insta 800.

Dialogen med miljö- och hälsoskyddsverksamheten har stärkts, vilket har bidragit till en ökad samsyn kring krav och arbetssätt. Detta har skapat bättre förutsättningar för städverksamheten att vidareutveckla rutiner och processer samtidigt som tillsynsverksamheten kan genomföras i en anpassad takt. Det löpande utbildningsarbetet i samverkan med fastighetsverksamheten har också gett resultat och bidragit till att flera äldre tillsynsärenden kunnat avslutas.

Framåt är fortsatt samverkan med miljö- och hälsoskyddsverksamheten viktig för att säkerställa en långsiktigt hållbar utveckling. Regelbundna avstämningar planeras därför att genomföras under året. Parallellt fortsätter arbetet tillsammans med utbildningsverksamheten för att tydliggöra ansvarsfördelningen inom identifierade gråzoner. Arbetet kan leda till behov av justeringar av nuvarande servicenivåer, vilket i så fall kommer att lyftas till tekniska nämnden för vidare hantering.

Inriktningsmål och program

Inriktningsmål 1: Umeås tillväxt ska klaras med social, ekologisk, kulturell och ekonomisk hållbarhet med visionen om 200 000 medborgare år 2050

Arbetet inom Teknik- och fastighetsförvaltningen stärker Umeås attraktivitet för investeringar, kompetens och etableringar. Utmärkelsen Årets samhällsbygge, satsningen på en eldriven hjullastare och beviljade stöd från Tillväxtverket och Myndigheten för samhällsskydd och beredskap bidrar till hållbar tillväxt, innovation och en mer robust kommun.

Uppdrag/aktivitet	Status/kommentar
Fokus på effektiv och säker implementering av IT och digitaliseringslösningar för att bidra till kommunens tillväxt och omställning.	DoIT har pågående aktiviteter för att realisera kommunens Plan för digital omställning vilket inkluderar bland annat samarbetsformer med kommunens förvaltningar och förutsättnings-skapande teknikutveckling. Det pågår också en översyn av IT- och digitaliseringsstyrningen för att utreda behov av förändrat reglemente och kompletterande policys och riktlinjer med syfte att stärka kommunens förmåga till omställning med IT.
Fokus på genomförande av investeringar	Ett arbete görs med översyn av processer för att kunna presentera fler mogna projekt i ett tidigare stadie.

Inriktningsmål 2: Umeå ska växa hållbart utan några utsatta områden

Arbetet bedrivs fortsatt i enlighet med tidigare fastställda styrdokument och inom ramen för nämndens grunduppdrag. En viktig utgångspunkt är att bidra till social hållbarhet. Genom planering, drift och underhåll av det offentliga rummet skapas trygga, säkra och inkluderande utemiljöer för alla. Insatser inom bland annat belysning, parker och naturområden stärker den sociala tryggheten, främjar möten och delaktighet samt bidrar till jämlika livsmiljöer i hela kommunen.

Uppdrag/aktivitet	Status/kommentar
Stadsdelssatsningar, fortsätta arbetet enligt av nämnden fastställd plan.	Stadsdelsdialoger har genomförts i kommun- och stadsdelarna Holmsund och Rödäng/Västerslätt. Planering pågår för genomförandet av trygghetsvandringar i dessa områden under hösten.
Stadsdelslyft Ålidhem	Socionomstråket nedanför fotbollsplanen har i sommar omvandlats till en sommargata. Platsen har utvecklats i samarbete med elever från Ålidhemsskolan och studenter från Arkitekthögskolan. Det har placerats ut sitt- och umgängesmöbler i trä,

	blomsterurnor samt färgglad markmålning för att undersöka platsens potential som social mötesplats. Syftet med den tillfälliga platsbildningen har varit att utforska om platsen kan användas för möten och utevistelse med målet att öka kvaliteten och variationen i Ålidhems utemiljö samt för prioritering av gående och cyklister i trafiken.
TN-uppdrag 2025:1	Arbetet med stadsdelssatsningarna fortgår enligt nämndens fastställda plan. Under första halvan av 2026 har vi påbörjat genomförandet av åtgärder i Obbola, Umedalen/Backen och Hörnefors. Medborgardialoger har under försommaren genomförts i Holmsund och på Västerslätt/Rödäng.

Inriktningsmål 3: Umeå kommun ska skapa förutsättningar för kvinnor och män att ha samma makt att forma samhället såväl som sina liv

Teknik och fastighet bidrar till kommunens jämställdhetsmål genom att skapa trygga, tillgängliga och inkluderande fysiska miljöer som kan användas på lika villkor av kvinnor och män. Genom ett jämlikt samhällsbyggande, hållbara mobilitetslösningar och välskötta offentliga rum stärks möjligheterna för alla att delta i samhällslivet och forma sina egna liv. Verksamheten bidrar även internt genom arbetssätt som ökar delaktighet och inflytande.

Uppdrag/aktivitet	Status/kommentar
Öka medborgardelaktigheten	Det är andra året dialogerna i samband med Stadsdelssatsningarna hålls på försommaren. Det har varit positivt att vara ute den ljusa årstiden. Upplevelsen är att det är lättare att få kontakt med medborgarna och fler tar sig tid att stanna och prata med oss. Elevenkäter är skickade till högstadieskola även i år.
Utveckla tryggare mötesplatser	På Västra Esplanaden har mer grönska, bänkar och en ny lekplats tillförts för att skapa en mer attraktiv och trivsam miljö. På Bölesholmarna har en ny paviljong öppnat och bidrar med sociala och rekreativa värden samtidigt som den ökar tryggheten genom att locka fler besökare till området. I Obbola genomförs belysningsåtgärder vid Ängen, bland annat vid lekplatsen, pulkabacken och fotbollsplanen. Insatserna stärker tryggheten och möjliggör fler aktiviteter under årets mörkare perioder.

Inriktningsmål 4: Umeå ska vara klimatneutralt till 2040

Under perioden har teknik- och fastighetsförvaltningen fortsatt arbetet med omställning och insatser inom inriktningsmålets fokusområden: klimat, energi, cirkulär ekonomi och hållbara transporter. Under året pågår flera utvecklings- och testprojekt för att minska förvaltningens klimatpåverkan och skapa underlag för framtida arbetssätt.

Flera aktiviteter kommer att utvärderas senare under året och bidrar till förvaltningens långsiktiga arbete mot klimatneutralitet och måluppfyllelse. Insatserna syftar bland annat till att stärka kunskap, engagemang och medvetna val hos både medarbetare och invånare. Genom exempelvis utbildningsinsatser, kommunikation och praktiska åtgärder skapas förutsättningar för en hållbar omställning som bidrar till Umeå kommuns inriktningsmål.

Uppdrag/aktivitet	Status/kommentar
Transporter	
Testa elektrisk hjullastare i verksamhet. Hållbart resande under byggtiden i ett gatuombyggnadsprojekt genom MM.	Elektrisk traktor i egen drift har testats av Gator och parker under sex månader med start under vintern 2026. Elektriska arbetsmaskiner blir allt vanligare och det finns flera fördelar, exempelvis färre partiklar från avgaser, lägre klimatpåverkan i drift, minskat buller och förbättrad arbetsmiljö för föraren. Under testets gång har Gator och parker provat eltraktorn vid plogning och efterarbeten samt vid sopning av grus med gott resultat. Under T2 fortsätter arbetet med Mobility management i pilotprojektet Norra Obbolavägen. Fokus ligger på att genomföra de åtgärder som tagits fram under T1 för att underlätta hållbara transportval under byggskedet. Under hösten genomförs en testresenärsaktivitet riktad till boende och förbipasserande i området, där cirka 100 periodkort erbjuds under en testperiod. Hastighetsdisplayer sätts upp i bostadsområdet och arbetet med att testa det nya digitala informationsverktyget BUKO fortsätter. Erfarenheter från aktiviteterna kommer att följas upp och användas i det fortsatta arbetet med Mobility management i gatuombyggnadsprojekt.
Bygg och anläggning	
Upphandla ett byggprojekt med utsläppsfri byggarbetsplats Klimatberäkna ett anläggningsprojekt	Fastighet testar att genomföra projektet Malmen 27 med utsläppsfri byggarbetsplats, arbetet pågår. Gator och parker klimatberäknar Renmarkstorget och Fastighet klimatberäknar utemiljön på Älvan 1, båda pågår och resultat förväntas under hösten.
Energi (el och fjärrvärme)	
Anordna ett energiutbildningstillfälle för Fastighets drifttekniker Testa digitalt verktyg för visualisering av byggnaders energiprestanda Testa effekthantering och beteendecoaching i storkök	Utbildning inom energi har genomförts under april. Fler utbildningar planeras till hösten 2026. Envista testas just nu på fastighetsbeståndet för att visualisera byggnadernas energiprestanda. Utvärderas senare under 2026. Awareify, effekthantering och beteendecoachning, testas just nu i sex stycken olika storkök och kommer att utvärderas senare under 2026.
Cirkulär ekonomi	

Utöka möjligheten att sortera kartong och plast för Städs verksamhetsavfall genom inköp av avfallskärl Lansera digitalt återbruks-verktyg för teknik- och fastighetsförvaltningens medarbetare Förlänga livslängd på digitala enheter genom aktiv hantering och återbruk	Utökning av möjligheten att sortera kartong och plast från Städs verksamhetsavfall har genomförts på aktuella städobjekt. Appen "Återbruksportalen" är lanserad och används av teknik- och fastighetsförvaltningens medarbetare för att öka cirkularitet av förvaltningens produkter. Användandet av appen har kommit i gång bra. Nästa steg är att automatisera sammanställning av statistik för produkter som återbrukas via Återbruksportalen. Hittills under 2026 motsvarar förvaltningens besparingar genom återbruk ca 2,9 miljoner kronor och ca 35 tusen ton kg CO2e. Digital omställning och IT jobbar kontinuerligt med att förlängs livslängd på digitala enheter. Digital omställning och IT jobbar kontinuerligt med att förlängs livslängd på digitala enheter. DoIT har övergått från egen regi till att återbruka utrustning via ram-avtalspart.
Övergripande insatser	
Genomföra en hållbarhetsutbildning för Måltidsservices medarbetare	Hållbarhetsutbildning för Måltidsservices medarbetare hålls under hösten 2026.
Skapa en film för vårdnadshavare om hållbarhetsarbete kring livsmedel	Film för vårdnadshavare är framtagen.
Genomföra en temadag med lokala varor/livsmedel	Regnbåge från Kalix har funnits på menyn under våren samt är planerad till en gång varje månad inom äldreomsorgen under året. Måltidsservice undersöker fler alternativ till temadag med lokala varor/livsmedel

Tilläggsuppdrag från kommunfullmäktige

Uppdrag	Status, jan–aug	Motivering/kommentar	Prognos, status helår
Tilläggsuppdrag 2025:1 Kommunfullmäktige ger alla nämnder i uppdrag att genomföra en analys av konsekvenser utifrån förändrade demografiska förutsättningar. Arbetet ska säkerställa att kommunen inte åtar sig kostnader som inte kan bäras över tid, samt ske i enlighet med av fullmäktige fastställd riktlinje för god ekonomisk hushållning. Förslag på förändring av principiell karaktär ska tillställas fullmäktige.	Delvis genomfört	Samtliga verksamheter inom Tekniska nämnden arbetar med sina respektive analyser.	Genomfört
Tilläggsuppdrag 2025:2 Kommunfullmäktige ger tekniska nämnden i uppdrag att som en konsekvens av förändrade	Delvis genomfört	Det pågår dialoger med övriga nämnder avseende deras analyser av tilläggsuppdrag 2025:1 inför TNs tilläggsuppdrag 2025:2	Genomfört

demografiska förutsättningar säkerställa ett fortsatt effektivt lokalnyttjande, inklusive att tillse att frigjorda lokaler så långt det är möjligt nyttjas till verksamheter med ökade behov av lokaler, i syfte att hålla nere kommunens lokalkostnader och minska investeringsbehovet i nya lokaler. Förändrade investeringsbehov ska lyftas inom ramen för ordinarie planeringsprocess.			
Tilläggsuppdrag 2025:3 Kommunfullmäktige ger tekniska nämnden och individ- och familjenämnden i uppdrag att analysera behovet och utreda förutsättningarna för annan boendeform.	Delvis genomfört	Arbetet med rapporten är uppstartad.	Genomfört
Tilläggsuppdrag 2025:4 Kommunfullmäktige ger kommunstyrelsen, gymnasie- och vuxenutbildningsnämnden, samt tekniska nämnden i uppdrag att i dialog med berörda verksamheter och externa parter ta fram förslag på samverkan kring och samnyttjande av anläggningar för djurhållning.	Genomfört	Utredningen är klar och under hösten planeras beslut tas i våra nämnder och uppdraget avslutas.	Genomfört
Tilläggsuppdrag 2025:5 Kommunfullmäktige ger tekniska nämnden och gymnasie- och vuxenutbildningsnämnden i uppdrag att analysera behovet och utreda förutsättningarna för 20 (64) idrottshall för Vasaskolan, samt att gymnasie- och vuxenutbildningen ges i uppdrag att se över framtida programstrukturen på kommunens gymnasieskolor.	Delvis genomfört	Utredning och dialog pågår med GVN för att se över om det går att uppfylla nämndens önskan och behov av en idrottshall.	Genomfört

Tilläggsuppdrag 2025:6 Kommunfullmäktige ger kommunstyrelsen, fritidsnämnden, gymnasie- och vuxenutbildningsnämnden och tekniska nämnden i uppdrag att i dialog med berörda verksamheter och föreningslivet utreda förutsättningarna för att utveckla idrottsanläggningarna Gammlia Arena, Visionite Arena och Nolia Arena ur ett tillväxtperspektiv.	Delvis genomfört	Det finns en styrgrupp och en arbetsgrupp samt sammanhållande projektledare från Näringsliv. Utredning pågår.	Delvis genomfört
Tilläggsuppdrag 2023:1 Kommunfullmäktige ger kommunstyrelsen och nämnderna i uppdrag att öka omställningen av nämndernas verksamheter för att klara grunduppdraget i takt med att personalbristen ökar.	Genomfört	Omställningsarbetet inom verksamheten hanteras löpande. Fokus är att säkerställa grunduppdraget genom anpassade arbetssätt och effektiv resursanvändning.	Genomfört
Tilläggsuppdrag 2023:2 Kommunfullmäktige ger kommunstyrelsen och nämnderna i uppdrag att öka samarbetet och ansvarstagandet över förvaltnings- och nämndgränser.	Delvis genomfört	Löpande arbete pågår för att öka samarbetet och ansvarstagandet över förvaltningsgränser.	Delvis genomfört
Tilläggsuppdrag 2021:8 Kommunfullmäktige ger kommunstyrelsen i uppdrag att tillsammans med kommunens nämnder och bolag undersöka risken för att skattemedel, som bekostar verksamheter inom välfärdssektorn, även med annan utförare än kommunen, används på ett felaktigt sätt och/eller i kriminellt syfte, till exempel för att finansiera organiserad brottslighet, samt att ta fram förslag på åtgärder för att förebygga och förhindra detta.	Delvis genomfört	Arbete pågår tillsammans med bl a Upphandlingsenheten för att utveckla metoder för att minska risken att skattemedel finansierar organiserad brottslighet.	Delvis genomfört

Personaluppföljning

Nämndens arbete för att nå personalpolitiska mål

	Bedömning av nämndens arbete med personalpolitiska mål januari-augusti 2026	Prognos för januari-december 2026
Mål 5: Umeå kommun ska klara kompetensförsörjningen genom att vara en attraktiv arbetsgivare och spegla mångfalden i samhället.	Enligt plan.	Enligt plan.
Mål 6: Umeå kommun ska ha ledarskap som ges och ger förutsättningar för goda resultat, där riktvärdet för antalet medarbetare per chef inte är fler än 30.	Enligt plan.	Enligt plan.
Mål 7: Umeå kommuns sjukfrånvaro ska minska genom fokus på friskfaktorer och jämställda arbetsförhållanden.	Enligt plan.	Enligt plan.

Åtgärder och viktig utveckling/viktiga händelser inom målområdena

Kompetensförsörjning och attraktiv arbetsgivare (mål 5)

Den årliga lönekartläggningen har genomförts inom Umeå kommun och förvaltningen Teknik och fastighet. Resultatet visar att lönerna inom förvaltningen är jämställda mellan kvinnor och män, både utifrån löneläge och arbetsvärdering. I arbetsvärderingen ingår bland annat arbetets krav, utbildningsnivå och marknadspåverkan.

Lönekartläggningen genomförs i syfte att upptäcka, åtgärda och förebygga osakliga löneskillnader mellan kvinnor och män i enlighet med diskrimineringslagen. Inom Teknik och fastighet finns cirka 70 olika befattningar som har jämförts med varandra samt med övriga befattningar inom Umeå kommun. Att vi kan visa på jämställda och rättvisa löner är en viktig faktor, inte minst för arbetsgivarvarumärket. Det bidrar också till att stärka kommunens och förvaltningens attraktivitet som arbetsgivare

Under perioden har det nuvarande lärplattformen Learning Management Systemet (LMS) utvärderats utifrån hela Umeå kommuns behov. Utvärderingen visar att systemet bör avvecklas och ersättas med ett liknande system som redan används Infocaption Kunskapsbanken. Förändringen bedöms ge en mer effektiv budgetanvändning och bättre möta verksamhetens behov.

HR-enheten Teknik och fastighet har genomfört en workshop för chefer inom Fastighet med fokus på dialog och erfarenhetsutbyte inom kompetensförsörjning. Dialogerna berörde karriär, utveckling, arbetsgivarvarumärke samt resultat- och utvecklingssamtal.

Workshopen kopplades till verksamhetens kompetensförsörjningsplan och syftade till att stärka det strategiska arbetet med att utveckla, behålla och attrahera kompetens.

En omvärldsbevakning genomfördes för att få en bild av fastighetsbranschen, dess utveckling och de behov som finns inom området.

Ledarskap (mål 6)

Fokusområdet för ledarskapet inom Teknik och fastighet är chefers förutsättningar och synliggöra samt tillvarata lärande i arbetsvardagen. Under april samlades Ledarforum i Medlefors i Skellefteå för nätverkande och erfarenhetsutbyte inom förvaltningen. När cheferna har rätt förutsättningar att leda blir vardagen bättre för alla som arbetar inom förvaltningen.

Friskfaktorer (mål 7)

I maj genomfördes en workshop med Teknik och fastighets nya skyddsombud och nya chefer på har genomförts. Workshopen handlade om roller och ansvar, arbetsmiljöns regler och vikten med att göra riskbedömningar.

Nu har arbetet i projektet SAMBA (Samverkansmodell för att behålla arbetskraft) resulterat i tio prototyper på nya och effektiva samverkansformer med målet att behålla arbetskraft på arbetsmarknaden, sex från hösten 2025 och fyra under vårterminen 2026. Prototyperna kommer finnas med i det fortsatta arbetet under hösten där planen är att djupdyka i förutsättningar, möjligheter och behov i de egna deltagande organisationers rehabprocesser, bla inom Teknik och fastighet, för att fånga upp tidiga signaler och möjliggöra och etablera tidiga insatser.

Som en del av implementeringen av arbetet med säkerhetskultur har förvaltningens arbetsmiljöingenjör genomgått utbildning i MTO (Människa, Teknik och Organisation). MTO-metodiken ger stöd för att identifiera såväl riskfaktorer som friskfaktorer och bidrar till ett mer systematiskt arbetsmiljöarbete. Kompetenshöjningen utgör en grund för det fortsatta arbetet med att utveckla en stark säkerhetskultur och en hållbar arbetsmiljö inom verksamheten.

Nyckeltal	Utfall jan–aug 2026			Utfall jan–aug 2025		
	kvinnor	män	totalt	kvinnor	män	totalt
Heltidsanställda, procent	95	98	96	95	98	97
Långtidsfriska, procent	58	68	63	56	64	60
Personalomsättning, procent						
Sjukdagar per årsarbetare, antal	16,5	9,4	13,4	18,4	11	15,2
Sjukfrånvaro, procent	6,6%	3,8%	5,4%	7,3%	4,6%	6,1%
Sysselsättningsgrad, genomsnittlig	98	99	99	98	99	99
Tillsvidareanställda, procent	94	94	94	95	95	95
Utomnordisk bakgrund, procent	29	20	25	28	19	24

Ekonomiuppföljning, tekniska nämnden

Budgetavvikelse, åtgärder och årsprognos

Nämndens resultat per aug är ett överskott på 48,6 mnkr jämfört med budget. Jämfört med resultatet samma period föregående år, 8,2 mnkr, så är resultatet cirka 40 mnkr bättre. Det som skiljer mellan åren är i huvudsak att vintern är mer kostnadsmässigt gynnsam.

På intäktssidan finns det bland annat ett budgetöverskott kopplat till hyresintäkter för lägenheter övertagna från GVN samt engångsintäkt för lokalhyra, samt statsbidrag för civil beredskap som var okända vid budgetering. Förutom överskott inom vinterväghållning och snöröjning finns för perioden även överskott inom livsmedel och civil beredskap, medan negativa budgetavvikelser för energi inom fastighet samt ökade kostnader för färdtjänst kopplat till ett nytt ettårigt avtal på grund av en konkurs tidigare under året drar ner överskottet något för perioden.

Prognosen för året är ett överskott på 7 mnkr. Det stora överskottet för vinterväghållning och snöröjning bedöms ligga kvar till största del. De ökade kostnaderna för färdtjänst bedöms bli stora och dra ner resultatet med ca -20 mnkr mot budget. Även kostnader för ny säkerhetslagstiftning inom DoIT bedöms kosta ca -5 mnkr över budget, inom fastighet bedöms kostnader kopplat till underhåll bli ett par mnkr dyrare än budget samt kostnader för insatser inom civil beredskap finns planerade under resterande del av året. Övriga överskott per aug bedöms till stor del nyttjas till normal verksamhet under året, vilket ger en prognos betydligt lägre än resultatet för perioden. Faktorer som kan påverka nämndens prognos nämnvärt är pågående omvärldsfaktorer med krig, energikostnader samt hur den kommande vintern blir med snömängder, kyla och vindar. Det är mer sannolikt att resultatet blir bättre än prognosen än sämre vid årets slut.

(mnkr med en decimal)	Budget jan−aug 2026	Utfall jan−aug 2026	Budget-avvikelse jan−aug 2026	Budget-avvikelse jan−aug 2025	Budget helår 2026	Prognos helår 2026	Årsprognos budgetavvikelse 2026
Verksamhetens intäkter	100,9	124,3	23,4	18,6	158,6	174,0	15,0
Verksamhetens kostnader	-1 191,5	-116,2	25,2	-10,4	-1 827,7	-1 836,0	-8,0
Verksamhetens nettokostnad	-1 090,6	-1042	48,6	8,2	-1 669,1	-1 662,0	7,0

Investeringar

Tekniska nämndens totala investeringar uppgår per augusti till -652,9 mnkr, 302,1 mnkr lägre än budget. Årsprognosen är -1 226,9 mnkr, vilket är 286,9 mnkr lägre än budget.

(mnkr med en decimal)	Budget 31 aug 2026	Utfall 31 aug 2026	Budget-avvikelse 30 aug 2026	Utfall helår 2025	Budget helår 2026	Prognos helår 2026	Årsprognos budgetavvikelse 2026
Verksamhetens netto-investeringar	-955,0	-652,9	302,1	-1 263,1	-1 513,8	-1 226,9	286,9

(mnkr med en decimal)	Budget 31 aug 2026	Utfall 31 aug 2026	Budget-avvikelse 30 aug 2026	Utfall helår 2025	Budget helår 2026	Prognos helår 2026	Årsprognos budgetavvikelse 2026
Fastighet	-674,2	-496,5	117,7	-665,1	-1092,7	-879,6	213,1
Gator och parker	-208,3	-113,7	94,6	-526,4	-312,5	-265,5	56
IT	-53,9	-39	14,9	-59,1	-80,8	-77,7	3,1
Övrigt	-18,6	-3,7	14,9	-12,5	-27,8	-13,1	14,7
Summa	**-955**	**-652,9**	**302,1**	**-1263,1**	**-1513,8**	**-1226,9**	**286,9**

Fastighet

För perioden är utfallet ett överskott mot budget med 117,7 mnkr. Fastighets totala investeringsbudget för 2026 uppgår till -1 092,7 mnkr och prognosen för året är satt till -879,6 mnkr, dvs ett överskott på 213,1 mnkr. Orsaker till överskottet både för perioden och i årsprognosen är att flera projekt inte har startat än, pausats eller har en förskjuten tidsplan, även om flera projekt har en tidigarelagd tidsplan också. Genomförandegrad med nuvarande prognos är ca 80 procent.

Nedan är en tabell med de tio största projekten samt förklarande text kring status och prognos per projekt.

(mnkr med en decimal)	Budget 31 aug 2026	Utfall 31 aug 2026	Budget-avvikelse 31 aug 2026	Utfall helår 2025	Budget helår 2026	Prognos helår 2026	Årsprognos budgetavvikelse 2026
Vasaskolan gymn elevökn	-118,7	-89,9	-28,8	-62,1	-151,5	-141,0	10,5
Brandstation Umeå Östra	-41,5	-38,3	3,2	-6,5	-97,4	-66,0	31,4

Hedlundaskolan ny- & ombyggn F-6	-42,5	-45,0	-2,5	-32,8	-52,4	-59,6	-7,1
Rödängs skola utbyggnad en parallell F-6	-4,0	-0,9	3,1	-0,2	-50,0	-2,0	48,0
Grisbackaskolan matsal	-34,7	-27,6	7,1	-46,0	-45,5	-36,8	8,6
Daglig verksamhet	-16,9	-16,9	0,0	-3,3	-39,4	-41,0	-1,6
Kulturskola	-20,7	-10,6	10,0	-9,3	-37,1	-34,3	2,8
Gruppboende 2024 1, Prydnadsbusken 2 plan	-24,2	-26,9	-2,6	0,0	-30,6	-34,0	-3,4
Förstärkt serviceboende Malmen 27 2 plan	-14,5	-7,9	6,6	-3,6	-29,2	-20,0	9,2
Innertavle ersätt en byggnad för åk 4-5	-16,7	-8,1	8,6	-10,9	-26,5	-15,0	11,5
Summa	**-344,3**	**-272,0**	**62,3**	**-174,8**	**-559,7**	**-449,7**	**110,0**

Om- och tillbyggnaden av **Vasaskolan**, som i framtiden kommer att benämnas **Vasagymnasiet**, pågår för att möta ett ökade elevantal. Projektet omfattar bland annat tillbyggnad av två flyglar, ombyggnad av Vasaskolan och Rosa huset. I de norra och södra flyglarna pågår byggnadsarbeten, installationsarbeten för el, ventilation och VS. I södra flygeln påbörjas dessutom montering av skärmtegel under september. I Rosa huset pågår gjutning av mellanbjälklag samtidigt som stommen till tillbyggnaden monteras. Under oktober och november planeras installationsarbetena att påbörjas även där. I Vasaskolan pågår fönsterbyten med nya fönsterbrädor av sten och justering av ventilation. Prognosen för projektet för 2026 uppgår till -141,0 mnkr och projektets bedömda slutkostnad uppgår till -265,7 mnkr. Detta innebär en avvikelse mot budget om 10,5 mnkr för år 2026 och totalt 90,0 mnkr för hela projektet. En bidragande orsak till den positiva budgetavvikelsen är att den tidigare planerade idrottshallen har utgått ur projektet. Projektet har påverkats av tidsmässiga förskjutningar till följd av omfattande asbestsanering och hantering av sulfidjord i Rosa huset. Förutsatt att inga ytterligare hinder uppstår bedöms slutbesiktning kunna genomföras i mars 2027 för Vasaskolan och flyglar och i början av juni 2027 för Rosa huset.

Nya **brandstation Umeå östra** på Tomtebo Strand är inne i entreprenadskedet och just nu arbetar man med yttertaket av byggnaden och räknar med att ha ett tätt klimatskal i slutet av september. Entreprenaden är planerad att färdigställas i slutet av november 2027. Budgeten för 2026 är -97,4 mnkr och prognosen är på -66,0 mnkr. Den totala prognosen i projektet ser ut att hamna under budget med god marginal. Anbudet låg under de kalkyler

som tagits fram under planeringsskedet. Kalkylerna baserades på nyckeltal från andra nyligt byggda brandstationer i landet och projektet ser ut att markant landa under kostnaden för andra nyligt byggda brandstationer.

På **Hedlundaskolan** blev den nya byggnaden färdigställd i november 2025 med godkänd slutbesiktning och verksamheten flyttade in och startade upp i lokalerna i januari 2026. Nu befinner sig projektet i sin andra fas där renovering och utbyggnad av befintliga byggnader är i full gång. Det har dykt upp mer asbest än planerat vilket har resulterat i extra kostnader och tid samt att entreprenadindex har stigit mer än planerat. Tidplanen för entreprenaden är förlängd med en vecka jämfört med avtalad tid, men verksamhetsstart är fortsatt planerad till vårterminen 2027. Prognosen för 2026 är -59,6 mnkr och budget är -52,4 mnkr, dvs 7,1 mnkr över budget för året och prognosen för hela projektet ser ut att hamna strax över totala budgeten. De största osäkerheterna just nu är utvecklingen av index samt några fåtal, men stora tillkommande arbeten, där ansvarsfrågan för kostnaderna är under utredning.

Rödängs skola utbyggnad en parallell F-6 är i programskede där planlösning utformas tillsammans med verksamheten. Programskedet har tagit längre tid och därför har projektet förskjutits i tid. Projektet har minskats jämfört med ursprunglig plan och det gör att den totala prognosen understiger budgeten. Budgeten för 2026 är -50,0 mnkr och prognosen visar på -2,0 mnkr.

Utbyggnaden av kök och matsal på **Grisbackaskolan** för att möta det ökade elevantalet befinner sig i slutet av första huvuddelen som är själva tillbyggnaden och slutbesiktning utfördes i juni 2026 och verksamheten har flyttat in. Efter det fortsätter ombyggnad av befintliga matsalen, ombyggnad av skolgård och rivning av paviljong och de arbetena kommer att bli klara under höst/vinter 2026. Budgeten för året är på -45,5 mnkr och prognosen visar på -36,8 mnkr. Slutprognosen för hela projektet ser ut att kunna hållas. Under hösten pågår ombyggnation av by02 och den kommer stå klar för slutbesiktning i december 2026. Även markarbete på skolgården pågår och kommer stå klar för slutbesiktning i september 2026. Allt arbete ligger i fas.

Nybyggnaden av hus på Magistervägen på **Sofiehem 5:2 för daglig verksamhet** inom IFN är nu i inne i slutfasen av arbetet med stommen. De sista gjutningarna på betongstommen är utförda och nu pågår arbete med yttertak och utfackningsväggar. Byggnaden kommer ha ett tätt klimatskal i slutet av september. Entreprenaden har kommit i gång som den ska och entreprenören har för avsikt att färdigställa entreprenaden till årsskiftet 2027/2028, ca 5 månader innan kontraktstiden löper ut. Prognosen för 2026 ligger på -41,0 mnkr och budget -39,4 mnkr. Den ackumulerade budgeten i projektet ser ut att kunna hållas med stor

marginal, vilket bland annat beror på låga anbud med anledning av hård konkurrens om jobben.

Projektet med **Kulturskola** består egentligen av två byggprojekt i två olika fastigheter, Nanna 5 vid Vasagymnasiet och Hamnmagasinet på Stormen 1. Projektet på Nanna 5 är klart och verksamheten har flyttat in under sommaren 2026. Det här projektet har en delbudget på -16,5 mnkr och en prognos på -15,0 mnkr. Projektet blev försenat med ca 5 veckor på grund av komplicerade avväxlingar som behövde omprojekteras och utföras då det var brister i K-relationsritningar. Projektet på Hamnmagasinet på Stormen 1 är ute på upphandling, första upphandlingen avbröts då samtliga anbudslämnare blev diskvalificerade. Planen är att komma i gång med byggskedet under oktober månad. Det här projektet har en delbudget på -30,0 mnkr och har just nu en total prognos på -34,0 mnkr tills anbuden är öppnade. Projekteringsskedet förlängdes med 4 veckor på grund av svåra akustiklösningar kring en stor del av bottenvåningen och utmaningar kring ventilationen. Tidplanen är att nya Hamnmagasinet ska vara i klart för inflyttning under sen vår 2027.

Projektet med **Gruppboende 2024, 1 Prydnadsbusken 2 plan** är i byggskede och byggnaden förväntas vara klar i december 2026. Budgeten för året är på 30,6 mnkr och prognosen visar på att -34,0 mnkr. Den totala budgeten på 46,0 mnkr ser ut att hållas.

Projektet för **förstärkt serviceboende Malmen 27 2 plan** är upphandlad och tilldelad entreprenör och själva byggnationen har startat i maj 2026. Projektet fortlöper enligt tidplan. Prognosen för året är uppdaterat utefter entreprenörens betalplan och är korrigerad till -20,0 mnkr och budget är på -29,2 mnkr. Den totala prognosen för projektet kommer att rymmas inom den totala budgeten på -46,0 mnkr och tidplanen ser ut att hållas.

Projektet med **Innertavle skola ersätt en byggnad för åk 4-5** upphandlades i våras för själva byggnaden. Tilldelningen överklagades av en entreprenör och förvaltningsrätten har under vecka 34 avslagit överklagan. Plattan på marken är dock på plats. Planen var att byggnaden skulle vara klar att tas i bruk till höstterminen 2027. Denna tidplan kommer inte att hålla på grund av överklagan på tilldelningsbeslutet. Ny tidplan kommer tas fram tillsammans med entreprenör då de har rätt till tidsförlängning enligt gällande villkor i upphandlingen. Budget för 2026 uppgår till -26,5 mnkr och prognosen till -15,0 mnkr. Projektet fick en utökad budget med -14,0 mnkr till totalt -54,0 mnkr i vårens budgetbeslut. Den totala prognosen ser ut att hållas inom nya budgeten.

Gator och parker

Utfallet för Gator och parker är per augusti -113,7 mnkr, 94,6 mnkr lägre än budget. För året prognostiseras att -256,5 mnkr kommer att nyttjas, vilket är ett överskott på 56 mnkr.

Nedan specificeras de tio största projekten samt en summeringsrad för övriga projekt.

(mnkr med en decimal)	Budget 31 aug 2026	Utfall 31 aug 2026	Budget-avvikelse 31 aug 2026	Utfall helår 2025	Budget helår 2026	Prognos helår 2026	Årsprognos budgetavvikelse 2026
Renmarkstorget	-29,3	-4,8	24,4	-9,5	-43,9	-7,7	36,2
Norrbyskär	-21,3	-40,8	-19,5	-4,8	-32,0	-56,0	-24,1
Stadsutveckling innanför ringen	-17,5	-2,7	14,8	-3,1	-26,2	-8,1	18,2
Tvärån klimatanpassning	-16,5	-0,1	16,4	-0,2	-24,8	-0,2	24,6
Kungsgatan	-9,8	-4,0	5,7	-1,4	-14,6	-7,0	7,7
Norra Obbolavägen	-7,7	-5,6	2,1	1,4	-11,6	-6,1	5,5
Planskildhet Holmsund Järnvägspassage	-6,3	-0,0	6,3	-0,2	-9,5	-1,5	8,0
Djupbäcken klimatanpassning	-13,7	-0,4	13,2	-4,5	-20,5	-7,5	13,0
Framkomlighetshöjande kollektivtrafik	-4,6	-3,6	1,0	-1,8	-6,9	-3,9	3,0
Cykelparkering Umeå Ö & Umeå C	-4,0	-0,1	3,9	0,0	-6,0	-6,0	0,0
Övriga	-77,7	-52,1	25,6	-502,3	-116,5	-152,7	-36,1
Summa	**-208,3**	**-113,7**	**94,6**	**-526,4**	**-312,5**	**-256,5**	**56,0**

Renmarkstorget, ombyggnationen av torget blir något senarelagt då dagvattenanläggningen under torget måste åtgärdas först. Ombyggnationen börjar projekteras under 2027. Prognos för helår är ett överskott på 36,2 mnkr.

Norrbyskär, kraftiga fördyrningar pga. bristfälliga handlingar från konsult som har medfört förseningar och ökade kostnader genom bland annat att en tillfällig kaj har behövt byggas. Skadeståndsprocess gentemot konsult är inledd.

Stadsutveckling innanför ringen, första åtgärder genomförda, ombyggnation av cykelstället vid Västra Esplanaden har påbörjats för att tillföra mer grönska samt lekmöjligheter i stadsmiljö. Prognos för helår är ett överskott på 18,2 mnkr. Större åtgärder kommer genomföras under kommande år.

Tvärån klimatanpassning, prognos för helår är ett överskott på 24,6 mnkr. Mindre åtgärder utförs under året medan större åtgärder fortfarande utreds.

Djupbäcken klimatanpassning, framtagande av systemhandling pågår och färdigställs i januari 2027. Under tiden systemhandlingen pågår genomförs åtgärder vid Sandaparken och Sandbackadammen, där medfinansiering har beviljats av Myndigheten för civilt försvar. Prognos för helår är ett överskott på 13,0 mnkr.

Kungsgatan, projektering pågår och planerad byggstart är oktober/november 2026. Prognos för helår är ett överskott på 7,7 mnkr. Projektet fortsätter under 2027 och förväntas färdigställas under 2029.

Norra Obbolavägen, projektet löper på och förväntas vara färdigt hösten 2028. Prognos för helår är ett överskott på 5,5 mnkr.

Planskildhet Holmsund Järnvägspassage (tidigare Järnvägspassage Holmsund), handlingar färdiga för upphandling av konsult, avtal med Trafikverket är framtaget och underskrivet. Projektering påbörjas under hösten och pågår till och med våren 2027. Prognos för helår är ett överskott på 8,0 mnkr.

Framkomlighetshöjande kollektivtrafik, utredningar genomförda på Ersboda som resulterat i en åtgärdsplan för kommande år. Största fokus under 2026 är slutförandet av Västra Kyrkogatan som blir klar under hösten. Prognos för helår är ett överskott på 3,0 mnkr.

Cykelparkering Umeå Ö och Umeå C, bygglovsansökan är beviljar och projektet hoppas kunna färdigställas under 2026. Prognos för helår är ett resultat på 0,0 mnkr.

DoIT och övrigt

För perioden har DoIT ett utfall på -39 mnkr, vilket är 14,9 mnkr lägre än budget. Årsprognosen ett överskott på ca 3,1 mnkr, investeringar i IT-utrustning bedöms bli ca 15 mnkr lägre än budget medan investeringar i servrar, ink inköp till ITKN, bedöms bli ca -11,9 mnkr över budget. Dock osäkert om inköp för ca -7,4 mnkr hinner göras innan årets slut.

Under övrigt ingår städ- och verksamhetsservice, måltidsservice och civil beredskap. Här finns ett överskott för perioden på ca 14,9 mnkr och en årsprognos på ca 14,7 mnkr över budget. Det är främst inom civil beredskap som överskottet bedöms uppstå då inte alla medel hinner förbrukas i år.

UMEÅ KOMMUN

Tjänsteskrivelse
2026-08-31

Tekniska nämnden

Diarienr: TN-2026/00693

Teknisk ramjustering gällande postdistribution och Väven

Förslag till beslut
Tekniska nämnden beslutar

att föreslå kommunstyrelsen att bevilja en teknisk ramjustering om 251 tkr från kommunstyrelsen till tekniska nämnden avseende postdistribution samt att bevilja en teknisk ramjustering om -464 tkr från kommunstyrelsen till tekniska nämnden avseende Kulturväven. Ramjustering gäller från 1 jan 2027.

Ärendebeskrivning
I samband med avskaffandet av internfakturering var det den nämnd som bedrev verksamhet och stod för den externa kostnaden som erhöll den ekonomiska ramen för kostnaderna. Kommunstyrelsen har senare beslutat om principer som ska vara vägledande när enskilda frågor som kvarstår efter avskaffandet av interna affärer ska lösas ut (2021-2-09 §17). Bland principerna framgår att intäkter och kostnader bör följas åt så långt det är möjligt. Mot bakgrund av detta föreslås att medel för postdistribution samt hyresintäkter avseende Kulturväven förs till tekniska nämnden, som ombesörjer aktiviteterna.

Justeringen är kostnadsneutral och tillser renodling av verksamheter, där kostnader och intäkter följs åt.

Beslutsunderlag
Checklista för handläggning av ärenden inför politiska beslut anses inte tillämpbar.

Beredningsansvariga
Anna Engman, controller

Beslutet ska skickas till
Marcus Bystedt
Anette Sjödin, SLK ekonomi

Tjänsteskrivelse

Dnr: TN-2026/00693

Anna Engman, SLK ekonomi
KSdiarium

Förnamn, Efternamn	Annika Lind
Befattning	Chef myndighet och administration

UMEÅ KOMMUN

Tjänsteskrivelse
2026-03-31

Tekniska nämnden

Diarienr: TN-2026/00081

Beslut av riskbedömning och fortsatt användning av Microsoft

Förslag till beslut
Tekniska nämnden beslutar

att det finns tillräckligt beslutsunderlag för att kunna ta ställning till Microsoft som leverantör och strategisk partner.

att Umeå kommun kan fortsätta nyttja Microsoft som leverantör och strategisk partner.

att nämnden årligen i december följer upp riskbedömning och åtgärder som görs löpande under året för att reducera risker.

att kontinuerligt omvärldsbevaka och utvärdera tjänster inom Sverige eller EU/EES som alternativ till Microsofts tjänster.

Ärendebeskrivning
Umeå kommun har sedan många år Microsofts molntjänst 365 för samtliga anställda och förtroendevalda. Sedan införandet har regelverk och lagar för amerikanska tjänster och leverantörer skärpts. Kommunen har inte haft någon uppdaterad helhetsbedömning av Microsoft och deras tjänster vilket hämmat utvecklingstakten och skapat en osäkerhet i kommunens verksamheter.

I syfte att lyfta Umeå kommuns användning av Microsoft från ovisshet till ett aktivt vägval med en tydlig plan, har det genomförts en omfattande juridisk bedömning av Microsoft som leverantör. Bedömningen har gjorts utifrån granskning mot Dataskyddsförordningen (GDPR) och Offentlighets- och sekretesslagen (OSL) där vi haft stöd av externt upphandlat expertis, se Bilaga A, tillsammans med kommunintern kompetens inom juridik, dataskydd, informationssäkerhet samt Digital omställning och IT. För specifika frågor har det också skett direkt dialog med Microsoft. En mer utförlig beskrivning av bakgrund, arbetsgång, juridiska förutsättningar och riskbedömning framgår i promemoria Bilaga B.

Tjänsteskrivelse

Dnr: TN-2026/00081

Efter information om riskbedömningen i Tekniska nämnden beslutade nämnden att ärendets underlag inklusive framtaget förslag till beslut, skulle skickas till kommunstyrelsen för yttrande innan beslut i Tekniska nämnden, Bilaga C.

Remissvar Kommunstyrelsen

Kommunstyrelsen har beslutat att den inte, utifrån av Tekniska nämnden tillhandahållet underlag, kan yttra sig om den fortsatta användningen av Microsoft är laglig och säker. Styrelsen har bedömt att Tekniska nämnden behöver utreda och dokumentera frågan ytterligare, Bilaga D.

Utifrån KS remissvar inklusive dess bilagda beslutsunderlag anlitades åter en extern jurist som stöd för bedömning och hantering för att ge Tekniska nämnden förutsättningar att förstå och beakta KS synpunkter. Likt tidigare är det ATEA som anlitats men vid detta tillfälle är det en annan jurist än den som först var med i processen. Juristen första svar kom i form av en rapport, Bilaga E. Det visade sig dock att juristen inte fått ta del av materialet som tidigare tagits fram vilket medförde att rapportens synpunkter blev missvisande. Efter inläsning av tidigare utredningar samt förtydliganden i mejl, Bilaga F, och mindre korrigerar i tjänsteskrivelsen har alla synpunkter besvarats. Dataskyddsombudet har fått ta del av underlagen med möjlighet att lämna eventuella synpunkter, Bilaga G.

Samråd med Tekniska nämndens dataskyddsombud

Samråd har skett med nämndens dataskyddsombud, fullständiga rekommendationer med kommentarer finns i Bilaga H.

Dataskyddsombudet rekommenderar att verksamhetens utredning kompletteras med i vart fall, sekretessprövning gällande utlämnande av personuppgifter till Microsoft (en annan prövning än den som den verksamheten tar upp i tjänsteskrivelsen), dokumentation gällande effektiviteten av ”EU Data Bounary”, utredning och bedömning av Microsofts egen behandling av nämndens personuppgifter, identifiering och bedömning av risker med överföring enligt CLOUD Act till Australien och Storbritannien. Utan dessa kompletteringar går det inte att göra en fullständig bedömning av möjligheten att anlita Microsoft som personuppgiftsbiträde.

På befintligt underlag rekommenderas nämnden att komplettera avtalet med Microsoft så att det som utgångspunkt förbjuder Microsoft att bryta mot GDPR och annan svensk lag, istället för att som i dag instruerar Microsoft att bryta mot lag. De av verksamheten föreslagna skyddsåtgärderna i tjänsteskrivelsen har ingen effekt på denna brist.

Tjänsteskrivelse

Dnr: TN-2026/00081

Om avtalet inte ändras rekommenderas nämnden att vidta åtgärder som skyddar uppgifterna från Microsoft t.ex. kryptering där Microsoft inte har tillgång till nyckeln, eller annan effektiv skyddsåtgärd.

Om inga kompletterande åtgärder vidtas bedöms i nuläget anlitandet av Microsoft som personuppgiftsbiträde inte vara förenligt med GDPR och det rekommenderas att nämnden avbryter personuppgiftsbehandlingen i Microsofts tjänster tills det gått att säkerställa att behandlingen följer reglerna i GDPR och annan svensk lag.

Uppdaterad tjänsteskrivelse efter samråd med dataskyddsombud
För att möta dataskyddsombudets synpunkter har tjänsteskrivelsen i hög grad kompletterats med förtydliganden och beskrivningar som saknats för att tydliggöra bedömningsgrunder och vidtagna åtgärder. Den uppdaterade tjänsteskrivelsen har bollats med dataskyddsombudet innan slutgiltig version sammanställts.

Dataskyddsombudet har efter samrådet inte sett skäl att ändra sin rekommendation till nämnden, se bilaga H.

Teknik- och fastighetsförvaltningens bedömning
Tillräcklig utredning
Förvaltningen bedömer att den utredning som är gjord är tillräcklig för att kunna ta ställning till Microsoft som leverantör. Utredningen har redovisat behov, redogjort för de rättsliga förutsättningarna och möjliga riskreducerande åtgärder i tillräcklig grad för att kunna identifiera, reducera och ansvarsfullt acceptera risker i proportion till nytta och uppdrag.

Förvaltningen har genomfört en omfattande juridisk och riskbaserad genomlysning med:

- Extern juridisk expertbedömning (ATEA)
- Kommunintern kompetens inom juridik, dataskydd, informationssäkerhet och DoIT i samverkan
- Dialog med Microsoft
- Identifierade och beslutade riskreducerande åtgärder

Samtidigt är det viktigt att förstå att kvarstående risker relaterade till tredjelandslagstiftning och ändrat rättsläge inte kan elimineras fullt ut. Därför är det ett viktigt arbete att kontinuerligt följa den politiska och juridiska utvecklingen samt utvärdera och testa tjänster som kan bli tillräckligt bra alternativ till Microsofts produkter.

GDPR (särskilt artikel 28 – personuppgiftsbiträde)

Tjänsteskrivelse

Dnr: TN-2026/00081

Syfte till personuppgiftsbehandling

Kommunen har behov av att kunna kommunicera och samarbeta både internt och externt för att genomföra sitt uppdrag. För att stödja verksamhetens arbetssätt, hantera informationsutbyte och möta krav som följer av lagstiftning och andra åtaganden används digitala verktyg och plattformar. Microsoft 365 utgör en av de plattformar som används för att möjliggöra kommunikation, samarbete och informationshantering inom organisationen.

Behandling

För varje enskild behandling dokumenteras den tillämpliga rättsliga grunden i organisationens register över personuppgiftsbehandlingar. Valet av rättslig grund görs utifrån behandlingens specifika ändamål och följer principen att en behandling ska stödjas på en rättslig grund.

Kommunen beaktar de krav som följer av dataskyddsförordningen (GDPR) vid utformningen av insamlings- och behandlingsprocesserna, i syfte att stödja en laglig, korrekt och transparent behandling av personuppgifter. Uppgifterna kan komma från flera olika källor, inklusive lokala system såsom Active Directory (AD), och hanteringen varierar mellan tjänsterna utifrån deras specifika användningsområden.

Varje insamling dokumenteras separat för behandlingen och omfattar:

- Vilka personuppgifter som samlas in.
- Källan till personuppgifterna (lokala system, registrerade individer eller andra system).
- Syftet med insamlingen och den efterföljande behandlingen.

Miljön är konfigurerad för så att endast nödvändiga data för funktionerna i Microsoft 365 behandlas. Dataöverföringarna är krypterade och kräver autentisering.

Systematisk övervakning

Microsoft 365 omfattar behandlingar som i vissa delar kan anses utgöra systematisk övervakning enligt dataskyddsförordningen (GDPR). Detta beror främst på att plattformen kontinuerligt registrerar och analyserar användarrelaterade aktiviteter genom loggning, diagnostik och säkerhetsfunktioner.

Plattformen genererar automatiskt tekniska loggar och metadata kopplade till användningen av tjänster såsom Exchange Online, SharePoint Online, Microsoft Teams och Entra ID. Dessa uppgifter kan bland annat avse

inloggningar, åtkomst till information, filhantering och användning av olika funktioner inom tjänsterna.
Microsoft 365 innehåller även säkerhetsfunktioner som löpande övervakar användnings- och åtkomstmönster för att upptäcka, förebygga och hantera säkerhetsincidenter, obehörig åtkomst och andra avvikelser. Exempel på detta är analys av inloggningsförsök, riskbaserad åtkomstkontroll och automatiserade säkerhetsvarningar.

Den kontinuerliga insamlingen och analysen av användarrelaterade uppgifter innebär att användares aktiviteter kan registreras och följas över tid inom ramen för plattformens drift- och säkerhetsfunktioner. Behandlingen sker huvudsakligen i syfte att upprätthålla informationssäkerhet, funktionalitet, spårbarhet och efterlevnad av kommunens och lagstiftningens krav.

Kommunen arbetar löpande med tekniska och organisatoriska åtgärder som begränsar datainsamling till det som är absolut nödvändigt för säker drift och efterlevnad.

Lagring och behandling i EU/EES
Umeå kommuns Microsoftmiljö är konfigurerad enligt Microsoft EU Data Boundary vilket begränsar lagring och behandling av personuppgifter till EU/EES. Vissa definierade undantag kan dock förekomma, exempelvis för säkerhetsrelaterade åtgärder eller felsökning. För dessa situationer används särskilda skyddsåtgärder, såsom pseudonymisering, tokenisering och minimering av loggdata. Microsoft beskriver i sin dokumentation vilka typer av uppgifter som kan omfattas av sådana undantag samt de skyddsmekanismer som tillämpas.

Juridisk bedömning av Microsofts roll
Microsoft Ireland behandlar personuppgifter inom ramen för sitt uppdrag att tillhandahålla organisationens Microsoft 365-tjänster. Detta regleras genom ett personuppgiftsbiträdesavtal (PUB-avtal) som säkerställer att behandlingen sker enligt dokumenterade instruktioner från den personuppgiftsansvarige.

Personuppgifterna får inte användas av Microsoft för egna ändamål, såsom marknadsföring eller profilering.

Vid användning av Microsoft 365 som plattform kan överföring av personuppgifter till tredjeland förekomma, men detta sker endast i mycket begränsad omfattning och under särskilda förutsättningar.

Tjänsteskrivelse

Dnr: TN-2026/00081

I vissa specifika tekniska processer, såsom supportåtgärder, felsökning eller säkerhetsåtgärder, innebära tillfällig och begränsad åtkomst till data från tredjeland, framför allt från USA. Sådana överföringar sker inte som huvudregel, utan endast per specifik behandling och under tydligt kontrollerade former.

För att uppfylla kraven enligt Schrems II-domen har Microsoft även infört ett antal åtgärder:

- Kryptering av data i vila och under överföring
- Pseudonymisering av loggar och systemdata
- Strikta åtkomstkontroller
- Policyramverk för att bestrida myndighetsförfrågningar som strider mot EU-rätt

Adekvansbeslutets giltighet

Högsta domstolen i USA har nyligen tagit ett beslut (Trump v. Slaughter) som sätter fokus på om USA:s tillsynsorgan kan anses vara oberoende och om detta kommer att påverka adekvansbeslutets giltighet framöver. IMY följer utvecklingen och kommer, inom ramen för EDPB att analysera domens eventuella konsekvenser för överföringar till USA. IMY uttalar på sin hemsida att det finns fortfarande ett gällande adekvansbeslut för USA. Myndigheten påtalar att det är viktigt för organisationer att hålla sig informerade och ha beredskap för hur man gör om adekvansbeslutet skulle upphävas i framtiden.

Sammantagen analys och bedömning GDPR

Baserat på extern juridisk utredning, EU-kommissionens gällande adekvansbeslut, Integritetsskyddsmyndighetens och Europeiska dataskyddsstyrelsens (EDPB) uttolkningar samt identifierade risker och åtgärder bedömer förvaltningen att Microsoft, i nuläget, kan anlitas som personuppgiftsbiträde enligt GDPR.

OSL (10 kap. 2 a §)

Eftersom Microsoft 365-tjänsterna har olika syften och användningsområden kan omfattningen och karaktären på personuppgiftsbehandlingen skilja sig mellan tjänsterna. Varje tjänst genomgår därför en individuell bedömning och dokumentation. Bedömningen omfattar bland annat vilka personuppgifter som behandlas, vilka tekniska och organisatoriska säkerhetsåtgärder som tillämpas, samt

om personuppgifter överförs till tredjeland och vilka mekanismer som används för att säkerställa en adekvat skyddsnivå vid sådana överföringar. Förvaltningen bedömer att de verktyg/tjänster som Microsoft hanterar för Umeå kommuns räkning är konfigurerade på ett sådant sätt att de är begränsade till teknisk bearbetning och lagring av uppgifter. I nästa steg kommer respektive verktyg/tjänst att bedömas för att se över vilken typ av information utifrån bland annat skyddsrekvisit i OSL som kan hanteras i de olika tjänsterna och på vilket sätt samt bedöma lämpliga säkerhetsåtgärder i tjänsten.

Exempel på hur en bedömning skulle kunna se ut
En bedömning av tjänsten Teams skulle efter genomförd analys, inklusive riskbedömning och identifierade åtgärder, bedömas kunna användas för bearbetning och lagring av information upp till och med skyddsklass 2 (begränsad). Analysen visar vidare att en specifik deltjänst – krypterade Teams-samtal mellan två parter, där information endast bearbetas och inte lagras (ingen transkribering, inspelning eller chatt) – kan tillåtas för information upp till och med skyddsklass 4 (hög), under förutsättning att kompletterande åtgärder regleras i rutiner.

Respektive verksamhet behöver därefter genomföra en konsekvensbedömning utifrån sina behov, i relation till tjänstens riskbedömning, som underlag för beslut om och hur Teams kan användas i den egna verksamheten.

Vid ett eventuellt scenario där Microsoft åläggs att lämna ut uppgifter enligt Cloud Act till amerikanska myndigheter visar exemplet med Teamssamtal att den information som Microsoft får del av som leverantör och som kan lämnas ut är knapphändig. Det förutsätter i så fall att Microsoft skulle vidta annan behandling än vad som framgår i avtalet och det är inget som på något sätt finns anledning att utgå ifrån.

Mot bakgrund av vad som beskrivs ovan om konfiguration och analys som kommer att genomföras för varje tjänst bedömer förvaltningen att ett utlämnande av uppgifter till Microsoft som leverantör är förenligt med 10 kap. 2 a § OSL.

Känsliga och/eller extra skyddsvärda personuppgifter
Enligt kommunens Informationssäkerhetsriktlinje (bilaga) är det inte tillåtet att hantera sekretess (skyddade personuppgifter hör hit), extra skyddsvärda eller känsliga personuppgifter (gul information) samt data med hög sekretess (Röd) i Microsofts molntjänster, men det finns ingen teknisk begräsning som hindrar en användare att lägga in den typen av data vilket medför en riskhantering som vilar på individers

regelefterlevnad. I vissa tjänster, exempelvis Fabric, kan data anonymiseras för att minska känsligheten.

Det är känt att vissa förvaltningar idag lagrar data som är känslig och extra skyddsvärd utifrån att den omfattar hälsa. Det pågår införande av en kompletterande säker lagringstjänst för att kunna lyfta ut den här typen av behov från Microsoftmiljö.

Sammantagen analys och bedömning OSL
Sammanfattningsvis bedömer förvaltningen att en fortsatt användning av Microsoft som leverantör i nuläget är förenligt med offentlighets- och sekretesslagen.

Ställningstagande om kvarstående risker
Förvaltningen konstaterar att kvarstående risker kopplade till tredjelandslagstiftning och leverantörens jurisdiktion inte helt kan elimineras. Vi bedömer att dessa risker är strukturella, inte leverantörsspecifika, och att riskreducerande åtgärder har vidtagits.
Mot denna bakgrund tar vi ställning till att dessa kvarstående risker kan accepteras under förutsättning att kontinuerlig uppföljning och möjlighet till omprövning sker.

Därmed är slutsatsen att rekommendera Tekniska nämnden att besluta att fortsätta nyttja Microsoft som strategisk partner, under förutsättning att riskreducerande åtgärder genomförs, bland annat:

- **Informationsklassning:** Rätt data på rätt plats med skarpare sortering av skyddsvärd data, exempelvis med känslighetsetiketter för att förenkla administration av klassningen. Utifrån bedömning av respektive tjänst i Microsoft 365 avgörs vilken informationsklass som kan lagras och behandlas.
- **Skydd:** Fortsätta införa kryptering och tekniska spärrar där det är funktionellt och ekonomiskt möjligt
- **Kontroll:** Ökad övervakning och spårbarhet i systemen
- **Utvärdering:** Kontinuerlig utvärdering av rättsläget, teknisk utveckling samt omvärldsläge

Det ska löpande genomföras omvärldsbevakning för alternativa leverantörer och tjänster inom Sverige och EU/EES samt göras löpande riskbedömning av Microsoft för att identifiera eventuellt behov att ompröva beslutet.
Med utgångspunkt i de riskbedömningar av Microsoft och deras tjänster som DoIT samordnar ska också respektive verksamhet bedöma vilka

tjänster som är acceptabla för deras användning och eventuellt komplettera med användaranvisningar där det behövs.

Beslutsunderlag

Bilaga A - Juridisk bedömning av Microsoft som leverantör (ATEA). Bilaga.
Bilaga B - PM om arbetsgång och juridiska överväganden inför rekommendation om fortsatt användning av Microsoft. Bilaga.
Bilaga C - TN-2026_00081-2 Protokollsutdrag 2461290_1_1. Bilaga.
Bilaga D - Beslut av riskbedömning och fortsatt användning av Microsoft, sammanfogat remissvar. Bilaga.
Bilaga E - Juridisk bedömning av molntjänster i förhållande till TN 2026_00081 (feedback efter granskning). Bilaga.
Bilaga F - E-post_återkoppling efter feedback på granskning av KS remissvar. Bilaga.
Bilaga G - E-post_För kännedom och eventuella synpunkter senast 16 augusti. Bilaga.
Bilaga H - DSO samrådsyttrande augusti 2026 TN 2026_0081. Bilaga.
Riktlinjer för informationssäkerhet, Umeå kommun. Bilaga.

Checklista för handläggning av ärenden inför politiska beslut bedöms inte tillämpbar.

Beredningsansvariga

Mattias Wallmark, DoIT
Hannes Fries, DoIT

Beslutet ska skickas till
KSdiarium
Dataskyddsombud Eric Lindström
SLK-juridik – chefsjurist Maria Törnblom
Informationssäkerhetssamordnare Hanna Öberg (SLK)
Verksamhetschef Mattias Wallmark (DoIT)
Verksamhetsutvecklare Hannes Fries (DoIT)
Stabschefsnätverket Malin Ärlebrant

RAPPORT - Juridisk bedömning av Microsoft som leverantör

7 april 2025

Umeå Kommun

Hannes Fries

hannes.fries@umea.se

Atea Sverige AB
Box 18
164 93 Kista
Org. Nr. 556448-0282

ATEA

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Umeå kommun, tillsammans med andra offentliga myndigheter, står inför ett ökat behov av digitalisering där användande av molntjänster i många fall utgör en förutsättning för att lyckas. Att använda molntjänster ger emellertid upphov till frågor av både juridisk och teknisk karaktär.

Umeå kommun har upphandlat konsultstöd för att genomföra en omfattande utredning i linje med dessa krav och principer, som blir tillämpliga för myndigheter.

I denna rapport ska en bedömning av Microsoft som leverantör göras, för att utreda ifall de kan uppfylla kraven i artikel 28 Dataskyddsförordningen (GDPR). Rapporten ska även utreda möjligheten för kommunen att lagligt hantera information som omfattas av sekretess enligt offentlighets- och sekretesslagen (OSL) i Microsofts tjänster. Analysen ska även innehålla Microsofts förmåga att uppfylla andra regulatoriska krav t.ex. i GDPR och OSL.

1.2 Avgränsning

Denna rapport har två huvudpunkter i fokus, Microsoft i förhållande till Artikel 28 i GDPR och möjligheten att hantera sekretessbelagd information i Microsofts verktyg. Övriga lagrum som berörs i rapporten kan komma att behöva ytterligare granskas djupare, då dessa lagrums tillämplighet snarare har konstaterats, än att analyseras. Denna avgränsning har gjorts med beaktande av den tids- och kostnadsram som Umeå kommun gjorde i dess upphandling.

1.3 Begreppslista

Personuppgiftsansvarig: Bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till, i Umeå kommun är varje ansvarig nämnd ytterst ansvariga för personuppgifterna inom sin verksamhet.

Personuppgiftsbiträde: Behandlar personuppgifter för den personuppgiftsansvariges räkning. Genom reglementet för Umeå kommuns styrelse och nämnder, så har det reglerats där att i de fall som den Tekniska nämnden ansvarar för drift av system som behandlar personuppgifter för andra nämnder är Tekniska nämnden personuppgiftsbiträde till dessa nämnder.

Molntjänster: En infrastruktur, plattform eller mjukvara som bearbetas eller lagras på en centraliserad plats som inte är fysiskt belägen hos användaren. Tjänsterna är hostade på en eller flera avlägsna servrar som drivs av en molnleverantör. Dessa servrar är sedan tillgängliga för användare via internet.

Amerikanska molntjänster: Molntjänster som oavsett etableringsort ägs av ett amerikanskt moderbolag.

Utkontraktering av uppgifter: leverantör som har i uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifterna för den uppgiftslämnande myndighetens räkning.

Informationsklassning: En metod som hjälper verksamheten att välja rätt åtgärder för att skydda information.

Behandling: Med behandling av personuppgifter menas i princip allting som går att göra med personuppgifterna. Det kan till exempel vara att samla in, registrera, lagra, samköra eller skriva ut uppgifterna. Utan en rättslig grund är behandlingen av personuppgifter inte laglig.

Utkontraktering av IT-drift: En myndighet överlåter hela eller delar av sin IT-drift till en extern aktör, ofta ett privat företag, som ansvarar för drift, underhåll och support av IT-systemen.

Samordning av IT-drift: Avser att en myndighet hanterar IT-driften åt en eller flera andra myndigheter, vilket innebär att flera myndigheter delar på IT-resurser och kompetens för att uppnå effektivitet och säkerhet

Riskmitigering: När man minskar sannolikheten att risken ska ske eller påverkan som den kan ha via diverse olika åtgärder.

2 Dataskydd

Vid behandling av personuppgifter behöver efterlevnad av dataskyddsförordningen ske. Beroende på vilka personuppgifter, hur och vart de behandlas aktualiseras olika förutsättningar som behöver beaktas vid behandlingen. Grundläggande för personuppgiftsbehandling är att den behöver vara nödvändig.

I dataskyddsförordningen står det att personuppgiftsbehandlingen ska vara "nödvändig" för flera av de olika rättsliga grunderna i Artikel 6, till exempel för att man ska kunna fullgöra ett avtal eller utföra en uppgift av allmänt intresse. Även om ett avtal skulle kunna fullgöras eller en uppgift skulle kunna utföras utan att personuppgifter behandlas på ett visst sätt, så kan behandlingen anses vara nödvändig och därmed tillåten om den leder till effektivitetsvinster.

Men om en arbetsuppgift kan utföras nästan lika enkelt och billigt utan att personuppgifter behandlas, så är det inte nödvändigt att behandla personuppgifterna i den här bemärkelsen.

2.1 Tredjelandsöverföringar och adekvansbeslut

Dataskyddsförordningen gäller för all behandling som sker inom EU/EES innebärande det finns ett grundläggande skydd för personuppgifter. Dataskyddsförordningen reglerar emellertid även när personuppgifter överförs till länder utanför EU/EES, s.k. tredjelandsöverföring. Dataskyddförordningen ställer särskilda krav för att en sådan överföring ska vara laglig, vilket utgår från att upprätthålla en fortsatt skyddsnivå avseende personuppgifterna även utanför dataskyddsförordningens territoriella tillämpningsområde.

Tredjelandsöverföring regleras i dataskyddsförordningens 5:e kapitel vilket medger vissa överföringsmekanismer som gör överföringen laglig. EU-kommissionen kan besluta att ett land har en tillräckligt hög skyddsnivå och personuppgifter kan överföras dit utan något särskilt tillstånd, landet har då adekvat skyddsnivå. Detta är en av de överföringsmekanismer som finns enligt kap. 5 GDPR.

10 juli 2023 fattade EU-kommissionen beslut om att USA har adekvat skyddsnivå genom EU-US Data Privacy Framework. Detta grundas på ett utfärdat presidentdekret och innebär i praktiken ifrån EU att USA bedöms ha en tillräckligt hög skyddsnivå för att personuppgifter lagligen kan överföras till USA. Tillämpning av EU-US Data Privacy Framework förutsätter att den leverantör som ska behandla personuppgifterna har certifierat sig och därigenom accepterat att följa vissa villkor

för att upprätthålla viss nivå av skydd och därmed finns med på Data Privacy Framework list som finns digitalt på USA:s handelsdepartement[1].

2.2 Tekniska och organisatoriska åtgärder

I Dataskyddsförordningens artikel 32 framgår de skyldigheter som ska uppfyllas genom att implementera lämpliga tekniska och organisatoriska åtgärder och därmed vara ett tillräckligt skydd för fysiska personers rättigheter och friheter.

Tekniska åtgärder är sådana som ger: data- eller systemsäkerhet, kommunikationssäkerhet eller fysisk säkerhet. Medan organisatoriska åtgärder omfattar sådant som: konsekvensbedömning, styrdokument, processer, rutiner, metoder analyser etc.

När lämplig säkerhetsnivå bedöms så ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

2.3 Avtalsmässiga villkor

Enligt Dataskyddsförordningens artikel 28.3 ska personuppgiftsansvariga och personuppgiftsbiträden reglera sina relationer genom ett skriftligt avtal (eller annan rättsakt).

De personuppgiftsansvariga får endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att skyldigheterna i GDPR kommer att uppfyllas och att de registrerades rättigheter skyddas, vilket föreskrivs i Dataskyddsförordningens artikel 28.4. Hur omfattande åtgärder som behövs beror på risker som finns med personuppgiftsbehandlingen.

I artikel 28.5 beskrivs att ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att tillräckliga garantier tillhandahålls och att i artikel 28.6 så får ett sådant avtal eller annan rättsakt som avses i punkterna 3 och 4 i artikel 28 får, utan att det påverkar tillämpningen av ett enskilt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet, helt eller delvis baseras på sådana standardavtalsklausuler som avses i punkterna 7 och 8 i artikel 28, inbegripet

[1] Länk till Privacy Framework List, https://www.dataprivacyframework.gov/list

när de ingår i en certifiering som i enlighet med artiklarna 42 och 43 beviljats den personuppgiftsansvarige eller personuppgiftsbiträdet.

Verksamheter som vill använda standardavtalsklausuler i sina biträdesavtal måste särskilt uppmärksamma att klausulerna inte får ändras. Precis som vid upprättande av egna biträdesavtal ansvarar verksamheterna både för att säkerställa att avtalen återspeglar de faktiska förhållandena mellan avtalsparterna och för att instruktioner till biträden och underbiträden är korrekta.

2.4 Bedömning av Microsoft i förhållande till artikel 28 GDPR

Microsoft har ett standardiserat personuppgiftsbiträdesavtal (DPA)[2] där det konstateras att man behandlar data i form av personuppgifter. Där framgår även att man kan komma att lämna ut sådan information om det krävs enligt lag. Detta åsyftar i första hand den amerikans underrättelselagstiftning som Microsoft som amerikanskt bolag är ålagd att följa. I DPA bilaga C understryker Microsoft att om bolaget mottar en sådan begäran ska de i första hand hänvisa denna direkt till kunden och i annat fall använda alla lagliga medel för att bestrida begäran.

Den europeiska dataskyddsstyrelsen (EDPB) har yttrat sig om fall där ett biträde kan komma att ge ut information till myndighet i strid med personuppgiftsbiträdesavtalet. EDPB är tydliga med att det är den personuppgiftsansvariga som är ansvarig att bedöma om den potentiella behandlingen skulle strida mot GDPR och det är personuppgiftsbiträdets roll att på ett transparent sätt redovisa de och dess underbiträden kommer hantera personuppgifterna. EDPB understryker dock att en potentiell behandling, inte är olaglig i sig, utan det krävs att det faktiska utlämnandet realiseras, och först då så kan frågan om lagligheten utredas. Även här har EDPB poängterat att den personuppgiftsansvarigas ansvar kvarstår att tillse att den tredjelandslagstiftning som blivit aktuell för personuppgiftsbiträdet att rätta sig efter, i stora drag uppfyller likvärdig skyddsnivå som GDPR.[3]

I och med Data Privacy Framework så har EU fattat ett adekvansbeslut, i enlighet med artikel 45 GDPR, kopplat till personuppgifter som överförs till USA. En del i detta beslut är att EU granska relationen mellan landet i fråga i förhållande till europeisk lagstiftning som rör integritet och rättigheter generellt. När detta gjordes så bedömde alltså EU lagstiftningen i USA som potentiellt kommer tvinga företag att lämna ut

[2] Länk till Microsofts DPA, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=32
[3] Länk till EDPB:s yttrande, https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub-processors_en.pdf

information till begärande nationell myndighet. Den typen av avtalsvillkor som Microsoft har i sitt standard DPA bör alltså, i ljuset av bedömningen som EU har gjort, vara i linje med artikel 28.3 GDPR.

Frågan om personuppgiftsansvarigs instruktion till personuppgiftsbiträde framgår utav Microsofts DPA. Personuppgiftsansvarig får i det samtycka till att avtalet mellan sig och Microsoft, i detta inryms DPA-villkoren och dess framtida uppdateringar. I detta samtycker även personuppgiftsansvarig till produktdokumentation, kundens användning och konfigurering av funktioner i produkterna. Dessa ska ses som de fullständiga instruktionerna till Microsoft för behandling av personuppgifterna.

Utöver detta så ges också Microsoft tillstånd via DPA att utföra ”verksamhetsutövning”. Detta definierar Microsoft som: Att skapa sammanställda, icke-personliga uppgifter från data som innehåller pseudonymiserade identifierare (såsom användningsloggar som innehåller unika, pseudonymiserade identifierare), att beräkna statistik som avser kunddata eller data i ”Professionella tjänster”. Detta ska alltid utföras utan att få åtkomst till eller analysera innehållet i Kunddata eller data i ”Professionella tjänster” och begränsat till att uppnå de syften som anges nedan, och alltid för att ”tillhandahålla Kunden Produkterna och Tjänsterna”. Microsofts syfte med ”verksamhetsutövning” är: fakturering och kontohantering, ersättning, till exempel beräkning av personalens provision eller partnerincitament, intern rapportering och företagsmodellering, till exempel prognostisering, intäkter, kapacitetsplanering, produktstrategi och ekonomisk rapportering. Microsoft ska utifrån ”verksamhetsutövning” tillämpa principer om dataminimering och ska aldrig använda personuppgifter för: användarprofilering, marknadsföring eller liknande kommersiella syften eller, något annat syfte än de syften som anges i detta avsnitt. Som övrigt hanterande enligt Microsofts DPA, styrs behandlingen för verksamhetsutövning av Microsofts sekretesskyldigheter och de åtaganden som finns beskrivna under rubriken ”Utlämnande av behandlade data”.

Granskning av Microsofts anlitande av ”underordnade personuppgiftsbiträden” regleras i deras DPA och där har Microsoft ett på förhand givet tillstånd att anlita nya biträden med förbehåll att kund har möjlighet att göra invändningar mot ett anlitande inom ett satt tidsfönster för kund att inkomma med ett skriftligt meddelande om uppsägning. De underordnade personuppgiftsbiträdena tillgängliggörs på en Microsoft-webbplats som kund har möjlighet att får prenumerationsutskick ifrån. Som nämnt ovan så kan Microsofts underordnade personuppgiftsbiträden komma att behandla personuppgifter i de fall kunden använder sig av vissa typer av tjänster. Dessa personuppgifter ska då alltså pseudonymiseras, men de är ändå att beakta som personuppgifter under behandling. Den behandlingen stödjer man genom 2021 års standardavtalsklausuler som överföringsmekanism i enlighet med kapitel V GDPR.

Vilka premisser en granskning av Microsoft som personuppgiftsbiträde ska ske på framgår av DPA att Microsoft och kunden gemensamt innan granskning avtalar om

omfattning, tidpunkt, varaktighet, kontroll, beviskrav samt avgifter för granskningen. Microsoft förordar att en sådan granskning görs av en behörig oberoende revisionsfirma. Granskningsresultatet ska vara Microsofts konfidentiella information och tydligt visa granskarens väsentliga fynd. Microsoft ska omgående åtgärda problem som tas upp i Microsofts granskningsrapport enligt granskarens önskemål och som innebär att Microsoft är skyldig att avhjälpa brister.

Microsoft är certifierat i enlighet med EU:s och USA:s dataskyddsramverk (Data Privacy Framework) som är upprättat av USA:s handelsdepartement. EU-kommissionen ska regelbundet se över det aktuella adekvansbeslutet, och den första översynen genomfördes i juli 2024 där resultaten har presenterats i en rapport från EDPB. Rapporten utgår ifrån kommersiella aspekter och amerikanska myndigheters tillgång till personuppgifter som överförts till och från EU från organisationer som innehar certifiering enligt Data Privacy Framework. Utifrån det kommersiella perspektivet så framhåller EDPB att USA vidtagit samtliga åtgärder för certifieringsprocessen och klagomålshantering från EU-medborgare. Utifrån den andra aspekten tar EDPB avstamp ifrån Executive Order 14086, i och med den skriver man att man numera har ett effektivt genomförande av skyddsåtgärderna och det har skett många förbättringar i dataskyddet bl.a. genom att det nu finns en domstol som rättsligt kan pröva frågan kring registrerades rättigheter.

3 OSL – teknisk bearbetning eller lagring

I offentlighet- och sekretesslagens 10 kap. 2 a § har det sedan 2023 funnits en sekretessbrytande bestämmelse som skapar bättre förutsättningar för myndigheter att utkontraktera eller samordna sin IT-drift.

Ett uppdrag att tekniskt bearbeta eller lagra uppgifter kan exempelvis bestå i att införa, förvalta, utveckla och så småningom avveckla en it-driftstjänst. Under dessa olika faser kan en mängd olika åtgärder behöva vidtas för att upprätthålla den tillgänglighet, funktionalitet och prestanda i tjänsten som har avtalats mellan parterna. Det kan röra sig om förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration med andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Det kan också röra sig om säkerhetstester och andra säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering. Vid avveckling av en tjänst kan myndighetens uppgifter behöva migreras eller exporteras tillbaka till myndigheten eller till en annan uppdragstagare.

3.1 Lämplighetsbedömning

En uppgift får inte lämnas ut om det med hänsyn till omständigheterna är olämpligt. Det innebär att en myndighet, innan en uppgift lämnas ut, ska pröva om det finns skäl som talar emot att uppgiften lämnas ut. De omständigheter som ska beaktas är som utgångspunkt sådana som har koppling till den utlämnande myndigheten och till uppgiftsmottagaren likväl som till de uppgifter som är eller kan bli föremål för utlämnande. Det ska alltså göras en allsidig prövning av alla omständigheter som är relevanta i det enskilda fallet.

Som myndighet så är en del att man behöver kunna motivera sin utkontraktering på ett tydligt sätt. Denna bedömning kan grunda sig i ekonomiska anledningar, i att den tekniska kompetensen saknas på myndigheten för att kunna motsvara verksamhetens krav på funktionalitet dylikt.

Vad som definieras som teknisk bearbetning eller lagring är en bred flora av tekniska uppgifter. Enligt förarbetet[4] till lagrummet kan den tekniska bearbetningen eller lagringen innefatta allt ifrån Införande, förvaltning, utveckling och avveckling av IT-driftstjänster till konfiguration, test och utveckling m.m.

En viktig del i lämplighetsbedömningen är att identifiera om uppgifterna är av särskilt känslig natur, såsom uppgifter av synnerlig betydelse för rikets säkerhet eller andra sekretessbelagda uppgifter. Även om en uppgift inte direkt faller under kategorin “synnerlig betydelse för rikets säkerhet”, kan andra faktorer göra det olämpligt att lämna ut den för teknisk bearbetning eller lagring.

Omständigheter som kan ha betydelse är exempelvis vilken typ av uppgifter det rör sig om, vilka intressen som ligger till grund för sekretessen och uppgifternas omfattning. En omständighet som med viss tyngd kan tala emot ett utlämnande är att det är fråga om uppgifter av särskilt känsligt slag, exempelvis uppgifter av synnerlig betydelse för rikets säkerhet när det gäller totalförsvaret.

Vidare ska den utlämnande myndigheten ta hänsyn till om de uppgifter som lämnas ut kommer att samlokaliseras med uppgiftsmängder som tillhör andra kunder och bedöma om detta innebär några särskilda risker. Det kan vara lämpligt att den uppgiftsutlämnande myndigheten dokumenterar de avvägningar och bedömningar som görs vid ett utlämnande som omfattar en större uppgiftsmängd eller uppgifter som är av känslig karaktär. Om det rör sig om säkerhetsskyddsklassificerade uppgifter gäller särskilda bestämmelser enligt säkerhetsskyddslagen (2018:585).

[4] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s. 16–17

Innan utkontraktering eller samordning kan ske behöver avtal eller överenskommelser upprättas som bl.a. reglerar mottagarens hantering av de utlämnade uppgifterna. Några av de krav som finns på ett avtal mellan myndigheten och tjänsteleverantören är:

- Tydliga bestämmelser om skydd av uppgifterna, inklusive hantering av underleverantörer och kontroll över uppgifterna.
- Åtkomstkontroller, loggning av händelser samt krav på rapportering av säkerhetsincidenter.
- Att det finns avtalsvillkor för avveckling av tjänsten, såsom migrering av uppgifter tillbaka till myndigheten eller till en annan leverantör.
- Avtalsvillkoren får inte frånta den utlämnande myndigheten kontrollen över uppgifterna.
- Att avtalet fastställer mekanismer för att övervaka och verifiera tjänsteleverantörens efterlevnad av avtalet.

Andra avtalsförhållanden mellan parterna som också måste beaktas är sådana avtalsvillkor som riskerar att frånta den utlämnande myndigheten kontrollen över uppgifterna.

Som en del i avtal eller överenskommelser behövs det även beskrivas hur man verifierar att tjänsteleverantören och dess personal omfattas av lagstadgad eller avtalsreglerad tystnadsplikt för att skydda de utlämnade uppgifterna. Det bör också beaktas vilka åtgärder som uppgiftsmottagaren vidtar för att skydda uppgifterna och om denne omfattas av en lag- eller avtalsreglerad tystnadsplikt.

Den myndighet som utkontrakterar IT-drift behöver beakta var uppgifterna kommer att hanteras och lagras geografiskt, eftersom detta kan påverka skyddet av uppgifterna och medföra olika juridiska konsekvenser. Detta gäller även för eventuella underleverantörer som potentiellt kan få tillgång till uppgifterna.

3.2 Relevanta säkerhetsfunktioner hos Microsoft

Det är den myndigheten som utkontrakterar sin drift som behöver kvantifiera vad som är tillräckligt säkert. Myndigheten behöver därför granska den sekretessbelagda informationen i förhållande till de säkerhetsåtgärder som kund och leverantör vidtar för att skydda informationen. Nedan beskrivs viss säkerhetsfunktionalitet hos Microsoft som är relevant för rapporten.

Microsoft EU Data Boundary

Microsoft EU Data Boundary är en geografisk avgränsning som kunder kan välja för att begränsa behandling av data till att ske inom EU.

Microsoft Sovereignity

Microsoft Sovereignity är ett ramverk som kan användas för att styra var data behandlas enligt specifika regler gällande åtkomst, aktivitet och användning.

Defender for Endpoint och Defender for Office
Avancerat skydd mot skadlig kod genom Microsoft Defender for Endpoint (klienter och servrar) och Microsoft Defender for Office 365 (SafeLink/SafeAttachments)

Customer Lockbox
Säkerställer att Microsoft inte kan komma åt innehåll för att utföra tjänsteoperationer utan kunds uttryckliga godkännande. Customer Lockbox involverar kund i godkännandeflödet som Microsoft använder för att säkerställa att endast auktoriserade förfrågningar tillåter åtkomst till dess innehåll.

3.3 Övriga bedömningar

3.3.1 Allmänna handlingar, handlingsoffentlighet och arkivvård

Det är av högsta vikt att en myndighet som ska utkontraktera sin IT-drift utreder följderna av detta i förhållande till Tryckfrihetsförordningen (1949:105) och Arkivlagen (1990:782). En sådan bedömning behöver Umeå kommun göra för varje verktyg/applikation där information hanteras. Bedömningen behöver klargöra ifall informationen utgör allmän handling och hur den då bl.a. ska tas tillvara, gallras och vid begäran om det delge det som allmän handling. Bedömningen behöver också inkludera huruvida Umeå kommuns myndigheter har kapacitet och förmåga att leva upp till ovannämnda krav i lagstiftningen.

3.3.1.1 Tjänst- och diagnostikdata (telemetri)

Tjänst- och diagnostikdata har utifrån GDPR berörts under rubriken *Bedömning av Microsoft i förhållande till artikel 28 GDPR*. Det finns dock andra aspekter kopplat till denna typ av data som är relevant att uppmärksamma. I samband med nyttjandet av vissa produkter från Microsoft så kan dessa inhämta tjänst- och diagnostikdata från Umeå kommun beroende på hur dessa tjänster är uppsatta eller vad de har för standardinställningar. Det är därför av vikt att Umeå kommun i första hand inhämtar information och anvisningar från Microsoft om hur sådan insamling kan stängas av eller konfigureras, eller att man i andra hand utreder överförandet av denna data till Microsoft och huruvida dessa handlingar är att anse som allmänna och hur detta i sådana fall påverkar Umeå kommun utifrån Tryckfrihetsförordningen och Arkivlagen.

3.4 Identifierade risker, riskmitigerande åtgärder och andra påverkansfaktorer

3.4.1 Påverkan ifrån amerikansk lagstiftning

Under stycket *Bedömning av Microsoft i förhållande till artikel 28 GDPR* berörs till stor denna fråga, allt när det gäller eventuell tillgång till data från en amerikansk myndighet. Här bör även poängteras att enbart risken för att ett tredjeland får tillgång till personuppgifter anses inte motsvara en överföring av uppgifter i den mening som

avses i artikel 46 i Dataskyddsförordningen, om det inte har visats att personuppgifter har överförts till eller gjorts tillgängliga för en mottagare som är etablerad i ett tredjeland. Med andra ord kan risken för ett åsidosättande av artikel 46 inte likställas med ett direkt åsidosättande av bestämmelsen.[5] Däremot så är risken svår att kvantifiera för myndigheter som vill utkontraktera IT-drift till Microsoft, men den bör likväl inte ignoreras. Den bör snarare vägas samman med andra perspektiv som är relevanta utifrån myndighetens helhetsperspektiv när den överväger att utkontraktera sin IT-drift till Microsoft. Risken för otillåtet utlämnande till amerikanska underrättelsemyndigheter och brottsutredande myndigheter kan även med hjälp utav administrativa och organisatoriska åtgärder åtgärdas. Utöver detta så har Microsoft själva varit väldigt tydliga med att de kommer ”*använda alla lagliga medel för att bestrida ordern om utlämnande baserat på rättsliga brister enligt den begärande partens lagar eller eventuella relevanta lagkonflikter med tillämplig lag i EU eller tillämplig medlemsstat*”.[6]

3.4.2 Data Privacy Framework förklaras ogiltigt

Så som rättsläget nu ser ut, så är det Data Privacy Framework som till stod del ligger till grund för att överföringen av personuppgifter till Microsoft och med andra ord USA som land. Överföringen av personuppgifter mellan EU och USA har under tiden som GDPR varit lagstiftning varit en omdebatterad fråga, med utgångspunkt i huruvida USA har tillräckliga skyddsåtgärder för EU-medborgares personuppgifter, och ifall den amerikanska övervakningslagstiftningen kan anses vara i linje med GDPR.

För tillfället är svaret på den frågan JA, vilket både EDPB och IMY som instanser har yttrat sig om. Huruvida denna rättsliga förutsättning kan komma att förändras i framtiden är en risk som är svår att kvantifiera. Det är uppenbart att de geo-politiska förändringarna som skett sedan 2025 års start, med hänvisning till framför allt presidentskiftet i USA som händelse, hitintills inte varit gynnande för Data Privacy Frameworks fortsatta existens.

3.4.3 Risk för minskad insyn för medborgare

En risk som till viss del har berörts i tidigare delar är ifall den utkontraktade myndigheten inte utreder i tillräcklig grad hur skyldigheterna i Tryckfrihetsförordningen ska upprätthållas i och med anskaffning av verktyg från

[5] Mål T-354/22 Thomas Bindl v European Commission punkt 135
[6] Bilaga C - Bilaga om ytterligare säkerhetsåtgärder (Dataskyddstillägg för Microsofts produkter och tjänster)

Microsoft. I de fall där allmänna handlingar förvaras eller upprättas i ett Microsoft-verktyg så har myndigheten skyldigheter i förhållande till Tryckfrihetsförordningen, och behöver se till att dess anställda har tillräckligt med kunskap för att se till att denna lag efterföljs. Denna risk har dock uppenbara riskåtgärder knutna till sig, vilka exempelvis skulle kunna vara regelbundna stickkontroller, utbildning för anställda eller andra åtgärder som ökar förståelsen för hur Umeå kommun är skyldiga att se till att allmänna handlingar kan bli offentliga. Samma risker och riskåtgärder gäller för informationen i ett Microsoft-verktyg i förhållande till Arkivlagen. Allmänna handlingar som förvaras eller upprättas i ett Microsoft-verktyg måste gallras i enlighet med lagstiftningen.

3.5 Förvaltning

Kopplat till Umeå kommuns Microsoft-verktyg är det av vikt att se över förvaltningen av dessa verktyg. Det har historiskt visat sig vara av vikt att ha processer för hur man hanterar verktyg som förändras med tiden, både när det gäller de funktionella, eller förändringar som endast rör verktygens gränssnitt.

Verktyg från Microsoft kräver att IT-verksamheten är proaktiva och justerar rutiner och regelverk för att optimera användningen av verktygen, men också att man agerar på förändringar som rör alltifrån kostnader till säkerhet i tjänsterna.

Umeå kommun behöver på sikt etablera strategier för större förändringar i Microsofts verktyg, men även strategier för att vid behov kunna lämna dem, en så kallad exitstrategi. Det är även viktigt att Umeå kommun i sitt ordinarie kontinuitetsarbete har strategier utifrån eventuella beroenden av Microsofts verktyg, och hur man vid störningar eller dylikt, har alternativa arbetssätt/rutiner när dessa verktyg inte är tillgängliga.

3.6 Slutsatser kring utkontraktering av IT-drift till Microsoft

3.6.1 Slutsatser

Den här rapporten görs i ljuset av artikel 28 GDPR och OSL:s 10:2 a paragraf. I rapporten så har dessa lagrum beskrivits i detalj, och i förhållande till de beskrivningarna kommer här ett par slutsatser.

I förhållande till GDPR och artikel 28 i synnerhet så bör Microsofts DPA anses motsvara de uppsatta kraven som personuppgiftsbiträdet både ska vidta, men också kunna redovisa för hur man vidtar kraven. Övriga krav, eller risker, i bruten lagefterlevnad genom eventuellt domstolsbegäran om kunddata har bedömts både utav svenska tillsynsmyndigheten (Integritetskyddsmyndigheten) och den europeiska dataskyddsstyrelsen (EDPB). Dessa menar båda på att leverantörer som finns med

Data Privacy Framework List är att anses som leverantörer som uppfyller GDPR. Detta resonemang förstärks även utav Bindl-domen (Mål T-354/22) som hänvisas till ovan. Där är Tribunalen tydlig i att enbart risken för att ett tredjeland får tillgång till personuppgifter anses inte motsvara en överföring av uppgifter i den mening som avses i artikel 46 i GDPR. Det är dock självfallet viktigt att man som myndighet framgent bevakar frågan, för att dessa förutsättningar inte ändras, och att behandlingen inte längre kan anses vara laglig.

I förhållande till OSL:s 10:2 a paragraf så är rapporten begränsad till vilka slutsatser som kan göras. Microsoft har flertalet verktyg med olika grundkonfiguration. Det är således viktigt att man som kund ser över varje enskilt verktyg så att det är konfigurerat på ett sådant sätt att Microsoft endast kan anses tekniskt bearbeta och lagra informationen, för att paragrafen ska vara tillämplig.

Det är den utkontrakterade myndigheten som själva måste fatta beslut kring den vidtagna säkerheten för sekretessen som leverantören ska hantera. Det innebär att Umeå kommun kommer behöva se till vilken information (och eventuell sekretess) som hanteras i olika verktyg och bedöma den vidtagna säkerheten i verktyget. Det ska alltså understrykas att Umeå kommuns dokumentation och ställningstagande är grundbulten för att utkontrakteringen av IT-driften ska kunna anses vara laglig. Det är således sannolikt att Umeå kommun kommer komma fram till bedömningen att viss sekretess i vissa Microsoft verktyg är lagenlig, medan annan sekretess, som dess myndigheter har i uppdrag att hantera, anses falla utanför tolkningsutrymmet i OSL:s 10:2 a paragraf.

3.6.2 Leveransen i Del 1 och fortsättning

I rapporten så har nu de juridiska förutsättningarna för utkontraktering av drift till Microsoft analyserats. Det är dock viktigt att understryka att denna bedömning inte enbart är juridisk och därmed heller inte kan påstås vara fullständig utan kompletterande bitar från myndigheten som ska utkontraktera sin drift. Denna rapport, enligt ovannämnda slutsatser, behöver kompletteras med tekniska och organisatoriska säkerhetsåtgärder utifrån både OSL och GDPR, som kan motivera användande av Microsoft som leverantör. För denna dokumentation så har även material för juridisk bedömning bifogats (Bilaga 1 och 2). Dessa lathundar ger ett stöd för myndigheten som vill utkontraktera (eller samordna) sin drift, oavsett om det gäller en amerikansk molnleverantör eller inte. Lathundarna är ett arbetsmaterial som Umeå kommun tar över, de är inte fullständiga utifrån all lagstiftning som kan tänkas behöva beaktas, utan likt denna rapport så inriktar den sig på GDPR och 10:2 a i OSL.

Vidare arbete behöver precisera konfigurationer och eventuella säkerhetsbrister och/eller lösningar i Umeå kommuns enskilda Microsoft-verktyg som skulle begränsa användande av information i tjänsterna utifrån informationsklassning eller lagstiftning.

I det arbetet behöver även riskanalyser göras utifrån informations-, och IT-säkerhetsperspektiv, för att i djupare detalj bedöma om befintliga tekniska säkerhetsåtgärder och befintliga administrativa rutiner/regelverk för de enskilda Microsoft-verktygen är tillräckliga eller om de behövs kompletteras.

Det är slutligen återigen viktigt att poängtera att rättsområdet är i konstant förändring, och Umeå kommun behöver kontinuerligt bevaka relevanta rättsliga förändringar, och i viss mån även geo-politiska sådana, som kan påverka förutsättningarna för laglighet hos vald leverantör. Umeå kommun behöver även bevaka förändringar i tjänst eller funktion hos Microsoft som påverkar exempelvis diagnostikdata, attribut och tjänstdata i informationsflödet eller annat relevant.

BILAGA 1 - Lathund bedömning utifrån GDPR och OSL

1.1 Lathund bedömning utifrån GDPR

För att säkerställa lagefterlevnad i enlighet med Dataskyddförordningen bör följande aspekter beaktas.

1.1.1 Överföringsmekanismer

Under vissa förutsättningar är det tillåtet att överföra personuppgifter utanför EU/EES. Dessa förutsättningar kallas för överföringsmekanismer.

Personuppgifterna i personuppgiftsbehandlingen får överföras utanför EU/EES därför att:

- ❑ Landet dit personuppgifter kommer att överföras har ett beslut från EU-kommissionen om att landet säkerställer så kallad adekvat skyddsnivå
- ❑ Landet dit personuppgifter kommer att överföras har ett beslut från EU-kommissionen om att landet säkerställer så kallad adekvat skyddsnivå och om deras nationella lagstiftning för skydd av personuppgifter inom privat sektor är tillämplig på personuppgiftsbehandlingen (Kanada).
- ❑ Landet dit personuppgifter kommer att överföras har ett beslut från EU-kommissionen om att landet säkerställer så kallad adekvat skyddsnivå och finns med på Data Framework Privacy List (USA).
- ❑ Det har vidtagits skyddsåtgärder, i form av bindande företagsbestämmelser (så kallade Binding Corporate Rules, BCR) eller standardavtalsklausuler (så kallade Standard Contractual Clauses, SCC).

1.1.2 Tekniska och organisatoriska åtgärder

Flera skyldigheter enligt dataskyddsförordningen ska uppfyllas genom att implementera lämpliga tekniska och organisatoriska åtgärder för att uppnå syftet med skyldigheten.

Tekniska åtgärder som är vidtagna

- ❑ Autentisering
- ❑ Kryptering (specificera nyckelhantering)
- ❑ Pseudonymisering
- ❑ Behörighetsstyrning
- ❑ Kontroll av åtkomst, loggranskning, loggkontroll
- ❑ Nätverkssegmentering
- ❑ Fysisk säkerhet

- ❑ Driftssäkerhet (så som uppdatering, patchning, och härdning av system)
- ❑ Säkerhet för lagrade personuppgifter
- ❑ Kommunikationssäkerhet
- ❑ Säkerhetskopiering
- ❑ Skydd mot skadlig kod
- ❑ Övrig teknisk åtgärd _____

Organisatoriska åtgärder som är vidtagna

- ❑ Har identifierat om en konsekvensbedömning enligt artikel 35 behöver utföras
- ❑ Styrdokument, _____
- ❑ Stärkta processer, _____
- ❑ Rutiner, _____
- ❑ Metoder, _____
- ❑ Hot-, risk- och sårbarhetsanalyser
- ❑ Riskbedömningar, konsekvensbedömningar, lämplighetsbedömningar
- ❑ Kontroll och avstämning (av att åtgärderna implementerats korrekt)
- ❑ Revision och uppföljning/utvärdering
- ❑ Incidenthantering
- ❑ Kontinuitetsplanering

1.2 Avtalsförhållanden utifrån GDPR

Enligt dataskyddsförordningen ska personuppgiftsansvariga och personuppgiftsbiträden reglera sina relationer genom ett skriftligt avtal (eller annan rättsakt).

De personuppgiftsansvariga får endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att skyldigheterna i GDPR kommer att uppfyllas och att de registrerades rättigheter skyddas.

Personuppgiftsbiträdet garanterar efterlevnad av lagstiftning genom

- ❑ Lokal avtalsmall används
- ❑ Annan typ av avtal _____

Avtalet mellan personuppgiftsansvarig och personuppgiftsbiträde reglerar

- ❑ Att behandling endast får ske enligt dokumenterade instruktioner från den personuppgiftsansvariga
- ❑ Försäkran om konfidentialitet eller lagstadgad tystnadsplikt
- ❑ Lämpliga säkerhetsåtgärder
- ❑ Villkor för anlitande av underbiträden
- ❑ Skyldighet att vidta åtgärder för att uppfylla de registrerades rättigheter

- ❑ Att biträde bistår den personuppgiftsansvariga i fråga om dennes skyldigheter enligt artikel 32–36
- ❑ Hur personuppgifter ska hanteras när avtalet upphör
- ❑ Skyldighet att gå med på och bistå vid granskning och inspektioner.
- ❑ Förbud mot att lämna ut uppgifter, enligt lag, utanför EU/EES
- ❑ Förbud mot att lämna ut uppgifter (när tillämpligt, vid exempelvis sekretess)
- ❑ Förbud mot att vidareanvända uppgifterna för egna ändamål

1.3 Lathund bedömning av lämplighet vid extern drift

För att säkerställa en korrekt och säker hantering av uppgifter vid teknisk bearbetning eller lagring enligt 10 kap. 2 a § offentlighets- och sekretesslagen (OSL) bör följande aspekter beaktas

1.3.1 Orsak till extern drift

Kryssa för de alternativ som är tillämpliga

- ❑ Tillräcklig teknisk kompetens eller kapacitet saknas internt. Extern drift behövs för att upprätthålla verksamhetens funktionalitet.
- ❑ Mer kostnadseffektivt än att utveckla och underhålla egna likvärdiga system, gäller särskilt när det gäller avancerad teknik eller specialiserade tjänster.
- ❑ Ger tillgång till expertis och teknik som inte finns internt, vilket kan vara avgörande för att möta specifika verksamhetsbehov.
- ❑ Annat

  _____

1.3.2 Extern drift, omfattning

Den påtänkta externa driften ska vara avgränsad till hantering av uppgifter vid teknisk bearbetning eller lagring i enlighet med 10 kap. 2 a § OSL.

Checklista

- ❑ Utförandet av den externa driften begränsas till drifts- och säkerhetsrelaterad information, såsom användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar, samt andra uppgifter i läsbar form.
- ❑ Tjänsteleverantören har inte något självständigt ansvar för innehållet i uppgifterna eller fattar beslut baserat på dem.

1.3.3 Är uppgifterna av särskilt känsligt slag?

Identifiera om uppgifterna är av särskilt känsligt slag, såsom uppgifter av synnerlig betydelse för rikets säkerhet eller andra sekretessbelagda uppgifter. Även om en uppgift inte direkt faller under kategorin “synnerlig betydelse för rikets säkerhet”, kan andra faktorer göra det olämpligt att lämna ut den för teknisk bearbetning eller lagring.

Uppgifterna som är aktuella för tekniska bearbetningen eller lagringen är

- ❑ Uppgifter av synnerlig betydelse för rikets säkerhet
- ❑ Sekretessbelagda uppgifter utan “synnerlig betydelse för rikets säkerhet”, men av särskilt känsligt slag
- ❑ Uppgifterna är inte av känslig känsligt slag

En särskild bedömning behöver även göras ifall det rör sig om samlokalisering

- ❑ Informationen kommer inte att samlokalisera med andra kunders information
- ❑ Information kommer att samlokaliseras med andra kunders information och detta är inte olämpligt
- ❑ Information kommer att samlokaliseras med andra kunders information och detta är olämpligt på grund av uppgifternas särskilt känsliga slag

1.3.4 Tjänsteleverantörens status

Myndigheten behöver precisera om det rör sig om utkontraktering av IT-drift eller samordning av IT-drift och kunna motivera valet att använda sig av endera.

Den tilltänkta externa driften avser Utkontraktering av IT-drift

- ❑ Tjänsteleverantören är en enskild aktör, såsom ett privat företag, som har i uppdrag att tekniskt bearbeta eller lagra uppgifter för myndighetens räkning.
- ❑ Leverantörens erfarenhet och kompetens inom IT-drift, inklusive tidigare uppdrag för offentliga eller privata organisationer är tillfredställande
- ❑ Leverantören har nödvändiga certifieringar och följer relevanta standarder för IT-säkerhet och dataskydd.

Den tilltänkta externa driften avser Samordning av IT-drift

- ❑ Myndigheten _____ som ansvarar för den samordnade IT-driften (tjänsteleverantören) har kapacitet att hantera ytterligare uppgifter.
- ❑ Har infrastruktur och resurser för att säkerställa att de kan möta de deltagande myndigheternas behov.

- ❑ Har erfarenheter av samordnad IT-drift och identifiera eventuella utmaningar eller framgångsfaktorer.

1.3.5 Hantera sekretess och tystnadsplikt

Myndigheten behöver verifiera att tjänsteleverantören och dess personal omfattas av lagstadgad eller avtalsreglerad tystnadsplikt för att skydda de utlämnade uppgifterna.

Tjänsteleverantören omfattas av:

- ❑ Lagstadgad tystnadsplikt
- ❑ Avtalsreglerad tystnadsplikt

För både utkontraktering och/eller samordning:

- ❑ Avtal innehåller tydliga bestämmelser om tystnadsplikt och konsekvenser vid brott mot denna.
- ❑ Anställda hos leverantören, inklusive underleverantörer, har undertecknat sekretessavtal och genomgått relevant utbildning i hantering av känslig information.
- ❑ Tjänsteleverantören har rutiner för att förhindra obehörig åtkomst till uppgifterna, inklusive åtkomstkontroller, loggning och regelbundna säkerhetsrevisioner.
- ❑ Det finns mekanismer för att hantera säkerhetsincidenter.
- ❑ Säkerhetsincidenter rapporteras till berörda parter i enlighet med gällande lagstiftning.

1.3.6 Geografisk placering och följdeffekter av denna

Beakta var uppgifterna kommer att hanteras och lagras geografiskt, eftersom detta kan påverka skyddet av uppgifterna och medföra olika juridiska konsekvenser.

Geografisk placering för datalagring:

- ❑ Datalagring kan begränsas till Sverige
- ❑ Datalagring kan begränsas till EU
- ❑ Datalagring begränsas i dagsläget till _____

Säte för leverantören:

- ❑ Sverige
- ❑ Inom EU/EES
- ❑ Utanför EU/EES _____

Påverkas leverantören av extraterritoriell lagstiftning som kan få effekter för personuppgiftsbehandlingen:

- ❑ Nej
- ❑ Ja _____

1.4 Avtalsförhållanden

Granska avtalet mellan myndigheten och tjänsteleverantören för att säkerställa att det:

- ❑ Innehåller tydliga bestämmelser om skydd av uppgifterna, inklusive hantering av underleverantörer och kontroll över uppgifterna.
- ❑ Reglerar åtkomstkontroller, loggning av händelser samt krav på rapportering av säkerhetsincidenter.
- ❑ Att det finns avtalsvillkor för avveckling av tjänsten, såsom migrering av uppgifter tillbaka till myndigheten eller till en annan leverantör.
- ❑ Säkerställ att avtalsvillkoren inte fråntar den utlämnande myndigheten kontrollen över uppgifterna.
- ❑ Avtalet fastställ mekanismer för att övervaka och verifiera tjänsteleverantörens efterlevnad av avtalet.

BILAGA 2 - Samlad bedömning – utifrån GDPR och OSL

1.1 Dataskyddsförordningen

Innan personuppgiftsbehandlingen påbörjas så ska myndigheten se till att behandlingen inte strider mot Dataskyddsförordningen, och ha dokumenterat hur personuppgiftsbehandlingen är inom ramarna för lagstiftningen.

Vi som har utfört bedömningen har i rollen som uppgiftsägare noggrant övervägt alla relevanta faktorer, inklusive personuppgiftsbehandlingens art, potentiella risker utifrån enskildas grundläggande rättigheter och friheter, genom att

- ❑ Konstatera personuppgiftsbehandlingens nödvändighet
- ❑ Sett till så att behandlingens personuppgiftsflöde är lagligt
- ❑ Myndigheten har vidtagit tekniska och organisatoriska åtgärder för att säkra en säker och laglig behandling
- ❑ Har skriftligt reglerat avtalsförhållandet för personuppgiftsbehandlingen mellan sig själv, personuppgiftsansvarig, och leverantören, personuppgiftsbiträdet

Framtida efterlevnad uppnås genom att

- Genomföra kontroller och revision var _____ för att säkerställa att tjänsteleverantören följer avtalsvillkor och lagstadgade krav.
- Ansvarig _____, kontinuerligt utvärderar om det finns nya risker eller krav som påverkar personuppgiftsbehandlingen.

1.2 Offentlighets- och sekretesslagen

Innan uppgifterna lämnas ut ska myndigheten göra en allsidig prövning av alla relevanta omständigheter för att avgöra om det är olämpligt att lämna ut uppgifterna. Dokumentera alla bedömningar som gjorts för att motivera utlämnande, inklusive identifierade risker och motåtgärder.

Vi som har utfört bedömningen har i rollen som uppgiftsägare noggrant övervägt alla relevanta faktorer, inklusive uppgifternas art, potentiella risker vid utlämnande och de säkerhetsåtgärder som tjänsteleverantören har implementerat. Säkerställ att dokumentationen tydligt visar hur sekretess- och säkerhetskrav uppfyllts.

- ❑ Det går att stödja sig på OSL:s lagrum 10.2 för teknisk bearbetning och lagring

Extern drift för uppgifterna är

- ❑ Lämpligt utifrån uppgifternas art och känslighet, bedömningen av tjänsteleverantörens säkerhetsåtgärder och rutiner samt möjliga risker med underleverantörer och geografisk hantering
- ❑

Framtida efterlevnad uppnås genom att

- Genomföra kontroller och revision var _____ för att säkerställa att tjänsteleverantören följer avtalsvillkor och lagstadgade krav.
- Ansvarig _____, kontinuerligt utvärderar om det finns nya risker eller krav som påverkar den tekniska bearbetningen eller lagringen.

Utredning om Microsoft som leverantör

Ärende: Riskbedömning och fortsatt användning av Microsoft som leverantör

Bakgrund: Underlag till beslut i Tekniska nämnden, TN-2026/00081

Bakgrund

Umeå kommun har under lång tid använt Microsoft 365 som gemensam arbetsplatsplattform. Samtidigt har rättsläget kring amerikanska molntjänster skärpts, vilket skapat osäkerhet kring juridiska förutsättningar, särskilt kopplat till behandling av personuppgifter enligt dataskyddsförordningen (GDPR) och för hantering av sekretessbelagda uppgifter enligt offentlighets- och sekretesslagen (OSL). Kommunen saknade en uppdaterad helhetsbedömning av Microsoft (MS) som leverantör, vilket har hämmat utvecklingstakten och försvårat verksamheternas arbete med digitalisering, data och AI. Mot denna bakgrund initierades en samlad och strukturerad genomlysning för att gå från ovisshet till ett aktivt och medvetet vägval.

Arbetsgång

Arbetet har genomförts med en bred kompetensbas bestående av externt upphandlad juridisk expertis samt kommunintern kompetens inom juridik, informationssäkerhet och Digital omställning och IT. Bedömningen har utgått från två perspektiv, ett juridiskt och ett tekniskt, med fokus på de tjänster kommunen använder.

Det juridiska arbetet har haft två delar:

- **Juridisk analys:** Granskning av Microsoft som leverantör utifrån GDPR (särskilt artikel 28 om personuppgiftsbiträdesavtal), tredjelandsöverföringar samt OSL, inklusive tillämpningen av 10 kap. 2 a § OSL om teknisk bearbetning och lagring.
- **Dialog och beredning:** Dataskyddsombudets frågor och invändningar har utretts och hanterats genom löpande dialog med Microsoft, inklusive digitala möten och en fördjupad genomgång på plats i Umeå. Avtalsvillkor, tekniska skyddsåtgärder och återstående tolkningsfrågor har analyserats.

Juridiska förutsättningar

Offentlighets- och sekretesslagen

Att lämna ut sekretessbelagda uppgifter till en molntjänstleverantör förutsätter en sekretessbrytande bestämmelse. 10 kap. 2 a § OSL är en sekretessbrytande bestämmelse som möjliggör för myndigheter att utkontraktera sin IT-drift. Det förutsätter att:

1. Att uppgiften lämnas ut endast för teknisk bearbetning eller teknisk lagring,

2. Att tjänsteleverantören endast hanterar uppgifterna för den utlämnande myndighetens räkning, och

3. Att det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut.

Microsoft har en mängd verktyg/tjänster exempelvis Teams, Outlook, Copilot som har olika grundkonfiguration. När det gäller punkterna 1 och 2 behöver Umeå kommun se över varje enskilt verktyg som MS erbjuder så att verktyget är konfigurerat på sådant sätt att MS endast kan anses teknisk bearbeta och lagra informationen på det sätt som beskrivs i punkterna. Detta arbete har påbörjats och omhändertas genom tekniska och organisatoriska åtgärder för varje tjänst.

När det gäller punkt 3 behöver Umeå kommun för varje tjänst bedöma vilken typ av sekretessbelagda uppgifter det är fråga om samt på vilket sätt uppgifterna ska hanteras (exempelvis muntligt vid Teamsmöten men inte lagring i Teams). I det här sammanhanget är det viktigt att förklara vad US CLOUD Act (Cloud Act) är då MS är baserade i USA och lyder under amerikansk lagstiftning. Cloud Act är en amerikansk lag som gör det möjligt för amerikanska myndigheter att begära ut data som lagras utanför USA:s territorium från tjänsteleverantörer som omfattas av USA:s jurisdiktion. Syftet med lagen är att underlätta utredningsarbetet för brottsbekämpande myndigheter. För att en amerikansk myndighet ska kunna begära ut uppgifter från en tjänsteleverantör med stöd av CLOUD Act krävs vanligtvis ett beslut av en amerikansk domstol. Domstolen gör då en bedömning om det är sannolikt att ett specifikt brott har ägt rum eller kommer att göra det. CLOUD Act öppnar även upp för att en myndighet i vissa situationer kan ställa mer ospecifika krav. Därutöver finns det möjligheter för myndigheter att beordra tjänsteleverantörer att lämna ut information utan domstolsbeslut. Tjänsteleverantören måste då lämna ut denna data oavsett om den lagras i eller utanför USA och oavsett vad avtal säger.

Dataskyddsförordningen (GDPR)

MS behandlar företrädesvis personuppgifter och annan information för Umeå kommuns räkning i Sverige. I vissa fall behandlas personuppgifter i EU/EES. Behandlingen är därmed i överensstämmelse med GDPR ur den aspekten.

Cloud Act kan dock innebära att MS tvingas lämna ut personuppgifter till amerikanska myndigheter och därmed överförs personuppgifter till USA.

Enligt ATEAS rapport och Integritetsskyddsmyndigheten har USA i nuläget en adekvat skyddsnivå för personuppgifter vilket gör att sådana uppgifter får överföras till USA under vissa förutsättningar. Det så kallade adekvansbeslutet som är beslutat av EU-kommissionen innebär att kommissionen har bedömt att USA säkerställer en tillräckligt hög skyddsnivå och att det därmed är tillåtet att överföra personuppgifter till USA, utan att vidta lämpliga skyddsåtgärder enligt art 46 GDPR (till exempel standardavtalsklausuler eller bindande företagsbestämmelser) förutsatt att den mottagande organisationen omfattas av EU–U.S. Data Privacy Framework (DPF). EU-kommissionen har genom sitt beslut gjort en helhetsbedömning av amerikanska lagar, internationella åtaganden, registrerades möjligheter att få rättslig prövning, innehållet i ramverket osv. med slutsatsen att skyddsnivån sammantaget är tillräcklig. Av lista på Integritetsskyddmyndighetens hemsida framgår att MS är en sådan organisation som omfattas av DPF.

Samlad bedömning och rekommendation

Bedömningen är att förutsättningarna för att kunna ta ställning till om MS fortsatt kan anlitas som leverantör har utretts i tillräcklig omfattning. Utifrån en samlad avvägning av verksamhetsbehov, risk och rättsläge är rekommendationen att fortsätta nyttja Microsoft som leverantör. Dataskyddsombudet anser att det inte är förenligt med GDPR och OSL att anlita MS som personuppgiftsbiträde.

Den juridiska utmaningen är konflikten mellan amerikansk lagstiftning och europeiskt dataskydd samt konsekvenserna i förhållande till OSL och sekretess.

Om och vilken typ av sekretessbelagd information som kan hanteras i MS tjänster behöver bedömas utifrån konfigurationen av tjänst och det sätt på vilken informationen delas. I bedömningen måste också vägas in den omständigheten att uppgifterna kan komma att behöva lämnas ut till amerikanska myndigheter. Som ovan sagts behandlar MS personuppgifter inom EU/EES. Om det skulle bli aktuellt att överföra personuppgifter till amerikanska myndigheter utifrån Cloud Act är det i nuläget förenligt med GDPR utifrån adekvansbeslutet och att MS är en sådan organisation som omfattas av DPF.

Microsoft möjliggör verksamheternas behov av datadriven verksamhetsutveckling, teknikstöd för en modern och säker digital arbetsplats, effektiv samverkan och informationsdelning samt förutsättningar för att arbeta strukturerat med dataanalys, automatisering och AI-stöd i verksamhetsprocesser. En utfasning av Microsoft i nuläget bedöms medföra oproportionerligt stora negativa konsekvenser för verksamhet, ekonomi och utvecklingsförmåga. Externa beräkningar visar att en utfasning skulle ta ett flertal år. Kommunen skulle lämna marknadsstandard och tappa innovationstakt. Det skulle också innebära mycket omfattande kostnader och sänkt effektivitet.

Riskreducerande åtgärder behöver genomförs och följas upp löpande. Det handlar om att rätt data finns på rätt plats med skarpare sortering av skyddsvärddata. Det handlar om skydd i form av kryptering och tekniska spärrar. Det handlar om kontroll i form av ökad övervakning och spårbarhet i systemen samt att kontinuerligt utvärdera rättsläge, tekniskt läge och omvärldsläge. Den juridiska bedömningen behöver följas och alternativ till MS inom Sverige/EU/EES behöver fortsatt omvärldsbevakas.

Hannes Fries, verksamhetsutvecklare DoIT

Mattias Wallmark, verksamhetschef DoIT

Umeå kommun
Tekniska nämnden

Protokollsutdrag
2026-02-19

§ 17
Diarienr: TN-2026/00081

Beslut av riskbedömning och fortsatt användning av Microsoft

Beslut

Tekniska nämnden beslutar

att innan beslut i Tekniska nämnden, skicka underlaget till KS för yttrande.

Ärendebeskrivning

Umeå kommun har sedan många år Microsofts molntjänst 365 för samtliga anställda. Sedan införandet har regelverk och lagar för amerikanska tjänster och leverantörer skärpts. Kommunen har inte haft någon uppdaterad helhetsbedömning av Microsoft och deras tjänster vilket hämmat utvecklingstakten och skapat en osäkerhet i kommunens verksamheter.

I syfte att lyfta Umeå kommuns användning av Microsoft från ovisshet till ett aktivt vägval med en tydlig plan, har det genomförts en omfattande juridisk bedömning av Microsoft som leverantör. Bedömningen har gjorts utifrån granskning mot GDPR och OSL(Offentlighets- och sekretesslagen) där vi haft stöd av externt upphandlat expertis tillsammans med kommunintern kompetens inom juridik, informationssäkerhet samt Digital omställning och IT. För specifika frågor har det också skett direkt dialog med Microsoft.

Den samlade bedömningen är att vi utrett och vidtagit de åtgärder som är möjliga i proportion till nyttan för kommunen. Vidare har det konstaterats att en utfasning av Microsoft i nuläget skulle få oproportionerligt stora negativa konsekvenser för kommunens verksamheter så väl som ekonomi. Därmed är slutsatsen att rekommendera Tekniska nämnden att besluta att fortsätta nyttja Microsoft som strategisk partner, under förutsättning att riskreducerande åtgärder genomförs, bland annat:

- **Informationsklassning:** Rätt data på rätt plats med skarpare sortering av skyddsvärd data, exempelvis med känslighetsetiketter för att förenkla administration av klassningen. Utifrån bedömning av respektive tjänst i Microsoft 365 kan information upp till informationsklass gul och röd lagras och behandlas.
- **Skydd:** Fortsätta införa kryptering och tekniska spärrar
- **Kontroll:** Ökad övervakning och spårbarhet i systemen
- **Utvärdering:** Kontinuerlig utvärdering av rättsläget, teknisk utveckling samt omvärldsläge

Det skall löpande genomföras omvärldsbevakning för alternativa leverantörer och tjänster samt löpande riskbedömning av Microsoft för att identifiera eventuellt behov att ompröva beslutet.

Förslag på sammanträdet
Christina Bernhardsson (S) yrkar på att beslutet ska bli

att innan beslut i Tekniska nämnden, skicka underlaget till KS för yttrande.

Tekniska nämndens beslutsordning
Ordföranden frågar om nämnden kan besluta i enlighet med Christina Bernhardssons (S) yrkande och konstaterar att så är fallet.

Originalförslag i tjänsteskrivelsen:
att Umeå kommun kan fortsätta nyttja Microsoft som strategisk partner under förutsättning att riskreducerande åtgärder genomförs löpande.

att nämnden årligen i december följer upp den juridiska bedömningen,

att omvärldsbevaka alternativ till amerikanska leverantörer och tjänster till förmån för alternativ inom Sverige eller EU/EES.

Beslutsunderlag

Checklista för handläggning av ärenden inför politiska beslut bedöms inte tillämpbar.

Beredningsansvariga

Mattias Wallmark, DoIT
Hannes Fries, DoIT

Umeå kommun
Tekniska nämnden

Protokollsutdrag
2026-02-19

Beslutet ska skickas till
KSdiarium
Maria Törnblom
Dan Gideonsson
Mattias Wallmark
Hannes Fries

Justerares sign:

Utdraget bestyrks:

UMEÅ KOMMUN

Tjänsteskrivelse
2026-04-01

Kommunstyrelsens
näringslivs- och arbetsutskott

Diarienr: KS-2026/00246

Beslut av riskbedömning och fortsatt användning av Microsoft

Förslag till beslut
Kommunstyrelsen beslutar

Kommunstyrelsen kan ej, utifrån det av tekniska nämnden tillhandahållna underlaget, yttra sig om den fortsatta användningen av Microsoft är laglig och säker. Tekniska nämnden behöver utreda och dokumentera frågan ytterligare.

Ärendebeskrivning
Tekniska nämnden har i ärende TN-2026/00081 önskat kommunstyrelsens yttrande över riskbedömning och fortsatt användning av Microsofts tjänster.

Dataskydd
Då det saknas tillräcklig utredning för att det ska gå att göra en korrekt bedömning har jag som tekniska nämndens dataskyddsombud rekommenderat nämnden att inte går vidare med aktuellt beslutsförslag.

Det pågår ett utredningsarbete på DoIT och jag har rekommenderat att frågan utreds färdigt och slutsatser och bedömningar dokumenteras. Denna dokumentation kan sedan ligga till grund för en bedömning och beslut gällande frågan om Microsoft kan anlitas som personuppgiftsbiträde och vilka ev. åtgärder som behöver vidtas för att tekniska nämnden ska kunna anlita Microsoft som personuppgiftsbiträde (alltså om Microsoft kan anses uppfylla kraven i artikel 28 GDPR, eller inte).

Av den anledningen rekommenderas kommunstyrelsen att rekommendera tekniska nämnden att utreda färdigt frågan om lagligheten av att använda Microsoft som personuppgiftsbiträde. I dagsläget, på befintligt underlag, bedöms behandlingen inte vara förenligt med GDPR med risker för både enskilda så väl som nämnderna i kommunen. (Se bilaga 1 för mer information och rekommendationen till tekniska nämnden.)

Tjänsteskrivelse

Dnr: KS-2026/00246

Juridik

Det juridiska arbete som utredningen hänvisat till utgörs av 2 delar - GDPR samt Offentlighets- och sekretesslagen (OSL). Vad gäller de juridiska bedömningar som avser GDPR hänvisas till dataskyddsombudets utlåtanden. Angående OSL så rör utredningen i huvudsak tillämpningen av 10:2a OSL, därav kommer mina synpunkter och slutsatser att ansluta till samma lagrum.

Lagtext
”Sekretess hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut.”

Lagregleringen innehåller en sekretessbrytande bestämmelse som möjliggör för en myndighet, som behandlar uppgifter som omfattas av sekretess, att under vissa omständigheter utkontraktera sin it-drift till en privat tjänsteleverantör eller ansluta sig till en samordnad it-driftslösning.

Den sekretessbrytande bestämmelsen blir bara tillämplig om uppdraget begränsas till att endast avse teknisk bearbetning eller lagring av uppgiften.

Ytterligare en förutsättning för att uppgifter ska få lämnas ut med stöd av den sekretessbrytande bestämmelsen är att det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut.

Teknisk bearbetning/lagring (definieras enligt följande):
Ett uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifter kan exempelvis bestå i att införa, förvalta, utveckla och så småningom avveckla en it-driftstjänst. Under dessa olika faser kan en mängd olika åtgärder behöva vidtas för att upprätthålla den tillgänglighet, funktionalitet och prestanda i tjänsten som har avtalats mellan parterna. Det kan röra sig om förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration med andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Det kan också röra sig om säkerhetstester och andra säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering.
Vid avveckling av en tjänst kan myndighetens uppgifter behöva migreras eller exporteras tillbaka till myndigheten eller till en annan uppdragstagare. Vilka slags åtgärder som kan omfattas av uttrycket teknisk bearbetning

Tjänsteskrivelse
Dnr: KS-2026/00246

eller teknisk lagring kan komma att förändras över tid med anledning av den tekniska utvecklingen (prop. 2022/23:97)

Lämplighetsbedömning
En uppgift får inte lämnas ut om det med hänsyn till omständigheterna är olämpligt. Med detta avses att en myndighet, innan en uppgift lämnas ut, ska pröva om det finns skäl som talar emot ett sådant.

Vad som ska prövas är de omständigheter som har koppling till den utlämnande myndigheten och till uppgiftsmottagaren - liksom de uppgifter som är eller kan bli föremål för utlämnande. Det ska alltså göras en omfattande och noggrann prövning av alla omständigheter som är relevanta i det aktuella ärendet.

Omständigheter att bedöma är exempelvis vilken typ av sekretessbelagda uppgifter det rör sig om (exempelvis personuppgifter?), vilka intressen som ligger till grund för sekretessen och uppgifternas omfattning.

Det bör också beaktas vilka åtgärder som uppgiftsmottagaren vidtar för att skydda uppgifterna och om denne omfattas av en lag- eller avtalsreglerad tystnadsplikt – (jfr Cloud-act).

I sammanhanget kan de i Esams vägledning, Utkontraktering ES2023-06, ingående checklistorna verka vägledande (se bilaga 2).

Informationssäkerhet

Vid bedömning om en molntjänstleverantör kan uppfylla informationssäkerhetsrelaterade krav bör det dessförinnan vara fastställt att informationshanteringen efterlever de juridiska krav som ställs. Innan detta är utrett kan de informationssäkerhetsrelaterade riskerna och kraven inte analyseras och bearbetas på ett korrekt sätt. Om informationshanteringen inte uppfyller lagkrav kan säkerhetsåtgärder vara otillräckliga eller irrelevanta även om de är relevanta ur informationssäkerhetsperspektiv.

Slutsats

Sammanfattningsvis är slutsatsen att det inte går att ta ställning till aktuell fråga (*är det lagligt och säkert för tekniska nämnden att anlita Microsoft som leverantör/personuppgiftsbiträde*) på det material som tekniska nämnden hittills tagit fram och tillhandahållit. Det rekommenderas därför att kommunstyrelsen beslutar att rekommendera tekniska nämnden att

Tjänsteskrivelse

Dnr: KS-2026/00246

utreda frågan om användningen av Microsoft färdigt och dokumentera bedömningarna.

Beslutsunderlag

Tekniska nämndens protokoll 2026-02-19
Bilaga 1 Samrådsyttrande från Dataskyddsombudet med rekommendation gällande tekniska nämndens anlitande av Microsoft som personuppgiftsbiträde
Bilaga 2 Checklista Esams

Beredningsansvariga

Lennart Nilsson, Kommunjurist
Eric Lindström, Dataskyddsombud
Hanna Öberg, Informationssäkerhetssamordnare

Beslutet ska skickas till

Tekniska nämnden

Lennart Nilsson
kommunjurist

UMEÅ KOMMUN

2026-03-31

Samrådsyttrande från dataskyddsombudet med rekommendation gällande Tekniska nämndens anlitande av Microsoft som personuppgiftsbiträde

TN-2026/00081 och KS-2026/00246.

Med anledning av samråd i ärendena TN-2026/00081 och KS-2026/00246 lämnar jag som nämndernas dataskyddsombud i huvudsak följande rekommendationer:

Det rekommenderas att Tekniska nämnden inte går vidare med aktuellt beslutsförslag då frågan ännu inte är tillräckligt utredd och dokumenterad. I stället rekommenderas att frågan utreds färdigt av nämnden och slutsatser och bedömningar dokumenteras. Denna dokumentation kan sedan ligga till grund för en bedömning ifall Microsoft kan anlitas som personuppgiftsbiträde och/eller vilka åtgärder som behöver vidtas för att Tekniska nämnden ska kunna anlita Microsoft som biträde (alltså om Microsoft kan anses uppfylla kraven i artikel 28 GDPR, eller inte).

<u>På Tekniska nämndens befintligt underlag</u> kan nämnden inte anses ha visat att Microsoft kan lämna tillräckliga garantier om att uppfylla GDPR eller att företaget kan garantera att registrerades rättigheter skyddas (artikel 28 och 5.2 GDPR). Frågetecken finns också kring lämplig teknisk och organisatorisk säkerhet (artikel 25 och 32 GDPR). Av den anledningen rekommenderar jag **<u>på Tekniska nämnden befintligt underlag</u>,** att Tekniska nämnden avbryter behandlingen av personuppgifter i Microsofts tjänster. Alternativt att det skyndsamt vidtas effektiva skyddsåtgärder för att förhindra att Microsoft får åtkomst till några personuppgifter. Åtgärderna måste vara sådana att Microsoft inte har, eller kan få, åtkomst till personuppgifter. Kan inga effektiva skyddsåtgärder vidtas är behandlingen oförenlig med GDPR och behöver avbrytas.

En fortsatt behandling av personuppgifter i Microsofts tjänster, enligt det förslag som Tekniska nämnden har att ta ställning till, kan i nuläget innebära skada för enskilda så väl som för nämnderna i kommunen som använder Microsofts tjänster. IMY kan utfärda sanktionsavgift på upp till 10 000 000 kr mot varje nämnd i kommunen eller omedelbart förbjuda behandlingen som sker i tjänsterna. Enskilda har också möjlighet att rikta skadeståndsanspråk mot nämnderna i kommunen, där finns ingen övre beloppsgräns. Frågan om förenligheten med sekretesslagstiftningen är inte utredd och dokumenterad, resultatet av en sådan prövning kan också komma att påverka konsekvensfrågan.

Inledning

Dataskyddsombudet ska informera och ge råd till personuppgiftsansvarig (de kommunala nämnderna) och deras anställda om deras skyldigheter enligt GDPR och andra EU och nationella dataskyddsbestämmelser (art. 39.1a GDPR). Dataskyddsombudet ska övervaka efterlevnaden av GDPR och annan EU och nationell dataskyddslagstiftning och nämndernas strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning (art. 39.1b GDPR).

Tekniska nämnden, Kommunstyrelsen och övriga nämnder är skyldiga att säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter (art. 38.1 GDPR).

Som Tekniska nämndens dataskyddsombud har jag stöttat DoIT i deras pågående utredning av möjligheten för Tekniska nämnden att anlita Microsoft som personuppgiftsbiträde. Dock togs ingen kontakt inför att förslaget till nämndsbeslut skulle tas fram. Av den anledningen hade jag ingen möjlighet att lämna någon rekommendation till Tekniska nämnden inför beslutet.

Här ska tilläggas att i dagsläget finns det, enligt vad som gjorts känt för mig som dataskyddsombud, inte någon färdig dokumenterad utredning av Microsofts möjlighet att kunna anlitas som personuppgiftsbiträde. Det pågår ett arbete på DoIT men det är inte slutfört (refereras ofta till som ”del 1” på DoIT). Inte heller har det skett någon dokumenterad bedömning av om utlämnande av uppgifter till Microsoft är förenligt med reglerna i offentlighets- och sekretesslagen (OSL). Några sådana dokument verkar, utifrån protokollet, inte heller varit del av underlaget till Tekniska nämnden.

Det ska också påtalas att problematiken kring att anlita Microsoft som personuppgiftsbiträde och de medföljande begränsningarna i möjligheten till informationshantering i Microsofts tjänster har varit känd för Tekniska nämnden sedan i vart fall 2019.

Lagstiftning

Inledningsvis ska först noteras att samtliga nämnder i kommunen är bundna av lag. Jmf. 1 kap. 1 § 2 st regeringsformen ”*Den offentliga makten utövas under lagarna*”. Ingen nämnd har rätt att fatta ett beslut som skulle strida mot svensk lag eller EU lagstiftning. **Det finns alltså inget utrymme att göra någon proportionalitetsbedömning gällande ifall Tekniska nämnden ska följa lag, eller inte.**

Dataskyddsförordningen (GDPR) är en EU förordning och gäller som lag i Sverige. GDPR härleds ur europeiska kongestionen för mänskliga rättigheter (art. 8 EKMR rätten till privat- och familjeliv). Europakonventionen för mänskliga rättigheter är också införd som svensk lag (SFS 1994:1219).

Personuppgifter

En personuppgift är all information som direkt eller indirekt kan identifiera en levande människa och som hanteras helt eller delvis automatiserat. Exempel på personuppgifter är personnummer, för- och efternamn, telefonnummer, e-postadresser, fastighetsbeteckningar, IP-nummer, chassinummer, vissa GPS-koordinater, m.m.

Frågan som nu är aktuell omfattar en stor mängd personuppgifter både i typ och antal samt ett stort antal registrerade. Kategorierna av registrerade är i stor omfattning i underläge till personuppgiftsansvariga nämnder. Det rör sig om anställda, elever, barn, brukare, vårdandashavare, tjänsteleverantörer, osv, osv. Många registrerade har inte heller något val gällande ifall de vill att nämnderna ska behandla deras personuppgifter, eller inte.

Enligt kommunens riktlinje för informationssäkerhet ska sekretesskyddade, känsliga eller extra skyddsvärda personuppgifter inte behandlas i Microsofts tjänster då tjänsterna inte bedömts som säkra nog för den typen av information. Så sker också normalt, även om det finns två nämnder som tidigare beslutat om att avvika från denna riktlinje. Individ- och familjenämnden samt Äldrenämnden har beslutat, i strid med dataskyddsombudets rekommendation, att ändå behandla känsliga och sekretesskyddade personuppgifter i Microsofts molntjänster.

Det är alltså i dagsläget frågan om en stor mängd personuppgifter för kategorier av registrerade som ofta är i underläge till de personuppgiftsansvariga nämnderna där det också förekommer känsliga och sekretesskyddade uppgifter.

Personuppgiftsbiträde

För att få anlita ett personuppgiftsbiträde krävs enligt artikel 28.1 i GDPR bl.a. att biträdet ger ”*… tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas*.” Detta kompletteras sedan av art 5.2 i GDPR som stadgar att personuppgiftsansvarig (nämnd) ska kunna visa att kraven i artikel 28 efterlevs. Detta innebär i praktiken att Tekniska nämnden ska kunna ”bevisa” att Microsoft som personuppgiftsbiträde uppfyller ovan angivna krav innan företaget får anlitas som personuppgiftsbiträde. Om biträdet efter anlitande vid något tillfälle inte längre uppfyller dessa krav får det inte längre anlitas. **I dagsläget saknas dokumenterad utredning som visar att Microsoft kan efterleva kraven i artikel 28.1 och Tekniska nämnden kan alltså redan av den anledningen inte anses uppfylla kraven i GDPR (jmf. art 5.2).**

Microsoft som personuppgiftsbiträde

CLOUD Act och tredjelandsöverföringar

Ett av de identifierade problemen med anlitandet av Microsoft (eller annan amerikansk molnleverantör som t.ex. Google, Amazon, Oracle, osv.) som personuppgiftsbiträde är en amerikansk lag som heter CLOUD Act. CLOUD Act ”kortsluter” den normala vägen när uppgifter ska lämnas ut mellan stater. Myndigheter i USA och andra anslutna länder kan använda CLOUD Act för att via domstol begära ut data direkt från Microsoft i stället för att gå via bilaterala överenskommelser. CLOUD Act gäller oavsett var i världen som uppgifterna lagras. Det är alltså inte ett skydd att personuppgifter lagras i Sverige. CLOUD Act innehåller också en möjlighet till s.k. ”gag order” (kallas också för ”protective order”, se punkten 28) som innebär att Microsoft inte alltid får berätta för sina kunder att de tillgodosett en CLOUD Act begäran. Det finns också möjlighet för andra länder att ansluta sig till CLOUD Act, dokumentation och riskbedömning behöver således inte bara ske gällande överföringar till USA utan också övriga anslutna länder (hittills har Australien och Storbritannien anslutit sig).

Den behandling som sker för att uppfylla en CLOUD Act begäran saknar, enligt Europeiska dataskyddsstyrelsens (EDPB) juridiska bedömning av CLOUD Act, rättslig grund. Den granskning av amerikansk lagstiftning som skett av EU kommissionen som det hänvisas till i ”*Utredning om Microsoft som leverantör*” (som DoIT tagit fram till Kommunstyrelsens beslut), gäller endast överföring av uppgifter som omfattas av EU-US Data Privacy Framework (adekvansbeslutet). Adekvansbeslutet gäller inte för överföringar till amerikanska myndigheter. Till skillnad från vad som påstås i det hänvisade dokument är det alltså inte förenligt med GDPR att behandla personuppgifter för att uppfylla en CLOUD Act begäran.

Vidtar Microsofts åtgärder för att garantera att kraven i GDPR efterlevs?

Avtalsrättsligt skydd

En dokumenterad analys av Tekniska nämndens avtal med Microsoft saknas. **Bedömning och rekommendation blir därför utifrån vad som framkommit hittills i DoITs pågående utredning.**

Det finns ett tecknat personuppgiftsbiträdesavtal (PUB-avtal) mellan Tekniska nämnden och Microsoft. Microsoft har själva, ensidigt, skrivit det PUB-avtal som tecknats med Tekniska nämnden. Tekniska nämnden har i praktiken liten eller ingen möjlighet att påverka den behandling som Microsoft ska utföra åt nämnden. Samtidigt är det enligt GDPR Tekniska nämnden (eller annan nämnd i kommunen) som är ansvariga ifall instruktionen Microsoft skrivit bryter mot lag eller om nämnden skulle anlita ett biträde som de vet kommer bryta mot lag.

Av den utredning som skett där jag som dataskyddsombud varit delaktig och i övrigt känner till kan i huvudsak konstateras följande.

Av Tekniska nämndes avtal med Microsoft benämnt ”Dataskyddstillägg för Microsofts produkter och tjänster” framgår under punkten ”Utlämnande av behandlade data” bl.a. följande ” … *Microsoft ska inte lämna ut eller ge åtkomst till Behandlade data till rättsvårdande myndighet såvida inte detta krävs enligt lag. Om rättsvårdande myndighet skulle kontakta Microsoft med en begäran om behandlade data ska Microsoft försöka hänvisa den rättsvårdande myndigheten till att begära dessa data direkt från Kunden. Om Microsoft är tvungna att lämna ut eller ge åtkomst till Behandlade data till rättsvårdande myndighet ska Microsoft omgående meddela Kunden och tillhandahålla en kopia av begäran, såvida inte Microsoft är förhindrande enligt lag att göra så …*”. I Bilaga C till ovan angivna avtal framgår bl.a. att om ” … *Microsoft eller något av deras koncernbolag fortfarande tvingas lämna ut personuppgifter ska Microsoft endast lämna ut den minsta mängd av dessa data som är nödvändig för att uppfylla ordern om tvingat utlämnande …*”

DoIT har begärt ett förtydligande från Microsoft ifall de ger några garantier för att detta inte skulle innebära en behandling i strid med GDPR t.ex. genom att Microsoft skulle tillgodose en CLOUD Act begäran. På denna begäran svarade Microsoft bl.a. följande i meddelande inkommen till Tekniska nämnden den 7 november 2025 ”*… Dessvärre kan Microsoft meddela att vi inte kommer kunna ge några ytterligare förtydligande, utfästelser eller kommentarer i dagsläget kopplat till innebörden av denna text. Microsoft hänvisar istället till redan gjorda utfästelser i avtal och till principer för datautlämning som finns publicerade på Microsofts webbsidor.*”. Alltså ingen utfästelse att endast behandla personuppgifter enligt GDPR och svensk lag. Microsoft erbjuder alltså inget avtalsrättsligt skydd gällande garantier att endast behandla personuppgifter i enlighet med GDPR.

Det är också allmänt känt, enligt Microsofts egen utsaga, att företaget lämnar ut kunders data vid en lagakraftvunnen begäran enligt bl.a. CLOUD Act https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data och https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/

Microsofts egen hantering av de personuppgifter nämnden ansvarar för

Det har hittills identifierats en situation (och kan ev. finnas fler då frågan ännu inte är fullt utredd) i samband med den pågående analysen av de Microsoft tjänster som används i kommunen. I den pågående konsekvensbedömningen av Entra ID, (den tjänst som används för att skapa användare i Microsofts program/tjänster) framgår att Microsoft gör sig själva till personuppgiftsansvariga för vissa personuppgifter de får av Tekniska nämnden som nämndens biträde. Detta är som utgångspunkt förbjudet i GDPR och kan endast ske i vissa undantagsfall. Det har, så vitt det gjorts känt för mig, inte skett någon analys eller dokumenterad bedömning ifall denna hantering är förenligt med GDPR. Utan denna dokumentation kan artikel 5.2 inte anses uppfylld och det går heller inte att göra en korrekt prövning av om kraven i art. 28.1 är uppfyllda. Det finns också en möjlighet att det är frågan om en behandling i strid med GDPR.

Underbiträden och tredjelandsöverföringar

Art 28.4 GDPR ställer krav på att personuppgiftsbiträdet (här Microsoft) ska överföra de villkor som gäller för dem på ev. underbiträden. Detta innebär med Microsofts avtalstext, att i de fall där Microsoft anlitar ett underbiträde där underbiträdet omfattas av nationell lagstiftning som kräver att uppgifterna lämnas ut till det landets myndigheter kan också dessa länder (utöver de som ges möjlighet enligt CLOUD Act) få del av uppgifter som lämnats ut till Microsoft.

Det är inte utrett eller dokumenterat ifall de underbiträden som behandlar Tekniska nämndens personuppgifter omfattas av någon nationell lag som skulle kunna innebära att de lämnar ut personuppgifter i strid med GDPR eller hur Microsoft tillämpar möjligheten att överföra de instruktioner om överlämnats på dem till sina underbiträden. Även här är det brister i efterlevnaden av art. 5.2 GDPR vilket påverkar möjligheten för Tekniska nämnden att säkerställa att art. 28 GDPR följs.

Säkerställer Microsoft registrerades rättigheter?

De personuppgifter som förs över till USA av Microsoft som inte omfattas av avtalet mellan EU och USA (adekvansbeslutet) har inte motsvarande skydd som de har i EU/EES, se t.ex. EU-domstolens dom Schrems ii (st 185). Av den utredning jag fått del av framgår att det inte finns några avtalsrättsliga förbud mot sådana överföringar samt att Microsoft gör sådana överföringar. Microsoft kan alltså inte, på befintlig utredning, anses garantera att registrerades rättigheter skyddas om personuppgifter lämnas ut till dem. Hanteringen innebär då att Tekniskas nämnden behandlar personuppgifter i strid med art 5.2 och 28 GDPR.

Det är i dagsläget inte utrett eller dokumenterat ifall Microsoft överför personuppgifter till andra länder än USA eller ifall de eller någon av underleverantörerna omfattas av sådan nationell lagstiftning som gör att de behöver lämna ut nämndens personuppgifter till utländska myndigheter. Det går därför inte att göra en bedömning i den frågan i dagsläget. Tekniska nämnden bryter däremot ändå mot art. 5.2 GDPR eftersom nämnden i så fall inte kan visa att Microsoft kan säkerställa registrerades rättigheter.

Är det möjligt att anlita Microsoft som personuppgiftsbiträde?

Aktuell frågeställning går i dagsläget inte att tillfullo besvara då Tekniska nämnden som personuppgiftsansvarig inte har gjort någon fullständig dokumenterad utredning av frågan. Utifrån vad som hittills framkommit i den pågående utredningen och som tillgängliggjorts för mig som dataskyddsombud framgår följande.

Microsoft lämnar inte avtalsrättsliga garantier att följa GDPR och skydda registrerades rättigheter. Microsoft gör sig själva till personuppgiftsansvarig för personuppgifter de får som personuppgiftsbiträde på oklar rättslig grund. Microsoft behandlar personuppgifter i strid med GDPR när de uppfyller en CLOUD Act begäran men lägger formellt över ansvaret i Tekniska

nämndens som då står risken trots att nämnden i praktiken inte kan påverka behandlingen. Microsoft kan inte garantera registrerades rättigheter när de överför personuppgifter till USA utanför adekvansbelutet. Det kan inte heller uteslutas att det sker annat utlämnande i strid med GDPR men frågan är inte utredd av Tekniska nämnden.

Många frågor är ännu inte utredda eller dokumenterade men Tekniska nämnden kan, i nuläget på befintligt underlag, inte anses ha visat att Microsoft ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att kraven i GDPR är uppfyllda och registrerades rättigheter skyddas. Microsoft får alltså enligt artikel 28.1 i GDPR inte anlitas som Tekniska nämndens personuppgiftsbiträde och behandlingen som sker i Microsofts tjänster i dagsläget sker i strid med GDPR med risk för registrerade och kommunala nämnder som följd.

Kort om sekretesskyddet och GDPR

GDPR ser offentlighets- och sekretesslagen (OSL) som ett organisatoriskt skydd. Genom att Tekniska nämnden inte ha tagit ställning till frågan och dokumenterat en sekretessprövning för utlämnandet av personuppgifter till Microsoft har nämnden inte heller uppfyllt kraven i GDPR, artiklarna 25, 32 och 5.2.

I aktuellt fall bör en prövning gentemot Microsoft omfatta 21 kap. 7 § OSL då det, utifrån vad som är känt i dagsläget, se ovan, kan finnas skäl att anta att personuppgifter efter utlämnande till Microsoft kan komma att behandlas i strid med reglerna i GDPR. I en sådan situation omfattas alla personuppgifter, oavsett typ eller vilken verksamhet de förekommer i, av sekretess gentemot Microsoft. Notera att om 21:7 OSL är tillämplig är ett utlämnande av personuppgifter till Microsoft också en straffbar handling enligt 20 kap. 3 § brottsbalken. De hänvisningar till den sekretessbrytande grunden i 10:2a OSL, som görs i underlaget till Kommunstyrelsen är också bara tillämplig om Microsoft enbart hanterar uppgifterna för teknisk bearbetning och lagring vilket inte uppenbart är fallet om Microsoft också använder uppgifterna för egna ändamål.

Dataskyddsombudets bedömning och rekommendation till Tekniska nämnden

DoIT har påbörjat ett arbete för att utreda frågan om det är möjligt för Tekniska nämnden att anlita Microsoft som personuppgiftsbiträde. Det rekommenderas att detta arbete (kallat ”del 1”) slutförs i syfte att få ett underlag. Det underlaget kan sedan användas som utgångspunkt för att kunna bedöma lagligheten av att anlita Microsoft som personuppgiftsbiträde och samtidigt uppfylla kravet i artikel 5.2 GDPR på dokumentation. Utan komplett utredning går det heller inte bedöma vilka skyddsåtgärder som kan vara lämpliga att vida, eller bedöma skyddsåtgärdernas förväntade effektivitet.

Med nuvarande dokumentation och vad som är känt om Microsofts hantering av personuppgifter skulle förslaget på beslut i Tekniska nämndens ärende TN-2026/00081 innebära att nämnden beslutar om personuppgiftsbehandling i strid med GDPR som innebär risker för både enskilda individer så väl som nämnderna i Umeå kommun.

Av det som hittills framkommit i arbetet på DoIT med att utreda möjligheten för Tekniska nämnden att anlita Microsoft som personuppgiftsbiträde har det identifierats brott mot **artikel 5.2** (skyldighet för Tekniska nämnden att följa GDPR och kunna visa att GDPR följs), **artikel 28.1** (Microsoft kan inte garantera att de följer GDPR och skyddar registrerades rättigheter och friheter, istället finns indikationer på motsatsen), **artikel 25** (Tekniska nämnden har brister i tekniska och organisatoriska skyddsåtgärder som innebär att kraven i GDPR inte uppfylls och registrerades rättigheter inte skyddas t.ex. genom att ingen sekretessprövning är gjord) och **artikel 32** (Tekniska nämnden brister i säkerheten eller att alla risker inte är identifierade eller bedömda) i GDPR. Ev. kan brott mot artiklarna 44 och 48 (Tekniska nämnden/Microsoft överför personuppgifter till land utanför EU/EES i strid med GDPR) också ha förekommit men det är ytterst oklart och är enbart hypotetiskt i nuläget, vidare utredning behöver ske för att utesluta möjligheten att så skett.

Som dataskyddsombud rekommenderar jag, på befintlig information ifall nämnden väljer att inte utreda frågan vidare trots ovanstående rekommendation, att personuppgiftsbehandlingen hos Microsoft avbryts. Ska nämnderna fortsätta behandla personuppgifter i Microsofts tjänster, utifrån befintlig information, behöver det skyndsamt vidas skyddsåtgärder som kan garantera att Microsoft inte får tillgång till några personuppgifter. Notera att ev. skyddsåtgärder i så fall också behöver uppfylla krav som kan komma att behöva ställas enligt offentlighets- och sekretesslagen vilka kan vara annorlunda än de som ställs enligt GDPR.

Möjliga konsekvenser

Nämnderna

För samtliga personuppgiftsansvariga nämnder i kommunen innebär Tekniska nämndens anlitande av Microsoft som personuppgiftsbiträde att de i dagsläget bryter mot lag. Som konsekvens kan nämnderna åläggas sanktionsavgift från Integritetsskyddsmyndigheten (IMY) på upp till 10 000 000 kr per nämnd. IMY har också möjlighet att förbjuda behandlingen. Varje enskild registrerad (person) har också rätt att kräva skadestånd. Där finns ingen begränsning i GDPR på något maxbelopp. Den praxis som finns indikerar belopp på ca 3 000 - 4 000 kr per registrerad. Möjlighet att föra grupptalan finns. Som referens kan också nämnas att EU-domstolen i ett avgörande (T-354/22) ansåg att överföringen av ett IP-nummer till USA i strid med GDPR vid ett tillfälle motsvarande ett skadestånd på 400 €. Med tanke på antalet registrerade och typen av personuppgifter som nämnderna har i Microsofts tjänster kan det bli frågan om högre belopp här. Det är möjligt för nämnderna att få betala både sanktionsavgift och skadestånd samtidigt, det ena utesluter inte det andra.

Enskilda

För de enskilda innebär aktuell hantering att de riskerar att fråntas kontrollen av sina personuppgifter och att deras rättigheter kränks/inte skyddas. Hanteringen innebär också att uppgifterna kan komma att överföras utom registrerades kontroll och kännedom till länder där Microsoft, eller något av deras underbiträden är verksamma. Det är dessutom frågan om individer som är i underläge till de kommunala nämnderna och som ofta inte har något annat val än att ge sina personuppgifter till de kommunala nämnderna.

Frågan om möjlig straffbarhet för enskilda finns med men är ytterst oklar då det saknas en dokumenterad bedömning av sekretessfrågan.

Eric Lindström

Dataskyddsombud

Bilaga 1 Checklista

Checklista, hantering av allmänna handlingar vid utkontraktering

- Innebär utkontrakteringen att allmänna handlingar uppstår?
- Innefattar utkontrakteringen hantering av allmänna handlingar?
  - Kan handlingarna bevaras på tillfredställande sätt?
  - Finns möjligheter till gallring?
  - Har myndigheten smidig tillgång till handlingarna?
  - Kan myndigheten vid behov ta tillbaka handlingarna?
  - Finns det risk att de allmänna handlingarna förloras eller obehörigen sprids?

Checklista, sekretessöverväganden vid utkontraktering

Är det fråga om sekretessreglerade uppgifter?

- Kommer uppgifterna att röjas?
- Är det fråga om en osjälvständig uppdragstagare?
- Kan uppgifterna krypteras på ett fullgott sätt gentemot leverantören?

Kan utkontraktering ske med stöd av den sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL?

- Gäller det utkontraktering för teknisk bearbetning eller teknisk lagring?
  - Hanteras överlämnad information endast för uppdragsgivande myndighets räkning?
  - Är it-tjänstens karaktär enbart av teknisk natur?
  - Tillförs informationen något nytt eller kompletterande innehåll?
  - Förekommer hantering av samma uppgifter i något annat flöde hos leverantören och är det i så fall möjligt att hålla dessa flöden helt åtskilda?
- Är det olämpligt att utkontraktera för teknisk bearbetning eller teknisk lagring?
  - Är det fråga om uppgifter av känsligt slag?
  - Kan aggreggering innebära att den totala informationsmängden blir mer skyddsvärd?

- Finns det risk för att myndigheten avhänder sig kontroll över uppgifter i den samhällsbärande verksamheten?
- Förekommer underleverantörer och kan i så fall skyddet upprätthållas hos dessa?
- Finns det risk för att lag- eller avtalsreglerad tystnadsplikt inte kan efterföljas?
- Är den interna åtkomsten hos leverantören begränsad med tekniskt eller med organisatoriska rutiner?
- Kan leverantörens geografiska lokalisering påverka möjligheten att upprätthålla skyddet för uppgifterna?
- Är leverantören eller dess underleverantörer bundna av extraterritoriell lagstiftning eller annan lagstiftning som innebär att skyddet för uppgifterna inte kan upprätthållas?
- Har myndigheten tagit hänsyn till kända faktorer och vilka krav som är möjliga att ställa i en upphandling?
- Ger en allsidig bedömning utfallet att ett utlämnande inte är olämpligt?

Kan utkontraktering ske efter prövning av en sekretessbestämmelses rekvisit?

- Gäller s.k. absolut sekretess eller är sekretessbestämmelsen reglerad med ett skaderekvisit?
- Hur skyddsvärda är uppgifterna, typiskt sett?
  - Är det uppgifter av känslig art?
  - Har mottagaren rätt att lämna uppgifterna vidare eller själv utnyttja dem (dvs risk för spridning)
  - Kan avtalsmässiga och tekniska begränsningar göras?

Kan utkontraktering ske med stöd av någon annan sekretessbrytande bestämmelse?

- Om tjänsteleverantören är en myndighet, är utlämnandet en följd av en lag- eller förordningsreglerad uppgiftsskyldighet eller kan utlämnandet ske med stöd av den s.k. generalklausulen eller någon sektorsspecifik sekretessbrytande bestämmelse?
- Om tjänsteleverantören är en enskild aktör, kan uppgifterna lämnas med förbehåll att uppgifterna inte får lämnas vidare eller nyttjas av leverantören?
  - Är det fråga om en enstaka åtgärd?
- Oavsett om tjänsteleverantören är en myndighet eller en privaträttslig aktör, kan utlämnandet anses vara ”nödvändigt”?

- Kan myndighetens uppdrag rimligen fullgöras utan att utlämnande sker?
- Motiveras utlämnandet även av andra skäl än rent ekonomiska?
- Har alla alternativ till utlämnande övervägts noggrant?
- Framstår utkontrakteringen som den enda realistiska lösningen?

Juridisk bedömning av molntjänster i förhållande till TN-2026/00081

2026-04-30
Thed Lindström
IT-rättsjurist
Atea Sverige AB

Innehållsförteckning

1. Sammanfattning

Tekniska nämndens beslutsförslag och dataskyddsombudets samrådsyttrande representerar två positioner som båda har rättsligt stöd i delar men som båda blir otillräckliga om de drivs till sin spets. Nämndens position blandar samman riskaccept med legalitetsprövning och vilar på dokumentation som inte föreligger. Dataskyddsombudets position är juridiskt välgrundad, men för rekommendationen om att avbryta behandlingen krävs en realism om vad som är praktiskt möjligt och vad som är hållbart över tid.

Användning av amerikansk hyperscaler-molntjänst för personuppgifter kan inte vara fullt ut förenlig med EDPB:s strikta tolkning av Schrems II och samtidigt funktionellt likvärdig med tjänstens normala användning. Detta är en strukturell konflikt mellan EU-rätten och amerikansk extraterritoriell lagstiftning som inte kan kompromisseras bort på teknisk väg så länge tjänsten levereras under amerikansk jurisdiktion. Konsekvensen är att varje personuppgiftsansvarig som väljer fortsatt användning av Microsoft 365 fattar beslutet inom en zon av rättslig osäkerhet, inte ett efterlevnadsbeslut i strikt mening.

Tillsynsmyndigheternas faktiska praxis motsvarar inte den strikta läsningens kategoriska konsekvenser. Ingen europeisk organisation har, så vitt känt, ålagts sanktionsavgift specifikt för att ha använt amerikansk molntjänst som sådan. De sanktioner och förbud som faktiskt utfärdats har genomgående gällt bristande dokumentation, utebliven konsekvensbedömning eller otillräckliga tekniska och organisatoriska åtgärder, inte molntjänsten i sig. Detta ska beaktas vid riskbedömning och beslutsfattande utan att förväxlas med en rättslig friskrivning.

Denna juridiska bedömning syftar inte till att underkänna någon parts position utan till att tillhandahålla det rättsliga och tekniska underlag som behövs för att Tekniska nämnden, Kommunstyrelsen och Dataskyddsombudet ska kunna föra processen vidare på en gemensam faktagrund.

2. Den centrala rättsliga motsättningen

Schrems II-domen från Europeiska unionens domstol (mål C-311/18) fastslog att överföringar av personuppgifter till USA inte uppnår en skyddsnivå som är väsentligen likvärdig med EU-rättens, särskilt med hänsyn till FISA 702 och EO 12333. Domstolen pekade på frånvaron av effektiva rättsmedel för icke-amerikanska personer och avsaknaden av begränsningar som motsvarar proportionalitetsprincipen i artikel 52 i EU:s rättighetsstadga.

Adekvansbeslutet under EU-US Data Privacy Framework från juli 2023 (kommissionens genomförandebeslut (EU) 2023/1795) reglerar tredjelandsöverföringar till amerikanska organisationer som anslutit sig till DPF genom självcertifiering. Beslutet bygger delvis på presidentorder EO 14086 och inrättandet av Data Protection Review Court. Beslutet adresserar dock inte i samma mening myndighetsåtkomst utan integrerade samtycken, och det gemensamma yttrandet från EDPB och EDPS av den 10 juli 2019 om CLOUD Act drog slutsatsen att amerikanska brottsbekämpande myndigheters direktbegäran till leverantörer i regel saknar rättslig grund enligt GDPR utan en internationell överenskommelse. EDPB Guidelines 02/2024 om artikel 48 GDPR (version 2.1, antagen den 4 juni 2025) upprepar att en utländsk myndighetsbegäran inte i sig utgör vare sig rättslig grund enligt artikel 6 eller överföringsgrund enligt kapitel V.

Detta innebär att även när data lagras inom EU och täcks av DPF för kommersiella ändamål kvarstår en rättslig osäkerhet kring hur en CLOUD Act-begäran ska hanteras inom GDPR-ramverket. Microsofts egen avtalstext, som dataskyddsombudet korrekt citerar, utfäster att företaget i sista hand kommer att lämna ut den minsta mängd data som krävs för att uppfylla en lagligen bindande begäran. Microsofts svar till DoIT den 7 november 2025, där företaget avstår från att lämna ytterligare garantier utöver vad som redan finns i avtalstexten, är symptomatiskt för leverantörsledets oförmåga att lämna sådana garantier under amerikansk jurisdiktion.

EDPB:s Recommendations 01/2020 paragraf 94 innehåller en av de mest centrala men sällan citerade slutsatserna i sammanhanget. För det användningsfall där en molntjänstleverantör behöver tillgång till data i klartext för att kunna leverera tjänsten, och där tredjelandets lagstiftning ger myndigheter åtkomst utöver vad som är nödvändigt och proportionerligt, anger EDPB följande:

"the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on the data subject's fundamental rights."

Detta är inte en teknisk begränsning som EDPB tror kan lösas senare. Det är ett strukturellt konstaterande om att kryptering, kontraktsklausuler och datalokalisering inte kan kompensera för åtkomst till data i klartext om molntjänsten behöver bearbeta data. Microsoft 365 i normal drift är just det användningsfall som EDPB beskriver i sin Use Case 6.

3. Vad som krävs för rättsligt försvarbar användning

Frågan är därför inte om M365-användning är fullt ut förenlig med GDPR, utan om den är dokumenterat försvarbar inom det rättsläge som faktiskt råder. Dokumenterad försvarbarhet innebär här att kommunen har genomfört och dokumenterat de bedömningar som artikel 5.2 GDPR kräver och att dessa bedömningar innehåller intern juridisk granskning, inte att efterlevnaden är säkerställd i materiell mening. Försvarbarheten kräver fyra delar.

Dokumentation enligt artikel 5.2 GDPR

Den personuppgiftsansvarige ska kunna visa efterlevnad. Detta kräver konkret dokumentation som idag synes saknas i ärendet:

- En dokumenterad analys av Microsofts Data Protection Addendum mot kraven i artikel 28.3 GDPR, klausul för klausul, inklusive bedömning av underbiträdesregleringen i artikel 28.2 och 28.4.
- En konsekvensbedömning enligt artikel 35 GDPR. För en kommun som behandlar uppgifter om barn, brukare, anställda och vårdnadshavare i M365 är skyldigheten att genomföra DPIA i praktiken given. Integritetsskyddsmyndigheten utdömde i ärende IMY-2023-1647 (Barn- och utbildningsnämnden i Östersunds kommun, beslut 2023-11-28) en sanktionsavgift på 300 000 kronor enbart för utebliven konsekvensbedömning vid införande av Google Workspace, oberoende av den materiella behandlingens innehåll.
- En registerförteckning enligt artikel 30 GDPR som korrekt återspeglar M365-behandlingarna.
- En självständig bedömning av de delar där Microsoft enligt sin egen DPA (Data Protection Addendum) agerar som personuppgiftsansvarig. Detta omfattar bland annat telemetri, säkerhetsåtgärder, produktutveckling och delar av Entra ID. Dataskyddsombudet har korrekt identifierat detta som en kritisk fråga. När en leverantör behandlar data för egna ändamål faller den behandlingen utanför artikel 28-konstruktionen och kräver självständig rättslig grund enligt artikel 6 GDPR.

Tredjelandsbedömningen enligt artikel 44 till 49 GDPR

En tredjelandsöverföringsbedömning (transfer impact assessment, TIA) ska utföras enligt EDPB:s sex-stegsmetodik i Recommendations 01/2020. Bedömningen behöver inte vara en akademisk genomgång av rättssystemen i alla länder där underbiträden finns. Den ska fokusera på de faktiska åtkomstriskerna i den specifika tjänstekonfigurationen, prövade mot European Essential Guarantees i Recommendations 02/2020. Dessa fyra kriterier (klar och precis lagstiftning, nödvändighet och proportionalitet, oberoende tillsyn och effektiva rättsmedel) är referensramen, inte hela tredjelandets rättsordning.

Med tanke på att flera amerikanska underrättelseprogram inte uppfyller dessa kriterier enligt EU-domstolens bedömning i Schrems II punkt 168 till 185, kommer en ärlig TIA att landa i att kompletterande åtgärder krävs. Frågan blir då vilka åtgärder som faktiskt fungerar.

Tekniska och organisatoriska åtgärder

Här ligger den största delen av det praktiska arbetet och även den största delen av missförstånden. Vilka åtgärder har vilken effekt:

Microsofts standardkryptering av data at rest och in transit räknas inte som en effektiv kompletterande åtgärd enligt EDPB Recommendations 01/2020 paragraf 95, eftersom Microsoft har tillgång till krypteringsnycklarna och därmed kan tvingas lämna ut data i klartext under en CLOUD Act-begäran.

Customer Key ger kunden kontroll över de nycklar som krypterar data at rest, men nycklarna måste vara tillgängliga för Microsofts driftsmiljö för att tjänsten ska fungera. Detta begränsar skyddet mot myndighetsbegäran.

Double Key Encryption (DKE) är den enda Microsoft-erbjudna lösningen där Microsoft kryptografiskt utestängs från kund-nyckeln. Detta gör DKE till den enda tekniska åtgärd som materiellt motsvarar kraven i EDPB Recommendations 01/2020 för Use Case 6. Samtidigt har DKE betydande funktionella begränsningar. Enligt Microsofts officiella dokumentation fungerar DKE idag enbart i fullversionerna av Word, Excel, PowerPoint och Outlook på Windows. Lösningen fungerar inte i webbversionen av Office, inte i mobila Office-applikationer, inte i Teams och inte i SharePoint Online för redigering. DKE-skyddade dokument kan lagras i molnet men kan inte indexeras av Microsoft Search, inte hanteras av Copilot, inte skannas av DLP eller antivirus och inte samredigeras. Metadata, inklusive filnamn, mappstrukturer, åtkomstmönster och behandlingsspår, omfattas inte av DKE-skyddet utan är fortfarande synliga för Microsoft.

Detta innebär att den enda tekniska åtgärd som materiellt skulle bringa M365 i linje med EDPB:s krav samtidigt motverkar grundsyftet med digitalisering och med användandet av en molntjänst. En bredspektrumimplementation av DKE skulle eliminera samredigering, mobil åtkomst, sökning, integration med samverkansflöden och Copilot, det vill säga de funktioner som motiverar valet av M365 i första hand. DKE är därmed en realistisk åtgärd endast för en avgränsad högkänslig dokumentkategori inom en sluten Windows-miljö. Den är inte en lösning för bredare M365-användning. Resultatet bekräftar slutsatsen i avsnitt 1: ingen kombination av tekniska åtgärder kan göra M365 fullt ut förenligt med EDPB:s strikta läsning utan att tjänsten upphör att fungera som molntjänst.

Övriga åtgärder med dokumenterad effekt enligt EDPB:s ramverk är pseudonymisering före överföring (Use Case 2), uppdelad behandling (split processing) mellan icke-samverkande jurisdiktioner (Use Case 5), och datalokalisering till EU Data Boundary kombinerat med striktare avtalsklausuler. Ingen av dessa eliminerar risken kategoriskt, men de reducerar den och dokumenterar att den personuppgiftsansvarige har vidtagit åtgärder.

Sekretessprövning enligt OSL

För kommunal verksamhet tillkommer prövningen enligt offentlighets- och sekretesslagen som en separat fråga från GDPR. Den sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL, införd genom prop. 2022/23:97, kräver att leverantörens hantering är begränsad till enbart teknisk bearbetning eller teknisk lagring. Av prop. 2022/23:97 sidan 11 och 17 framgår att rekvisitet är strikt. Om leverantören behandlar uppgifter för egna ändamål, vilket Microsoft enligt sin DPA gör i delar av tjänsten, faller hela bestämmelsen i den delen.

Detta innebär att Tekniska nämndens skrivning om att Microsofts hantering är begränsad till teknisk bearbetning och lagring inte är hållbar för hela tjänsten. Den behöver differentieras per behandling och funktion. För de delar där Microsoft agerar personuppgiftsansvarig krävs antingen att utlämnandet stöds av annan sekretessbrytande bestämmelse, att sekretess inte föreligger för uppgifterna, eller att behandlingen styrs bort från tjänsten.

Olämplighetsbedömningen enligt 10 kap. 2 a § OSL ska enligt prop. 2022/23:97 vara allsidig och beakta extraterritoriell lagstiftning, underbiträden, geografisk placering och avtalsförhållanden som kan beröva myndigheten kontrollen. eSams vägledning ES 2023:06 avsnitt 5.4 och 5.5 är vägledande för hur denna prövning ska dokumenteras.

4. Bemötande av tekniska nämndens beslutsförslag

Mot denna bakgrund kan följande sägas om beslutsförslaget i sin nuvarande utformning.

Den föreslagna formuleringen att nämnden beslutar att acceptera kvarstående risker kopplade till tredjelandslagstiftning och leverantörens jurisdiktion är juridiskt felkonstruerad. Riskaccept är ett verktyg inom ramen för informationssäkerhetsriskbehandling enligt ISO/IEC 27001 klausul 8.3, dvs. ett medel att hantera identifierade risker inom tillåten behandling. Det kan inte legitimera behandling som i sig strider mot förordningen. Tekniska nämnden kan inte genom riskacceptbeslut ersätta den prövning av personuppgiftsbiträdets garantier som artikel 28.1 GDPR kräver. Som dataskyddsombudet korrekt framhåller utövas den offentliga makten under lagarna enligt 1 kap. 1 § andra stycket regeringsformen.

Hänvisningen till EU-kommissionens gällande adekvansbeslut är delvis missvisande. DPF täcker den kommersiella överföringen men adresserar inte myndighetsåtkomsten under CLOUD Act eller FISA 702 på det sätt som beslutsförslaget antyder. eSams promemoria ES 2025-18 av den 15 september 2025 understryker dessutom att DPF befinner sig i en juridiskt och politiskt instabil situation efter PCLOB-händelserna i januari 2025 (avsättningarna ogiltigförklarades därefter av amerikansk domstol och ledamöterna återinsattes, men händelsen visar att ramverkets institutionella stabilitet är beroende av amerikansk inrikespolitik). Presidentorder EO 14086 är dessutom ensidigt återkallbar.

Påståendet att Microsofts hantering är begränsad till teknisk bearbetning och lagring är inte motiverat på det underlag som föreligger och motsägs delvis av nämndens egen pågående analys av Entra ID, där Microsoft enligt sin DPA agerar som självständigt personuppgiftsansvarig för vissa data.

Argumentet att riskerna är strukturella och inte leverantörsspecifika är empiriskt korrekt men juridiskt otillräckligt som beslutsformulering. Att problemet är systemiskt befriar inte den enskilde personuppgiftsansvarige från ansvarsskyldigheten enligt artikel 5.2 GDPR. Schrems II punkt 134 till 135 är tydlig på att den personuppgiftsansvarige ska göra en individuell bedömning i det enskilda fallet.

5. Bemötande av dataskyddsombudets samrådsyttrande

Dataskyddsombudets analys av rättsläget är väsentligen korrekt. Identifieringen av brister i förhållande till artiklarna 5.2, 28.1, 25 och 32 GDPR är välgrundad på det underlag som föreligger. Hänvisningen till 21 kap. 7 § OSL och kopplingen till 20 kap. 3 § brottsbalken är välfunnen och bör tas på allvar. Den principiella analysen är välunderbyggd.

Rekommendationen att avbryta behandlingen

Rekommendationen att avbryta personuppgiftsbehandlingen i Microsofts tjänster är juridiskt försvarbar givet det underlag som föreligger, men förtjänar nyansering i flera avseenden.

För det första är rekommendationen i praktiken oförenlig med kommunens grunduppdrag. Att inom rimlig tid lämna en hyperscaler-baserad samverkansplattform för en kommun av Umeås storlek är inte ett realistiskt scenario utan betydande verksamhetspåverkan, och alternativen i form av suveräna europeiska lösningar är ännu inte funktionellt likvärdiga. Detta är en realitet som även dataskyddsombudet rimligen ser, men som beslutsfattaren behöver kunna förhålla sig till.

För det andra finns en mellanposition som dataskyddsombudet inte uttryckligen behandlar i sitt yttrande. Den består i att slutföra dokumentationsarbetet, implementera de kompletterande åtgärder som är genomförbara, styra känslig och sekretessreglerad information bort från tjänsten genom strikt informationsklassning, och samtidigt bygga beredskap för avveckling. Denna position är inte fullt förenlig med GDPR enligt EDPB:s strikta läsning, men den är dokumenterat försvarbar i den meningen som anges i avsnitt 2 ovan, och i linje med hur tillsynsmyndigheter i Europa de facto har bedömt jämförbara fall, inklusive Helsingør och Europeiska kommissionen.

Det är rimligt att tolka dataskyddsombudets rekommendation som att den första delen, att slutföra del 1-utredningen, är det grundläggande kravet, och att rekommendationen att avbryta behandlingen aktiveras endast om detta arbete inte slutförs eller om det visar att åtgärder inte kan vidtas.

Konsekvensbeskrivningens proportionalitet

Yttrandets konsekvensbeskrivning förtjänar ett särskilt bemötande. Yttrandet anger att IMY enligt 6 kap. 2 § andra stycket dataskyddslagen kan utfärda sanktionsavgift på upp till 10 000 000 kronor per nämnd för överträdelser av artikel 83.5 och 83.6 GDPR (bl.a. grundläggande principer, registrerades rättigheter, tredjelandsöverföring) och upp till 5 000 000 kronor för överträdelser av artikel 83.4 (bl.a. artikel 28 och 35). Yttrandet anger vidare att enskilda kan rikta skadeståndsanspråk utan beloppsgräns, att praxis indikerar belopp om 3 000 till 4 000 kronor per registrerad, samt hänvisar till Tribunalens dom av den 8 januari 2025 i mål T-354/22 (Bindl mot kommissionen), där 400 EUR utdömdes till klaganden för en specifik olovlig tredjelandsöverföring. Vidare hänvisas till möjlig straffbarhet enligt 20 kap. 3 § brottsbalken om 21 kap. 7 § OSL är tillämplig.

Var och en av dessa uppgifter är formellt korrekt, men beloppstaken ska differentieras per artikelöverträdelse, och Tribunalens 400 EUR utgjorde ett ex aequo et bono-belopp för en specifik händelse, inte en generell norm. Det är också nödvändigt att kontextualisera siffrorna mot tillsynspraxis. De mest relevanta tillsynsbesluten avseende offentlig sektors användning av amerikansk molntjänst är följande.

Helsingør kommun (Datatilsynet, Danmark, 2020 till 2024). Den danska tillsynsmyndigheten utfärdade 2022 ett föreläggande att upphöra med behandlingen avseende Google Chromebooks och Google Workspace i kommunens grundskolor. Förbudet upphävdes i september 2022 efter att kommunen vidtagit kompletterande åtgärder och dokumenterat sin behandling. Praxis utvidgades därefter till omkring 50 kommuner som använder samma teknikstack. Ingen sanktionsavgift utdömdes i något av besluten. Tillsynsmyndighetens åtgärder var korrigerande, inte bestraffande.

Östersunds kommun (IMY, Sverige, 2023). Sanktionsavgift på 300 000 kronor utdömdes med stöd av artikel 35.1 GDPR för utebliven konsekvensbedömning före införandet av Google Workspace. Sanktionen avsåg uttryckligen den uteblivna DPIA:n, inte molntjänsten som sådan, och inte tredjelandsöverföringen. IMY noterar i beslutet att tredjelandsöverföring var en relevant del av riskbilden, men sanktionen kopplades till den dokumenterade procedurbristen.

Europeiska kommissionen (EDPS, mars 2024). Europeiska datatillsynsmannen fann i beslut av den 8 mars 2024 (ärende 2021-0518) att Europeiska kommissionens egen användning av Microsoft 365 stod i strid med flera bestämmelser i förordning (EU) 2018/1725, särskilt avseende ändamålsbegränsning, internationella dataöverföringar och otillåtna utlämnanden. EDPS ålade kommissionen omfattande korrigerande åtgärder. Ingen sanktionsavgift utdömdes. Kommissionen lämnade in efterlevnadsrapport den 6 december 2024, och i juli 2025 förklarade EDPS att överträdelserna åtgärdats. Ärendet illustrerar att frånvaron av sanktion inte är liktydig med materiell tillåtelse, eftersom det krävde substantiella avtalsändringar och tekniska förändringar att nå förenlighet.

Conseil d'État (Frankrike, 12 mars 2021, mål 450163, Doctolib/AWS). Frankrikes högsta förvaltningsdomstol avvisade en ansökan om att avbryta franska hälsoministeriets samarbete med Doctolib, vars plattform hostas av AWS Sarl (Luxemburg-dotterbolag till Amazon). Avgörandet baserades på en bedömning av faktiska skyddsåtgärder, däribland kryptering med extern nyckelförvaring och avtalsklausuler om motverkande av myndighetsåtkomst. Domstolen lade också vikt vid att de behandlade uppgifterna i det specifika ärendet inte utgjorde hälsodata i strikt mening utan bokningsuppgifter, vilket begränsar avgörandets räckvidd.

Frånvaron av kategoriska uppmaningar från tillsynsmyndigheter är också relevant. EDPB:s Coordinated Enforcement Action 2022 om offentlig sektors användning av molntjänster, vars slutrapport antogs den 17 januari 2023, sammanfattade resultaten från 22 tillsynsmyndigheters samordnade granskning och konstaterade utbredda brister i tredjelandsbedömningar, DPIA och avtalsanalys. Slutsatsen blev rekommendationer och vägledning, inte krav på avveckling. Tysklands dataskyddskonferens (DSK) konstaterade 2022 att efterlevnadskrävande användning av Microsoft 365 var problematisk men avstod från generella förbud. Bayerns tillsynsmyndighet utfärdade 2023 detaljerad vägledning för hur TIA ska utformas. Frankrikes CNIL har i specifika ärenden, främst hälsodatasammanhang, rekommenderat europeiska alternativ men accepterat amerikansk hosting med kompletterande åtgärder i andra fall. IMY har inga publicerade beslut som kategoriskt avråder från amerikansk molntjänst.

Den realistiska bedömningen är att sannolikheten att en kommun av Umeås storlek, med normal användning av M365 och utan känsliga personuppgifter i tjänsten, drabbas av en sanktionsavgift specifikt för molntjänstanvändningen är historiskt sett låg. De triggers som faktiskt har lett till tillsyn har varit klagomål från registrerade eller intresseorganisationer (Helsingør, EU-kommissionen efter den ursprungliga klagan från Maximilian Schrems), eller egen anmälan. Den närmaste analogin är Helsingør, där förbudet var temporärt och avhjälptes genom dokumentation. Den närmaste sanktionsanalogin är Östersund, där sanktionen var 300 000 kronor och kopplad till uteblivna procedursteg.

De skadeståndsbelopp som dataskyddsombudet refererar till är teoretiskt möjliga enligt artikel 83.4 till 83.6 och artikel 82 GDPR samt 6 kap. 2 § dataskyddslagen, men har i praktiken inte realiserats i något jämförbart svenskt eller europeiskt fall. Att presentera dessa som sannolika konsekvenser av nuvarande hantering riskerar att ge en felaktig bild av den faktiska risken.

Bristande dokumentation enligt artikel 5.2 GDPR är fortfarande en överträdelse, och en personuppgiftsansvarig som inte uppfyller dokumentationskraven är fortfarande exponerad för tillsynsåtgärder vid en eventuell utredning. Frånvaro av historiska sanktioner legitimerar inte bristande dokumentation, men ger organisationen tid att åtgärda dokumentationsbrister innan en faktisk trigger inträffar. Det juridiskt försvarbara förhållningssättet är att använda denna tid aktivt, inte att förlita sig på den.

En slutlig observation: det finns en genuin spänning mellan EDPB:s strikta tolkning av Schrems II och tillsynsmyndigheternas faktiska praxis. Spänningen kan inte lösas på rättslig nivå utan endast genom strukturell förändring, antingen genom hållbara internationella överenskommelser eller genom uppbyggnad av europeisk molnkapacitet. Tills detta sker kommer den de facto-jämvikt som råder att fortsätta: strikta krav på papperet, pragmatisk hantering i praktiken. För beslutsfattaren innebär detta att den juridiskt försvarbara positionen inte är att hävda full efterlevnad enligt EDPB:s strikta läsning, utan att etablera en styrning som hanterar osäkerheten transparent och som dokumenterar de aktiva valen. Denna position kombinerar ett pragmatiskt förhållningssätt till verksamheten med en juridisk realism.

Dataskyddsombudets roll I den fortsatta processen

Dataskyddsombudets roll enligt artiklarna 38 och 39 GDPR förutsätter aktiv medverkan i alla frågor som rör skyddet av personuppgifter. Den omständighet som dataskyddsombudet själv påtalar, att kontakt inte togs inför att beslutsförslaget togs fram, är en självständig brist i processen och bör adresseras explicit i den fortsatta hanteringen. Det finns ingen anledning att upprepa detta i nästa beslutsomgång

6. Förslag till väg framåt

Mot denna bakgrund föreslås följande process.

Skjut upp beslutsförslaget i nuvarande form

Det nuvarande förslaget bör inte fattas i sin föreliggande utformning. Skälet är inte att fortsatt M365-användning är otänkbar, utan att beslutsformuleringen blandar samman riskaccept med legalitetsprövning och vilar på dokumentation som inte föreligger. Ett beslut i nuvarande form skulle vid en eventuell tillsyn kunna åberopas som indikation på oaktsamhet enligt artikel 83.2 b GDPR (överträdelsens uppsåtliga eller oaktsamma karaktär), eftersom det skulle visa att nämnden var medveten om problematiken men valde att inte slutföra utredningen.

Slutför utredningen

Tekniska nämnden bör återkomma med ett beslutsförslag först när den utredning som DoIT (kommunens IT-funktion) benämner del 1 är slutförd och dokumenterad. Detta omfattar:

- Dokumenterad analys av Microsofts DPA mot artikel 28.3 GDPR.
- Genomförd transfer impact assessment enligt EDPB Recommendations 01/2020 sex-stegsmetodik.
- Genomförd och dokumenterad konsekvensbedömning enligt artikel 35 GDPR för de behandlingar som sker i tjänsten.
- Dokumenterad bedömning av rollfördelningen, särskilt för de delar där Microsoft agerar personuppgiftsansvarig såsom telemetri och delar av Entra ID.
- Dokumenterad sekretessprövning enligt 10 kap. 2 a § OSL och 21 kap. 7 § OSL, differentierad per informationskategori.
- Dokumenterad analys av underbiträdeskedjan med fokus på faktiska åtkomstrisker.

Implementera kompletterande åtgärder i prioriteringsordning

Parallellt med utredningen bör följande åtgärder genomföras eller verifieras som genomförda:

- Skarp informationsklassning som styr känsliga personuppgifter enligt artikel 9 GDPR och sekretessreglerad information enligt OSL bort från tjänsten eller till DKE-skydd.
- Aktivering av EU Data Boundary för de tjänster där detta är möjligt.
- Aktivering av Customer Lockbox för support-scenarier.
- Användning av Customer Key för data at rest där det är funktionellt och ekonomiskt möjligt.
- DKE-implementation för en avgränsad högkänslig dokumentkategori, med insikt om de funktionella begränsningarna.
- Översyn av avtalsmässiga villkor avseende transparens, granskningsrätt och hantering av myndighetsbegäran. Microsoft har i flera europeiska upphandlingar accepterat tilläggsklausuler, och det förtjänar prövas om motsvarande kan uppnås för Umeå kommuns avtal.
- Loggning och övervakning som möjliggör detektion av onormal åtkomst.

Omformulera beslutet

När underlaget är komplett bör beslutet omformuleras. Den juridiskt och politiskt hållbara formuleringen är inte att nämnden accepterar kvarstående risker, utan att nämnden:

- konstaterar att fortsatt användning av Microsoft 365 sker inom en zon av rättslig osäkerhet som inte kan elimineras inom amerikansk jurisdiktion,
- konstaterar att de åtgärder som genomförts gör behandlingen dokumenterat försvarbar inom denna osäkerhetszon, i den begränsade meningen att kommunen kan visa att den genomfört de bedömningar som GDPR kräver, utan att detta innebär att efterlevnaden är säkerställd i materiell mening enligt EDPB:s strikta läsning,
- beslutar om kontinuerlig förvaltning, inklusive tvärfunktionell uppföljning enligt eSams ES 2025-18, årlig juridisk omprövning, och löpande omvärldsbevakning,
- beslutar om beredskap för avveckling i händelse av att DPF faller, väsentliga rättsliga förändringar inträffar, eller tillsynspraxis skärps.

De två formuleringarna har olika rättslig betydelse. Den första formuleringen påstår en legalitet som nämnden inte kan bevisa. Den andra formuleringen erkänner osäkerheten och dokumenterar de aktiva valen. Vid en eventuell tillsyn är den senare positionen avsevärt starkare.

Etablera tvärfunktionellt arbetssätt

Förvaltningen av beslutet kräver enligt eSams ES 2025-18 ett tvärfunktionellt arbetssätt med kompetens inom verksamhet, IT-förvaltning och IT-arkitektur samt informationssäkerhet, cybersäkerhet och juridik. Detta gäller även dataskyddsombudets fortsatta involvering enligt artikel 38.1 GDPR.

7. Avslutande synpunkter

Den underliggande spänningen i ärendet är inte unik för Umeå kommun. Den är ett uttryck för att GDPR och amerikansk extraterritoriell lagstiftning är fundamentalt oförenliga, och att europeisk offentlig sektors digitala infrastruktur är beroende av amerikansk teknologi. Att fullt ut implementera Schrems II skulle kräva att europeiska myndigheter lämnade hyperscaler-marknaden, vilket inte är ett kortsiktigt realistiskt scenario.

Den långsiktiga riktningen är dock tydlig. Frankrike har genom doktrinen "cloud au centre", och Tyskland genom finansiering av sovereign cloud-initiativ, påbörjat arbetet med att hantera beroendet av icke-europeiska leverantörer. Den kommun som idag fattar beslut om fortsatt användning av amerikansk hyperscaler bör därför fatta det med medvetenhet om att riktningen över tid pekar mot mindre, inte mer, beroende av sådana leverantörer. Detta påverkar hur avvecklingsberedskapen ska utformas och vilka avtalstider som är försvarbara.

Den position som är hållbar över tid är inte att hävda att fortsatt användning är säkert laglig, utan att etablera en styrning som kontinuerligt prövar förutsättningarna och som möjliggör snabb omställning vid förändrade omständigheter. Det är mot denna position som beslutsförslaget bör utformas.

Outlook

Re: Juridisk bedömning angående molntjänster och microsoft

Från Thed Lindström <thed.lindstrom@atea.se>
Datum Tis 2026-05-12 20:41
Till Mattias Wallmark <mattias.wallmark@umea.se>
Kopia jonas.bokstrom <jonas.bokstrom@atea.se>

Hej Mattias,

Jag har nu haft möjlighet att granska det underlag som min kollega tog fram till er tidigare, dvs ’Juridisk bedömning av Microsoft som leverantör’. I anledning av det (för mig) tillkomna underlaget har jag reviderat mina ståndpunkter i enlighet med den tillkomna informationen. Se mina svar färgade i lila nedan.

- Dokumenterad analys av Microsofts DPA mot artikel 28.3 GDPR.
  - Vi har också tidigare haft juriststöd från ATEA under hela processen och utgick från att detta var täckt i arbetet. Vad är det egentligen som återstår att göra?

    Jag hade inte tillgång till det underlaget vid min initiala bedömning. Efter att ha granskat det materialet så står det klart att en s.k. artikel 28-bedömning av Microsoft har skett och finns dokumenterad. Denna rekommendationen kan ni därför bortse ifrån.

- Genomförd transfer impact assessment enligt EDPB Recommendations 01/2020 sex-stegsmetodik.
  - Vi har också tidigare haft juriststöd från ATEA under hela processen och utgick från att detta var täckt i arbetet. Vad är det egentligen som återstår att göra?

    Denna rekommendation är till följd av kritiken i samrådsyttrandet från dataskyddsombudet. Det relaterar primärt till eventuella tredjelandsöverföringar som kan ske till underbiträden till Microsoft som befinner sig i länder som inte omfattas av ett adekvansbeslut. Detta blir inte relevant om ni kommer att använda er av Microsoft EU Data Boundary.

- Genomförd och dokumenterad konsekvensbedömning enligt artikel 35 GDPR för de behandlingar som sker i tjänsten.
  - Tolkningen har varit att detta är en bedömning som sker senare, per tjänst och användning i kommunens verksamheter där personsuppgiftsbehandlingen sker. Vad är det som återstår i den juridiska bedömningen av Microsoft och vad är det som behöver kompletteras per tjänst som vi inte har?

    Denna rekommendation är relevant inför behandling av personuppgifter och om ni har aktivt valt att avvakta med denna del till ett senare skede så kan ni bortse från denna rekommendationen i nuläget.

- Dokumenterad bedömning av rollfördelningen, särskilt för de delar där Microsoft agerar personuppgiftsansvarig såsom telemetri och delar av Entra ID.
  - Detta har berörts i bedömningen av EntraID. Är det något som saknas där? Dessutom undrar vi om det är klarlagt att Microsoft agerar personuppgiftsansvar för t ex telemetri (vi har bilden att det är anonymiserad telemetridata)?

- KOMMENTAR: I mötet med Microsoft svarade de på ett sätt Eric tyckte var bra och det ströks från listan. Citat från PUB-avtalet *"kunden ger Microsoft tillåtelse att skapa sammanställda, **icke-personliga uppgifter** från data som innehåller pseudonymiserade identifierare"*

  Avseende denna rekommendation har jag utgått från samrådsyttrandet vari det framgår att det saknas en dokumenterad bedömning av Entra ID och Microsofts eventuella egna personuppgiftsansvar i relationen med Umeå Kommun. Om detta har blivit utrett i samförstånd med Microsoft i ett senare skede så förutsätter jag att invändningen från dataskyddsombudet har blivit ombesörjd. Under förutsättning att så är fallet så är inte heller denna rekommendation relevant längre.

- Dokumenterad sekretessprövning enligt 10 kap. 2 a § OSL och 21 kap. 7 § OSL, differentierad per informationskategori.
  - Är inte också detta en bedömning som kommer i vår andra del, per tjänst och sedan per tillämpning av verksamheten?

    Jo, det blir samma situation som för konsekvensbedömningarna.

- Dokumenterad analys av underbiträdeskedjan med fokus på faktiska åtkomstrisker
  - Är det något mer vi ska göra annat än det som redan är sammanställt?

    Om ni väljer att använda Microsoft EU Data Boundary så blir denna rekommendation inte relevant. I annat fall behöver det klarläggas huruvida underbiträden som är etablerade i länder vars lagstiftning medför risk för obehörig åtkomst (så som t.ex. CLOUD Act) kommer att användas. Om så är fallet behöver en Transfer Impact Assessment (TIA) genomföras innan någon behandling av personuppgifter kan utföras utav dessa underbiträden.

Återkom gärna ifall det kvarstår några frågetecken eller oklarheter.

Vänligen,

Thed Lindström

It-rättsjurist

Direct: +46 40 31 42 27

thed.lindstrom@atea.se

Sensitivity: Confidential

From: Thed Lindström <thed.lindstrom@atea.se>
Date: Tuesday, 5 May 2026 at 13:53
To: mattias.wallmark <mattias.wallmark@umea.se>
Cc: Jonas Bokström <jonas.bokstrom@atea.se>
Subject: Re: Juridisk bedömning angående molntjänster och microsoft

Hej Mattias,

Min bedömning är baserad på följande dokument:

- Protokollsutdrag: Beslut av riskbedömning och fortsatt användning av Microsoft (KS-2026/00246, Kommunstyrelsen 2026-04-14)
- Bilaga 1 - Samrådsyttrande från dataskyddsombudet med recommendation gällande Tekniska nämndens anlitande av Microsoft som personuppgiftsbiträde
- Tjänsteskrivelse TN-2026/00081 Beslut riskbedömning och fortsatt användning av Microsoft (Tekniska nämnden 2026-03-31)
- KS invändningar och argumentation

Jag har nu även fått tillgång till rapporten som vi har bistått med och kommer att besvara dina frågor efter att jag har gått igenom den.

Vänligen,

Thed Lindström

It-rättsjurist

Direct: +46 40 31 42 27

thed.lindstrom@atea.se

From: Mattias Wallmark <mattias.wallmark@umea.se>
Date: Tuesday, 5 May 2026 at 08:50
To: Jonas Bokström <jonas.bokstrom@atea.se>; Thed Lindström <thed.lindstrom@atea.se>
Cc: hannes.fries <hannes.fries@umea.se>
Subject: Sv: Juridisk bedömning angående molntjänster och microsoft

Hej!

Nu har jag läst igenom noggrannare och har några följdfrågor. Framför allt eftersom vi har haft stöd av ATEA under hela processen och DSO har också varit med från dag 1. Arbetet har ju delats upp i två faser där den första är med fokus på juridik och Microsoft som leverantör, medan andra delen är bedömning av ett antal tjänster. Med risk att allt material inte var tillgängligt för dig Thed så funderar jag lite vad punkterna i rekommendationerna faktiskt betyder eftersom det inte har nämnts av ATEA tidigare. Se röd text.

- Dokumenterad analys av Microsofts DPA mot artikel 28.3 GDPR.
    - Vi har också tidigare haft juriststöd från ATEA under hela processen och utgick från att detta var täckt i arbetet. Vad är det egentligen som återstår att göra?
- Genomförd transfer impact assessment enligt EDPB Recommendations 01/2020 sex-stegsmetodik.
    - Vi har också tidigare haft juriststöd från ATEA under hela processen och utgick från att detta var täckt i arbetet. Vad är det egentligen som återstår att göra?
- Genomförd och dokumenterad konsekvensbedömning enligt artikel 35 GDPR för de behandlingar som sker i tjänsten.

    - Tolkningen har varit att detta är en bedömning som sker senare, per tjänst och användning i kommunens verksamheter där personsuppgiftsbehandlingen sker. Vad är det som återstår i den juridiska bedömningen av Microsoft och vad är det som behöver kompletteras per tjänst som vi inte har?
- Dokumenterad bedömning av rollfördelningen, särskilt för de delar där Microsoft agerar personuppgiftsansvarig såsom telemetri och delar av Entra ID.
    - Detta har berörts i bedömningen av EntraID. Är det något som saknas där? Dessutom undrar vi om det är klarlagt att Microsoft agerar personuppgiftsansvar för t ex telemetri (vi har bilden att det är anonymiserad telemetridata)?
    - KOMMENTAR: I mötet med Microsoft svarade de på ett sätt Eric tyckte var bra och det ströks från listan. Citat från PUB-avtalet *"kunden ger Microsoft tillåtelse att skapa sammanställda,* ***icke-personliga uppgifter*** *från data som innehåller pseudonymiserade identifierare"*
- Dokumenterad sekretessprövning enligt 10 kap. 2 a § OSL och 21 kap. 7 § OSL, differentierad per informationskategori.
    - Är inte också detta en bedömning som kommer i vår andra del, per tjänst och sedan per tillämpning av verksamheten?
- Dokumenterad analys av underbiträdeskedjan med fokus på faktiska åtkomstrisker
    - Är det något mer vi ska göra annat än det som redan är sammanställt?

Bifogar också dessa två slides som tydliggör lite mer om arbetets syfte och upplägg

@Jonas, vi ser ju att behöva hantera restpunkter från det tidigare arbetet. Hur kan vi lösa det på bästa sätt så vi kan komma i mål med detta?

med vänlig hälsning

Mattias

Från: Thed Lindström <thed.lindstrom@atea.se>
Skickat: Torsdag, 30 april 2026 16:39
Till: Mattias Wallmark <mattias.wallmark@umea.se>
Kopia: jonas.bokstrom <jonas.bokstrom@atea.se>
Ämne: Juridisk bedömning angående molntjänster och microsoft

Du får inte ofta e-post från thed.lindstrom@atea.se. Läs om varför det här är viktigt

Hej,

Här kommer bedömningen av molntjänster i förhållande till TN 2026/00081.
Ursäkta att det kom i sista stund men det tog sin tid att få ihop underlaget.

Trevlig valborg och långhelg!

Vänligen,

Thed Lindström

It-rättsjurist

Direct: +46 40 31 42 27

thed.lindstrom@atea.se

Atea Sverige AB

Pildammsvägen 6

211 46 Malmö

Switchboard: +46 8 477 47 00

atea.se

Outlook

För kännedom och eventuella synpunkter senast 16 augusti

Från Mattias Wallmark <mattias.wallmark@umea.se>
Datum Mån 2026-08-03 15:07
Till Eric Lindström <eric.lindstrom@umea.se>
Kopia TN Diarium SHBK <tndiarium@umea.se>

1 bifogad fil (302 kB)
Juridisk bedömning av molntjänster i förhållande till TN 2026_00081 (feedback efter granskning).pdf;

Hej,

För dataskyddsombudets kännedom med möjlighet till eventuella synpunkter senast 16 augusti inför kommande Teknisk nämnd den 27 augusti, där beslut i ärendet förväntas föreslås.
Kopia till TN diarium för kännedom och diarieföring

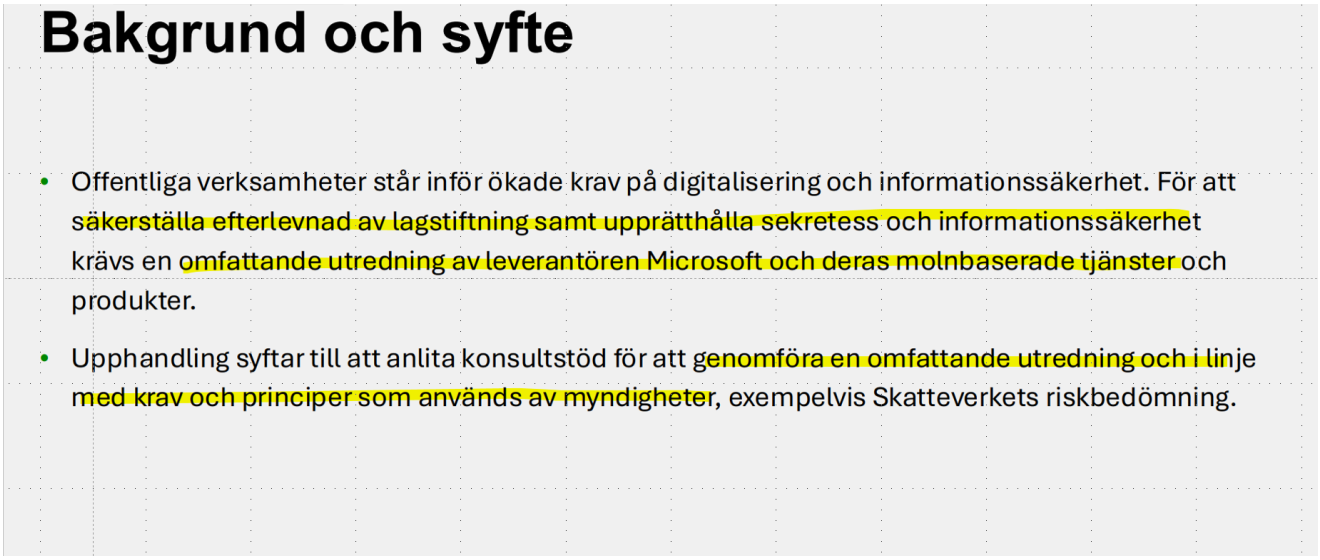
Utifrån KS remissvar (KS-2026/00246) inklusive dess bilagda beslutsunderlag har vi åter anlitat extern jurist som stöd för bedömning och hantering för att ge Tekniska nämnden förutsättningar att förstå och beakta KS synpunkter. Likt tidigare är det ATEA som anlitats men vid detta tillfälle är det en annan jurist än den som först var med i processen.

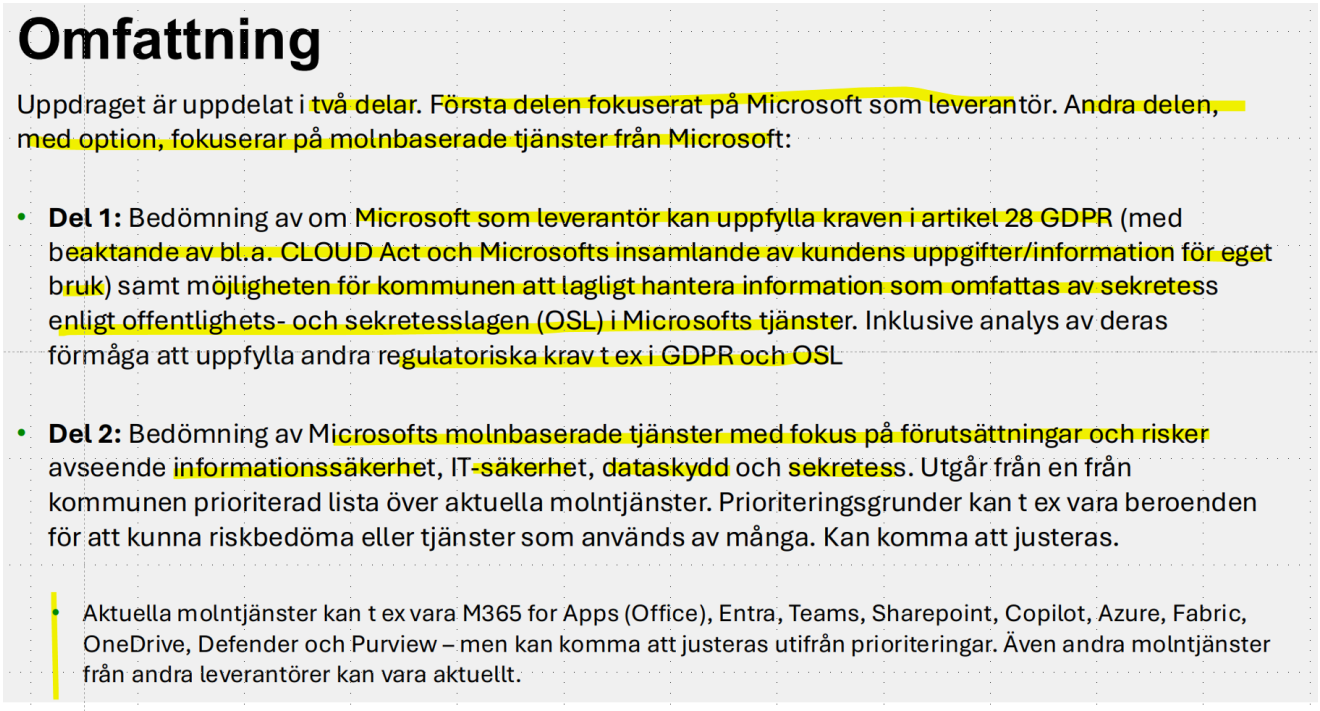
Den första återkopplingen "Juridisk bedömning av molntjänster i förhållande till TN 2026_00081 (feedback efter granskning)" är bifogat detta mejl. Detta väckte en hel del frågetecken som formulerades som frågor enligt nedan:

Nu har jag läst igenom noggrannare och har några följdfrågor. Framför allt eftersom vi har haft stöd av ATEA under hela processen och DSO har också varit med från dag 1. Arbetet har ju delats upp i två faser där den första är med fokus på juridik och Microsoft som leverantör, medan andra delen är bedömning av ett antal tjänster. Med risk att allt material inte var tillgängligt för dig Thed så funderar jag lite vad punkterna i rekommendationerna faktiskt betyder eftersom det inte har nämnts av ATEA tidigare. Se röd text.

- *Dokumenterad analys av Microsofts DPA mot artikel 28.3 GDPR.*
  - *Vi har också tidigare haft juriststöd från ATEA under hela processen och utgick från att detta var täckt i arbetet. Vad är det egentligen som återstår att göra?*
- *Genomförd transfer impact assessment enligt EDPB Recommendations 01/2020 sex-stegsmetodik.*
  - *Vi har också tidigare haft juriststöd från ATEA under hela processen och utgick från att detta var täckt i arbetet. Vad är det egentligen som återstår att göra?*
- *Genomförd och dokumenterad konsekvensbedömning enligt artikel 35 GDPR för de behandlingar som sker i tjänsten.*
  - *Tolkningen har varit att detta är en bedömning som sker senare, per tjänst och användning i kommunens verksamheter där personsuppgiftsbehandlingen sker. Vad är det som återstår i den juridiska bedömningen av Microsoft och vad är det som behöver kompletteras per tjänst som vi inte har?*
- *Dokumenterad bedömning av rollfördelningen, särskilt för de delar där Microsoft agerar personuppgiftsansvarig såsom telemetri och delar av Entra ID.*
  - *Detta har berörts i bedömningen av EntraID. Är det något som saknas där? Dessutom undrar vi om det är klarlagt att Microsoft agerar personuppgiftsansvar för t ex telemetri (vi har bilden att det är anonymiserad telemetridata)?*
  - *KOMMENTAR: I mötet med Microsoft svarade de på ett sätt Eric tyckte var bra och det ströks från listan. Citat från PUB-avtalet "kunden ger Microsoft tillåtelse att skapa sammanställda, **icke-personliga uppgifter** från data som innehåller pseudonymiserade identifierare"*
- *Dokumenterad sekretessprövning enligt 10 kap. 2 a § OSL och 21 kap. 7 § OSL, differentierad per informationskategori.*
  - *Är inte också detta en bedömning som kommer i vår andra del, per tjänst och sedan per tillämpning av verksamheten?*
- *Dokumenterad analys av underbiträdeskedjan med fokus på faktiska åtkomstrisker*
  - *Är det något mer vi ska göra annat än det som redan är sammanställt?*

Bifogade också dessa två slides som tydliggör lite mer om arbetets syfte och upplägg





Svaret denna gång blev följande:

Hej Mattias,

Min bedömning är baserad på följande dokument:

- *Protokollsutdrag: Beslut av riskbedömning och fortsatt användning av Microsoft (KS-2026/00246, Kommunstyrelsen 2026-04-14)*
- *Bilaga 1 - Samrådsyttrande från dataskyddsombudet med recommendation gällande Tekniska nämndens anlitande av Microsoft som personuppgiftsbiträde*
- *Tjänsteskrivelse TN-2026/00081 Beslut riskbedömning och fortsatt användning av Microsoft (Tekniska nämnden 2026-03-31)*
- *KS invändningar och argumentation*

Jag har nu även fått tillgång till rapporten som vi har bistått med och kommer att besvara dina frågor efter att jag har gått igenom den.

Efter att juristen läst igenom tidigare underlag fick vi följande återkoppling (med kommentarer i lila text):

Jag har nu haft möjlighet att granska det underlag som min kollega tog fram till er tidigare, dvs 'Juridisk bedömning av Microsoft som leverantör'. I anledning av det (för mig) tillkomna underlaget har jag reviderat mina ståndpunkter i enlighet med den tillkomna informationen. Se mina svar färgade i lila nedan.

- *Dokumenterad analys av Microsofts DPA mot artikel 28.3 GDPR.*
  - *Vi har också tidigare haft juriststöd från ATEA under hela processen och utgick från att detta var täckt i arbetet. Vad är det egentligen som återstår att göra?*

    Jag hade inte tillgång till det underlaget vid min initiala bedömning. Efter att ha granskat det materialet så står det klart att en s.k. artikel 28-bedömning av Microsoft har skett och finns dokumenterad. Denna rekommendationen kan ni därför bortse ifrån.

- *Genomförd transfer impact assessment enligt EDPB Recommendations 01/2020 sex-stegsmetodik.*
  - *Vi har också tidigare haft juriststöd från ATEA under hela processen och utgick från att detta var täckt i arbetet. Vad är det egentligen som återstår att göra?*

    Denna rekommendation är till följd av kritiken i samrådsyttrandet från dataskyddsombudet. Det relaterar primärt till eventuella tredjelandsöverföringar som kan ske till underbiträden till Microsoft som befinner sig i länder som inte omfattas av ett adekvansbeslut. Detta blir inte relevant om ni kommer att använda er av Microsoft EU Data Boundary.

- *Genomförd och dokumenterad konsekvensbedömning enligt artikel 35 GDPR för de behandlingar som sker i tjänsten.*
  - *Tolkningen har varit att detta är en bedömning som sker senare, per tjänst och användning i kommunens verksamheter där personsuppgiftsbehandlingen sker. Vad är det som återstår i den juridiska bedömningen av Microsoft och vad är det som behöver kompletteras per tjänst som vi inte har?*

    Denna rekommendation är relevant inför behandling av personuppgifter och om ni har aktivt valt att avvakta med denna del till ett senare skede så kan ni bortse från denna rekommendationen i nuläget.

- *Dokumenterad bedömning av rollfördelningen, särskilt för de delar där Microsoft agerar personuppgiftsansvarig såsom telemetri och delar av Entra ID.*
  - *Detta har berörts i bedömningen av EntraID. Är det något som saknas där? Dessutom undrar vi om det är klarlagt att Microsoft agerar personuppgiftsansvar för t ex telemetri (vi har bilden att det är anonymiserad telemetridata)?*
  - *KOMMENTAR: I mötet med Microsoft svarade de på ett sätt Eric tyckte var bra och det ströks från listan. Citat från PUB-avtalet "kunden ger Microsoft tillåtelse att skapa sammanställda, **icke-personliga uppgifter** från data som innehåller pseudonymiserade identifierare"*

    Avseende denna rekommendation har jag utgått från samrådsyttrandet vari det framgår att det saknas en dokumenterad bedömning av Entra ID och Microsofts eventuella egna personuppgiftsansvar i relationen med Umeå Kommun. Om detta har blivit utrett i samförstånd med Microsoft i ett senare skede så förutsätter jag att invändningen från dataskyddsombudet har blivit ombesörjd. Under förutsättning att så är fallet så är inte heller denna rekommendation relevant längre.

- *Dokumenterad sekretessprövning enligt 10 kap. 2 a § OSL och 21 kap. 7 § OSL, differentierad per informationskategori.*
  - *Är inte också detta en bedömning som kommer i vår andra del, per tjänst och sedan per tillämpning av verksamheten?*

    Jo, det blir samma situation som för konsekvensbedömningarna.

- *Dokumenterad analys av underbiträdeskedjan med fokus på faktiska åtkomstrisker*
  - *Är det något mer vi ska göra annat än det som redan är sammanställt?*

    Om ni väljer att använda Microsoft EU Data Boundary så blir denna rekommendation inte relevant. I annat fall behöver det klarläggas huruvida underbiträden som är etablerade i länder vars lagstiftning medför risk för obehörig åtkomst (så som t.ex. CLOUD Act) kommer att användas. Om så är fallet behöver en Transfer Impact Assessment (TIA) genomföras innan någon behandling av personuppgifter kan utföras utav dessa underbiträden.

Avslutningsvis har vi noterat beslutet i USA:s högsta domstol som väcker frågan om USA:s tillsynsorgan kan anses oberoende och om detta kan påverka adekvansbeslutets giltighet. Vi följer utvecklingen genom IMY med beredskap i

händelse av att adekvansbeslutet skulle upphävas i framtiden.

med vänlig hälsning

Mattias Wallmark
IT- och digitaliseringschef
090-16 11 52
mattias.wallmark@umea.se

Umeå kommun
Digital omställning och IT
901 84 Umeå
Besöksadress: Skolgatan 31A
www.umea.se

UMEÅ KOMMUN

Bilaga H

Umeå 2026-08-25

TN-2026/00081

Samrådsyttrande från dataskyddsombudet med rekommendation gällande Tekniska nämndens anlitande av Microsoft som personuppgiftsbiträde

Ersätter tidigare samrådsyttrande lämnat 26-03-31

Sammanfattning

Utifrån tjänsteskrivelsen och därtill befogade handlingar lämnar jag som Tekniska nämndens dataskyddsombud (DSO) följande huvudsakliga rekommendation till nämnden.

Utredningen är inte komplett, det saknas underlag för att kunna göra en fullständig bedömning av om Microsoft uppfyller artikel 28 i GDPR.

- Frågan om det är förenligt med offentlighets- och sekretesslagen att lämna ut personuppgifter till Microsoft är inte prövad och dokumenterad (notera att detta är en annan prövning än den som beskrivs av verksamheten i tjänsteskrivelsen, den behöver också göras men är en senare prövning).
  Rekommendation från DSO: Genomför och dokumentera en sekretessprövning som visar om/att det är förenligt med offentlighets- och sekretesslagen att lämna ut personuppgifter till Microsoft.

- Det finns uppgifter om att Microsoft behandlar nämndens personuppgifter för egna ändamål men det är inte utrett och dokumenterat om och när det i så fall sker och om det är lagligt för Microsoft och nämnden att så sker. Om denna fråga är outredd får det effekten att varken sekretess- eller artikel 28 frågan går att bedöma.
  Rekommendation från DSO: Utred och dokumentera om och i så fall på vilken grund som Microsoft använder personuppgifter de får som personuppgiftsbiträde för egna ändamål och om behandlingen och överföringen av personuppgifter från nämnden till Microsoft är laglig enligt GDPR (får effekt på både artikel 28 bedömningen och sekretessprövning).

- Det saknas också utredning/bedömning om den föreslagna skyddsåtgärden ”Microsoft EU Data Boundary” ger ett faktiskt skydd mot att myndigheter från länder utanför EU/EES får del av nämndens personuppgifter.
  Rekommendation från DSO: Säkerställ och dokumentera att inget av Microsoft anlitat underbiträde i EU/EES (eller dess moderbolag) omfattas av lag i annat land med extraterritoriell effekt. Se över och justera avtalet med Microsoft vid behov för att säkerställa ovanstående. Bevaka frågan fortlöpande.

- Det finns ingen bedömning eller dokumentation kring riskerna gällande utlämnande enligt CLOUD Act till Australien eller Storbritannien.
  Rekommendation från DSO: Utred och bedöm ev. risker och lagligheten kopplade till Microsofts överföring av personuppgifter till Australien och Storbritannien. Dokumentera bedömningen.

Av utredning framgår att Microsoft inte erbjuder något avtalsrättsligt skydd gällande garantier att endast behandla personuppgifter i enlighet med GDPR och svensk lag. Istället framgår att Microsoft instrueras att bryta mot lag. Det framgår vidare av andra källor att Microsoft följer ett beslut om utlämnande enligt CLOUD Act och att en behandling av personuppgifter och efterföljande överföring till USA enligt CLOUD Act sker i strid med

reglerna i GDPR. Detta sammantaget med att europeiska medborgares rättigheter inte anses kunna skyddas i USA (vid överföringar utanför adekvansbeslutet vilket är vad som sker vid en CLOUD Act överföring) innebär att Microsoft på befintligt underlag inte kan anses uppfylla kraven i artikel 28 GDPR.

Rekommendation från DSO: Säkerställ att avtalet med Microsoft och instruktionen i personuppgiftsbiträdesavtalet, som utgångspunkt, förhindrar Microsoft och dess underbiträden att tillgodose en begäran om utlämnande enligt CLOUD Act eller annan utländsk lag som skulle innebära en behandling i strid med GDPR eller annan svensk lag. Bedöm och dokumentera risken för att Microsoft trots förbud ändå tillmötesgår en, enligt svensk lag, olaglig begäran och vidta lämpliga risksänkande åtgärder. Sådan åtgärd kan t.ex. vara att förena avtalsbrott med avskräckande viten och att regelbundet genom tredje part kontrollera avtalsefterlevnaden så att det säkerställs att avtalet har faktisk effekt. Fortsätt följa utvecklingen kring adekvansbeslutet och ha beredskap att snabbt kunna agera ifall rättsläget förändras.

Om avtalet inte går att ändra och personuppgifter ska behandlas i Microsofts tjänster rekommenderas att åtgärder vidtas som skyddar personuppgifterna från Microsoft t.ex. kryptering där nyckeln inte hanteras av Microsoft utan av kommunen eller betrodd part i EU/EES, eller annan åtgärd som bedöms som lämplig för att skydda informationen från Microsoft (och i förlängningen också utländska myndigheter).

Om ingen av ovanstående åtgärder (kan)vidtas eller sekretessprövningen visar att personuppgifter inte får lämnas ut till Microsoft avråds nämnden från att fortsätta anlita Microsoft som personuppgiftsbiträde tills det säkerställts att behandlingen följer reglerna i GDPR och svensk lag. I dagsläget kan Microsoft inte anses uppfylla kraven för att kunna anlitas som personuppgiftsbiträde enligt GDPR.

Inledning

Dataskyddsombudet ska informera och ge råd till personuppgiftsansvarig (de kommunala nämnderna) och deras anställda om deras skyldigheter enligt GDPR och andra EU och nationella dataskyddsbestämmelser (art. 39.1a GDPR). Dataskyddsombudet ska också bl.a. övervaka efterlevnaden av GDPR och annan EU och nationell dataskyddslagstiftning samt nämndernas strategi för skydd av personuppgifter (art. 39.1b GDPR). Utifrån detta görs följande bedömning och ges följande rekommendationer till Tekniska nämnden. Detta yttrande ersätter tidigare lämnat yttrande (26-03-31) då aktuellt beslutsförslag och underlag markant skiljer sig från tidigare förslag som lämnades till nämnden. Dataskyddsombudets rekommendationer finns i slutet av varje avsnitt och är markerade med *kursiv text*.

Microsoft som personuppgiftsbiträde

Personuppgiftsbiträde

För att få anlita ett personuppgiftsbiträde krävs enligt artikel 28.1 i GDPR bl.a. att biträdet ger *”… tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.*” Detta kompletteras sedan av art 5.2 i GDPR som säger att personuppgiftsansvarig (nämnd) ska kunna visa att kraven i artikel 28 efterlevs. Detta innebär i praktiken att Tekniska nämnden måste säkerställa att Microsoft följer GDPR och kunna ”bevisa” att Microsoft uppfyller ovan angivna krav innan företaget får anlitas som personuppgiftsbiträde. Om biträdet efter anlitande vid något tillfälle inte längre uppfyller dessa krav får det inte längre anlitas.

CLOUD Act och tredjelandsöverföringar

Ett av de identifierade problemen med anlitandet av Microsoft (eller annan amerikansk molnleverantör som t.ex. Google, Amazon, Oracle, osv.) som personuppgiftsbiträde är en amerikansk lag som heter CLOUD Act. CLOUD Act ”kortsluter” den normala vägen när uppgifter ska lämnas ut mellan stater. Myndigheter i USA och andra anslutna länder kan använda CLOUD Act för att via domstol begära ut data direkt från Microsoft i stället för att gå via bilaterala överenskommelser (direkta överenskommelse mellan två eller flera länder). CLOUD Act gäller oavsett var i världen som uppgifterna lagras så länge det är ett amerikanskt företag (av viss typ) som har informationen. Det är alltså inte ett skydd mot CLOUD Act att personuppgifter lagras av Microsoft i Sverige eller Europa. CLOUD Act innehåller också en möjlighet till s.k. ”gag order”, kallas också för ”protective order” (se punkten 28), som innebär att Microsoft inte alltid får berätta för sina kunder att de tillgodosett en CLOUD Act begäran. Det finns också möjlighet för andra länder att ansluta sig till CLOUD Act.

Dokumentation och riskbedömning behöver därför inte bara ske för överföringar till USA utan också övriga anslutna länder (hittills har Australien och Storbritannien anslutit sig).

Den behandling som sker för att uppfylla en CLOUD Act begäran saknar, enligt Europeiska dataskyddsstyrelsens (EDPB) juridiska bedömning av CLOUD Act, rättslig grund och är alltså olaglig i sig. Den granskning av amerikansk lagstiftning som skett av EU kommissionen som det hänvisas till i ”*Bilaga A - Juridisk bedömning av Microsoft som leverantör (ATEA)*”, gäller endast överföring av uppgifter som omfattas av ”EU-US Data Privacy Framework” (adekvansbeslutet). Adekvansbeslutet gäller bara för överföringar som sker till amerikanska verksamheter som anslutit sig till ramverket och finns listade här Data Privacy Framework List. Amerikanska myndigheter finns inte listade och adekvansbeslutet omfattar alltså inte överföringar till amerikanska myndigheter. Till skillnad från vad som påstås i bilagorna A och B är det alltså tydligt att det inte är förenligt med GDPR att behandla och överföra personuppgifter för att tillgodose en CLOUD Act begäran från USA. Det finns ingen utredning gällande möjligheten att överföra uppgifter till australiensiska och brittiska myndigheter i underlaget, den frågan är alltså fortfarande oklar och kan därför inte bedömas i dagsläget.

Det rekommenderas att lagligheten av och risker med att Microsoft överför personuppgifter vid en CLOUD Act begäran till Australien och Storbritannien utreds och bedöms samt att detta dokumenteras.

Ger Microsoft tillräckliga garantier att vidta åtgärder så att behandlingen efterlever kraven i GDPR?

Avtalsrättsligt skydd

Det finns ett tecknat personuppgiftsbiträdesavtal (PUB-avtal) mellan Tekniska nämnden och Microsoft. Tekniska nämnden har i praktiken liten eller ingen möjlighet att påverka den behandling som Microsoft ska utföra åt nämnden då Microsoft ensidigt skrivit avtalet och hittills inte varit villiga att gå med på förändringar av texten. Samtidigt är det enligt GDPR Tekniska nämnden som är ansvariga ifall instruktionen Microsoft skrivit bryter mot lag eller om nämnden anlitar ett biträde de vet inte kommer följa avtal eller instruktion.

Av den utredning som finns och där jag som dataskyddsombud varit delaktig eller i övrigt känner till kan i huvudsak konstateras följande.

Av Tekniska nämndes avtal med Microsoft benämnt ”Dataskyddstillägg för Microsofts produkter och tjänster” framgår under punkten ”Utlämnande av behandlade data” bl.a. följande ” … *Microsoft ska inte lämna ut eller ge åtkomst till Behandlade data till rättsvårdande myndighet såvida inte detta krävs enligt lag. Om rättsvårdande myndighet skulle kontakta Microsoft med en begäran om behandlade data ska Microsoft försöka*

hänvisa den rättsvårdande myndigheten till att begära dessa data direkt från Kunden. Om Microsoft är tvungna att lämna ut eller ge åtkomst till Behandlade data till rättsvårdande myndighet ska Microsoft omgående meddela Kunden och tillhandahålla en kopia av begäran, såvida inte Microsoft är förhindrande enligt lag att göra så …". I Bilaga C till ovan angivna avtal framgår bl.a. att om " … *Microsoft eller något av deras koncernbolag fortfarande tvingas lämna ut personuppgifter ska Microsoft endast lämna ut den minsta mängd av dessa data som är nödvändig för att uppfylla ordern om tvingat utlämnande …*"

DoIT har begärt ett förtydligande från Microsoft ifall de ger några garantier för att detta inte skulle innebära en behandling i strid med GDPR t.ex. genom att Microsoft skulle tillgodose en CLOUD Act begäran. På denna begäran svarade Microsoft bl.a. följande i meddelande inkommen till Tekniska nämnden den 7 november 2025 "*… Dessvärre kan Microsoft meddela att vi inte kommer kunna ge några ytterligare förtydligande, utfästelser eller kommentarer i dagsläget kopplat till innebörden av denna text. Microsoft hänvisar istället till redan gjorda utfästelser i avtal och till principer för datautlämning som finns publicerade på Microsofts webbsidor.*". Det vill säga ingen utfästelse att endast behandla personuppgifter enligt GDPR och svensk lag. Microsoft erbjuder alltså inget avtalsrättsligt skydd gällande garantier att endast behandla personuppgifter i enlighet med GDPR.

Det är också allmänt känt, enligt Microsofts egen utsaga, att företaget lämnar ut kunders data vid en lagakraftvunnen begäran enligt bl.a. CLOUD Act https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data och https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/

I dagsläget är avtalet mellan Tekniska nämnden och Microsoft skrivet med utgångspunkten att Microsoft kommer (och instrueras av Tekniska nämnden) att bryta mot GDPR och annan svensk lag om det krävs för att tillgodose utländsk lag med extraterritoriell effekt t.ex. CLOUD Act. Hur ofta ett utlämnande kan komma att ske är här irrelevant att bedöma eftersom utlämnandet i sig redan är förbjudet. Utlämnandet får som utgångspunkt inte inträffa (inte ens en gång) och åtgärder ska vara vidtagna för att säkerställa detta, t.ex. förbud i avtal. Det som ska bedömas är alltså inte HUR OFTA ett utlämnande kan ske (eftersom det är förbjudet att lämna ut) utan OM ett utlämnande trotts skyddsåtgärder ändå kan ske. Risken för utlämnande vid en begäran enligt CLOUD Act är här enligt avtalet med Microsoft 100% (avtalet säger att det är vad som ska ske och Microsoft själva säger att så sker). Detta innebär att med befintligt avtal kan Microsoft inte anses uppfylla kraven i artikel 28 GDPR då avtalet har lagbrott som utgångspunkt (i stället för tvärtom som det borde vara). De förslagna åtgärderna i tjänsteskrivelsen varken åtgärdar eller minskar den risk som avtalet innebär/medför.

Det rekommenderas därför att avtalet som Tekniska nämnden har med Microsoft ändras så att det har lagefterlevnad som utgångspunkt genom att Microsoft åtar sig att endast tillmötesgå begäranden om utlämnande från utländska myndigheter om det sker i enlighet

med GDPR och svensk lag i övrigt samt med Tekniska nämndens föregående tillstånd. Den risk som sedan ska bedömas är om Microsoft kommer följa avtalet, där kan en risksänkande åtgärd vara att förena utlämnande med avskräckande viten samt följa upp avtalet regelbundet och låta extern part (ska tillåtas i personuppgiftsbiträdesavtalet enligt artikel 28 GDPR) granska så att inget utlämnande i strid med avtalet skett.

Microsofts egen hantering av de personuppgifter nämnden ansvarar för

Det har hittills identifierats en situation där Microsoft gör sig själva till personuppgiftsansvarig för information de får som biträde (det kan ev. finnas fler då frågan ännu inte är fullt utredd t.ex. skulle det kunna ske genom CSAM förordningen och vid en CLOUD Act begäran?). I den pågående konsekvensbedömningen av Entra ID, (den tjänst som används för att skapa användare i Microsofts program/tjänster) framgår att Microsoft gör sig själva till personuppgiftsansvariga för vissa personuppgifter de får av Tekniska nämnden som nämndens biträde. Detta är som utgångspunkt förbjudet i GDPR och kan endast ske i vissa undantagsfall. Det har, så vitt det gjorts känt för mig som nämndens dataskyddsombud, inte skett någon analys eller dokumenterad bedömning ifall denna hantering är förenligt med GDPR. Utan denna dokumentation går det heller inte att göra en korrekt prövning av om kraven i art. 28 är uppfyllda eller om utlämnande enligt OSL är tillåten (vilket i sin tur påverkar art. 28 prövningen).

Det rekommenderas därför att det identifieras om och när Microsoft gör sig själva till personuppgiftsansvarig för uppgifter de får som nämndens biträde och att det bedöms och dokumenteras om denna hantering är förenlig med GDPR. Denna bedömning kan sedan läggas till den sammantagna bedömningen av lagligheten av anlitandet av Microsofts som biträde. Det har också påverkan på sekretessfrågan kopplat till om Microsoft endast tekniskt bearbetar och lagrar nämndens information vilket i sin tur har påverkan på om Microsoft kan anses uppfylla kraven i artikel 28 GDPR.

Underbiträden och tredjelandsöverföringar

Art 28.4 GDPR ställer krav på att personuppgiftsbiträdet (här Microsoft) ska överföra de avtalsvillkor som gäller för dem på ev. underbiträden. Detta innebär, med Microsofts avtalstext, att i de fall där Microsoft anlitar ett underbiträde där underbiträdet (eller dess moderbolag enligt vissa lagar) omfattas av nationell lagstiftning som kräver att uppgifterna lämnas ut till det landets myndigheter kan också dessa länder (utöver de som ges möjlighet enligt CLOUD Act) få del av uppgifter som lämnats ut till Microsoft. Enligt förvaltningen är denna fråga hanterad genom att avtal tecknats med Microsoft som ska förhindra att data hanteras av biträden utanför EU/EES s.k. ”Microsoft EU Data Boundary”. Med undantag för ev. underbiträden som kan omfattas av extraterritoriell verkan inom EU/EES (på samma sätt som Microsoft gör), kan detta vara en lämplig åtgärd för att förhindra att data behandlas i strid med GDPR av underbiträden. Det är dock inte dokumenterat ifall Microsoft anlitar

underbiträden i Europa som kan omfattas av lagar med extraterritoriell effekt vilket gör det faktiska skyddet av vald åtgärd svårbedömt på aktuellt underlag.

Det rekommenderas därför att det säkerställs och dokumenteras att de underbiträden som Microsoft anlitar inom EU/EES (och deras moderbolag) inte omfattas av någon nationell lagstiftning utanför EU/EES med extraterritoriell effekt så att effektiviteten av skyddsåtgärden ”Microsoft EU Data Boundary” kan bedömas samt att löpande uppföljning sker av frågan (primärt att byten av underbiträden bevakas och bedöms löpande). Vid behov kan avtalet med Microsoft komma att behöva justeras.

Framgår det att Microsoft säkerställer registrerades rättigheter?

De personuppgifter som förs över till USA av Microsoft och som inte omfattas av adekvansbeslutet (t.ex. överföringar för att uppfylla CLOUD Act) har inte motsvarande skydd som de har i EU/EES, se t.ex. EU-domstolens dom Schrems ii (st 185). Av de avtalshandlingar jag fått del av framgår att det inte finns några avtalsrättsliga förbud mot sådana överföringar, det är också allmänt känt att Microsoft gör sådana överföringar till USA. Microsoft kan alltså inte, på befintlig utredning, anses kunna garantera att registrerades rättigheter skyddas om personuppgifter lämnas ut till dem främst p.g.a. att de överför personuppgifter till USA (i strid med GDPR) där registrerade inte har rättigheter motsvarande de som ges i GDPR. Verksamhetens förslag på skyddsåtgärder i tjänsteskrivelsen åtgärdar eller minskar inte denna risk för registrerade.

Det är i dagsläget inte utrett eller dokumenterat vad som gäller när Microsoft överför personuppgifter till andra länder än USA (enligt CLOUD Act) eller ifall någon av underbiträdena inom EU/EES omfattas av sådan nationell lagstiftning som gör att de behöver lämna ut nämndens personuppgifter till utländska myndigheter utanför EU/EES. Det går därför inte att göra en fullständig bedömning av frågan i dagsläget. Det åligger dock Tekniska nämnden enligt GDPR att kunna visa att Microsoft kan säkerställa registrerades rättigheter när de anlitas som personuppgiftsbiträde.

Det rekommenderas därför att frågorna i ovanstående stycke utreds så att det går att göra en bedömning om Microsoft kan anses säkerställa registrerades rättigheter. Denna utredning och bedömning bör dokumenteras och ev. risker som identifieras bör åtgärdas.

Offentlighets- och sekretesslagen

GDPR ser offentlighets- och sekretesslagen (OSL) som ett organisatorisk skydd. Detta innebär att nämnden också måste göra en bedömning av om utlämnande av personuppgifter till Microsoft uppfyller kraven i OSL för att det ska gå att göra en fullständig bedömning av om anlitandet av Microsoft som personuppgiftsbiträde är förenligheten med GDPR. Utifrån vad som framkommit ovan bör det vid en sådan prövning läggas särskild vikt vid 21 kap. 7 § OSL

som i huvudsak säger att om det kan antas att personuppgifter efter utlämnande kommer behandlas i strid med GDPR föreligger sekretess (notera att detta innebär att alla typer av personuppgifter omfattas av sekretess inte bara de som ”typiskt” klassas som sekretess t.ex. uppgifter inom socialtjänst eller hälsovård). Då avtalet med Microsoft inte säkerställer att personuppgifter endast behandlas i enlighet med GDPR utan istället uttryckligen beskriver och instruerar hantering som står i strid med GDPR gör att det finns särskild anledning att föra resonemang kring om det kan antas att en behandling i strid med reglerna i GDPR kommer ske om personuppgifter lämnas ut till Microsoft. Frågan om lagligheten av att Microsoft gör sig själv till personuppgiftsansvarig för uppgifter företaget får som biträde och i så fall på vilken grund är också av stort intresse här. Frågan är dock inte utredd av verksamheten i befintligt underlag.

Gällande undantaget i 10 kap. 2a § OSL som tas upp i tjänsteskrivelsen blir frågan om Microsoft i något skede behandlar personuppgifter för egna ändamål avgörande för att kunna bedöma att företaget endast behandlar personuppgifter för teknisk bearbetning och lagring, vilket är en förutsättning för att paragrafen överhuvudtaget ska kunna bli aktuell. Denna fråga är inte utredd och det rekommenderas därför ovan att så sker. I prövning av aktuell paragraf bör också vägas in syftet med skyddet som 21:7 OSL ska ge registrerade, typen av personuppgifter, volymen av personuppgifter och kategorier av registrerade när man gör olämplighetsbedömningen, m.m. Då någon sekretessprövning med avvägningar inte finns dokumenterad (ingen av bilagorna i tjänsteskrivelsen innehåller någon sådan) är det svårt att säga något om mer i frågan här.

Notera att den sekretessprövning som beskrivs ovan är en annan prövning än den som beskrivs i tjänsteskrivelsen (den behöver också göras) här är det frågan om en generell prövning utifrån frågan om det är möjligt att lämna ut personuppgifter till Microsoft oavsett typ av personuppgift eller Microsoft system, som behövs för art. 28 prövningen.

Det rekommenderas att en sekretessprövning för utlämnande av personuppgifter till Microsoft genomförs och dokumenteras, denna bör sedan utgöra en del av prövningen om Microsoft kan anses uppfylla kraven i artikel 28.

Framgår det av underlaget att det är visat att det är möjligt att anlita Microsoft som personuppgiftsbiträde (är artikel 28 i GDPR uppfylld)?

Det finns fortfarande flera outredda frågetecken som behöver rätas ut för att det ska gå att göra en mer säker bedömning av frågan. Utifrån vad som framkommit av utredningen, tjänsteskrivelsen och bifogade dokument framgår dock i huvudsak följande.

Microsoft lämnar inte avtalsrättsliga garantier att de kommer följa GDPR och skydda registrerades rättigheter. Istället framgår motsatsen i avtalen. Microsoft gör sig själv till personuppgiftsansvarig för personuppgifter de får som personuppgiftsbiträde på oklar rättslig grund och omfattning. Microsoft uppfyller CLOUD Act begäranden. När de gör det behandlar de personuppgifter i strid med GDPR men lägger formellt över ansvaret på

Tekniska nämndens som då förväntas stå risken. Genom att de överför personuppgifter till USA utanför adekvansbeslutet kan Microsoft inte anses garantera registrerades rättigheter. Det kan inte heller uteslutas att det sker annat utlämnande i strid med GDPR men frågan är inte helt utredd. Det är inte heller utrett och dokumenterat om/att ett utlämnande av personuppgifter till Microsoft är förenligt med OSL.

Då det inte finns komplett underlag går det inte att göra en fullständig bedömning av om Microsoft uppfyller kraven i artikel 28 GDPR, eller inte. Det har därför rekommenderats att ytterligare utredning görs så att nämnden får ett komplett underlag för prövningen om möjligheten att anlita Microsoft som personuppgiftsbiträde.

På befintligt underlag kan det dock inte anses visat att Microsoft ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att kraven i GDPR artikel 28 är uppfyllda och registrerades rättigheter skyddas eller att nämnden uppfyller kraven i artikel 5.2, 24, 28 och 32 vid anlitandet av Microsoft som underbiträde.

Det rekommenderas därför, om Microsoft (fortsatt) ska anlitas som nämndens biträde, att åtgärder vidtas för att antingen säkerställa att Microsoft som utgångspunkt endast behandlar personuppgifter i enlighet med GDPR och annan svensk lag eller att personuppgifter som hanteras i Microsofts tjänster skyddas från Microsoft t.ex. genom kryptering där nyckeln inte hanteras av Microsoft utan av kommunen eller betrodd part i EU/EES. En fortsatt behandling av personuppgifter i Microsofts tjänster utan skyddsåtgärder bedöms i nuläget inte vara förenlig med reglerna i GDPR och kan innebära skada för både registrerade och för nämnden.

Eric Lindström

Dataskyddsombud

UMEÅ KOMMUN

Riktlinje

Dokumentansvarig: Informationssäkerhetssamordnare	**Dokumentdatum:** 2021-12-07
Godkänd av: Kommunstyrelsen	**Reviderad:** 2025-02-11

Riktlinjer för informationssäkerhet

Innehåll

Informationsklass: Öppen

Revisionshistorik: se sista sidan

Inledning

Umeå kommuns informationssäkerhetspolicy är ett övergripande dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet. Detta dokument – Riktlinjer för informationssäkerhet – kompletterar informationssäkerhetspolicyn med mer detaljerad information och regler för hur information får hanteras inom kommunen. Dessa riktlinjer är fastställda av kommunstyrelsen.

Riktlinjernas omfattning

Dessa riktlinjer innehåller information och regler gällande säkerhet vid all hantering av information inom Umeå kommun. Riktlinjerna gäller för alla verksamheter i Umeå kommun, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från dessa. Riktlinjerna gäller inte för kommunens bolag, utan dessa beslutar om informationssäkerhetspolicy och riktlinjer för informationssäkerhet inom egen verksamhet. I vissa fall kan ändå dessa riktlinjer gälla för kommunens bolag, liksom för andra externa aktörer, exempelvis när dessa använder sig av kommunens informationstillgångar, eller då det finns särskilda behov av samordning.

Struktur och läsanvisningar

För att ge god läsbarhet är dokumentet uppdelat i fyra kapitel (A-D) som riktar sig till olika målgrupper:

Kapitel		Innehåll	Primär målgrupp	Sidor
A	Informationssäkerhet för medarbetare	Information och riktlinjer för hur information ska hanteras i olika situationer	Alla medarbetare	11–36
B	Styrning av informationssäkerhet	Ansvarsfördelning för informationssäkerhet. Information och riktlinjer för hur arbetet med informationssäkerhet ska bedrivas.	Verksamhetsansvariga, Informationsägare, alla som arbetar med IT-, eller informationssäkerhet	37–54
C	Informationssäkerhet i verksamhetsnära förvaltning	Information och riktlinjer för informationssäkerhet i förvaltningsobjekt som t.ex system och grupper av system.	Informationsägare, objektägare och förvaltningsledare	55–67
D	Informationssäkerhet i IT-miljön	Information och riktlinjer för hur information och IT ska hanteras inom IT-miljön, dvs. IT- och cybersäkerhet.	Chefer och medarbetare på IT funktionen	68–98

Varje kapitel består både av informativa avsnitt och av riktlinjer som är obligatoriska.

Samtliga riktlinjer är numrerade och i tabellform med svart huvud. Rader som innehåller riktlinjer för konfidentiell information och höga skyddskrav har röda linjer, tjockare linje och nämnda termer är dessutom fetmarkerade. Exempel från Kapitel A om lagring i molntjänster:

Riktlinjer för lagring i molntjänster	
A 5.12	Umeå kommuns information får inte lagras i *personliga* molntjänster (Dropbox mfl).
A 5.13	**Hög Sekretess** (Röd) information får inte lagras i molntjänster

Andra tabeller, som inte innehåller riktlinjer utan är mer av illustrerande karaktär, har tabellhuvuden i annan färg.

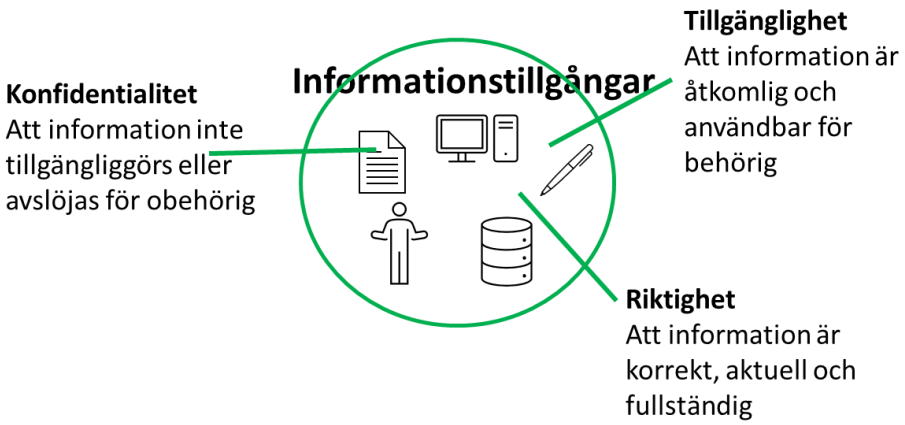
Informationsklassning är en central del i kommunens arbete med informationssäkerhet och finns med genomgående i riktlinjerna. Hur information klassas ska styra i vilken grad informationen ska skyddas. Umeå kommuns modell för informationsklassning beskrivs i Kapitel B och information och regler för hur information ska klassas och skyddas utifrån denna återfinns i respektive kapitel. Liksom vår informationssäkerhetspolicy är dessa riktlinjer baserade på den svenska och internationella standarden SS-ISO/IEC 27002.

Introduktion till informationssäkerhet

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Detta innefattar information i alla dess former (text, ljud, bilder, film osv) och oavsett hur information lagras, bearbetas och kommuniceras. Det kan vara med stöd av IT, papper eller direkt av oss människor i form av tal. Medan IT-säkerhet fokuserar på säkerhet i IT-baserad informationshantering handlar informationssäkerhet alltså om all information, oavsett form. Detta inkluderar förutom information i IT-system även pappersbaserad information och information som finns i våra huvuden.

Information och de resurser som används för att hantera information benämns informationstillgångar. Informationssäkerhet utgörs av tre aspekter; att informationstillgångar ska vara konfidentiella, riktiga och tillgängliga (se Figur 1)

Figur 1



Olika typer av händelser (incidenter), som kan vara avsiktliga eller oavsiktliga, kan försämra konfidentialiteten, riktigheten eller tillgängligheten hos informationstillgångar. Information kan på ett oönskat sätt till exempel stjälas, raderas, förändras, avslöjas för obehöriga eller göras otillgänglig. En viss informationstillgång har krav på sig gällande de tre aspekterna som kan vara interna eller härledas från rättsliga krav eller förväntningar och behov från externa aktörer. Rättsliga krav i form av lagar, förordningar, föreskrifter och avtal ställer krav på en verksamhets informationshantering som ofta inbegriper krav på informationens konfidentialitet, riktighet och tillgänglighet. Dessutom har ofta externa aktörer behov och förväntningar som påverkar organisationens informationssäkerhet. Vad som är lämplig nivå av skydd för en viss informationstillgång beror på dessa krav, hotbild, och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras osv.

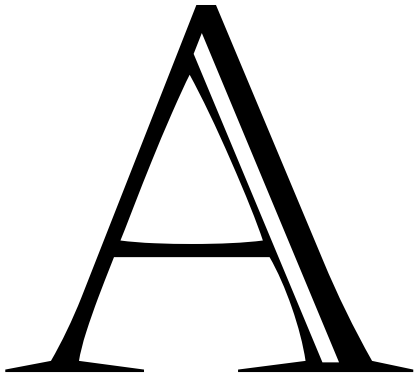
Termer och definitioner

Termer inom Informations- och IT-säkerhet är beskrivna i tabell på kommande sidor. Ytterligare termer rörande informationsförvaltning finns beskrivna i Umeå kommuns kvalitetsledningssystem, DOK.

Term	Definition
Autentisering	Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara.
Behörighet	Tilldelade rättigheter att använda information eller en IT-resurs på ett specificerat sätt.
Data	Omtolkningsbar framställning av information på ett formaliserat sätt lämpligt för kommunikation, tolkning eller bearbetning.
E-postbluff/ E-mail spoofing	En form av spam eller phishing, där kriminella avsändare förfalskar avsändarens e-postadress till en e-postadress som mottagaren litar på i syfte att orsaka skada i någon form
IKT	Informations- och Kommunikationsteknik
incident	enskild eller flera oönskade eller oväntade händelser som har negativa konsekvenser för verksamheten
Information	Kunskap om objekt, såsom fakta, händelser, saker, processer eller idéer, inklusive begrepp, som inom ett visst sammanhang har en särskild betydelse.
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss information
Informationssäkerhet	Bevarande av informationens konfidentialitet, riktighet och tillgänglighet
Informationssäkerhetsincident	enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet

Informationssäkerhetspolicy	Organisationens viljeinriktning med informationssäkerhet uttryckt av organisationens ledning.
Informationstillgång	En mängd information, definierad och hanterad som en enda enhet, så att den kan förstås, delas, skyddas och utnyttjas effektivt. Informationstillgångar har igenkännligt och hanterbart värde, risk, innehåll och livscykler.
IT-resurs	IT-baserad komponent som hanterar information, t.ex. system, verktyg, tjänster och infrastruktur i form av mjuk- och/eller hårdvara
IT-säkerhet	Säkerhet i IT-resurser för att uppnå och upprätthålla informationssäkerhet
Konfidentialitet	Att information inte tillgängliggörs eller avslöjas till obehörig
Ledningssystem för informationssäkerhet (LIS)	Ett sätt för organisationens ledning att på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering.
Mobila enheter	Lättportabla IT-resurser såsom bärbara datorer, mobiler, läsplattor mm
Molntjänst	Molnbaserad tjänst, (på engelska: cloud-based service) – tjänst som tillhandahålls via Internet från ett nätverk av servrar. I princip ska användaren inte behöva ha mer än en webbläsare och internetanslutning för att använda tjänsten.
Outsourcing	Utläggning av delar av ett företags eller myndighets produktion eller annan verksamhet till ett annat företag
Riktighet	Att information är korrekt, aktuell och fullständig
Sekretess	Förbud att i offentlig verksamhet röja uppgifter muntligen eller genom utlämnande av allmän handling. Regler om sekretess finns i offentlighets- och

	sekretesslagen respektive offentlighets- och sekretessförordningen.
Skadlig kod/program/Malware	En form av programvara som kriminella har skapat i syfte att infektera datorer och andra enheter. Detta kan t.ex. vara virus, trojaner, maskar, ransomware, spyware och adware
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs
Stark autentisering	Som stark autentisering räknas identifiering av en person och verifiering av personens autenticitet
Tillgänglighet	Att information är åtkomlig och användbar av behörig.
Verksamhetskritiska system	Kritiska system som har klassats med höga krav på konfidentialitet, integritet och/eller tillgänglighet



Kapitel A: Informationssäkerhet för medarbetare

Inledning

Detta kapitel vänder sig till alla medarbetare vid Umeå kommun. Riktlinjerna gäller även extern personal som har åtkomst till Umeå kommuns information, exempelvis inhyrda konsulter. Riktlinjerna beskriver det ansvar man som medarbetare har vid hantering av information i Umeå kommun och vilka regler som gäller. Umeå kommun är en stor organisation med många skilda verksamheter. Kompletterande regler till riktlinjerna kan därför finnas lokalt. Avvikelser från dessa riktlinjer får dock aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller. Dessa riktlinjer finns på informationssäkerhetssidan på Umeå kommuns intranät: Umeå kommun informationssäkerhet, på den sidan finns information om arbetet med informationssäkerhet i Umeå kommun samlad.

A1 Övergripande regler

Följande regler är övergripande och sammanställer grundläggande informationssäkerhetskrav på medarbetare:

Övergripande regler	
A 1.1	Medarbetare ska vara medveten om sin skyldighet att rapportera informationssäkerhetsincidenter och -brister i Umeå kommuns informationshantering och IT-säkerhet. Detta ska göras till IT Kundsupport eller till närmaste chef. En incident som rör personuppgifter rapporteras via IT

	Självservice. Genom incidentrapporteringen har vi chans att förbättra vårt informationssäkerhetsarbete. En incident kan vara skadlig kod (virus), att personuppgifter har hamnat i orätta händer eller hanterats felaktigt, ett dataintrång eller stöld och förlust av utrustning innehållandes information.
A 1.2	Du som medarbetare har ansvar att kontrollera informationsklass så att du kan vara säker på att informationen får rätt skydd. Informationsklass kan vara noterat på sidhuvud/sidfot eller elektroniskt i systemet.
A 1.3	Lösenordet som medarbetare skapar för sin inloggning i Umeå kommuns nätverk ska ha minst 12 tecken, innehålla en blandning av versaler, gemener och siffror. Forskning visar att ett lösenord på 12 tecken tar lång tid att knäcka.
A 1.4	Det är otillåtet att dela på personliga konton. Varje individ måste kopplas till – och vara ansvarig för sina handlingar. Delar du ditt konto så blir du ansvarig för den aktivitet som kan kopplas till kontot – oavsett om det var någon annan som utförde handlingen eller inte.
A 1.5	Medarbetare ska bara öppna länkar eller bifogade filer i e-postmeddelanden från betrodda avsändare. Det absolut vanligaste sättet att sprida skadlig kod för att stjäla information eller sabotera är att lura användare att klicka på länkar eller öppna bifogade filer i e-post.
A 1.6	Medarbetare får inte använda e-postadresser med domännamnet umea.se för privat bruk som registrering av ett privat konto i kommersiella tjänster. Sådan registrering kan medföra att Umeå kommun får krav på att teckna företagslicens för nyttjande av tjänsten.
A 1.7	Genom att låsa din dator (CTRL + ALT + DEL, Välj Lås) eller (Windowstangent+L) medverkar du till att skydda känsliga uppgifter mot obehörig insyn och förändring. Exempelvis när personer passerar eller går in till ditt arbetsrum. Detta ska du göra varje gång du lämnar din dator obevakad, även för korta stunder.
A 1.8	Umeå kommuns medarbetare ska följa svensk lag och kommunens interna riktlinjer vid internetanvändning.
A 1.9	Du som medarbetare har rätt till skydd för din kommunikation och ditt privatliv. Men vid allvarlig misstanke om illojalt eller brottsligt beteende kan det vara tillåtet för arbetsgivaren att ta del av själva innehållet inte bara i arbetsrelaterat material utan även i dina privata filer eller e-postmeddelanden som finns i kommunens IT-miljö. Chef har till ansvar att se till att du som medarbetare är

	medveten om detta.
A 1.10	Medarbetaren ska ha kännedom om och tagit del av de styrdokument som berör medarbetarens arbete. Dessa finns publicerade på Umeå kommuns intranät och/eller kvalitetsledningssystem eller dylikt. Chef ansvarar för att ge medarbetare en introduktion till de styrande dokument som gäller.
A 1.11	Under distansarbete behöver du som medarbetare ta stort eget ansvar för att skydda kommunens information mot obehörig åtkomst. I detta styrande dokument finns information om vad som gäller vid distansarbete under kristider.

Medarbetares ansvar för informationssäkerhet

Information är en viktig resurs för Umeå kommun som är av stor betydelse för alla våra verksamheter. I kommunen hanterar vi varje dag mängder av information som handlar om allt vad vi gör, och rör till exempel förskolor, grundskolor, gymnasium, socialtjänst, hemsjukvård, stadsplanering, biblioteksservice, bygglov med mera. Information kan förekomma i olika former, den kan vara muntlig, skriftlig eller finnas i IT-system. Information är främst i form av texter, men även bilder, symboler, filmer och ljud utgör information. Viss information är känslig och måste skyddas från obehöriga att ta del av. Det handlar ofta om hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada men också om sådan information som skulle kunna skada organisationen eller samhället om den sprids. Det finns en hel del lagar och föreskrifter som kommunen måste leva upp till. Privatpersoner, företag och andra har förväntningar och behov på att kommunen hanterar information på ett säkert sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för att motsvara dessa krav. Information behöver olika slag av skydd. Det kan vara tekniskt såsom en brandvägg i ett IT-nätverk, eller administrativt i form av regler (som dessa riktlinjer) eller fysiskt hur man skyddar utrymmen med dörrar, lås, skåp med mera. Även medarbetares kunskap och medvetenhet är ett nog så viktigt skydd, till exempel att arbeta på rätt sätt med pappersdokument och i IT-system och att vara försiktig med känslig information som till exempel känsliga personuppgifter.

Säkerhet är inte bättre än den svagaste länken, och det är viktigt att alla typer av skydd fungerar på ett bra sätt tillsammans. En stor del av Umeå kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen.

Umeå kommun ställer krav på att medarbetare följer våra riktlinjer för informationssäkerhet. Chefer har ett ansvar att delge information och erbjuda utbildning i informationssäkerhetsfrågor till sina medarbetare. Som anställd på Umeå kommun omfattas

du av en straffsanktionerad tystnadsplikt. Denna tystnadsplikt gäller även efter att din anställning upphört. Grundlagsstadgat finns din rätt att offentliggöra uppgifter enligt meddelarfriheten, med de begränsningar som finns i offentlighets- och sekretesslagen.

Om du är externt kontrakterad och har tillgång till känslig information ska du skriva under en tystnads- och sekretessförbindelse. En sådan förbindelse gäller även efter att avtalet upphört.
Vid underlåtenhet att följa dessa riktlinjer för informationssäkerhet följer Umeå kommun gällande regler enligt lagar och avtal. Lagbrott polisanmäls.

Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera informationssäkerhetsincidenter eller brister som misstänkts kunna medföra negativ påverkan på Umeå kommuns information. Det kan röra sig om t.ex.

- IT-angrepp/intrång
- Skadlig kod
- Oskyddad känslig information
- Personuppgiftsincidenter
- Brister i efterlevnad av dessa riktlinjer för informationssäkerhet

IT- säkerhetsrelaterade incidenter och brister ska rapporteras till IT Kundsupport (090161134). Rör incidenten personuppgifter så ska detta rapporteras via verktyget IT Självservice som nås via intranätet. Meddela även din chef. Medarbetare som har upptäckt incidenter eller svagheter där brott misstänks föreligga, ska dock inte själva försöka bevisa sådana då det kan försvåra framtida utredningar. Det är bra att dokumentera iakttagelser i samband med upptäckten av incidenten.

Informationssäkerhetssamordnare sammanställer en incidentrapport en gång per år som rapporteras till Stadsdirektörens ledningsgrupp och berörda verksamheter.
Rapporten omfattar:

- Intrång och försök till intrång
- Brott mot lagstiftning och internt regelverk
- Incidenter som orsakar eller skulle kunna orsaka betydande avbrott eller störningar
- Konsekvenser och förslag till åtgärder efter intrång eller funktionsfel

Informationsklasser

Viss information är mer känslig än annan. Behovet av skydd skiljer sig därför mellan olika typer av information och i olika situationer. Skyddsbehovet beror på legala krav och vilka

konsekvenser det skulle få för verksamheten eller för enskilda individer om informationen sprids till obehöriga. I Umeå kommun finns fyra klasser för hur känslig informationen är och hur den får spridas: Öppen, Begränsad, Känslig-Sekretess eller Hög Sekretess. Dessa illustreras i Figur 2.

Informationsklass	Behörighet/spridning	Exempel
4 Hög Sekretess (Röd)	Endast ett mycket begränsat antal behöriga personer	Skyddade personuppgifter, information som om den hamnar i orätta händer medföra fara för liv och hälsa eller samhällsskada
3 Känslig-Sekretess (Gul)	Endast den som behöver informationen för att klara sin arbetsuppgift, särskild åtkomstbegränsning med god spårbarhet	Känsliga personuppgifter, integritetskänsliga (extra skyddsvärda) såsom personnummer och sociala förhållanden, information under pågående upphandling, skalskyddsritningar
2 Begränsad (Grön)	Normal åtkomstbegräsning med viss spårbarhet	Allmänna personuppgifter, allmänna offentliga handlingar, födelsedata (6 första siffrorna i personnummer YYMMDD)
1 Öppen (Vit)	Ingen åtkomstbegränsning	Handlingar utan direkta eller indirekta personuppgifter

Figur 2 i Umeå kommun används fyra informationsklasser

Olika regler gäller för dessa fyra klasser vad gäller spridning och hantering av information:

- Öppen (Vit) information kan spridas fritt. Ibland krävs dock beslut för att öppen information ska publiceras, t.ex. på extern webbplats som www.umea.se.
- För Begränsad (Grön) information gäller normal åtkomstbegräsning och de normala hanteringsregler som finns nedan i avsnitt A1 – A9. Grön information kan normalt spridas internt inom kommunen och externt. Grön är en markering att informationen kan innehålla personuppgifter.

- För **Känslig-Sekretess (Gul)** information gäller särskilda åtkomsträttigheter och hanteringsregler. I detta kapitel är all information och alla riktlinjer som gäller för känslig information markerad med fetstil och med röda ramar i tabeller med riktlinjer. Om känslig information delas till extern aktör ska det finnas ett tydligt syfte med detta. Känslig information får bara delas till betrodda externa parter.
- För **Hög Sekretess (Röd)** information gäller mycket begränsade åtkomsträttigheter och minimal spridning. Uppgifterna kräver ofta strikt manuell hantering och ska så långt det är möjligt hållas borta från digitala miljöer. Uppgifter i denna klass kan om de sprids medföra fara för liv och hälsa för den som uppgifterna avser eller för en stor mängd individer. Även dessa är markerade med fetstil, tjockare ram och röd ram.

Det finns dessutom information som är klassat högre än **Hög sekretess (Röd)**, sådan information regleras av säkerhetsskyddslagstiftning. Observera att särskilda regler finns för hantering av sådan information, kontakta Umeå kommuns säkerhetsskyddschef.

Inom Umeå kommun är idag långt ifrån all information klassad enligt de fyra klasserna. Att klassa information på det här sättet är ett arbete som startades under 2018 och pågår fortfarande. Det viktigaste är att **Känslig-Sekretess (Gul)** och **Hög Sekretess (Röd)** information hanteras på rätt sätt. Det är bl.a. känsliga personuppgifter och sekretessklassad information. Om du är osäker på hur viss information ska klassas och hanteras så fråga din chef eller kommunens informationssäkerhetssamordnare.

Personuppgifter

Vid de flesta av Umeå kommuns verksamheter hanteras personuppgifter. Dessa måste behandlas enligt gällande författningar bl. a EU´s dataskyddsförordning (GDPR) och Lagen om behandling av personuppgifter inom socialtjänsten.

Personuppgifter kan vara klassade som **Hög Sekretess (Röd), Känslig-Sekretess (Gul)** eller Begränsad (Grön) information. Det beror på sammanhang, vilka personuppgifter som avses osv. Känsliga personuppgifter är dock alltid lägst klassade som **Känslig-Sekretess (Gul) information**. Till känsliga personuppgifter räknas uppgifter som avslöjar:

- Ras eller etniskt ursprung
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- genetiska uppgifter,
- biometriska uppgifter för att entydigt identifiera en fysisk person,
- uppgifter om hälsa,
- uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Utöver känsliga personuppgifter finns det också personuppgifter som Integritetsskyddsmyndigheten (IMY) kallar särskilt skyddsvärda. Detta är inte känsliga personuppgifter men uppgifter som IMY bedömt ändå kan orsaka stor skada ifall de inte

hanteras korrekt.
För särskilt skyddsvärda personuppgifter gäller en högre teknisk säkerhet än för ”vanliga” personuppgifter. T.ex. får särskilt skyddsvärda personuppgifter inte skickas via okrypterad e-post utan det måste säkerställas att endast avsedd mottagare kan ta del av personuppgifterna.

Särskilt skyddsvärda personuppgifter klassas som **Känslig-Sekretess (Gul)** information. Exempel på särskilt skyddsvärda personuppgifter är;

- personnummer
- vissa löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala förhållanden.

Skyddade personuppgifter är alltid **Hög Sekretess (Röd) information** och ska hanteras utifrån särskilda rutiner och regler. Fråga din chef om den verksamhet du arbetar i har särskilda rutiner för skyddade personuppgifter.

Allmänna handlingar och sekretess

En handling är allmän och ska registreras om den är förvarad, inkommen till, eller upprättad hos kommunen. Om handlingen omfattas av sekretess måste den diarieföras. Allmänheten ska kunna ta del av allmänna handlingar och kommunen är skyldig att, efter sekretessprövning, skyndsamt tillhandahålla den i läsbar form till den som så begär det.

Allmänna handlingar kan vara både i form av analog och digital information och ska hanteras, bevaras och gallras i enlighet med verksamheternas dokumenthanteringsplaner. Information som är allmän handling och sekretessbelagd enligt offentlighets- och sekretesslagen ska klassas som **Känslig-Sekretess** (Gul) eller **Hög Sekretess** (Röd) information.

Arbetsmaterial under ett ärendes beredning, minnesanteckningar, verksamhetsinterna meddelanden och personliga meddelanden är normalt inte allmänna handlingar. Denna information kan klassas som **Hög Sekretess** (Röd), **Känslig-Sekretess** (Gul), Begränsad (Grön) eller Öppen (Vit) information beroende på känslighet, t.ex. utifrån krav från författningar.

A 2 Lösenord

Riktlinjer för utformning av lösenord	
A 2.1	Lösenord som du skapar för din inloggning till Umeå kommuns nätverk ska vara minst 12 tecken långt
A 2.2	Lösenord ska innehålla minst 1 stor bokstav, minst 1 liten bokstav, minst 1 specialtecken
A 2.3	Lösenordet får **inte** innehålla å, ä, ö, Å, Ä, Ö
A 2.4	Lösenordet får **inte** innehålla användarens inloggningsnamn, för- eller efternamn eller delar av namnet

Riktlinjer för hantering av lösenord	
A 2.5	Lösenordet ska hanteras som en värdehandling och inte ligga framme uppskriven på en lapp. Bäst är att förvara lösenord endast i minnet. Behövs tekniskt stöd för att lättare hålla ordning på lösenord så kan man använda en så kallad lösenordshanterare. Det finns säkra och avgiftsfria lösenordshanterare på marknaden, kontakta IT Kundsupport för tips om sådana verktyg
A 2.6	Samma lösenord ska inte användas privat och i jobbet. Olika lösenord ska dessutom användas för olika tjänster på webben även om de är jobbrelaterade. På så vis minskas riskerna att någon kommer åt information
A 2.7	Lösenord ska bytas direkt om misstanke finns att det har röjts.
A 2.8	Lösenord till ett personligt användarkonto får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. Man kan i så fall bli ansvarig för något som någon annan har gjort. I de fall en dator delas av flera, ska ändå personliga inloggningar göras. Detta är viktigt för spårbarheten, för att kunna veta vem som har gjort vad i systemen.
A 2.9	Om en dator delas av flera är det viktigt att automatisk minnesfunktion för lösenordet inte används. Om man loggar in på webbsidor så ska man då inte låta webbläsare spara lösenordet, utan alternativet ”Nej” ska väljas om man får en sådan fråga. Webbläsare har funktioner för att i efterhand ta bort webbhistorik/ta bort lösenord, vilken kan användas om man är osäker på om lösenord har lagrats.

För att logga in till de flesta av Umeå kommuns IT-system används användar-ID och lösenord. Lösenorden är personliga och får inte göras kända för andra. Om en obehörig kommer över ditt lösenord och får tillgång till ditt användar-ID, kan den personen utföra aktiviteter i ditt namn. Hamnar ett lösenord i orätta händer kan det orsaka stor skada. De flesta webbläsare har automatiska minnesfunktioner för att minnas de lösenord som du matar in. Ta för vana att inte spara lösenord i dina webbläsare med automatik eftersom då kan andra som har tillgång till din dator logga in på dina sidor. De flesta webbläsare har en funktion där du kan ta bort sparade lösenord. Via Umeå kommuns lösenordshanterare blir du påmind om när lösenord behöver bytas och kan återställa till ett nytt om du har glömt ditt lösenord. Användar-ID och lösenord används för att skydda information som kan vara intern eller konfidentiell, och det är därför viktigt att följa nedanstående regler för skapande och hantering av lösenord. Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person, och dessutom ha en viss längd och komplexitet.

Mer information om lösenordshanteraren hittar du på intranätet under rubriken IT, mejl och telefoni / Inloggning, lösenord.

Tips: Ett sätt att skapa ett lösenord med bra kvalitet (starkt lösenord) kan vara att använda följande knep:

Skapa ett starkt lösenord genom att sätta ihop slumpmässiga ord tillsammans med siffror, specialtecken, stora och små bokstäver och är minst 12 tecken långt.

ex: kAtt1%Snarkar

Användar-ID och lösenord är i sig viktig information där Användar-ID är intern information medan lösenord är **känslig** information och ska hanteras på ett säkert sätt:

A3 E-post

Ansvar	
A 3.1	Din personliga brevlåda fornamn.efternamn@umea.se är din tjänstebrevlåda
A 3.2	Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den mejl som skickas från kontot
A 3.3	E-postkonton kan stängas vid misstanke om brott eller missbruk
A 3.4	E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga.
A 3.5	Mejl ska klassificeras enligt Umeå kommuns klassificeringsmodell

A 3.6	Skriv inte känsliga uppgifter i ämnesraden, eftersom inkorgens register över inkomna e-postmeddelanden räknas som allmän handling.
A 3.7	Ska du skicka mejl till större grupper så ska du använda dig av funktionen ”Hemlig kopia”. Om du använder ”hemlig kopia” när du skickar mejl till större grupper undviker du att någon råkar skicka sitt svar till alla i gruppen trots att det bara var ämnat för dig som avsändare. Dessutom avslöjar du inte andras mejladresser om du använder ”hemlig kopia”
A 3.8	Om du får hotelsebrev via mejl ska du spara mejlet och kontakta din chef
A 3.9	Vid avslut av anställning tas e-postkontot bort efter viss tid, se därför till att mejl som din verksamhet kan behöva efter du har slutat din anställning sparas och lämnas över till annan handläggare.

Privat e-post	
A 3.10	Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via e-post. Använd inte ditt epostkonto i Umeå kommun för privata ändamål, utan ha en privat e-postadress som du inte använder för arbetsrelaterat material.
A 3.11	Det är inte tillåtet att automatiskt vidarebefordra din personliga e-postbrevlåda på kommunen till externa e-postadresser.

E-post och känslig information	
A.3.12	**Känslig – Sekretess (Gul)** information får inte hanteras i O365 mejl.
A 3.13	Information som klassificerats som **Hög sekretess (Röd)** får inte hanteras i O365 mejl.
A 3.14	Dokument som skannas skickas ofta med mejl från skannern till mottagarens e-postadress. Skanning av dokument som innehåller **känslig - sekretess** (gul) och **Hög Sekretess (Röd)** information ska ske via verktyget Säker skanning, se intranätet för handledning.
A 3.15	Om mejl *inkommer* som innehåller **känslig - sekretess** (gul) och **Hög Sekretess (Röd)** ska denna genast flyttas till verksamhetssystem. Svara inte avsändaren eller vidarebefordra ej i samma mejlkonversation, utan påbörja ny mejltråd utan känslig och sekretessinformation. Varpå meddelandet ska raderas från e-

	postklienten.
A 3.16	Om mejl *inkommer* som innehåller **Hög Sekretess (Röd)** ska denna genast överföras till verksamhetssystem. Varpå meddelandet ska raderas från e-postklienten.

E-post (mejl) är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom kommunen och till externa parter. Det är dock viktigt att tänka på att kommunikation med mejl normalt är helt öppen. Att sända mejl som inte är skyddad, t.ex. med kryptering, kan jämföras med att skicka vykort.

A 4 Chatt/direktmeddelanden

Chat och känslig information	
A.4.1	**Känslig – Sekretess (Gul)** information får inte hanteras i chatt.
A 4.2	Information som klassificerats som **Hög sekretess (Röd)** får inte hanteras i chatt.
A 4.3	Om chatt *inkommer* som innehåller **känslig - sekretess** (gul) och **Hög Sekretess (Röd)** ska mottagaren genast meddelas att känslig dialog på grund av säkerhetsskäl inte kan hållas per chatt. Hänvisa avsändaren till andra säkra kommunikationskanaler. Svara inte avsändaren eller vidarebefordra ej i samma chattkonversation, utan påbörja känslig dialog i avsedda kommunikationskanaler. Varpå meddelandet ska raderas från chatten.

Chatt är för en del medarbetare ett vanligt och viktigt sätt att kommunicera internt inom kommunen och till vissa grupper av externa parter. Det är dock viktigt att tänka på att kommunikation med chatt normalt är helt öppen. Att sända chatt kan jämföras med att skicka vykort.

A5 Lagring och säkerhetskopiering

Riktlinjer för lagring och säkerhetskopiering	
A 5.1	Kommunens information ska lagras i kommunens tillhandahållna tjänster på så sätt att den finns tillgänglig för den som behöver den.

A 5.2	Om information i undantagsfall behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket eller till din OneDrive eller G Drive kopplat till ditt kommunkonto. Om hårddisken på din dator kraschar kommer annars informationen att vara förlorad.
A 5.3	Om information på nätverket eller i din OneDrive eller G Drive har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska IT Kundsupport eller Google systemadministratör kontaktas, förhoppningsvis kan de då återskapa den senaste säkerhetskopian.
A 5.4	**Känslig- Sekretess** (Gul) information ska i första hand lagras i verksamhetssystem
A 5.5	**Känslig- Sekretess** (Gul) information får endast lagras i avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan.
A 5.6	**Hög Sekretess (Röd)** information ska endast hanteras i verksamhetssystem om verksamhetssystemet har en tydlig funktion för sekretessmarkering. Saknar verksamhetssystemet stöd för detta får inte verksamhetssystemet hantera skyddade personuppgifter. Uppgifterna måste då vara fiktiva alternativt strikt hanteras utanför den digitala miljön.
A 5.7	Lokal lagring (synkronisering) av K**änslig – Sekretess** (Gul) information, t.ex. på en persondator, får endast ske på en krypterad kommunägd dator.
A 5.8	Lagring av **Känslig – Sekretess** (Gul) information på ett USB minne tillåts endast om informationen är rätt klassat och USB minnet är krypterat med krypteringsteknik som Umeå kommun tillhandahåller. Kontakta IT Kundsupport. USB minnet ska förvaras betryggande då det inte används.
A 5.9	Fysiska dokument som innehåller **Hög – Sekretess** (Röd) information ska förvaras inlåsta på så sätt att uppgifterna endast är tillgängliga för den personal som behöver dem.

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av diskkrasch, oavsiktlig radering m.m

Riktlinjer för lagring i molntjänster	
A 5.10	Endast godkända molntjänster är tillåtna att användas. Du ansvarar för att kontrollera vilka molntjänster som är tillåtna inom din verksamhet

A 5.11	Som användare ska du inte koppla en molntjänst du använder privat till din kommunala e-postadress.
A 5.12	Umeå kommuns information får inte lagras i *personliga* molntjänster (Dropbox mfl).
A 5.13	**Hög Sekretess** (Röd) information får inte lagras i molntjänster

Riktlinjer för lagring i OneDrive/SharePoint Online	
A 5.14	Du ansvarar för att allmänna handlingar tas om hand för registrering och arkivering, och att information i din OneDrive gallras enligt fastställda dokumenthanteringsplaner.
A 5.15	**Känslig Sekretess** (Gul) och **Hög Sekretess** (Röd) information får inte lagras i OneDrive eller SharePoint Online av juridiska skäl. På OneDrive sparar du annat material som du lätt vill komma åt att redigera när som helst, var som helst. Det är i OneDrive du har dina egna arbetsrelaterade dokument. Via OneDrive kan du dela ett dokument med en eller ett par kollegor om du behöver synpunkter eller dialog kring ett innehåll.
A 5.16	Använd inte OneDrive för information som din *arbetsgrupp eller flera användare* behöver ha åtkomst till. Gemensamt material kan delas via SharePoint Online eller annan lagringsplats. Kontakta din chef för att få information om vilka samarbetsytor ni använder er av.
A 5.17	När din anställning ska avslutas ansvarar du för att information som finns på din OneDrive och som kan vara av vikt för din arbetsplats, lagras på annan lagringsplats.

Riktlinjer för lagring i G Drive (Utbildning)	
A 5.18	Du ansvarar för att allmänna handlingar tas om hand för registrering och arkivering, och att information i din G Drive gallras enligt fastställda dokumenthanteringsplaner.
A 5.19	**Känslig Sekretess** (Gul) och **Hög Sekretess** (Röd) information får inte lagras i G Drive (Utbildning) av juridiska skäl. När din anställning ska avslutas ansvarar du för att information som finns på din G Drive (utbildning), och som kan vara av vikt för din arbetsplats, lagras på annan lagringsplats

Molntjänster är datortjänster som tillhandahålls över Internet, exempelvis lagring eller programvaror. G Suite och Office 365 är exempel på molntjänster som Umeå kommun valt att införa.

Lagring på mobila enheter, smarta telefoner och surfplattor

Se avsnitt Mobila enheter

A6 Mobila enheter

Riktlinjer för hantering av mobila enheter	
A 6.1	**Känslig och sekretessinformation** måste vara krypterad på mobila enheter
A 6.2	Mobila enheter ska låsas med lösenord eller liknande.
A 6.3	Mobila enheter som tillhandahålls av Umeå kommun är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera.
A 6.4	Uppsatta säkerhetsinställningar i enheter får inte ändras.
A 6.5	Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din närmaste chef
A 6.6	Viktig information bör inte lagras enbart på en bärbar enhet, i så fall ska den snarast kopieras över till kommunens nätverk så att informationen säkerhetskopieras
A 6.7	Privat utrustning kan anslutas till kommunens gästnät.
A 6.8	Kommunenheter får enbart anslutas till trådlösa nätverk som är betrodda och lösenordskyddade. Detta innebär att enheten inte får anslutas till ”öppna” nät till exempel på hotell, caféer, tåg eller flygplan.
A 6.9	Vid distansarbete måste kommunens utrustning användas för kommunens information.

Riktlinjer för fysisk hantering av mobila enheter	
A 6.10	Försiktighet ska iakttas vid mobilt arbete i publika miljöer, exempelvis kan

	skärmen på enheten skyddas med insynsskydd (s.k. sekretesskydd)
A 6.11	Arbete med **Känslig – Sekretess** (Gul) och **Hög sekretess** (Röd) information får inte ske i publika miljöer. Om man som anställd behöver behandla känslig information i publika rum som till exempel bibliotek är det viktigt att göra det på ett sådant sätt att risken för att känslig information sprids till obehöriga elimineras.
A 6.12	Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme
A 6.13	Förlust av enhet ska omedelbart anmälas till IT kundsupport, detta ska göras innan polisanmälan. I många fall finns möjligheter att fjärradera information
A 6.14	Vid avslut av anställning eller vid byte till en annan enhet ska mobila enheter återlämnas i enlighet med de rutiner som finns. I undantagsfall kan enheten behållas privat eller av en verksamhet, detta avgörs av närmaste chef tillsammans med IT funktionen.
A 6.15	Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, t.ex. skyddas mot värme och fukt.
A 6.16	Vid service ska den mobila enheten inlämnas enligt fastställda rutiner, dessa finner du på intranätet.
A 6.17	Om utrustningen måste lämnas in för service så ska du försäkra dig om att den inte innehåller **känslig eller sekretessinformation**

Den IT-utrustning som tillhandahålls av Umeå kommun kan vara stationär eller bärbar, en s.k. mobil enhet. Mobil enhet avser bärbar dator (laptop), USB-minne, CD/DVD-skiva, extern hårddisk samt smart telefon och surfplatta. Applikationsspecifika datorer, mobiler eller surfplattor kan ha specifika riktlinjer utöver dessa som presenteras här. Kolla med din chef om du är osäker vad som gäller.

Särskilda regler för smarta telefoner och surfplattor

Regler för smarta telefoner och surfplattor	
A 6.18	Umeå kommun är som arbetsgivare ägare till de smarta telefoner och surfplattor som tillhandahålls för arbetet och även till den arbetsrelaterade informationen som finns i dessa enheter. Enligt offentlighetsprincipen kan det också vara möjligt

	för allmänheten att begära ut allmänna handlingar, till exempel arbetsrelaterade SMS eller bilder, som förvaras på telefonen/surfplattan.
A 6.19	Det finns ett stort utbud av appar att ladda ner till den smarta telefonen eller surfplattan. Många av dessa appar kan innehålla skadlig kod. I syfte att minska denna risk är det inställt så att det är endast möjligt att hantera kommunens information i appar som finns att ladda ned i Umeå kommuns interna app-katalog (Företagsportalen)
A 6.20	Umeå kommuns information kan inte hanteras i smart telefon eller surfplatta om inte särskild av kommunen godkänd säkerhetslösning används på grund av risk för informationsläckage mellan appar.
A 6.21	Pinkod (6 siffror), fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor. Då pinkoder används ska ej enkla pinkoder som 000000, 123456 etc. användas, och inte samma pinkod som används i andra sammanhang, t.ex. pinkod till betalkort. Du får inte skriva upp koden på telefonen eller surfplattan.
A 6.22	Vårda utrustningen och använd exempelvis skärmskydd och skal.
A 6.23	Huvudregeln är att vid anställningens upphörande ska surfplatta och den smarta telefonen återlämnas till närmaste chef. Möjlighet kan dock ges att köpa ut telefonen. Detta avgör närmaste chef. Om telefonen behålls av den anställde ska arbetsrelaterad information flyttas från mobiltelefonen före anställningens avslutande.
A 6.24	Vid längre tjänstledighet kan telefonen behöva lämnas åter, det avgör närmaste chef.
A 6.25	En smart telefon är ett viktigt verktyg för säker inloggning till kommunens IT-resurser som kräver multifaktorinloggning – därför måste din smarta telefon som arbetsgivaren tillhandahållit hanteras som en värdehandling.

A7 Skadlig kod

Riktlinjer för skydd mot skadlig kod	
A 7.1	Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod
A 7.2	Anslut endast arbetsrelaterad IT-utrustning till kommunens administrativa

	nätverk
A 7.3	Var misstänksam och undvik att klicka på konstiga länkar eller fylla i kontouppgifter
A 7.4	Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad. Är du osäker, ring avsändaren och fråga.
A 7.5	Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod, gör så här: 1) koppla ifrån wifi/dra ur nätverkskabeln 2) låt datorn vara på 3) kontakta IT kundsupport. OBS! Anmälan till IT kundsupport ska ske per telefon eller besök, inte via e-post

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller ett nätverk utan administratörens samtycke, och har utvecklats i syfte att störa IT-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i IT-utrustning. Skadlig kod är ett växande problem och den blir mer och mer sofistikerad och ”intelligent” och kan vara svår att upptäcka och kan utföra avancerade operationer. Man behöver idag inte vara en teknisk kunnig hacker för att skapa skadlig kod, utan det mesta kan köpas och beställas på olika marknadsplatser på Internet.

Exempel på idag förekommande skadlig kod:

- Ett ökande problem är s k Ransomware där filer eller diskar på dator (eller smart mobil eller surfplatta) krypteras och man sedan krävs på en lösensumma för att få tillbaka åtkomsten till filerna
- Vissa trojaner, s k keyloggers, kan avlyssna lösenord och skicka dessa vidare.
- Det finns trojaner som skapar bakdörrar i datorer så att andra personer får tillgång till dessa utan ägarens vetskap. Exempelvis med syfte att lagra olaglig information.

Spridning av skadlig kod

Skadlig kod kan spridas till ens dator eller mobila enhet om man öppnar bilagor i e-post, importerar filer eller surfar på Internet och klickar på fel länkar, inklusive sådana som finns i sociala medier. Avsändare till e-post kan fejkas och webbsidor är inte alltid de som de utger sig för att vara. Identiteter kan kapas, till exempel på Facebook, och e-postadresser kan fejkas i syfte att lura mottagaren att klicka på länkar. Vid s k Phishing luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkonton. Var observant på detta och fyll aldrig i sådana uppgifter! Seriösa myndigheter, företag och andra organisationer ber aldrig om uppgifter på detta sätt. IT-utrustning som

drabbats av skadlig kod, även ett smittat USB-minne, kan om det kopplas upp i kommunens nätverk, sprida sig vidare i nätverket och orsaka stor skada. Kommunens datorer är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb. Alla medarbetare kan också bidra till ett bra skydd mot skadlig kod genom att följa dessa regler:

A8 Internet och sociala media

Riktlinjer för internetanvändning	
A 8.1	Internet är i arbetet på Umeå kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen.
A 8.2	Det är tillåtet att använda Internet för privat bruk om det inte inkräktar på arbetet eller medför kostnader för kommunen. Kommunen förutsätter att den som surfar på Internet endast besöker lagliga webbplatser.
A 8.3	Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i, eller via, Umeå kommuns nätverk.
A 8.4	Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning etcetera) eller har anknytning till kriminell verksamhet
A 8.5	Umeå kommun införde 2008 ett filter för att i förebyggande syfte förhindra oetisk internetsurfning och direkt brottslig verksamhet. I samband med detta infördes möjlighet till loggning av Internettrafik. Loggningen ska kunna tillhandahålla material som krävs för att bevisa eller motbevisa påståenden och misstankar om brottslig eller otillbörlig användning av Internet som anställd vid Umeå kommun
A 8.6	De regler som gäller i samhället i övrigt gäller självklart även inom Umeå kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt lagar som reglerar personuppgiftsbehandling är exempel på lagar som ibland måste beaktas när man använder Internet
A 8.7	För material på Internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik, m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren
A 8.8	Internet är ett öppet nätverk och endast öppen information får publiceras, alltså

	inte **Känslig - Sekretess** (gul) eller **Hög Sekretess** (röd) information

Användning av Internet och sociala medier kan vara till stor nytta och glädje, privat såväl som på arbetet. Förutom de riktlinjer som är kopplade till skadlig kod i avsnitt A7 finns här särskilda regler för användning av Internet och sociala medier.

Etiska riktlinjer	
A 8.9	All kommunikation på Internet från Umeå kommuns datorer ska vara öppen, saklig och etisk, oavsett om kommunikationen sker för privata syften eller inte, eftersom kommunens enheter lämnar spår på Internet som leder tillbaka till vår organisation
A 8.10	Publicera inte något på Internet som är oärligt, osant, vilseledande eller kränkande. Tänk på att det som publiceras är synligt och offentligt för allmänheten, sprids snabbt samt finns kvar under lång tid. Tänk därför igenom innehållet noga innan du publicerar

Uttalanden och andra aktiviteter som görs på Internet kan påverka allmänhetens uppfattning om den enskilde tjänstemannen som utför aktiviteten, och även för Umeå kommun som organisation. Det är därför särskilt viktigt att som representant för Umeå kommun beakta god etik och gott omdöme på Internet. Umeå kommuns etiska regler och värderingar ska följas även vid kommunikation via Internet och sociala medier.

Riktlinjer vid användning av sociala medier	
A 8.11	Vid användning av sociala medier, se till så att det inte framstår som om åsikter som uttrycks är Umeå kommuns
A 8.12	Det är viktigt att du skiljer på vad du gör i sociala medier som privatperson och som representant för Umeå kommuns verksamheter.
A 8.13	Du har självklart rätt att diskutera Umeå kommun och jobbrelaterade saker som privatperson i sociala medier (förutom ärenden som omfattas av sekretess, se nedan). Ibland kan du behöva vara extra tydlig och förklara i vilken roll du uttalar dig eftersom du kan förknippas med din yrkesroll även på fritiden

A 8.14	Hemliga uppgifter får inte spridas och ärenden som berörs av sekretess eller tystnadsplikt får aldrig avhandlas i sociala medier, varken i privata konton, direktmeddelanden eller som inlägg i kommunens kanaler.
A 8.15	Gör du inlägg eller kommenterar med Umeå kommuns profil/användare så representerar du Umeå kommun. Skriver du med ditt eget namn och profil som avsändare gör du det som privatperson.
A 8.16	I ditt personliga konto får du inte använda bilder och filmer som tillhör Umeå kommun utan att fråga fotografen först

Umeå kommun är aktivt på sociala medier. Den personal som är utsedda att skriva i Umeå kommuns namn har särskilda regler och kunskap om kommunikation.

Se vidare Umeå kommuns riktlinjer för sociala medier

A9 Spårbarhet och loggning

Riktlinjer för granskning av loggar	
A 9.1	Materialet får inte användas av arbetsgivaren i allmänt kontrollerande syfte.
A 9.2	Misstanke om överträdelse ska vara väl dokumenterat. Dokumentationen ska innehålla beskrivning av händelsen, namn på person eller personer som gjort iakttagelser, datum, tidpunkt etc. Det är en förutsättning för att loggning skall kunna genomföras. Avsaknad av dokumentation innebär att loggning av enskild person inte får slås på

Rutin vid fördjupad granskning

Om det finns behov av fördjupad granskning av uppgifter på individnivå gäller följande:

Riktlinjer för fördjupad granskning	
A 9.3	Vid granskningen skall alltid två personer närvara
A 9.4	Verksamhetschef utser person från verksamheten och IT-chef utser teknisk assistans. Personerna får endast tillgång till loggarna i samband med granskningen.
A 9.5	Granskningen ska genomföras skyndsamt och enligt fastställd teknisk rutin

A 9.6	Granskarna skall noggrant dokumentera anledningen till granskningen. I dokumentation skall det framgå vilka som genomfört den, samt datum, tid och plats för granskningstillfället

Gallring av loggar från granskning

Riktlinjer för gallring av loggar från granskning	
A 9.7	Granskningsloggar ska raderas efter ärendet är avslutat
A 9.8	Undantag ska göras för loggar som påvisat brottslig aktivitet eller brott mot regler samt loggar som berörs av påbörjad undersökning
A.9.9	Sådan undersökning innebär att det material som då finns tillgängligt sparas och är tillgängligt till dess att undersökningen avslutats

Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när och följa förloppet för olika händelser på datorn. All Internettrafik och e-post loggas centralt. Loggning sker i kommunens datorer och nätverk. Både filter och loggning är förenligt med GDPR. Loggarna används även för felsökning.
Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer. Umeå kommun kan, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och riktlinjer. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

Om användare, via Internet, surfar in på en webbsida eller annat tillgängligt som finns definierat som förbjudet i de tabeller som styr filtret, får användaren ett meddelande att denne nekas tillträde till sidan. Användaren får också ett meddelande att han/hon försökt nå en förbjuden adress. Ingen loggning görs av ett sådant försök. Det enda som händer är att användaren får en varningstext och att den sökta adressen inte visas.

För närvarande är följande kategorier av sidor spärrade:

- pornografiska
- anonymitetsservrar
- illegal fildelning

Pornografi

Enligt detta styrdokument, som upprättats med stöd av kommunens informationssäkerhetspolicy, är det inte tillåtet att titta eller lyssna på material av pornografisk karaktär. Enligt brottsbalken är innehav av barnpornografi straffbart (brottsbalken 16:10a).

Anonymitetsservrar

Innebär att användaren loggar in på en särskild server som erbjuder tjänsten anonymitet. Där kan användaren surfa runt på Internet utan att lämna några spår efter sig. Det som kan spåras är anonymitetsserverns IP-adress.

Illegal fildelning

Upphovsrätten innebär att den som skapat ett litterärt eller konstnärligt verk också har rätt till det. I den rätten ingår också att förfoga över verket genom att framställa exemplar av det och att göra det tillgängligt för allmänheten. Enligt upphovsrättslagen är det straffbart att dela ut den informationen till andra genom till exempel illegal fildelning. Förutom det personliga ansvaret riskerar den som medverkat till fildelning att bli skadeståndsskyldig till den som har upphovsrätt.

Rutin för loggning

GDPR medger rätt för arbetsgivaren, pga. allmänt intresse, att logga internettrafik utan personligt samtycke, med stöd av informationssäkerhetspolicy och för att säkerställa verksamhetens kontinuitet genom begränsande av internetanvändning för fildelning, kränkning/mobbning, rasism eller barnporr. Materialet får användas för att på ett strukturerat sätt beställa rapport på övergripande nivå (inte personrelaterad) där förbjudna sidor och på förhand definierade undersökningsområden fastställts.

Sådana områden skall vara kända av personalen.

Om det ur materialet kan påvisas att det skett slagningar mot förbjudna sidor eller frekvent användning på ett otillbörligt sätt kan verksamhetschef beställa fördjupad granskning av materialet.

Individuell loggning

Om det finns misstanke om överträdelse av regler eller misstanke om brottslighet kan verksamhetschef besluta om loggning av enskild persons användning av Internet eller internetanvändning för en grupp användare. Det innebär att samtliga lyckade internetsökningar loggas. Sparade loggar omfattar uppgift om vilken person som besökt adresserna.

Granskning av loggar

Direkt granskning av loggar får endast ske när det finns anledning misstänka att överträdelser sker.

A10 Säkert beteende

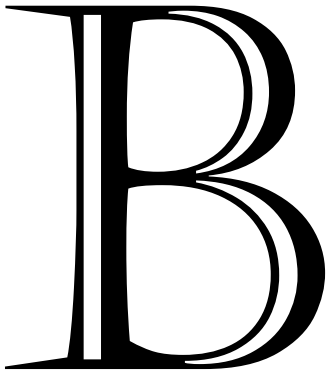
Riktlinjer för muntlig information	
A 10.1	**Känslig – Sekretess** (Gul) och **Hög Sekretess** (Röd) information har en begränsad krets av behöriga. Detta måste beaktas så att inte obehöriga kan höra sådan information på arbetsplatsen, både i arbetssituationer och i informella sammanhang, t.ex. vid fikabordet. Man ska enbart tala i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.
A 10.2	**Känslig – Sekretess** (Gul) och **Hög Sekretess** (Röd) information får överhuvudtaget inte kommuniceras muntligt i publika lokaler. Om man behöver behandla känslig information i kontakten med brukare i publika rum som till exempel bibliotek är det viktigt att föra samtalet på ett sådant sätt att risken för att känslig information sprids till obehöriga minimeras
A 10.3	Endast öppen information ska kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget, eller i telefonsamtal i kassakön.

Riktlinjer för information på skärmar och i pappersform	
A 10.4	Skriftligt material som innehåller **Känslig – Sekretess** (Gul) och **Hög Sekretess** (Röd) information får inte ligga framme så att obehöriga kan läsa den. Materialet ska låsas in i egen hurts eller eget skåp när man lämnar arbetsplatsen, även för kortare stunder.

A 10.5	**Känslig – Sekretess** (Gul) och **Hög Sekretess** (Röd) information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund. Om man har ett s k smart kort till datorn (SITHS el likn) ska detta tas ut då man lämnar arbetsplatsen.
A 10.6	**Känslig – Sekretess** (Gul) och **Hög Sekretess** (Röd) information ska skyddas från insyn med hjälp av sekretessfilter på datorskärm i de fall då sådan information hanteras på plats där insyn från sidan kan ske. Sekretessfilter kan efter bedömning av närmaste chef tillhandahållas av arbetsgivaren.
A 10.7	Besökare får inte vistas utan uppsikt i lokaler där **Känslig – Sekretess** (Gul) och **Hög Sekretess** (Röd) information kan finnas. Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler. Obekanta personer i sådana lokaler ska tillfrågas vem de söker och hjälpas tillrätta. Datorer i publika rum, till exempel bibliotek, med känslig information får inte lämnas utan uppsikt utan att låsas ner.
A 10.8	Vid fysisk posttjänst ska dubbla förslutna brev (internpostkuvert och kuvert) användas för intern information och rekommenderade försändelser ska användas om externbrev innehåller **Känslig – Sekretess** (Gul) och **Hög Sekretess** (Röd) information
A 10.9	Fax är ett väldigt osäkert kommunikationssätt. Därför håller kommunen på att ersätta faxen med Säker Digital Kommunikation, lösningen ska införas under 2022. Om **Känslig – Sekretess** (Gul) information överförs via fax ska man försäkra sig om att man har rätt nummer (t.ex. använda sig av kortnummer) och att mottagarens fax är övervakad under överföringstillfället. Man ska inte lämna faxen innan överföringen är klar.
A 10.10	Fax får inte användas till **Hög Sekretess** (Röd) information
A 10.11	Vid utskrift ska dokument omgående hämtas upp ur skrivare. Vid utskrift av **Känslig – Sekretess** (Gul) och **Hög Sekretess** (Röd) information måste så kallad Follow-me printing (inloggning med passerkort) användas. Utskriften ska alltid övervakas så att man är säker på att ingen obehörig kan läsa informationen. Det ska också säkerställas att samtliga dokument är helt utskrivna innan man lämnar skrivaren.
A 10.12	Pappersdokument som innehåller **Känslig – Sekretess** (Gul) och **Hög Sekretess**

	(Röd) information måste vid kassering strimlas eller kastas i godkända säkerhetskärl

En stor del av kommunens information hanteras muntligt och på papper. Vi kommunicerar dagligen informellt och formellt på detta sätt och vi måste bete oss särskilt försiktigt då vi hanterar **Känslig – Sekretess** (Gul) eller **Hög sekretess** (Röd) information. Tänk på att det alltid finns informell information som inte i förhand är definierad och klassad, utan som skapas i det ögonblick det uttalas eller skrivs. Det kan vara till exempel omdömen om chefer och medarbetare – skvaller, rykten m m – eller information om en oförutsedd händelse, t.ex. ett brott. Sådan information kan vara känslig och är i så fall att betrakta som **Känslig – Sekretess** (Gul) information.



Kapitel B Styrning av informationssäkerhet

Inledning

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Umeå kommun. Det beskriver också hur ansvarsfördelningen ser ut i stort. Ansvar för varje målgrupp återfinns också i varje kapitel, varför den övergripande ansvarsfördelningen i detta kapitel i huvudsak är informativ och ger en överblick över ansvaret för informationssäkerhet. Den primära målgruppen för detta kapitel är förutom informationsägare de som arbetar med informations- och IT-säkerhet eller har ansvar för informationssäkerhet i förvaltningsobjekt, projekt, processer eller andra verksamheter. Kapitlet kan även vara informativt för andra som är intresserade av hur arbetet med informationssäkerhet bedrivs i Umeå kommun, exempelvis sådana som arbetar med ledning och styrning av andra närliggande områden och processer som exempelvis kvalitet och annan säkerhet. I kapitlet ges en introduktion till informationsklassning och den modell för informationsklassning som Umeå kommun antagit i och med dessa riktlinjer.

B1 Roller och ansvar

Grundprincip

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från nämnd till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt o.s.v.) också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens informationsarkitekt, informationssäkerhetssamordnare, personuppgiftskoordinatorer och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som

stöd till medarbetare, verksamheter, kommunens ledning och nämnder för att de ska kunna ta ansvaret för informationssäkerheten.

Kommunfullmäktiges ansvar

Kommunfullmäktige fastställer övergripande mål och inriktning för informationssäkerhet genom en kommunövergripande informationssäkerhetspolicy.

Kommunstyrelsens ansvar

I kommunstyrelsens ledningsfunktion ligger att leda, samordna och utöva tillsyn gällande det kommunövergripande informationssäkerhetsarbetet. Stadsdirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunfullmäktige fastställda informationssäkerhetspolicyn. Kommunstyrelsen fastställer kommunövergripande riktlinjer för informationssäkerhet.

Ansvar inom varje nämnd och dess verksamheter

Varje nämnd är ansvarig för informationssäkerheten inom sitt verksamhetsområde. Nämnd kan vid behov besluta om instruktioner som kompletterar de centrala riktlinjerna för informationssäkerhet.

Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Verksamhetsledningen ansvarar för att verksamhetens medarbetare känner till och efterlever informationssäkerhetspolicyn och riktlinjer för informationssäkerhet. Verksamhetsledningen ska visa sitt stöd för styrande processer för informationssäkerhet och fungera som förebild i informationssäkerhetsfrågor.

Det åligger varje verksamhetsansvarig att se till att sina medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås. Säkerhetsansvaret i sig kan inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

Medarbetares ansvar

Alla medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler. Varje anställd har även skyldighet att rapportera informationssäkerhetsrelaterade brister och incidenter. Om någon enskild

befattningshavare ändå bryter mot gällande styrdokument bär vederbörande själv ansvaret för sitt handlande.

Riktlinjer för medarbetare återfinns i Kapitel A.

Personuppgiftsansvar

Kommunstyrelsen och övriga nämnder är personuppgiftsansvariga inom respektive verksamhetsområde och ska utse personuppgiftskoordinatorer. Som personuppgiftsansvariga har de inom sitt verksamhetsområde det yttersta ansvaret för all behandling av personuppgifter och informationssäkerheten knuten till den behandlingen. Varje personuppgiftsansvarig har till sitt stöd en eller flera personuppgiftskoordinator/-er som samordnar personuppgiftshanteringsarbetet i enlighet med lagstiftning och kommunens interna bestämmelser. Personuppgiftskoordinator är ett rådgivande och samordnande stöd till verksamhetens ledning i verksamhetens interna informationssäkerhetsarbete kopplat till personuppgiftshantering. Om behandlingen sker i strid med dataskyddslagstiftning eller andra bestämmelser kan den personuppgiftsansvarige ställas till ansvar, oavsett om denne haft uppsåt att handla i strid med lagen eller varit oaktsam. Den personuppgiftsansvarige har också en skyldighet att kunna visa att man följer dataskyddsförordningen, t.ex. genom fastställda rutiner eller andra styrdokument. I enlighet med EU´s dataskyddsförordning och nationell dataskyddslagstiftning ska varje nämnd utse ett dataskyddsombud. Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Personuppgiftsansvarig ska också stödja dataskyddsombudet i utförandet av dennes uppgifter (som avses i artikel 39 GDPR) genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden.

Arkivmyndigheten - Stadsarkivet

Kommunstyrelsen är kommunens arkivmyndighet. Arkivmyndigheten utövar tillsyn över att kommunens myndigheter fullgör sina skyldigheter beträffande arkivbindningen och dess syften samt över arkivvården i kommunen. Hos arkivmyndigheten finns ett stadsarkiv. Stadsarkivet är kommunens centrala arkiv. Stadsarkivet är arkivmyndighetens operativa organ och ger myndigheterna råd och anvisningar om arkivvård och dokumenthantering.

Stadsarkivarie är medlem i kommunens informationssäkerhetsråd.

Objektägares ansvar

Objektägare ansvarar för att förvaltningsobjekt efterlever informationssäkerhetspolicy och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om objektets informationssäkerhetsnivåer genom att klassning sker i enlighet med Umeå kommuns modell för informationsklassning. Informationssäkerhetsansvar hos övriga roller inom förvaltningsorganisationen beskrivs i Kapitel C.

I den mån det inte finns utpekade objektägare, t.ex. systemägare för ett system, följer ansvaret verksamhetsansvaret.

Riktlinjer för informationssäkerhet i verksamhetsnära förvaltning återfinns i Kapitel C

Ansvar i projekt

Verksamheten äger projektet via en utsedd projektägare som säkerställer att säkerhetsfrågorna beaktas. Styrgruppen är ansvarig för att säkerhetsfrågorna beaktas och ska tillsammans med projektägaren fastställa säkerhetsnivån för det som utvecklas. Under projektets gång ska styrgruppen följa upp hanteringen av de säkerhetsrelaterade frågorna. Projektledaren ansvarar för att fastslagen säkerhetsnivå beaktas i projektarbetet.

ITs ansvar

IT ansvarar för att tekniska säkerheten i kommunens IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är robust, tillräcklig och uppfyller verksamheters krav, legala krav samt informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet.

IT-säkerhetsansvarig

IT-säkerhetsansvarig samordnar arbetet med säkerheten i Umeå kommuns IT-miljö och som är stödjande vid kravställning på externa aktörer. Rollen IT-säkerhetsansvarig beskrivs utförligare i Kapitel D. IT-säkerhetsansvarig är medlem i kommunens informationssäkerhetsråd.

Informationssäkerhetssamordnare

Informationssäkerhetsarbetet i kommunen leds och samordnas av en informationssäkerhetssamordnare.

Informationssäkerhetssamordnare ansvarar för

• att kommunens styrande dokument inom området är aktuella, som informationssäkerhetspolicy och riktlinjer för informationssäkerhet,

• att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet,

• kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom kommunen, t.ex. genom rådgivning och utforma utbildning,

• att stödja verksamheterna i frågor som rör informationssäkerhet,

• att samordna kommunens personuppgiftskoordinatorer i informationssäkerhetsfrågor

• kontroll och uppföljning av informationssäkerheten,

• omvärldsbevakning inom informationssäkerhetsområdet,

• delta i kommunens informationssäkerhetsråd (se nedan).

Säkerhetsenheten

Säkerhetsenheten har uppdraget att utöva kommungemensam styrning av säkerhetsarbetet. Varje nämnd/bolagsstyrelse ansvarar för säkerhets- och trygghetsarbetet inom sitt område och sina respektive verksamheter.
Säkerhetsenheten ska verka som en organiserande och koordinerande process i kommunens säkerhetsarbete och ska stödja verksamheterna och de kommunala bolagen i deras säkerhetsarbete.

Säkerhetsskyddschef är medlem i kommunens informationssäkerhetsråd.

Informationssäkerhetsråd

Rådet leds av kommunens informationssäkerhetssamordnare. Informationssäkerhetsrådet ska sammanträda ca 8-10 gånger per år och har uppgift och befogenheter att:

• bereda ärenden ställda av informationsägare kring behov av specifika informationssäkerhetslösningar,

• bereda dokument, t.ex. styrande dokument, metoder och vägledningar,

• fungera som kommunens remissinstans och rådgivare i frågor relaterade till informationsarkitektur och informationssäkerhet,

• vara ett forum för erfarenhetsutbyte och omvärldsbevakning.

Dataskyddsombud

Dataskyddsombudets uppgift är att informera och ge råd till den personuppgiftsansvariga och dess organisation om de skyldigheter som gäller enligt dataskyddsförordningen. Dataskyddsombudet ska också övervaka att dataskyddslagstiftningens och personuppgiftsansvariges strategi för skydd av personuppgifter efterlevs, detta inbegriper ansvarstilldelning, information och utbildning till personal och tillhörande granskning. Den personuppgiftsansvarige ska stödja dataskyddsombudet i dennes utförande av dessa uppgifter.

Dataskyddsombudet ska på begäran ge råd om konsekvensbedömningar avseende dataskydd och övervaka genomförandet av konsekvensbedömningen.

Dataskyddsombudet ska samarbeta med tillsynsmyndigheten och vid behov fungera som kontaktpunkt för tillsynsmyndigheten. Dataskyddsombudet ska också fungera som kontaktperson för registrerade. Registrerade kan kontakta dataskyddsombudet i alla ärenden som har att göra med behandling av deras personuppgifter och utövandet av rättigheter med stöd av dataskyddsförordningen.

Dataskyddsombud är medlem i kommunens informationssäkerhetsråd.

Kommunens revisorer

Kommunens revisorer utför kontroll av informationssäkerheten inom ramen för ordinarie revisioner.

B2 Dokumentstruktur

Riktlinjer för dokumentstruktur för informationssäkerhet	
B 2.1	Umeå kommuns informationssäkerhet och dess behov ska analyseras i en informationssäkerhetsanalys. Analysen ska genomföras minst vart fjärde år och ska ligga till grund för hur arbetet med informationssäkerhet ska bedrivas och innehåll och utformning av övriga styrande dokument
B 2.2	Årliga handlingsplaner för informationssäkerhet ska tas fram baserade på informationssäkerhetsanalyser
B 2.3	Det ska finnas en för Umeå kommun övergripande informationssäkerhetspolicy som uttrycker ledningens viljeinriktning med informationssäkerhet
B 2.4	Det ska finnas kommunövergripande riktlinjer för informationssäkerhet som

	konkretiserar informationssäkerhetspolicyn och som riktar sig till relevanta målgrupper
B 2.5	Det ska finnas modeller, metoder, vägledningar och andra stöddokument som stödjer olika gruppers efterlevnad av informationssäkerhetpolicyn och riktlinjerna för informationssäkerhet

Det är fyra dokument som är centrala för kommunens arbete med informationssäkerhet:

- Informationssäkerhetspolicy
- Riktlinjer för informationssäkerhet *(detta dokument)*
- Informationssäkerhetsanalys (-er)
- Handlingsplan (-er) för informationssäkerhet

Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet (detta dokument) riktar sig till alla medarbetare inom Umeå kommun:

I**nformationssäkerhetspolicyn** är ett övergripande dokument som uttrycker kommunstyrelsens viljeinriktning med informationssäkerhet. Beslutas av Kommunfullmäktige och uppdateras vid behov.

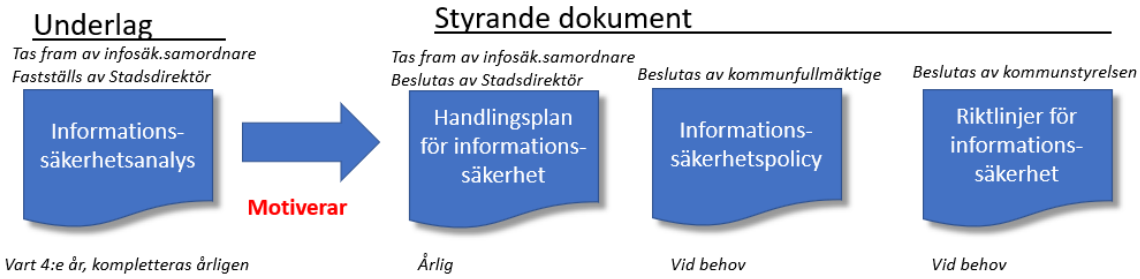
Riktlinjer för informationssäkerhet (detta dokument) innehåller riktlinjer för hantering av information. Riktlinjerna är uppdelade i kapitel för olika målgrupper. Beslutas av kommunstyrelsen och uppdateras vid behov.

Informationssäkerhetsanalys och **Handlingsplan** för informationssäkerhet riktar sig främst till de som arbetar med styrning av informationssäkerhet i Umeå kommun:

- Informationssäkerhetsanalysen är en genomlysning av informationssäkerheten i Umeå kommun innefattande hotbild, skyddsnivåer, kommunens inriktning och interna och externa krav. Analysen genomförs i full skala vart fjärde år men justeringar kan göras löpande beroende på förändringar i kommunen eller externt.
  Informationssäkerhetsanalysen ligger till grund för hur arbetet med informationssäkerhet ska bedrivas och innehåll och utformning av de övriga dokumenten.
- Handlingsplaner för informationssäkerhet tas fram årligen och innehåller konkreta mål och åtgärder baserade på informationssäkerhetsanalysen.

Se figur 3.

Figur 3



Modeller, metoder, vägledningar och andra stöddokument kan tas fram centralt för att stödja arbetet med informationssäkerhet på olika nivåer och att underlätta tillämpningen efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet.

Lokalt, t.ex. i förvaltningar och i verksamheter, kan mer specifika instruktioner och vägledningar tas fram i syfte att komplettera eller förtydliga riktlinjerna för informationssäkerhet.

B3 Informationsklassning

Riktlinjer för informationsklassificering	
B 3.1	Det ska finnas en kommungemensam modell för informationsklassificering
B 3.2	Umeå kommuns modell för informationsklassning ska tillämpas för kravställning på informationssäkerhet genom att information ska klassas i enlighet med modellen och krav på säkerhetsåtgärder ska kopplas till de olika nivåerna i klassningsmodellen

Informationsklassning är en grundläggande komponent i informationssäkerhetsarbetet. Genom att klassa information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet skapar man förståelse för, och kan styra vilket skydd som krävs för olika informationstillgångar. Främst handlar det om att skyddet ska bli tillräckligt, men ibland också för att undvika överskydd – med onödigt höga kostnader som följd. Klassning av information ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Umeå kommuns verksamheter.

Att klassificera information på ett enhetligt sätt utifrån konfidentialitet, riktighet och tillgänglighet är en fundamental aktivitet i ett ledningssystem för informationssäkerhet (LIS) och ett krav i standarden SS-ISO/IEC 27001, vilken Umeå kommun avser att följa i dess informationssäkerhetspolicy. Det är också en rekommendation från MSB – Myndigheten för

samhällsskydd och beredskap – att organisationer ska klassa sin information och bygga sina säkerhetsåtgärder utifrån klasserna. I den vägledande standarden SS-ISO/IEC 27002 rekommenderas att man ska ta fram en organisationsgemensam modell för informationsklassning. En sådan modell definierar nivåer av skyddskrav kopplat till de tre aspekterna konfidentialitet, riktighet och tillgänglighet så att information kan klassas på ett enhetligt sätt i hela organisationen.

Umeå kommun har i och med dessa riktlinjer antagit en egen modell för informationsklassning, se Figur 4.
Modellen baseras på Sveriges nationella modell för informationsklassning som är utgiven av MSB och SIS, men har anpassats till kommunens behov.

Figur 4

OBS! Det finns dessutom information som är klassat högre än **Hög sekretess (Röd)**, sådan information regleras av säkerhetsskyddslagstiftning.

Öppen information behöver alltså inte ha något skydd mot insyn och har normalt ingen begränsad åtkomst. Begränsad information behöver viss skydd av insyn då det ofta inbegriper personuppgifter. Däremot är det viktigt att förstå att all information – även

Öppen och Begränsad – har minst normala skyddskrav när det gäller dess riktighet och tillgänglighet. Det kan också krävas beslut för att viss information ska vara öppen och publik.

Idén med informationsklassning är att skydd ska anpassas till kraven på en viss informationstillgångs konfidentialitet, riktighet och tillgänglighet. En viss information kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet.

Även hela IT-system klassificeras. När man då klassar enligt KLASSA metoden ska informationsvärdet bedömas utifrån alla tre aspekterna.

Figur 5

KLASSA nivå	
(4) Synnerligen allvarlig skada	Systemet behandlar information som omfattas av sekretess och rör Sveriges säkerhet (hemliga uppgifter) där röjande av information, felaktig information eller otillgänglig information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Vid hantering av hemliga uppgifter ska Säkerhetsskyddslagstiftningen och Säkerhetsskyddsförordningen beaktas.
(3) Allvarlig skada	Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Känsliga personuppgifter kan ges stor spridning och orsaka allvarlig skada på den personliga integriteten.
(2) Betydande skada	Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. Personuppgifter kan spridas och orsaka betydande skada på den personliga integriteten.
(1) Måttlig skada	Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten.
(0) Försumbar skada	Inga svårigheter för verksamheten att nå målen. Ingen eller endast försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Ingen eller försumbar skada på den personliga integriteten för enskild individ, vare sig avseende fysisk, ekonomisk eller integritetsrelaterad skada.

IT stödet får då en viss profil, t.ex. 1-2-2. Här är några exempel på hur det kan se ut när information klassats:

Informationstyp	Konfidentialitet	Riktighet	Tillgänglighet
Öppettider badhus	0	1	1
Personaluppgift	1	1	1
Patientjournal	2	3	3

Informationstyp	Konfidentialitet	Riktighet	Tillgänglighet
Skyddade personuppgifter	3	3	3
Krisplan	1	3	3

Skyddsåtgärder kan sedan kopplas till de olika informationsklasserna. Olika typer av åtgärder kan användas för att uppfylla skyddskraven för de olika aspekterna. Exempel:

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet
Höga skyddskrav (3)	Kryptering, vid lagring och överföring. Stark inloggning.	Två-faktors autentisering, exvis SITHS-kort, BankID, Freja e-id	Spegling av databas, daglig säkerhetskopiering
Normala skyddskrav (1)	Inloggning med användarnamn och lösenord	Inloggning med användarnamn och lösenord	Regelbunden säkerhetskopiering

Vad ska klassificeras?

Det är informationen som är den primära tillgången och som ska klassas, och som sedan styr vilka skyddsåtgärder de olika nivåerna av skyddskrav medför. Resurser som används för att hantera informationen, t.ex. programvaror, tjänster och fysiska tillgångar, ska utformas och anpassas till de krav som klassningen i förlängningen ställer på dessa. IT-system ska klassas på grundval hur informationen är klassad som finns i eller hanteras av systemen. En viktig uppgift för objektägare och förvaltningsledare är därför att klassa sina system så att rätt skyddskrav erhålls. Riktlinjer för detta finns i Kapitel C.

Riktlinjer för informationssäkerhet i verksamhetsnära förvaltning återfinns i Kapitel C

Informationsklassning har nyligen påbörjats i Umeå kommun, och långt ifrån all information är klassad. Målsättningen är främst att kritisk information ska klassas som har höga skyddskrav för en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet.

Användningsområden och målgrupper

Modellen vänder sig dels till de i Umeå kommun som är verksamhetsansvariga och/eller ägare av information och förvaltningsobjekt, dels till de som ansvarar för att rätt nivå av skydd skapas och upprätthålls. Den klassade informationen utgör ett underlag för en

verksamhet vid kravställning av tjänster, exempelvis IT-tjänster, både internt och externt. Klassningsmodellen kan därigenom fungera som ett gemensamt ramverk och kommunikationsmodell vid förhandling mellan beställare och leverantör av tjänster.

Identifiering och klassificering av information bör ske initialt när informationssäkerhetsbehovet ska analyseras men även som ett led i löpande förbättring eller vid förändringar av verksamheter eller IT-system.

För de flesta medarbetare gäller endast aspekten Konfidentialitet, vilket betonas i Kapitel A som riktar sig till alla medarbetare. Där illustreras en version av klassningsmodellen som endast innehåller aspekten konfidentialitet (Figur 2 och figur 4).
En mer utförlig vägledning som stöd för informationsklassning avses att skapas i framtiden.

B4 Ledningssystem för informationssäkerhet

Riktlinjer för ledningssystem för informationssäkerhet (LIS)	
B 4.1	Umeå kommun ska designa och införa ledningssystem för informationssäkerhet

I Umeå kommuns informationssäkerhetspolicy anges att man ska bedriva ett systematiskt informationssäkerhetsarbete. Med fördel baseras detta på standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS).

Ett LIS är ett etablerat begrepp för ett systematiskt arbete med informationssäkerhet och innebär en metodik som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. LIS avser här inte ett IT-baserat system, även om IT-stöd kan användas i delar av ett LIS.

Eftersom kommunen och dess omvärld är i ständig förändring är informationssäkerhetsbehovet dynamiskt och måste ständigt anpassas till exempelvis organisationsförändringar, nya lagar, nya hotbilder och strömningar i samhället. Det räcker därför inte att skapa en skydd som svarar mot interna och externa förutsättningar idag, eftersom dessa kan se annorlunda ut i morgon. Ett systematiskt arbete med informationssäkerhet med ett LIS syftar i stort till att informationssäkerheten över tid anpassas efter interna och externa förutsättningar, och som därigenom upprätthåller en lämplig skyddsnivå över tid. I Umeå kommun har arbetet med att skapa ett LIS påbörjats i och med dessa riktlinjer där roller, ansvar och informationsklassning är viktiga element. Att planera och införa ett LIS kommer dock att fortgå under de närmaste åren.

Tillsynsmyndigheter (Integritetsskyddsmyndigheten, IVO m.fl.) rekommenderar att kommuners informationssäkerhetsarbete och LIS utgår från standardserien SS-ISO/IEC 27000. Standardserien innefattar en stor mängd standarder, men två standarder kan sägas utgöra seriens huvudstandarder:

- **SS-ISO/IEC 27001 – Informationsteknik – Säkerhetstekniker Ledningssystem för informationssäkerhet – krav.** Denna standard ställer som namnet antyder krav på ett LIS, dvs. vad det ska innefatta. I standardens bilaga A finns ett antal säkerhetsåtgärder som tjänar som utgångspunkt för vilka säkerhetsåtgärder som ska finnas
- **SS-ISO/IEC 27002 – Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder.** Denna standard ger vägledning för införande av säkerhetsåtgärderna i föregående standards bilaga A.

Dessa båda standarder är i Sverige och internationellt dominerande ramverk för styrning av informationssäkerhet. Sedan år 2009 är det exempelvis tvingande för svenska statliga myndigheter att tillämpa dessa enligt MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2016:1, tidigare MSBFS 2009:10). Standarderna i serien utgår från ett verksamhetsdrivet och riskorienterat arbete med informationssäkerhet, i motsats till ett teknikdrivet. Utgångspunkten är också att det är information som ska skyddas, utifrån de tre aspekterna konfidentialitet, riktighet och tillgänglighet, medan IT är sekundära resurser som används för att hantera informationen.

Att standardserien är så etablerad och spridd innebär fördelar. Förutom att man tar tillvara samlade kunskaper och erfarenheter från hela världen så använder man ett gemensamt ramverk och en gemensam terminologi som underlättar vid kommunikation och samverkan med andra aktörer, exempelvis i samband med utbildning, revisioner och upphandlingar. Det finns även andra standarder i standardserien som framöver kan vara av intresse för Umeå kommun, exempelvis för mätning av informationssäkerhet (27004) och hantering av informationssäkerhetsincidenter (27035).

Ett LIS för Umeå kommun kommer att planeras och införas under ledning av informationssäkerhetssamordnare, arbetet startade under år 2020. Detta kommer att omfatta samtliga delar av informationssäkerhetsarbetet i kommunen.

B 5 Personalsäkerhet

Riktlinjer för personalsäkerhet före och i samband med anställning	
B 5.1	Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras.
B 5.2	Anställning av kritiska roller ska genomgå förstärkt kontroll i form av

	kreditupplysning och kontroll i brottsregister.
B 5.3	För befattningar som har betydelse för Sveriges säkerhet, och som omfattas av Säkerhetsskyddslagen (2018:585) ska det i anställningsförfarandet genomföras en registerkontroll. Säkerhetsskyddschef beslutar om detta.
B 5.4	Nyanställda ska via anställande chef delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för medarbetare enligt dessa riktlinjer. Och annat ansvar som följer med rollen, t.ex. informationsägarskap
B 5.5	Anställda som får tillgång till **sekretess** information ska skriva på en sekretessförbindelse som används för att påminna om tystnadsplikten. Samtidigt ska den anställde informeras om meddelarfrihet.

Riktlinjer för personalsäkerhet under anställning	
B 5.6	Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet.
B 5.7	Roller som har särskilda uppgifter inom informationssäkerhet ska får lämplig fortbildning inom området som är relevant för deras befattning
B 5.8	Arbetsrättsliga åtgärder kan behöva vidtas då anställda har brutit mot gällande informationssäkerhetsregler.

Riktlinjer för personalsäkerhet för avslut eller ändring av anställning	
B 5.9	Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras vid anställningstillfället eller tillträdande av roll och framgå i sekretessförbindelse.
B 5.10	Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.
B 5.11	Närmaste chef är ansvarig för att avbeställa behörigheter, passerkort, utrustning, smarta kort (SITHS) mm utifrån fastställda rutiner som gäller vid avslutning av anställning.
B 5.12	När anställning avslutas ansvarar närmaste chef för att information som är av vikt för andra inom verksamheten lagras på annan lagringsplats än användarens

	OneDrive/Google Drive (Utbildning) mfl.

Personal är den viktigaste resursen i kommunen, och det är personal som dagligen hanterar information, manuellt eller med stöd av IT. Många roller kommer i kontakt med och hanterar kritisk och känslig information, och det är därför av största vikt att personalen får information och utbildning om informationssäkerhet, och att det finns rutiner i samband med anställning, förändring och avslut av anställning.

Före och i samband med anställning

Bakgrundskontroll av sökande till tjänster i Umeå kommun ska ske genom verifiering av sökandes meritförteckning, t.ex. genom kontakt med referenser och bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer.

För vissa kritiska tjänster krävs en förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister. Sådana kritiska tjänster är högre chefstjänster, säkerhetstjänster, eller för de som har åtkomst till känslig eller samhällsviktig information.

Lagsstiftningen om registerkontroll för skydd av barn och unga ska självklart efterlevas.

För befattningar som har betydelse för rikets säkerhet, och således omfattas av Säkerhetsskyddslagen (2018:585), ska det i anställningsförfarandet genomföras en registerkontroll. Registerkontrollen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. De befattningar som är aktuella framgår av Umeå kommuns säkerhetsskyddsanalys och -plan. Registerkontrollen administreras av säkerhetsskyddschef.

Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande hantering av personuppgifter.

Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för medarbetare enligt dessa riktlinjer. Delgivning och utbildning ska också ges kopplat till annat ansvar som följer med rollen, t.ex. informationsägarskap.

Alla anställda som får tillgång till sekretessinformation ska skriva på en sekretessförbindelse som används för att påminna om tystnadsplikten. Den anställde ska samtidigt informeras om sin rätt att offentliggöra uppgifter enligt meddelarfriheten, med de begränsningar som finns i offentlighets- och sekretesslagen. Den lagstadgade tystnadsplikten för sekretesskyddad information som den anställde får del av i tjänsten gäller även efter att anställningen upphört.

Under anställning

I enlighet med informationssäkerhetspolicyn ska medarbetare inom kommunen ha ett högt medvetande avseende informationssäkerhet. Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet.

Roller som har särskilda uppgifter inom informationssäkerhet, t.ex. inom IT-säkerhet eller förvaltningsorganisationen, ska få lämplig fortbildning inom området som är relevant för respektive befattning. Om anställda bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras individuellt av ansvarig chef med stöd från personalfunktionen på samma sätt som vid andra ärenden gällande misskötsamhet.

Avslut eller ändring av anställning

Vid avslut eller ändring av anställning kan ansvar och skyldigheter för informationssäkerhet förbli gällande, exempelvis sekretessförbindelse och tystnadsplikt om den anställde haft tillgång till konfidentiell information. Detta ska definieras och kommuniceras till den anställde vid anställning/tillträdande av roll och framgå i sekretessförbindelsen. Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.

B6 Leverantörsrelationer

Riktlinjer för leverantörsrelationer	
B 6.1	Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Umeå kommuns modell för informationsklassning. Vägledningen ska användas som stöd vid extern upphandling av IT-tjänster (se intranätet, IT upphandlingsmodellen)
B 6.2	Det ska finnas ett dokumentationsstöd för kontroll av IT-tjänst. Syftet med vägledningen ska vara att säkerställa att IT-tjänsten kan skydda verksamheten och dess information under hela dess livscykel

Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Umeå kommuns modell för informationsklassning. Kravkatalogen ska kunna användas som stöd vid extern upphandling av IT-tjänster såsom system och molntjänster. En kravkatalog baserad på KLASSA-krav togs fram under år 2019

Det ska finnas ett dokumenterat stöd som beskriver hur en kontroll av en IT-tjänst ska genomföras. Den ska kunna användas som stöd inför användandet av en ny tjänst eller vid kontroll av en befintlig tjänst/leverantör.

Riktlinjer för upphandling av IT-resurser återfinns i avsnitt D7.
Riktlinjer för kontroll av IT-tjänst återfinns i avsnitt C9.

B7 Efterlevnad och granskning

Riktlinjer för efterlevnad och granskning av informationssäkerhet	
B 7.1	Efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet ska följas upp.
B 7.2	Umeå kommuns informationssäkerhet ska utsättas för oberoende extern granskning

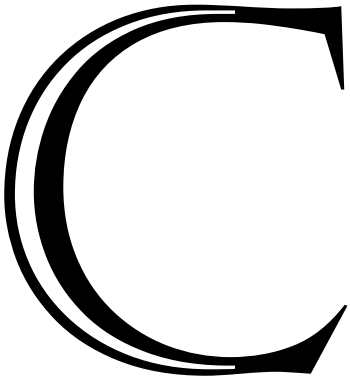
Efterlevnad av de styrande dokumenten Informationssäkerhetspolicy och detta dokument ”Riktlinjer för informationssäkerhet” ska följas upp. I praktiken innebär det främst att riktlinjerna för informationssäkerhet granskas och följs upp; att riktlinjerna efterlevs och att säkerhetsåtgärder införs och får avsedd verkan.
I synnerhet gäller detta de särskilda säkerhetsåtgärder som gäller för information, objekt och IT-resurser med **höga skyddskrav**.

Granskning och uppföljning av informationssäkerhet, inklusive dess styrning, kommer att utvecklas i och med det ledningssystem för informationssäkerhet (LIS) som ska införas i kommunen då en väsentlig del i ett LIS handlar om efterlevnadskontroll.

Granskning av hela eller stora delar av Umeå kommuns informationssäkerhet ska göras regelbundet, genom kommunrevisionen eller av annan granskande part.

Granskning av efterlevnad av informationssäkerhet bör också genomföras av extern part, exempelvis på uppdrag av kommunrevisionen.

Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till IT-säkerhetsansvarig. IT-säkerhetsansvarig avgör om informationssäkerhetsråd behöver informeras. Granskning av IT-säkerhet för IT-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls.
Detta regleras av riktlinjer i Kapitel D – Informationssäkerhet i IT-miljön (avsnitt D10).



Kapitel C Informationssäkerhet i verksamhetsnära förvaltning

Inledning

Umeå kommun har beslutat att tillämpa en modell för förvaltningsstyrning, och enligt kommunens modell för förvaltningsstyrning finns ett antal principer och regler som gäller för detta. Det här kapitlet kompletterar dessa och riktar sig främst till roller i denna. I Kapitel D som riktar sig till Umeå kommuns IT-funktion återfinns informationssäkerhetsrelaterade riktlinjer för den IT-nära förvaltningen. Om man för ett system eller en systemgrupp ännu inte har börjat tillämpa förvaltningsstyrning så ska det ändå finnas en utsedd ägare för det aktuella systemet och som då ansvarar för säkerheten i systemet. De riktlinjer som finns i detta kapitel gäller även för dessa.

Roller och ansvar

Här beskrivs ansvar rörande informationssäkerhet för rollerna i den verksamhetsnära förvaltningen. Motsvarande ansvar för de IT-nära rollerna återfinns i Kapitel D – informationssäkerhet i IT-miljön. Som nämnts ovan är dessa ansvar tillägg till generella ansvar enligt förvaltningsstyrningsmodellen.

Objektägare

I enlighet med Umeå kommuns informationssäkerhetspolicy är objektägare ansvarig för objektets informationssäkerhet. Objektägarens motsvarighet i den IT-nära förvaltningen är objektägare IT. Objektägaren ansvarar för att Umeå kommuns informationssäkerhetspolicy och dessa riktlinjer efterlevs i objektet. Objektägaren ska besluta om objekts informationssäkerhetsnivåer genom att klassning sker i enlighet med Umeå kommuns modell för informationsklassning. Objektägaren ska tilldela tillräckligt med resurser i objektets förvaltningsplaner så att informationssäkerhetsnivån kan uppnås.

Förvaltningsledare

Förvaltningsledaren leder förvaltningsarbetet och i det ansvaret ingår att system eller grupper av system (s.k. IT-komponenter) i förvaltningsobjekt klassas så att rätt skyddsnivåer uppnås, och att informationssäkerhetsrelaterade mål och åtgärder nås respektive

genomförs. Förvaltningsledarens motsvarighet i den IT-nära förvaltningen är förvaltningsledare IT. Förvaltningsledare kan vid behov delegera arbetsuppgifter till objektspecialister och objektsamordnare.

Objektspecialist

Objektspecialister ansvarar för att utföra informationssäkerhetsrelaterade aktiviteter på uppdrag av förvaltningsledare eller objektsamordnare.

Informationsägare

En informationsägare är den som har ansvar för en viss informationstillgång. Informationsägaren ska avgöra hur informationen ska klassas och utifrån denna ställa krav på hur information kan och får hanteras och användas. Om ett system har en homogen mängd information som kan kopplas till den verksamhet som en objektägare ansvarar för, är normalt objektägaren även informationsägare. I de fall objektägaren inte också är informationsägare för informationen i objektet (t.ex. ett diariesystem som hanterar många olika slag av information), så är informationsägare istället kravställare på objektägaren vad gäller säkerheten för den aktuella informationen.

C 1 Dokumentation av informationssäkerhet

Informationssäkerhet i förvaltningsplaner	
C 1.1	Informationsrelaterade mål och åtgärder ska finnas med i objekts förvaltningsplaner

Systemsäkerhetsbeskrivning	
C 1.2	System ska ha en systemsäkerhetsbeskrivning där systemets informationssäkerhet är dokumenterad.
C 1.3	Denna systemsäkerhetsbeskrivning ska gås igenom och vid behov revideras, förslagsvis årligen.

Informationssäkerhet ska vara en naturlig del i förvaltningen av objekt och de IT-komponenter som ingår i objekt. Ett system är en IT-komponent. Säkerhetsförhållanden ska vara dokumenterade i systemsäkerhetsbeskrivningar och planerade säkerhetsåtgärder ska

ingå i förvaltningsplan så att de formellt fastställs av objektägaren och har en budget. Informationsrelaterade mål och åtgärder ska finnas med i objekts förvaltningsplaner. Mål och åtgärder kan uppkomma eller motiveras med exempelvis resultat från riskanalyser och revisioner, erfarenheter från inträffade incidenter eller krav i dessa riktlinjer.

Systemsäkerhetsbeskrivning

Objekts säkerhetsförhållanden ska dokumenteras systemsäkerhetsbeskrivningar. En systemsäkerhetsbeskrivning ska finnas för varje system. Av systemsäkerhetsbeskrivningen ska det framgå:

• Vilka informationstillgångar som hanteras i systemet och hur dessa är klassade (se avsnitt C2)

• Hur systemet är klassat (se avsnitt C2)

• Hur behörighetshantering och loggning går till (se avsnitt C3)

• Hur ändringshantering går till (se avsnitt C4)

• Användarinstruktioner med inriktning på säkerhet (se avsnitt C5)

• Planerade och genomförda riskanalyser och resultat från dessa (se avsnitt C6)

• Hur incidenthantering går till och vilka incidenter som har inträffat med referenser till incidentrapporter (se avsnitt C7)

• Vilken kontinuitetshantering som finns (se avsnitt C8)

C 2 Informationsklassning och systemklassning

Riktlinjer klassning av förvaltningsobjekt	
C 2.1	Kritiska informationstillgångar i system ska vara inventerad och klassad enligt Umeå kommuns modell för informationsklassning
C 2.2	System ska klassas som helhet baserat på den klassning som är gjord av kritisk information i systemet
C 2.3	Särskilda rutiner och regler för ett system ska upprättas för hantering av **Hög Sekretess information**, som exempelvis skyddade personuppgifter.

Informationsklassning innebär att information klassas i olika nivåer utifrån dess skyddskrav. Genom att klassa information på detta sätt kan man identifiera känslig och kritisk

information så att denna får tillräckligt skydd, men ibland också för att undvika att information får onödigt överskydd med höga kostnader som följd. System ska också klassas och den klassningen ska baseras på hur den ingående informationen är klassad. Klassning av information och system ska ske i enlighet med Umeå kommuns modell för informationsklassning som beskrivs i Kapitel B.

Informationsklassning ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Umeå kommuns verksamheter. KLASSA verktyget ska användas som stöd för klassningen.

Frågor man ska ställa sig när man klassar är:

• Vilka konsekvenser blir det om informationen läcker till obehöriga (konfidentialitet)?

• Vilka konsekvenser blir det om informationen är felaktig eller inaktuell (riktighet)?

• Vilka konsekvenser blir det om (behöriga) inte får tillgång till informationen (tillgänglighet)?

När man klassar en informationstillgång enligt modellen ska den bedömas utifrån alla tre aspekter och får då en viss klassningsprofil. En viss informationstillgång kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet. En sådan informationstillgång kan då få klassningsprofilen 1-2-2.

Klassning av ett system ska baseras på klassningen av den information som systemet hanterar. Ett system kan lägst ges den klassning som den ingående informationen har.

Exempel:

Informationstillgång	Konfidentialitet	Riktighet	Tillgänglighet
Information 1	0	1	1
Information 2	1	2	1
Information 3	1	1	2
Systemklassning	1	2	2

Om ett system innehåller många olika mängder information som ännu inte är klassad kan man behöva göra preliminär klassning av systemet tills all informationsklassning är gjord. Om man vet att det finns **höga skyddskrav** för någon informationstillgång i någon aspekt så får systemet automatiskt **höga skyddskrav** för denna aspekt. Vid osäkerhet är det bättre att ”överklassa” än att ”underklassa”.

Det viktiga är att kritisk information, dvs. information med **höga skyddskrav** i någon av de tre aspekterna, är identifierad och klassad därefter så att tillräckligt skydd kan skapas för systemet. Hur system klassats utgör ett underlag vid kommunikation och kravställning mot den IT-nära förvaltningen eller mot externa leverantörer.
Kapitel D riktar sig mot kommunens IT-funktion och där finns särskilda säkerhetsåtgärder för system med **höga skyddskrav**.

Klassningen av system ger också ett underlag för hur användare kan och får arbeta i system. I Kapitel A som riktar sig till samtliga medarbetare finns en mängd hanteringsregler som i vissa fall skiljer sig beroende på hur information är klassad.
Särskilda rutiner och regler ska upprättas för hantering av **Hög Sekretess** information, som exempelvis skyddade personuppgifter. Sådana rutiner och regler ska finnas med i användarinstruktioner (se avsnitt C5).

C 3 Behörighetshantering och loggning

Riktlinjer för behörighetshantering och loggning	
C 3.1	Det ska finnas dokumenterade processer och/eller rutiner för hantering av behörigheter och rättigheter till system
C 3.2	Varje användare ska ha ett unikt Användar-ID.
C 3.3	Externa användares åtkomst bör vara tidsbegränsad samt föregås av sekretessförbindelse.
C 3.4	Det ska finnas dokumenterade rutiner för logghantering i objekt
C 3.5	**Höga skyddskrav** på konfidentialitet, riktighet eller tillgänglighet innebär också höga krav på spårbarhet. Loggning av användares aktiviteter i sådana system är obligatorisk
C 3.6	Förändringar i anställningar och roller ska omedelbart rapporteras av närmaste chef till personalavdelningen så att reglering sker i personal- och lönesystem
C 3.7	Uppföljning ska ske av behörighetshantering och logghantering i objekt

Behörigheter innebär vissa rättigheter att använda en informationstillgång, exempelvis ett system, på ett specificerat sätt. Behörigheter, eller åtkomsträttigheter, definierar vad en användare har rätt att utföra, t.ex. läsa, söka, skriva, radera, skapa eller köra ett program.

För att skydda information mot obehörig åtkomst behöver användare ange en identitet som kan verifieras (autentiseras), vanligen med användar-ID och lösenord. Ju känsligare information som bearbetas, desto högre är kravet på skydd mot obehörig åtkomst.

Grundprincipen för behörighet ska baseras på vilken information användare behöver för att kunna utföra sina arbetsuppgifter (s.k. need-to-know). Olika roller som använder ett system kan ha olika behov av information och ska därför ha olika typer av behörigheter eller s.k. åtkomstprofiler.
En förutsättning för rätt behörighetstilldelning är att informationen är strukturerad och klassad så att rätt åtkomstregler kan upprättas.

Inom vissa områden, som t.ex. vård och omsorg, behöver man ha (teknisk) behörighet till en stor mängd information. I akuta situationer måste kanske annan vårdande personal än den ordinarie ha åtkomst till patientinformation. Här behövs istället regelstyrd åtkomstkontroll, där regler säger att man inte får ta del av information som inte rör ens arbetsuppgifter. Sådan åtkomstkontroll måste kompletteras med funktioner för uppföljning, övervakning och loggning. Detta kan – och ska – påverka användarna så att dessa avhåller sig från otillåtna men tekniskt möjliga operationer i ett system.

Objektägare bestämmer vilka som ska få tillgång till system som ingår i objekt och vilka behörigheter dessa ska ha. Verksamhetens art och dess krav på informationens konfidentialitet och riktighet, tillsammans med legala krav som lagar, föreskrifter och avtal, styr hur behörigheterna ska se ut. För externa användare gäller att tilldelning av åtkomst, utöver de regler som gäller all åtkomsttilldelning även ska vara tidsbegränsad för endast den tiden som behövs för att utföra uppgiften samt föregås av sekretessavtal.

Varje användare ska ha ett unikt Användar-ID, dvs. gruppidentiteter är inte tillåtna (under vissa förutsättningar kan dock detta beviljas, se information under D.2.14).

Det ska finnas en process eller rutiner som underhåller och förvaltar behörigheter för ett system, exempelvis hantering av beställning, ändring och borttagning av behörigheter och rättigheter. Förändringar i användares roller måste återspeglas i behörighetshanteringen, t.ex. att användare får andra arbetsuppgifter eller avslutar sin anställning.

För priviligierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med priviligierade åtkomsträttigheter slutar eller byter tjänst. Sådana processer eller rutiner måste vara kopplade till den IT-nära förvaltningen så att tekniska förändringar genomförs. Objektägare IT ska säkerställa den del av rutinen som rör införande, förändring samt borttagning av åtkomst i IT-resurser. I Kapitel D finns riktlinjer för hur åtkomstkontroll ska ske i IT-miljön (avsnitt D2 – Styrning av åtkomst). Exempelvis ska stark autentisering finnas

för åtkomst till system som innehåller information med **höga skyddskrav** på konfidentialitet och riktighet.

Vid anställning, förändring av roll eller arbetsuppgifter samt vid upphörande av anställning ska närmaste chef omedelbart rapportera detta till personalavdelningen så att reglering sker i personal- och lönesystemet.

Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

Logghantering

För att erhålla spårbarhet och att exempelvis möjliggöra incidentutredningar samt för att upptäcka avvikelser från legala eller interna regelverk bör system övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Detta är särskilt viktigt, och obligatoriskt, om system hanterar information med **höga skyddskrav** eller om regelstyrd behörighetshantering används i stället för teknisk dito.

Då loggning används ska det finnas processer eller rutiner för dess hantering. Sådana ska innefatta hur loggning går till, hur loggar skyddas mot manipulation och obehörig åtkomst, hur länge de sparas och hur de granskas. I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av Dataskyddsförordningen. Detta innebär bland annat att om kontroller utförs för andra syften än det ursprungliga är lagkravet att personen ska informeras och ge sitt samtycke. Processer och rutiner för loggning ska följas upp och dokumenteras.

C4 Ändringshantering

Riktlinjer för ändringshantering	
C 4.1	Det ska finnas dokumenterade processer eller rutiner för hantering av ändringar i system.
C 4.2	Vid avveckling av system ska en plan upprättas för hur information ska migreras, raderas eller slutarkiveras (i enlighet med den kommungemensamma arkiveringsplanen).

Ändringar i system ska ske i enlighet med Umeå kommuns beslutade förvaltningsobjektmodell. Det innebär att ändringar ska ske på ett strukturerat sätt för att säkra systemets säkerhet, funktionalitet och användbarhet och för att minimera antalet fel orsakade av förändringen.

Ändringar kan bero på exempelvis, önskemål från verksamhet/användare, fel eller brister, förändringar i legala krav eller nya versioner från systemleverantörer.

Ändringar i system ska vara samordnade med en Change management-process el.likn. inom den IT-nära förvaltningen.

I Kapitel D som riktar sig till den IT-nära förvaltningen finns riktlinjer som rör bl.a. systemtest och hantering av testdata (avsnitt D7 – Anskaffning och utveckling av IT-resurser).

Avveckling av system ska ske på ett strukturerat sätt och i samråd med Stadsarkivet så att information hanteras i enlighet med den kommungemensamma arkiveringsplanen.

Större förändringar i eller omkring ett system ska föregås av en riskanalys (se avsnitt C6 – Riskanalyser).

C 5 Användarinstruktioner

Riktlinjer för användarinstruktioner	
C 5.1	Informationssäkerhetsregler ska finnas med i användarinstruktioner.
C 5.2	Det ska finnas särskilda instruktioner för hantering av **konfidentiell** information som t.ex. skyddade personuppgifter (**Hög Sekretess** (Röd))

Objektägare ansvarar för att det finns användarinstruktioner för samtliga användare till ett system. Användare ska utbildas enligt instruktionerna och kontroll ska göras att instruktionerna efterlevs. Användarinstruktionerna ska omfatta följande delar inom informationssäkerhet:

- Regler kring inloggning och lösenordshantering
- Behörigheter
- Särskilda instruktioner för hur konfidentiell information får hanteras, t.ex. känsliga eller skyddade personuppgifter
- Information om vad som loggas och konsekvenser av att bryta mot användarinstruktioner, t.ex. att ta del av eller sprida konfidentiell information
- Incidentrapportering – användare ska vara vaksamma på brister och incidenter i systemet och veta hur man ska rapportera dessa (se avsnitt C7 – Incidenthantering).
- Eventuell sekretessförbindelse

Användare är naturligtvis även skyldiga att följa riktlinjerna i Kapitel A.

C6 Riskanalys

Riktlinjer för riskanalyser	
C 6.1	Riskanalyser ska genomföras i samband med större förändringar i eller omkring system
C 6.2	Riskanalysresultat ska dokumenteras. Akuta risker ska tas om hand skyndsamt och återstående åtgärder ska tas med i förvaltningsplaner
C 6.3	Ett riskhanteringsbeslut ska fattas för varje allvarlig risk som identifieras under riskbedömning. En åtgärdsplan kan vara ett sådan riskhanteringsbeslut.

Risker är tänkbara oönskade händelser som kan inträffa och som kan ha en negativ påverkan på mål. Antingen på mål med själva systemet eller på verksamheters mål. En risk är en kombination av hur sannolikt det är att en händelse inträffar och vilken konsekvens händelsen innebär. Vid större förändringar, t.ex. större systemuppdateringar, nyutveckling, nya användargrupper eller extern åtkomst, liksom när en ändring påverkar andra system som inte förvaltas inom samma objekt, ska en riskanalys genomföras där Umeå kommuns grundmetod för riskanalys ska användas. Det kan också vara förändringar utanför själva systemet eller dess kontroll som motiverar en riskanalys, exempelvis ägarbyte av en systemleverantör eller en omorganisation som berör den verksamhet som systemet stödjer. Riskanalysens resultat ska dokumenteras. En riskanalys kan leda till åtgärdsbehov som behöver genomföras omedelbart eller på lite längre sikt och kan då tas med i kommande förvaltningsplan.

C 7 Incidenthantering

Riktlinjer för incidenthantering	
C 7.1	Det ska finnas rutiner för hur användare ska rapportera incidenter
C 7.2	Akuta incidenter ska åtgärdas skyndsamt
C 7.3	Allvarliga incidenter ska utredas och dokumenteras enligt gällande mall[1].
C 7.4	Avbrottsplaner ska upprättas som innehåller ansvarsförhållanden, kontaktpersoner och eskaleringsvägar.
C 7.5	Samtliga incidenter som rör objektet ska dokumenteras och sammanställas[2].

[1] Mall incidentrapport (länk)

	Kvarstående åtgärdsbehov ska tas om hand i förvaltningsplaner.
C7.6	Personuppgiftsincidenter kopplade till objektet ska anmälas enligt särskild rutin

Informationssäkerhetsrelaterade incidenter är oönskade händelser som kan, eller skulle kunnat, leda till brister i konfidentialitet, riktighet eller tillgänglighet hos information. Objektägare ansvarar för att incidenter relaterade till system upptäcks, samlas in, hanteras, sammanställs och dokumenteras.

Incidenter kan delas in i mindre incidenter och allvarliga incidenter (major incidents). Mindre incidenter är t.ex. mindre tekniska fel i system eller att enstaka användare inte följer användarinstruktioner. I systemets användarinstruktioner ska det finnas rutiner för hur användare ska rapportera mindre incidenter (se C5 – Användarinstruktioner). Incidentrapporter ska mottas och lämpliga åtgärder ska vidtas.

Allvarliga incidenter är större störningar i ett system som t.ex. ett längre avbrott (några timmar eller mer), dataintrång eller infektion av skadlig kod. En allvarlig incident kräver en utredning där dokumentation ska göras enligt gällande mall för allvarliga IT-relaterade incidenter. Utredningen ska drivas av förvaltningsledaren i samverkan med relevanta aktörer, inte minst driftchef på IT. Om personuppgifter behandlas ska en anmälan om personuppgiftsincident göras. Personuppgiftsincidenten utreds separat men resultatet från förvaltningsledarens utredning kan användas som underlag för bedömning av personuppgiftsincidenten, en samordning mellan personuppgiftskoordinator och förvaltningsledare kan därför vara lämpligt.

Förvaltningsledare ska upprätta avbrottsplaner att använda vid större avbrott och som ska innehålla ansvarsförhållanden, kontaktpersoner, eskaleringsvägar till interna och externa aktörer. Här ska samverkan ske med den IT-nära förvaltningen.

Flera fall av mindre incidenter av likadan art kan tillsammans utmynna i eller utgöra en allvarlig incident. Ett antal störningar i systemet av samma typ som var för sig betraktas som mindre incidenter kan tillsammans innebära en allvarlig incident. Både mindre och allvarliga incidenter kan vara av akut art och behöva åtgärdas skyndsamt.

Förvaltningsledare ska årligen sammanställa samtliga incidenter som varit kopplade till objektet och som har haft eller kunde ha haft påverkan för verksamhetens informationssäkerhet. Sammanställningen ska redovisas till objektägare för

[2] Använd underlag för aggregerad incidentanalys

förvaltningsobjektet, dokumentet är ett viktigt indata till ledningens genomgång för informationssäkerhet.

Kvarstående åtgärdsbehov som inträffade incidenter medfört ska tas om hand i förvaltningsplaner.

C 8 Kontinuitetshantering

Riktlinjer för kontinuitetshantering	
C 8.1	Reservplaner och manuella rutiner ska finnas för kritiska objekt med höga skyddskrav gällande tillgänglighet.
C 8.2	Nyckelpersonsberoende ska undvikas och åtgärdas

Krav på kontinuitet av driften av IT-komponenter sker i stora delar genom klassning. Höga skyddskrav för tillgänglighet innebär högre krav på säkerhetskopiering och redundans.

Avbrott kan dock ändå alltid ske oavsett vilka förebyggande skyddsåtgärder som finns. Beroendet av funktionalitet i IT-komponenter kan ibland vara så högt att IT-komponenter helt enkelt inte får ligga nere. I dessa fall måste verksamheten ha planer och rutiner för att kunna fullfölja sitt åtagande även vid teknikavbrott.

Nyckelpersonsberoende ska undvikas och i den mån det framkommer att organisationen är beroende av nyckelpersonal ska nyckelpersonberoendet åtgärdas t.ex. genom utbildning av ersättare. Nyckelpersonsberoende kan också minskas genom att använda vedertagen standard och standardprodukter.

C 9 Kontroll av IT-tjänst

Riktlinjer för kontroll av IT-tjänst	
C 9.1	Innan en verksamhetsansvarig börjar använda en IT-tjänst ska den kontrollera (enligt vägledningen för kontroll av IT-tjänst) att tjänsten kan leverera rätt skydd för verksamhetens information.
C 9.2	Innan en verksamhetsansvarig börjar använda en IT-tjänst ska den ta beslut kring de risker som ett sådant användande kan ge upphov till.
C 9.3	Endast information som är klassad (informationsklassning) får användas i externa IT-tjänster och molntjänster.

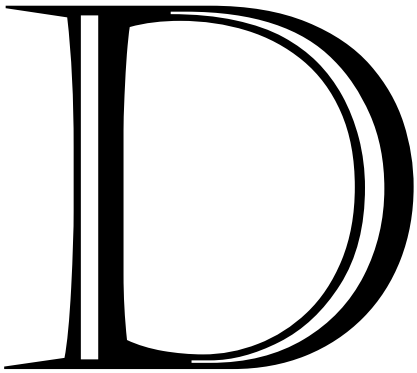
C 9.4	**Känslig Sekretess** (Gul) och **Hög Sekretess** (Röd) får endast lagras i en IT-tjänst som är tillräckligt kontrollerad, risken acceptabel och att lagringen av information inte bryter mot några författningar
C 9.5	IT-tjänster som lagrar **Känslig Sekretess** (Gul) och **Hög Sekretess** (Röd) information ska kontrolleras minst en gång om året.

Verksamhetsansvarig är ansvarig för informationssäkerheten inom sitt verksamhetsområde, det innebär även att säkerställa att dess processer, verktyg, personal och resurser har rätt skyddsnivå.

Korrekt informationssäkerhet ska säkerställas under hela livscykeln och innebär att verksamhetsansvarig behöver försäkra sig om att rätt skyddsnivå är uppnådd och tydligt acceptera eventuella risker.

Att avgöra rätt skyddsnivå innebär bland annat att genomföra verksamhets- och juridiska analyser genom informationsklassningar. Förutom att kontrollera en IT-tjänst innan användning är det lämpligt att genomföra kontroller med jämna mellanrum i den frekvens som verksamheten finner lämpligt.

Se även B.6.2 angående vägledning för kontroll av IT-tjänst.



Kapitel D: Informationssäkerhet i IT-miljön

Inledning

Detta kapitel innehåller riktlinjer rörande säkerhet Umeå kommuns IT-miljö. Riktlinjerna vänder sig därför främst till chefer och medarbetare inom Umeå kommuns IT-funktion. Riktlinjerna riktar sig också till externa parter som arbetar på uppdrag åt Umeå kommun, exempelvis inhyrda konsulter.

Informationssäkerhet i IT-miljön kan även benämnas IT-teknisk säkerhet och innefattar säkerhet i olika slag av IT-resurser som system, applikationer, verktyg och infrastruktur i form av hård- och mjukvara. Termen IT-resurser används genomgående i kapitlet på detta sätt som ett generellt samlingsnamn om ingen specifik hård- eller mjukvara avses.

Kapitlet är strukturerat utifrån nedanstående avsnitt i standarden SS-ISO/IEC 27002 som till största delar innehåller säkerhet i IT-miljöer:

Avsnitt		Kapitel i 27002
D1	Hantering av tillgångar	Kap 8
D2	Styrning av åtkomst	Kap 9
D3	Kryptering	Kap 10
D4	Fysisk och miljörelaterad säkerhet	Kap 11
D5	Driftsäkerhet	Kap 12
D6	Kommunikationssäkerhet	Kap 13
D7	Anskaffning och utveckling av IT system	Kap 14
D8	Incidenthantering	Kap 16
D9	Kontinuitetshantering	Kap 17
D10	Granskning och kontroll (även B7)	Kap 18

Standarden innehåller mer vägledning och information än vad som finns i dessa riktlinjer, och standarden kan därför användas som ett stödjande dokument för att efterleva riktlinjerna. Inom vissa områden i IT-miljön behöver mer detaljerade instruktioner tas fram som kompletterar eller konkretiserar dessa riktlinjer. Även för detta ändamål kan denna eller andra standarder liksom andra vägledningar, från t.ex. MSB, vara till stöd.

En central del i kommunens informationssäkerhetsarbete är informationsklassning. Information kan ha normala eller höga skyddskrav avseende konfidentialitet, riktighet och tillgänglighet i enlighet med Umeå kommuns klassningsmodell (se Kapitel B).

IT-resurser som hanterar information ska ges ett skydd i enlighet med dessa skyddskrav. Särskilda regler gäller i vissa fall för information som klassats enligt höga skyddskrav i en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet. Detta markeras genomgående med fetstil och rader i tabeller med riktlinjer har dubbla röda linjer.

Roller och ansvar

Ansvar för informationssäkerhet och IT-säkerhet inom IT-funktionen följer ordinarie verksamhetsansvar. Det innebär att chefer och medarbetare inom respektive ansvarsområde ansvarar för att upprätthålla rätt nivå av informations- och IT-säkerhet för de processer och de IT-resurser de ansvarar för.

Ytterst ligger ansvaret på IT-chefen i egenskap av chef för IT-funktionen. Därigenom är IT-chefen ytterst ansvarig för att säkerheten i IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt informationssäkerhetspolicyn och dessa riktlinjer för informationssäkerhet.

IT-säkerhetsansvarig

Den IT-säkerhetsansvarige samordnar arbetet med säkerheten i Umeå kommuns IT-miljö och är stödjande vid kravställning på externa aktörer.

Ansvaret för säkerheten i IT-resurser ligger inte på den IT-säkerhetsansvarige, utan dennes roll är att kravställa, stödja och kontrollera arbetet med att nå och upprätthålla rätt nivåer av säkerhet i dessa.

För den IT-säkerhetsansvarige innebär detta i huvudsak att:

- utforma och förvalta riktlinjer och instruktioner för IT-säkerhet,
- stödja verksamheter, förvaltningsobjekt och projekt i IT-säkerhetsfrågor,
- följa upp och granska efterlevnaden av riktlinjer och instruktioner för IT-säkerhet,
- stödja och bevaka framtagning och genomförande av handlingsplaner för att åtgärda brister som konstaterats i samband med säkerhetsgranskningar eller riskanalyser,
- bistå vid utredning av misstänkta och inträffade säkerhetsincidenter,
- stödja verksamheter vid extern kravställning rörande IT-säkerhet och uppföljning av externa leverantörers säkerhetsåtaganden,
- leda eller delta i verksamheters riskanalyser rörande IT-relaterade risker,
- verka för höjande av säkerhetsmedvetande inom IT,
- ta fram statusrapporter för kommunens IT-säkerhet, och
- besvara revisionsrapporter.

Den IT-säkerhetsansvarige arbetar nära kommunens informationssäkerhetssamordnare och ingår i Umeå kommuns informationssäkerhetsråd. Den IT-säkerhetsansvarige ska också

omvärldsbevaka, nätverka och samverka externt inom området med exempelvis MSB, cert.se, SIG Security, SKL och andra kommuner.

Roller i den IT-nära förvaltningen

Umeå kommun har beslutat att tillämpa en modell för förvaltningsstyrning, och i kommunens riktlinjer för förvaltningsstyrning finns ett antal principer och regler som gäller för detta. Detta kapitel kompletterar de riktlinjerna med särskilda riktlinjer rörande informationssäkerhet i den IT-nära förvaltningen.

Kapitel C riktar sig till den verksamhetsnära förvaltningen och innehåller informationssäkerhetsrelaterade riktlinjer för denna. Om man i en verksamhet ännu inte har börjat tillämpa objektförvaltningsstyrning så ska det ändå finnas en utsedd ägare för det aktuella systemet och som då har ansvaret för säkerheten i systemet. Det ska då finnas utsedda ägare, tekniker osv. på IT som kan fungera som motpart till dessa roller så att rätt nivå av säkerhet kan uppnås.

Objektägare IT

Objektägare IT ansvarar för att IT-säkerheten i IT-komponenter överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls och att aktuella IT-komponenter ges ett skydd som motiveras av klassningen av system. Objektägare IT:s motsvarighet i den verksamhetsnära förvaltningen är objektägare verksamhet. Objektägare IT ansvarar för att Umeå kommuns informationssäkerhetspolicy och dessa riktlinjer efterlevs och ska utse förvaltningsledare IT för objekt.

Förvaltningsledare IT

Förvaltningsledare IT samverkar med förvaltningsledare verksamhet och i det ansvaret ingår att IT-säkerhetsrelaterade mål och åtgärder i förvaltningsobjekt nås respektive genomförs.

Ägare av IKT-objekt

Det finns en mängd IT-komponenter som inte är förvaltningsobjekt med en ägare i verksamheten. Sådana IT-resurser ingår i IKT-objekt (Informations- och kommunikationsteknik) och kan vara underliggande infrastruktur, stödsystem m.m., och ska ha utpekade ägare som ansvarar för säkerheten i dessa.

Objektspecialister IT

Objektspecialister IT ansvarar för att utföra IT-säkerhetsrelaterade aktiviteter på uppdrag av objektägare IT, förvaltningsledare IT, ägare av IKT-objekt eller IT-säkerhetsansvarig, eller andra chefer och ansvariga inom IT.

Incident manager

En Incident Manager bevakar och analyserar incidentprocessen samt ansvarar för att rutiner för eskalering, larm och informationsspridning samt andra processer följs.

D1 Hantering av tillgångar

Riktlinjer för hantering av tillgångar	
D 1.1	IT-resurser ska identifieras och tilldelas en ägare med rollerna Objektägare IT eller IKT-objektägare.
D 1.2	Samtliga IT-komponenter som elektroniskt lagrar och bearbetar information och där information ägs av kommunal myndighet ska förtecknas i systemet RegIT. Rutiner ska finnas för att hålla förteckningen aktuell och den ska skyddas från åtkomst eller förändring av obehörig.
D 1.3	IT-komponenter ska klassas baserat på klassningen av den information som hanteras i IT komponenten och/eller baserat på klassningen av andra objekt som IT-komponenten stödjer eller påverkar.
D 1.4	Skyddsåtgärder i en IT-komponent ska motsvara dess klassning så att rätt nivå av IT-säkerhet upprätthålls under IT-komponentens hela livscykel, såväl vid införande, under drift som efter avveckling.
D 1.5	Informationssäkerhetskrav som gäller användandet av IT-komponenter ska förmedlas till användare i form av användningsinstruktioner.

Identifiering av IT-resurser och tilldelning av ägare

Samtliga IT-resurser ska vara identifierade och tilldelade en ägare. En förteckning över alla IT-resurser ska upprättas och underhållas. Förvaltningsobjekt som omfattas av förvaltningsorganisationen, exempelvis verksamhetssystem, har naturliga ägare inom IT i form av objektägare IT. Andra IT-komponenter som underliggande infrastruktur, stödsystem m.m., ingår i IKT-objekt och ska ha utpekade ägare.

Klassning av IT-resurser

IT-komponenter ska klassas i enlighet med Umeå kommuns modell för informationsklassning. Verksamhetssystem som klassats av den verksamhetsnära förvaltningen ska ges en nivå av IT-säkerhet som överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls. Underliggande IT-komponenter i form av infrastruktur, stödsystem m.m. ska ges minst motsvarande klassning. Ibland kan sådana underliggande IT-komponenter ges en högre klassning än de verksamhetssystem som de stödjer, exempelvis om IT-system stödjer ett flertal system som var för sig inte är kritiska. Om det inte går att göra en koppling mellan IT-komponenter och till klassade verksamhetssystem, får man klassa IT-komponenten utifrån en bedömning enligt konsekvensbeskrivningarna i klassningsmodellen. Eftersom långt ifrån all information och alla IT-komponenter är klassade inom kommunen, kan preliminära klassningar behöva göras för IT-komponenter. Vid osäkra fall är det viktigt att hellre ”överklassa” än ”underklassa”. Beroende på hur IT-komponenter är klassade ska olika säkerhetsåtgärder införas för att uppnå ett tillräckligt bra skydd. Bland annat ska dessa riktlinjer följas som riktar sig mot IT-miljön och som i vissa fall har särskilda krav för IT-komponenter som hanterar information med höga skyddskrav enligt en eller flera aspekter av konfidentialitet, riktighet och tillgänglighet. Ägare till IT-komponenter ansvarar för att säkerhetsnivån är tillräcklig över IT-komponentens hela livscykel, såväl vid införande, under drift som under avveckling.

Användningsinstruktioner

Det ska finnas regler och instruktioner till hur IT-komponenter får användas. Dessa ska baseras på IT-komponenternas klassning och skyddskrav enligt ovan. Regler och instruktioner ska finnas oavsett om IT-komponenten endast används inom IT, av medarbetare inom kommunen eller av externa användare. De som använder eller har tillgång till IT-komponenter ska få instruktioner om hur de hanterar dessa resurser, vilka villkor och vilket ansvar som gäller kring den åtkomst de fått sig tilldelad.

D2 Styrning av åtkomst

Riktlinjer för identifiering och autentisering	
D 2.1	Alla användare ska ha en unik användaridentitet.
D 2.2	Namn på användare, som underlag för t.ex. e-postadresser, ska vara enhetliga i kommunen och stämma överens med namnuppgift i folkbokföringen.

D 2.3	Vid åtkomst till information med **höga skyddskrav** avseende konfidentialitet eller riktighet ska stark autentisering användas.
D 2.4	Stark autentisering är krav vid fjärråtkomst till Umeå kommuns IT-miljö.
D 2.5	Fjärråtkomst för inloggning med administrativa (priviligierade) konton till IT-resurs med **höga skyddskrav** avseende konfidentialitet eller riktighet skall vara strikt styrt.
D 2.6	Lösenord är alltid konfidentiell information som har **höga skyddskrav** och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. För att minska risken för obehörig åtkomst ska följande skyddsfunktioner införas: • Tekniska funktioner implementeras där så är möjligt i IT-komponenten för att säkerställa att lösenordsregler för medarbetare avseende historik, komplexitet och åldring av lösenord följs. • Lösenord ska aldrig skickas/transporteras i klartext över nätverk. I de fall detta inte är möjligt ska tillfälliga lösenord i kombination med tvingande lösenordsbyte användas. Tillfälliga lösenord ska enbart vara giltiga för en (1) inloggning. • Lösenord får aldrig lagras på ett sätt som gör det möjligt att dekryptera dem till klartext.
D 2.7	För att minska risken för obehörig åtkomst ska samtliga klienter (datorer samt mobila enheter) förses med låsskärm så att skärm automatiskt låses efter en definierad tids inaktivitet och enbart kan aktiveras igen genom en förnyad autentisering

Styrning av åtkomst är grundläggande för att skydda information och IT-resurser. Behörigheter innebär vissa rättigheter att använda en informationstillgång, exempelvis ett system, på ett specificerat sätt. Behörigheter, eller åtkomsträttigheter, definierar vad en användare har rätt att utföra, t.ex. läsa, söka, skriva, radera, skapa eller köra ett program. Grundprincipen är att behörighetstilldelning ska baseras på användares behov till information eller till de IT-resurser (system, databaser, operativsystem eller nätverk) som dessa behöver för att kunna utföra sina uppgifter. Om information är strukturerad och klassad är det betydligt enklare att upprätta åtkomstregler och behörighetstilldelningar. Inom vissa områden kan man behöva ha (teknisk) behörighet till en stor mängd information. Det kan vara svårt att på förhand definiera arbetsuppgifter, eller i akuta situationer måste kanske annan personal än den ordinarie snabbt ha åtkomst till information, som t.ex. inom vård och omsorg. Då får teknisk åtkomstkontroll ersättas av regelstyrd åtkomstkontroll, där regler säger att man inte får ta del av information som inte rör ens arbetsuppgifter. I sådana system är det särskilt viktigt med funktioner för uppföljning, övervakning och loggning. Det samlade systemet för styrning av åtkomst i en (eller flera) IT-resurs(-er) benämns

behörighetskontrollsystem (BKS) och utgörs vanligen av både tekniska system och administrativa rutiner.

Ett BKS omfattar tre grundläggande säkerhetsåtgärder som tillsammans ska se till att verksamhetens säkerhetsregler (kontinuerligt) följs:

- Identifiering och autentisering av användares uppgivna identitet.
- Reglering av åtkomsträttigheter; vilken information man kommer åt och vad man kan göra med den, t.ex. läsa, skriva, ändra, radera
- Loggning av användarens aktiviteter.

Identifiering och autentisering

Identifiering innebär att aktiviteter och åtkomst till en IT-resurs kan knytas till en individ, därför ska alla användar-ID vara unika och personliga. Användar-ID och lösenord ger tillsammans en möjlighet till autentisering, dvs. verifiering av en uppgiven identitet.

Vid åtkomst till information med **höga skyddskrav** avseende konfidentialitet och/eller riktighet ska stark autentisering användas. Som stark autentisering räknas identifiering av en person och verifiering av personens autenticitet genom en kombination av minst två av följande tre delar:

1. Ett lösenord eller någonting annat som man *vet*

2. Ett smartkort eller någonting annat som man *har*

3. Ett fingeravtryck eller någon annan egenskap som man *är*

Stark autentisering är också krav vid extern åtkomst till Umeå kommuns IT-miljö.

Lösenord är alltid konfidentiella och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. Det innebär att rutiner ska finnas som säkerställer att lösenordet skyddas t.ex. från administratör eller handläggare oavsett om lösenordet tilldelas, förändras eller återställs.

Reglering av åtkomsträttigheter

Riktlinjer för reglering av åtkomsträttigheter	
D 2.8	Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS, i IT-resurser.
D 2.9	IT-resurser ska ha åtkomsträttigheter som motsvarar hur de är klassade.
D 2.10	Användaridentiteter och vilka individer dessa tillhör ska registreras i en gemensam AD-katalog och rutin ska finnas för att hålla denna katalog

	uppdaterad. För att garantera spårbarhet ska rutinen även innehålla kontroll så att inte tidigare identiteter återanvänds. Historikfunktion ska finnas så att förteckningen kan visa vilka identiteter som fanns och vilka individer dessa tillhörde vid varje given tidpunkt.
D 2.11	Behörigheter till IT-resurser ska vara aktuella och riktiga.
D 2.12	Åtkomst som inte längre behövs eller behov av ny åtkomst ska regleras snarast, för IT-resurser inom en arbetsdag efter att behov upphör eller uppstår. Det ska finnas rutiner kopplade till personalfunktionen för att säkerställa att sådan reglering av åtkomst kan ske vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning.
D 2.13	Administrativa rättigheter ska endast ges där så är uttryckligen nödvändigt och rättigheterna ska då vara tidsbegränsade. För tilldelning av administrativa rättigheter för användare på klienter gäller att sådan rätt i första hand ska ges tillfälligt för att t.ex. omfatta en installation av programvara och i andra hand ges för en viss tid med ett specifikt slutdatum. IT objektägare beslutar om tilldelning av priviligierad åtkomsträtt. Granskning av administrativa rättigheter ska ske löpande med täta intervall.
D 2.14	Gruppidentiteter är inte tillåtna. Eventuella undantag ska godkännas av Objektägare verksamhet och informationssäkerhetsansvarig i förening. Gruppidentiteter ska då enbart beviljas under följande förutsättningar: • Behov av gruppidentitet är tydligt beskrivet och alternativen utredda så att det framgår varför gruppidentiteten är nödvändig • Gruppidentiteten ska ha en registrerad ägare • Gruppidentiteten ska vara tidsbegränsade med tydligt slutdatum • En avvecklingsplan ska finnas för att ersätta gruppidentiteten med individuella identiteter • Ägaren av gruppidentiteten ska föra en förteckning alla som använder identiteten. Historikfunktion ska finnas så att förteckningen kan visa vilka användare som fanns vid en given tidpunkt • Autentiseringsinformation ska uppdateras om någon användare lämnar gruppidentiteten. Om en användare t.ex. lämnar en gruppidentitet med ett delat lösenord så ska lösenordet ändras och ett nytt lösenord distribueras till kvarvarande användare av gruppidentiteten • Ägaren av gruppidentiteten tar fullt ansvar för eventuellt missbruk av gruppidentiteten
D 2.15	För externa användare gäller att tilldelning av åtkomst, utöver övriga regler för åtkomsttilldelning även ska: • Tidsbegränsas att endast omfatta tiden som behövs för att utföra uppgiften • Föregås av sekretessavtal, konsultförbindelse

D 2.16	Prövning av den enskilde ska ske och den anställde ska skriva på en sekretessförbindelse som används för att påminna om tystnadsplikten innan åtkomst tilldelas till IT-resurs som innehåller information med höga skyddskrav avseende konfidentialitet.
D 2.17	Närmaste chef fattar beslut om behörighet till informationssystem och -tjänster, denne är också ansvarig för att beställa inaktivering eller avslut av behörigheter.

Åtkomst till IT-resurser ska baseras på dess klassning, exempelvis ställs större krav på metoder för autentisering vid åtkomst till information med höga skyddskrav (se ovan).

För verksamhetssystem är det objektägare eller förvaltningsledare i verksamheten som beslutar vilka som ska få tillgång till systemet och vilka behörigheter dessa ska ha, samt hur systemet är klassat. Objektägare IT ansvarar för att upprätta ett BKS som motsvarar dessa krav.

Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS, i IT-resurser. Detta inkluderar att underhålla och förvalta behörigheter, exempelvis hantering av beställning, ändring och borttagning av behörigheter och rättigheter. Förändringar i användares roller måste återspeglas i behörighetshanteringen, t.ex. att användare får andra arbetsuppgifter eller avslutar sin anställning.

Det ska finnas rutiner kopplade till personalenheten där man säkerställer att reglering av åtkomst sker vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning. Innan någon tilldelas åtkomst till IT-resurs som innehåller uppgifter konfidentiell information, ska alltid prövning av den enskilde ske och den anställde ska skriva på en sekretessförbindelse som används för att påminna om tystnadsplikten.

För externa användare gäller att tilldelning av åtkomst, utöver de regler som gäller all åtkomsttilldelning även ska vara tidsbegränsad för endast den tiden som behövs för att utföra uppgiften samt föregås av sekretessavtal.

För administrativa åtkomsträttigheter gäller att de ska vara restriktiva och ge endast de rättigheter som behövs för att utföra sitt uppdrag i den administrativa roll man har.

Regelbunden uppföljning och revision av samtliga åtkomsträttigheter ska ske kontinuerligt. För priviligierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med priviligierade åtkomsträttigheter slutar eller byter tjänst. Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

Säkerhetsloggning

Riktlinjer för säkerhetsloggning	
D 2.17	Vid åtkomst till IT-resurs och information med **höga skyddskrav** avseende konfidentialitet eller riktighet krävs loggning av åtkomst för att erhålla spårbarhet.
D 2.18	Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst, logginformation innehållande loggning av åtkomst har alltid **höga skyddskrav** avseende konfidentialitet eller riktighet.
D 2.19	Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser, ska skapas, bevaras en bestämd tid och granskas regelbundet. För loggar som innehåller systemadministratörers aktiviteter gäller att de ska granskas av loggadministratör som inte är samma person som systemadministratören

För att erhålla spårbarhet och möjliggöra incidentutredningar och att i efterhand kunna utreda vad som hänt och för att upptäcka avvikelser från kommunens regelverk ska kommunens IT-resurser övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Loggar ska skyddas mot manipulation och obehörig åtkomst, sparas en viss tid och granskas regelbundet av loggadministratör. I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av krav i Dataskyddsförordningen. Detta innebär bland annat att sådana loggar med personuppgifter ska skyddas från obehöriga. Det innebär också att om loggning används för att tekniskt övervaka ett system av säkerhetsskäl får loggen inte senare användas för andra syften. Om kontroller utförs för andra syften än det ursprungliga är lagkravet att personen ska informeras och en ny rättslig grund för personuppgiftsbehandlingen måste hittas, t.ex. samtycke, innan den får ske.

D3 Kryptering

Riktlinjer för kryptering	
D 3.1	Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av IT-säkerhetsansvarig.
D 3.2	Nyckelhantering ska säkerställas för att tillgodose de krav som finns för IT-resurs

	avseende • Revokering av nycklar • Validering av nycklars giltighet och autenticitet • Återställning av nycklar
D 3.3	Krypteringsnycklar är **konfidentiell** information och ska skyddas därefter

Kryptering kan användas för flera ändamål, såsom att genom kryptering förhindra obehörig åtkomst till information, eller genom kryptografiska signaturer garantera informationens riktighet eller äkthet. IT ska vid behov tillhandahålla godkända krypteringslösningar och instruktioner hur dessa ska användas. Behov av kryptering ska baseras på informationsklassning. Vanligen finns behov av kryptering då det föreligger höga skyddskrav på konfidentialitet och/eller riktighet.

Krypteringslösningar ska bygga på etablerade standarder och ska tas fram av objektägare IT i samråd med verksamhetsansvarig och IT-säkerhetsansvarig. Införande av krypteringslösningar ska godkännas av IT-säkerhetsansvarig.

Viktigt att tänka på är att ibland kan krypteringslösningar medföra nya risker relaterade till nyckelhantering.

D4 Fysisk och miljörelaterad säkerhet

Riktlinjer för fysisk och miljörelaterad säkerhet	
D 4.1	Tillträdet till säkra utrymmen ska vara begränsat och regleras minst med hjälp av låssystem med separat nyckelsystem. Nyckel-, kort- och kodinnehav ska vara förtecknade.
D 4.2	Rutiner för att arbeta i säkra utrymmen ska utformas och tillämpas. Roller med ansvar för ett säkert utrymme har också ansvar att ta fram en instruktion för hur arbete i respektive lokal får bedrivas.
D 4.3	Beslut om vem som ges tillträde att arbeta i säkra utrymmen ska vara dokumenterat.
D 4.4	Personal som beviljats tillfälligt tillträde till säkra utrymmen ska i möjligaste mån övervakas under hela besöket.
D 4.5	Åtkomstpunkter såsom leverans- och lastningsområden och andra punkter där obehöriga personer kan komma in i lokalerna ska styras och om möjligt isoleras från säkra utrymmen med IT-resurser för att undvika säkerhetsrisker

D 4.6	Inkommande gods ska registreras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.
D 4.7	Godkänt brandskydd och brandlarm ska installeras. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. Ventilations och andra genomföringar mellan brandceller ska förses med brandspjäll.
D 4.8	Utrymmet ska utformas så att utrustningen inte utsätts för vätskeläckage, korrosiva brand- och släckgaser, damm etc. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp
D 4.9	Utrymmen som innehåller informationstillgångar med **höga skyddskrav** ska uppfylla Skyddsklass 3 enligt SSF 200 Inbrottsskydd.
D 4.10	IT-resurser ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem
D 4.11	Synliga kablage för ström och telekommunikation för data eller stödjande informationstjänster ska skyddas från avlyssning, störningar och skada.
D 4.12	Åtgärder ska vidtas för att temperaturen hålls inom de gränsvärden som specificerats för aktuell utrustning, även vid störningar i elförsörjningen i de fall utrustning försetts med avbrottsfri kraft.
D 4.13	Underhåll och reparation ska utföras på sådant sätt att information eller IT-resurs inte riskerar att röjas eller skadas. Om utomstående ska utföra underhåll på IT-resurs med **höga skyddskrav** ska sekretessavtal tecknas. Vid **känslig information** ska informationen döljas, flyttas eller raderas från utrustningen.
D 4.14	Avveckling eller skrotning av IT-resurser och datamedia ska, efter att information som ska bevaras ha förts över till Stadsarkivet, ske genom att information skrivs över, raderas eller förstörs.
D 4.15	Avveckling eller skrotning av datamedia med **höga skyddskrav** på konfidentialitet sker genom att information skrivs över i multipla operationer, alternativt att mediet där informationen lagrats förstörs på ett fullständigt och oåterkalleligt sätt. Observera att krypterad datamedia inte är känslig om nyckel för dekryptering ges ett fortsatt skydd, eller att nyckel destruerats.

Fysisk och miljörelaterad säkerhet avser att förhindra otillåten fysisk åtkomst till, skador på och störningar i IT-resurser. Generellt gäller att informationsklassning ska användas som ett stöd för att utforma det fysiska skyddet som alltid måste utgå från vilken information som hanteras samt hur skyddsvärda IT-resurserna är.

Säkra utrymmen för IT-resurser

Säkra utrymmen med särskilda säkerhetskrav är exempelvis rum som används för servrar, switchar och annan kommunikationsutrustning samt e-arkiv. För IT-funktioner är det främst datorhallar och serverrum som är aktuella. Tillträden till säkra utrymmen ska vara restriktiva och endast ges till de personer som behöver tillträde för att utföra sitt uppdrag i den roll de har. Det ska finnas dokumenterade beslut om vem som ges tillträde att arbeta i säkra utrymmen.

Roller med ansvar för ett säkert utrymme har också ansvar att ta fram en instruktion för hur arbete i respektive lokal får bedrivas. Personer med arbetsuppgifter i säkra utrymmen ska ha god kännedom om de regler som gäller för arbetet i dessa lokaler.

Säkra utrymmen ska utformas så att utrustning inte utsätts för vätskeläckage, korrosiva brand- och släckgaser, damm etcetera. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp.

Godkänt brandskydd och brandlarm ska finnas. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. Ventilation och andra genomföringar mellan brandceller ska förses med brandspjäll.

Säkra utrymmen som innehåller IT-resurser med **höga skyddskrav** ska bevakas och fysisk närvaro ska loggas (till exempel tillträdes- eller videoövervakningsloggar).

Godsmottagning och lastning

Utrymme för godsmottagning och lastning ska avgränsas och organiseras så att de begränsar onödigt tillträde till känsliga områden och säkra utrymmen. Inkommande gods ska registreras och godkännas av vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.

Underhåll, reparation och avveckling

Underhåll av utrustning ska ske i enlighet med leverantörens anvisningar.

Reparation av utrustning och IT-resurser kräver ofta åtgärder från extern personal och auktoriserade reparatörer med utbildning på den utrustning som ska hanteras. Sådan personal har oftast varken behörighet till den information som hanteras i IT-resursen eller tillträde till sådana säkra utrymmen där IT-resurser finns placerade och detta kräver därför särskild uppmärksamhet.

Om underhåll och reparation ska utföras av utomstående på IT-resurs med **höga skyddskrav** avseende konfidentialitet ska vederbörande alltid underteckna sekretessavtal. Det kan ibland vara nödvändigt att vidta särskilda åtgärder, till exempel att känslig information flyttas, raderas eller krypteras innan någon utomstående hanterar utrustningen. Detsamma gäller avveckling av IT-resurser där avveckling eller återanvändning bör ske på ett sådant sätt att känslig information inte riskerar att komma i orätta händer. Datamedia där information inte har krypterats kan till exempel behöva skrivas över eller destrueras på ett säkert sätt innan den sänds till skrotning eller återanvändning. Observera att datamedia kan finnas i olika typer av IT utrustning till exempel skrivare.

Skydd av utrustning

Utrustning ska placeras och skyddas för att skyddas mot stöld och miljörelaterade hot som värme, kyla, fuktighet, vätska samt partiklar i luft. Användning ska ske i enlighet med de instruktioner som framtagits av utrustningens ägare. Riskerna för åverkan och stöld är högre i vissa av kommunens egna lokaler, till exempel där många externa personer frekvent vistas och i publika lokaler. Där krävs stöldskydd (till exempel fastlåsning) och märkning. Speciellt utsatt är också mobil utrustning där risken för förlust, stöld och skada är högre. Användning ska ske i enlighet med de instruktioner som gäller vid distansarbete och mobil utrustning där användare till exempel ska säkerställa att utrustning antingen övervakas eller låses in för att minska risken för stöld.

Elförsörjning

Säker elförsörjning (till exempel avbrottsfri kraft genom UPS och reservkraft) ska finnas så att IT-resurser skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem.

D5 Driftsäkerhet

Riktlinjer för driftrutiner	
D 5.1	Det ska finnas formella, beslutade och dokumenterade driftsrutiner för väsentliga processer och objekt. Dessa ska göras tillgängliga för alla användare som behöver dem.
D 5.2	Ändringar i IT-resurser ska följa fastställd process som säkerställer att ändringarna är riskbedömda, planerade, kommunicerade, testade och godkända (liknande ITIL Change Management).
D 5.3	Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

Dokumenterade driftsrutiner ska finnas och göras tillgängliga för alla användare som behöver dem.

Driftsrutiner ska vara formella och beslutade dokument. Förändringar i IT-resurser ska styras enligt fastställd ändringshanteringsprocess. Denna process ska säkerställa att alla ändringar som införs på tjänster, moduler och komponenter i IT-miljön är riskbedömda, planerade, kommunicerade, testade och godkända. Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken.

Skydd mot skadlig kod

Riktlinjer för skydd mot skadlig kod	
D 5.4	Det ska finnas metoder och programvara för skydd mot skadlig kod som förebygger, upptäcker skadlig kod och som återställer i kommunens IT-miljö efter angrepp.
D.5.5	IT-resurser som stöder objekt med **höga skyddskrav** ska regelbundet granskas med avseende på skadlig kod
D 5.6	System och applikationer ska regelbundet uppdateras för att hållas fria från säkerhetsbrister som kan exploateras av skadlig kod. Säkerhetspatchar ska regelmässigt och skyndsamt installeras på alla IT-resurser enligt tillverkarnas rekommendationer och enligt fastställd rutin
D 5.7	Det ska finnas en fastställd rutin för återställning av datorer om kommunen skulle

	drabbas av skadlig kod eller virusutbrott
D 5.8	Det ska finnas rutiner för att regelbundet samla in information om skadlig kod, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod (t.ex. cert.se)

För att skydda mot skadlig kod behövs metoder för att förebygga, upptäcka skadlig kod och för att återställa IT-miljön efter angrepp. Förutom tekniskt skydd är det även viktigt att alla som använder IT-resurser vet hur de kan minska risken att drabbas av skadlig kod samt vad de ska göra om de misstänker angrepp av skadlig kod (se Kapitel A, avsnitt A7 – Skadlig kod). Kommunens IT-resurser ska skyddas från skadlig kod genom att antivirusprogramvara installeras på klienter och servrar. Skyddet ska regelbundet uppdateras. Programvara ska i förebyggande syfte skanna efter skadlig kod i

- datorer i kommunens nätverk,
- filer som tas emot via nätverk eller någon form av media och
- i webbsidor.

IT-resurser med höga skyddskrav ska regelbundet granskas med avseende på skadlig kod. Om angrepp av skadlig kod inträffat ska det finnas en fastställd rutin för återställning av IT-resurser (se avsnitt D8 – Incidenthantering). Säkerhetsuppdateringar är en viktig komponent för att hålla system och applikationer fria från säkerhetsbrister som kan exploateras av skadlig kod. Det ska finnas rutiner för att regelbundet samla in information om skadlig kod, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod (t.ex. cert.se)

Säkerhetskopiering

Riktlinjer för säkerhetskopiering	
D 5.9	För IT-resurser med **höga skyddskrav** avseende tillgänglighet ska redundans finnas i delkomponenter, system, lagring och nätverk samt säkerställd infrastruktur för IT-drift. Tillgänglighet ska övervakas för att säkerställa att viktiga kvalitetsmått uppfylls.
D 5.10	Baserat på objekts klassning av riktighet och tillgänglighet ska krav definieras för säkerhetskopiering av information.
D 5.11	Det ska finnas en process för återlagring från säkerhetskopia, processen ska vara testad och dokumenterad.

D 5.12	Säkerhetskopiering av information med höga **skyddskrav** avseende konfidentialitet ska ske till krypterad backupmedia eller ges motsvarande skydd. Säkra återställningsrutiner ska användas med kontroller att återställning av konfidentiell information ges rätt skydd efter återställning, t.ex. bör dekryptering under återställning undvikas
D 5.13	Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet. Om lösning används där man skiljer på långtids- och korttidslagring är det tillräckligt att långtidslagringen är skild från originalmaterialet under förutsättning att korttidlagrade säkerhetskopior förvaras i ett säkert utrymme avsett för datamedia.

Säkerhetskopiering av information, program och speglingar av system är en viktig del av driftsäkerheten. Detta ger möjlighet att återställa en IT-resurs till ett fungerande tillstånd efter uppkomsten av ett fel, och att åtgärda både riktighet och tillgänglighet hos information. Säkerhetskopieringen syftar till att väsentlig information ska kunna rekonstrueras med hjälp av säkerhetskopior och återlagringsrutiner. Dock är det inte alltid möjligt att återställa all information. Sådan information som tillförts systemet efter senaste säkerhetskopiering går normalt inte att återställa.

Det finns en viktig skillnad mellan säkerhetskopiering och spegling (redundans). Den sistnämnda ger enbart ett skydd för tillgänglighet och inte riktighet, eftersom informationen är identisk vid spegling vilket innebär att eventuell felaktig information då återfinns på båda ställen. Säkerhetskopiering och spegling är tillsammans nödvändiga skyddsåtgärder för IT-resurser med krav på både riktighet och tillgänglighet.

Vilka skyddsåtgärder som vidtas för specifika system ska styras på av hur de är klassade i aspekterna tillgänglighet och riktighet. Stöd för detta kan vara att använda de två måtten RPO och RTO. Hur stor informationsförlust som kan accepteras kan definieras för varje IT-resurs genom att fastställa RPO (Recovery Point Objective). Den längsta acceptabla tiden för att återställa IT-resursen efter ett avbrott kan fastställas med målsättning för återställningstid RTO (Recovery Time Objective).

Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet för att skydda från fysiska incidenter och katastrofer som till exempel brand och översvämning. Ofta används lösningar där man skiljer på långtids- och korttidslagring där enbart långtidslagringen är skild från originalmaterialet. Då bör korttidslagring skyddas genom ett säkert utrymme avsett för datamedia, annars riskerar man att vid en brand förlora all information som tillförts

systemet sedan kopiering till långtidslagring skedde, vilket i vissa fall kan vara lång tid (se avsnitt D4 – Fysisk och miljörelaterad säkerhet).

Säkerhetskopior ska testas regelbundet för att säkerställa att återlagring fungerar som avsett.

Loggning och övervakning

Riktlinjer för loggning och (system)övervakning	
D 5.14	Loggning ska normalt ske i IT-resurser avseende fel, systemhändelser. Loggar ska sparas en viss tid samt regelbundet analyseras och övervakas. Typ och omfattning av loggar och övervakningssystem ska baseras på IT-resursers klassning och objektägares krav.
D 5.15	För att säkerställa all typ av loggning av händelser ska systemklockorna i alla relevanta IT-resurser synkroniseras mot en betrodd referenskälla för korrekt tid
D.5.16	Loggningsverktyg och logginformation har **höga skyddskrav** och ska skyddas mot manipulation och obehörig åtkomst.

Övervakning och loggning gör det möjligt att upptäcka händelser i IT-resurser. Genom loggning kan man i efterhand analysera vad som hänt och på så sätt möjliggöra korrigerande eller förebyggande åtgärder. Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser ska skapas, bevaras och granskas regelbundet.

Loggning av händelser utgör grunden för automatiserade övervakningssystem som är kapabla att skapa konsoliderade rapporter och varningar avseende säkerhet i system och tillämpningar.

Krav på loggar och övervakningssystem kan variera beroende på IT-resursens art och användningsområde. Det är IT-resursens klassning och objektägarens krav som utgör grunden för behovet.

Genom användning av loggverktyg samt att alla loggkällor använder gemensam och korrekt tid kan händelser i olika IT-resurser korreleras vilket ger en bättre och mera heltäckande bild av händelser jämfört med om logg övervakas i varje system för sig.

Loggar kan innehålla känsliga data och personinformation. Lämpliga säkerhetsåtgärder för ska därför vidtas.

Hantering av tekniska sårbarheter

Riktlinjer för hantering av tekniska sårbarheter	
D 5.17	Det ska finnas rutiner för att få information om, upptäcka, analysera och åtgärda tekniska sårbarheter i IT-resurser. Uppdateringar och säkerhetspatchningar ska göras regelbundet på IT-resurser.
D 5.18	I de fall säkerhetspatchning inte är praktiskt möjlig, ska information om tekniska sårbarheter i sådana IT-resurser inhämtas och analyseras och lämpliga åtgärder vidtas för att hantera den tillhörande risken
D 5.19	Säkerhetsgranskning av IT-resurser ska ske regelbundet och för verksamhetskritiska resurser minst årligen för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Sådan granskning kan t.ex. bestå av skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester.
D 5.20	Det ska finnas regler för programinstallationer som utförs av användare som definierar vilka typer av program och appar en användare kan installera och på vilket sätt.

Tekniska sårbarheter i IT-resurser kan innebära exponering för skadlig kod, dataintrång eller andra sårbarheter. Det ska finnas rutiner så att information om tekniska sårbarheter erhållas i tid, att sårbarheter kan analyseras och att lämpliga åtgärder kan vidtas för att behandla de risker som sårbarheter medför.

Okontrollerad installation av program kan medföra sårbarheter och incidenter, som exempelvis obehörig åtkomst till information, förlust av riktighet eller överträdelse av immateriella rättigheter. Regler för programinstallationer som utförs av användare ska upprättas och införas som definierar vilka typer av program en användare kan installera och på vilket sätt.

D6 Kommunikationssäkerhet

Kommunikationssäkerhet är skydd i IT-resurser och nätverk som används för datakommunikation i syfte att skydda den information som kommuniceras.

Nätverkssäkerhet

Riktlinjer för nätverkssäkerhet	
D 6.1	Krav på skydd vad gäller nätverkstjänster ska identifieras, dokumenteras och tillämpas samt inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster.
D 6.2	Trådlös datakommunikation innehållande information med normala eller **höga skyddskrav** avseende konfidentialitet är endast tillåtet från godkända klienter. Teknik för att kryptera och säkra kommunikationen ska alltid användas oavsett skyddskrav.
D 6.3	En grundläggande segmentering av nätverket ska göras för att skilja interna nät från Internet, samt att skilja utvecklings-, test- och produktionsmiljöer från varandra. Grupper av informationstjänster, användare och informationssystem kan ytterligare segmenteras i separata nätverks efter skyddsbehov. • Utrustning ska finnas för att kontrollera och förhindra obehörig nätverkstrafik mellan olika nätverkssegment.
D 6.4	Brandväggar ska konfigureras i enlighet med zero-trust modell.
D 6.5	Kommunikationstjänster mellan Umeå kommun och externa nätverk ska dokumenteras och godkännas av Objektägare IT innan inkoppling får ske.

Nätverk måste hanteras och styras för att skydda information i anslutna system och tillämpningar. Det ska finnas rutiner för hantering av nätverk och förvaltning ska ske av ansvariga som utpekas av ägare till nätverk. Skyddsåtgärder ska införas för att nå säkerhet för information i nätverk och anslutna tjänster utifrån klassningen av anslutna objekt, dvs. krav på konfidentialitet, riktighet och tillgänglighet. Krav på skydd ska inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster. Skydd för nätverkssäkerhet kan exempelvis vara:

- Autentisering av system
- Kryptering
- Regler för säkerhet och nätverksanslutning
- Begränsning av systemanslutningar
- Brandväggar och intrångsdetekteringssystem
- Loggning och övervakning av nätverk
- Separation av nätverk (segmentering)

Segmentering betyder att dela upp nätverket i olika segment för att till exempel tillåta enbart ekonomiadministratörer tillgång till nätverket med ekonomisystem. Segmentering av

nätverk ska användas som en del av den totala säkerhetslösningen för att skydda känslig information och övriga resurser.

En grundläggande segmentering av nätverket ligger i att skilja interna nät från Internet, samt att utvecklings-, test- och produktionsmiljöer ska vara skilda från varandra. Ytterligare segmentering ska göras då det är motiverat av säkerhetsskäl. Brandväggar och utrustning för segmentering av nätverk behöver revideras regelbundet för att hållas uppdaterade med rätt regler för kommunikation mellan olika IT-resurser över de olika nätsegmenten.

Informationsöverföring

Riktlinjer för informationsöverföring	
D 6.6	Kommunikation med **höga skyddskrav** avseende konfidentialitet och riktighet ska alltid krypteras och kommunicerande parter ska identifieras på ett säkert sätt.
D 6.7	Utgående massutskick av e-post ska begränsas för att förhindra att kapad mailbox används till att skicka ut stora mängder spam.
D 6.8	Överföringslösningar för verksamhetsinformation mellan Umeå kommun och externa parter ska regleras genom avtal.
D 6.9	Kommunikation med e-post till andra organisationer skyddas i samtliga e-postsystem genom att konfigurera och aktivera standardiserade säkerhetsfunktioner.

Information som hanteras genom elektronisk meddelandehantering ska ges lämpligt skydd. Om meddelande innehållande information med **höga skyddskrav** avseende konfidentialitet ska sändas till extern part ska lösning med kryptering och signering användas.

Avtal som reglerar säker överföring av verksamhetsinformation mellan Umeå kommun och extern part ska upprättas. Användandet av osäkra klartextprotokoll såsom t.ex. FTP och HTTP ska undvikas och ersättas av säkra alternativ om information med normala eller höga skyddskrav avseende konfidentialitet ska överföras.

D7 Anskaffning och utveckling av IT-resurser

Korrekt informationssäkerhet för IT-resurser ska säkerställas över hela livscykeln och börjar vid anskaffning eller utveckling.

Säkerhetskrav på IT-resurser

Riktlinjer för säkerhetskrav på IT-resurser	
D 7.1	Informationssäkerhet ska inkluderas i kraven för nya IT-resurser i förändringar av befintliga. Det gäller oavsett om IT-resursen upphandlas externt, utvecklas internt eller en kombination av båda (till exempel anpassning av ett inköpt standardsystem). Informationssäkerhetskraven ska baseras på den klassning som tilldelats IT-resursen och ska dokumenteras och granskas av alla berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas.

Krav som rör informationssäkerhet ska redan från början inkluderas i kraven för nya IT-resurser likväl som i krav för förbättringar av befintliga. Det gäller oavsett om IT-resursen upphandlas externt, utvecklas internt eller en kombination av båda (till exempel anpassning av ett inköpt standardsystem).

Informationssäkerhetskraven ska spegla den klassning som tilldelats IT-resursen och som baseras på till exempel författningar och interna regelverk, riskanalyser eller analys av incidenter.

Utveckling, anskaffning eller förändring av system som omfattas av verksamhetsnära förvaltning ska involvera parterna i förvaltningsorganisationen. Objektägare IT ansvarar för att rätt tekniska krav formuleras som överensstämmer med verksamhetens krav så att system ges skydd som korrelerar till klassningen.

Utveckling, anskaffning eller förändring av underliggande IT-resurser i form av infrastruktur, stödsystem med mera ska ha minst motsvarande krav som de system som de stöder. Ibland kan kraven vara ännu högre än för de system de stödjer, exempelvis om en IT-resurs stödjer ett stort antal system som var för sig inte är kritiska. Informationssäkerhetskrav ska dokumenteras och granskas av alla berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas.

Säkerhetskrav vid upphandling av IT-stöd

Riktlinjer för säkerhetskrav vid upphandling av IT-stöd	
D 7.2	Tydliga informationssäkerhetskrav ska ställas vid upphandling av IT-stöd och ska sedan användas vid utvärdering av anbud. Kraven ska baseras på den klassning som tilldelats IT-resursen.

D 7.3	IT-leverantörer ska på begäran kunna delge hur de bedriver säkerhetsarbete i såväl den operativa verksamheten som avseende säker systemutveckling.
D 7.4	Avtal med IT-leverantör ska innefatta stöd och support i händelse av fel och incidenter.
D 7.5	Avtal med IT-leverantör ska reglera hur kontroll av avtalets uppfyllande ska ske, t.ex. genom tredjepartsrevision eller granskning genomförd av Umeå kommun
D 7.6	Upphandling av system som ska driftas hos extern leverantör medför ytterligare krav, exempelvis: • Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (t.ex. certifieringar) • Leverantörens kontinuitetshantering • Rätt till tredjepartsrevision • Sekretessavtal • Personuppgiftsbiträdesavtal • Rätt till incidentrapporter från leverantören
D 7.7	Upphandling av IT-stöd ska göras i samverkan med Upphandlingsbyrån
D 7.8	För att säkerställa tillgänglighet till källkod samt underhåll och utveckling i händelse av oväntade förändringar hos IT-leverantör eller dess underleverantörer ska för verksamhetskritiska system och applikationer så kallad källkodsdeposition användas, där minst ett exemplar av källkoden lämnas i förvar hos tredje part.
D 7.9	Avtal med IT-leverantör ska innefatta: • Att leverantören innan leverans till Umeå kommun genomför säkerhetstestning av system och ingående komponenter. • Att testet genomföras av tredje part. • Att leverantören ska åtgärda eventuella säkerhetsbrister som identifierats i samband med acceptanstest och/eller leveranskontroll.
D 7.10	Om IT-leverantör använder underleverantör för hela eller del av leveransen ska ett avtal tecknas dem emellan som reglerar såväl affärsmässighet som säkerhet. Avtalet ska kunna delges. Följande punkter ska då minst beaktas avseende säkerhet: • Hur applicerbara krav i avtal med IT-leverantör säkerställs även mot dess underleverantör • Hur rättsliga krav uppfylls, exempelvis rörande lagstiftning om sekretess och personuppgifter • Vilka åtgärder som vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar, licensieringsarrangemang, äganderätt till koden och upphovsrätt • Vilka åtgärder som vidtas för att säkerställa kvalitet i leverans från underleverantör

Vid upphandling av IT-stöd gäller ovanstående riktlinjer för säkerhetskrav på IT-resurser. Det är än viktigare vid extern upphandling att vara tydlig när det gäller kravställning av informationssäkerhet. Externa leverantörer använder kanske annan terminologi och har annan förståelse för informationssäkerhet än vad som föreligger internt i kommunen. Exempelvis är man kanske inte familjär med klassning av information och objekt, och även om man är det kanske man tillämpar andra nivåer och tolkar de olika nivåerna på annat sätt.

Avtal med IT-leverantör ska reglera ansvar för implementation och upprätthållande av säkerhetsfunktioner och ansvar för testning och verifiering av dessa. Dessutom ska avtalet reglera ansvar för sådana brister som eventuellt upptäcks under drift. Om upphandlade system även ska driftas hos en leverantör eller om leverantör på annat sätt kommer få åtkomst till information tillkommer krav som kan innefatta:

- Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (till exempel certifieringar)
- Leverantörens kontinuitetshantering
- Rätt till tredjepartsrevision
- Sekretessavtal
- Personuppgiftsbiträdesavtal
- Rätt till incidentrapporter från leverantören

I kravspecifikationer ska alltid tydliga krav på säkerhet formuleras som sedan används vid utvärdering av anbud. Upphandling av IT-stöd ska alltid följa IT-upphandlingsmodellen och göras i samverkan med Upphandlingsbyrån.

Säkerhet vid systemutveckling

Riktlinjer för säkerhetskrav vid systemutveckling	
D 7.11	Processer, rutiner och regler ska finnas som reglerar att informationssäkerhet finns med under hela utvecklingscykeln av IT-resurser
D 7.12	Systemförändringar inom utvecklingscykeln ska styras genom ändringshanteringsprocess, jmfr Change managementprocessen.
D 7.13	För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT-resursens hela livscykel.
D 7.14	Systemutvecklare ska ha kompetens i programvarusäkerhet.
D 7.15	Vid outsourcad systemutveckling ska krav ställas att man tillämpar en etablerad modell för säker systemutveckling.

Processer och rutiner ska finnas på plats för att säkerställa att informationssäkerhet designas och införs under utvecklingscykeln av IT-resurser. Säkerhet måste vara en integrerad del i utvecklingsprocessen, från början till slut. Regler för säker utveckling av program och system ska upprättas och tillämpas vid systemutveckling. Systemförändringar inom utvecklingscykeln ska styras genom användning av Change management-processen. För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT-resursens hela livscykel. En säker utvecklingsmiljö inkluderar människor, processer och teknik som är involverad i systemutveckling och integration. Det innebär även att alla utvecklare måste ha en grundkompetens i programvarusäkerhet och att utvecklingsprocesser innehåller komponenter av utbildning och omvärldsbevakning.

Outsourcad systemutveckling ska övervakas och styras och säkerhetsfunktionalitet ska säkerställas vid utveckling. En fördel är om leverantören använder en etablerad modell för utveckling av säker programvara. Om ingen etablerad modell används av leverantören krävs en betydligt mer ingående analys för att säkerställa en säker utvecklingsprocess.

Säkerhetskrav vid test

Riktlinjer för säkerhetskrav vid test	
D 7.16	Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med riktlinjer för säker utveckling.
D 7.17	Produktionsdata ska inte användas i test utan all testdata ska väljas ut noggrant, skyddas och styras. Om produktionsdata ändå behöver används gäller följande: • Testdata ska alltid anonymiseras från personuppgifter • Rutiner för styrning av åtkomst som tillämpas för produktionssystem ska också gälla vid test av sådana system • Behörighet ska godkännas av objektägare IT varje gång produktionsdata kopieras till ett testsystem • Produktionsdata ska omgående raderas från testsystem efter avslutad test • Kopiering av produktionsdata ska loggas för att erhålla spårbarhet
D 7.18	Test- eller utvecklingsversioner får ej placeras i produktionsmiljö utan utvecklings-, test och driftmiljöer ska separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön
D 7.19	Driftsättning ska ske enligt fastställd process för ändringshantering avseende berört objekt (jmfr Change management-process)

Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med riktlinjer för säker utveckling. Vid test kan man dra nytta

av automatiserade verktyg, till exempel verktyg för kodgranskning eller för skanning av sårbarheter. Testning bör utföras i en realistisk testmiljö för att säkerställa att systemet inte kommer att införa sårbarheter i organisationens miljö och att testerna är tillförlitliga.

Testdata bör skyddas och kontrolleras. System- och acceptanstest kräver normalt avsevärda mängder testdata som är så snarlika produktionsdata som möjligt. Att använda produktionsdatabaser för test bör undvikas och personuppgifter måste i så fall först anonymiseras.

Test-, utvecklings- och driftmiljöer ska så långt som möjligt separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön. Utvecklare ska inte tillåtas att testa icke fastställda och godkända programversioner eller förändringar i driftmiljö.

Driftsättning ska ske enligt ändringshanteringsprocess, jmfr Change management-process.

D8 Incidenthantering

Riktlinjer för incidenthantering	
D 8.1	Det ska finnas en incidenthanteringsprocess på IT som omfattar informationssäkerhetsincidenter. Processen ska innefatta: • Mottagning av information om incidenten • Styrning av eventuella behov av omedelbara åtgärder. Dessa kan vara av temporär art tills en mer hållbar lösning kan komma på plats • Analys av orsaker till incidenten så att korrektiva och preventiva åtgärder kan vidtas • Återkoppling och kommunikation med dem som är påverkade av eller involverade i återhämtning efter incidenten liksom till den som rapporterat incidenten
D 8.2	Större incidenter ska sammanställas i incidentrapporter som respektive objektägare ansvarar för att ta fram i samverkan med IT.
D 8.3	Erfarenheter från inträffade incidenter, t.ex. genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar
D 8.4	Medarbetare är skyldiga att rapportera informationssäkerhetsincidenter såväl som informations- och IT-relaterade brister i system eller tjänster.
D 8.5	Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas och insamling av bevis med mera ska inte göras utan samråd med polisen. Medarbetare och deltagare i verksamheten som har upptäckt en incident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa detta då det

	kan försvåra utredningar

Med informationssäkerhetsincident avses en händelse som har eller skulle kunnat ha försämrat konfidentialitet, riktighet eller tillgänglighet hos information.

Alla medarbetare inom Umeå kommun är skyldiga att rapportera incidenter (se Kapitel A). Detta innefattar självklart även medarbetare på IT samt externa aktörer som exempelvis konsulter. Även svagheter i skydd (brister) ska rapporteras, exempelvis larm som inte fungerar, öppna dörrar till våra lokaler eller öppna fönster efter kontorstid osv. IT- och informationsrelaterade incidenter och brister ska rapporteras till IT Kundsupport.

Processer och rutiner ska finnas på plats för att säkerställa ett konsekvent och effektivt tillvägagångssätt för hantering av informationssäkerhetsincidenter inklusive kommunikation i samband med incidenterna.

För IT inspireras hantering av incidenter av ITIL-processen ”Incident Management”. Denna process innefattar fler typer av incidenter än vad som kan definieras som informationssäkerhetsincident enligt ovan, men incidenthanteringsprocessen måste självklart omfatta och hantera informationssäkerhetsincidenter. Dessa kan vara av olika typer, exempelvis:

- Obehöriga har fått tillträde till kommunens lokaler
- Obehöriga har kommit åt information
- Dokument, till exempel publika rapporter, har ändrats felaktigt eller utan behörighet
- Infektion av virus eller annan skadlig kod
- Information som borde ha funnits arkiverad har försvunnit
- IT-resurser missbrukas av medarbetare eller externa personer

Viktiga aktiviteter i incidenthanteringsprocessen är

- Mottagning av information om incidenten
- Styrning av eventuella behov av omedelbara åtgärder. Dessa kan vara av temporär art tills en mer hållbar lösning kan komma på plats
- Analys av orsaker till incidenten så att korrektiva och preventiva åtgärder kan vidtas
- Återkoppling och kommunikation med dem som är påverkade av eller involverade i återhämtning efter incidenten liksom till den som rapporterat incidenten.
- Lessons learned

IT ska i rollen som ”incident manager” leda hanteringen av IT-incidenter i samverkan med berörda ägare av objekt. Vid incidenter relaterade till förvaltningsobjekt ska IT samverka med relevanta roller i förvaltningsorganisationen.

Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas och insamling av bevis m.m. ska inte göras utan samråd med polisen.

Medarbetare och deltagare i verksamheten som har upptäckt en incident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa detta då det kan försvåra utredningar.

Kunskaper baserade på analyser av hanterade incidenter ska användas för att minska sannolikheten eller konsekvenser av framtida, liknande, incidenter. Kort sagt bör man lära av sådant som har inträffat så att man kan vidta åtgärder för att förhindra återupprepning. Vissa åtgärder kan behöva vidtas skyndsamt och i samband med att en incident inträffar.

Större incidenter ska sammanställas i incidentrapporter som respektive objektägare ansvarar för att ta fram i samverkan med incident manager. Mindre incidenter ska registreras och sammanställas och kan ligga till grund för kvantifiering och statistik.

Erfarenheter från inträffade incidenter, t.ex. genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar.

Krisorganisation och krisplan

Riktlinjer för krisorganisation och krisplan	
D 8.6	Det ska på IT finnas en krisorganisation för allvarliga incidenter och kriser, som tydligt beskriver roller och ansvar.
D 8.7	Det ska finnas en krisplan på IT som ska aktiveras vid händelse av en allvarlig incident eller kris. Krisplanen ska bland annat innehålla krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.
D 8.8	Krisplanen ska testas och övas minst en gång per år. Identifierade brister och svagheter ska åtgärdas i syfte att ständigt förbättra krisplanen för IT. Övning kan ske genom s.k table-top övning eller scenarioövning.

En krisplan ska finnas som ska aktiveras vid händelse av allvarliga incidenter eller kriser (s.k. major incidents) i IT-miljön. Krisplanen ska ha en ansvarig förvaltare och innehålla bland annat krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.

D9 Kontinuitetshantering

Riktlinjer för kontinuitetshantering	
D 9.1	Det ska finnas avbrottsplaner för samtliga kritiska IT-resurser med **höga skyddskrav** avseende tillgänglighet
D 9.2	Övning och testning av avbrottsplaner ska genomföras och utvärderas regelbundet och identifierade brister samt svagheter åtgärdas med syfte att ständigt förbättra kontinuiteten för IT.
D 9.3	Avbrottsplaner ska finnas tillgängliga för de medarbetare som ingår i aktiviteterna, men samtidigt utgör planerna information med **högt skyddsvärde** och förvaras skyddat så att de inte blir åtkomliga för obehöriga.

Kontinuitetshantering innebär att man i en organisation systematiskt arbetar med att och skapa en god återhämtningsförmåga för kritiska verksamhetsprocesser och minimera konsekvenserna av störningar, avbrott och katastrofer. Arbetet innefattar att identifiera kritiska verksamhetsprocesser och dessas beroenden av stöd och resurser som till exempel personal, lokaler och verktyg.

IT-resurser är ofta viktiga stöd för kritiska verksamhetsprocesser som ibland kan vara helt beroende av att det finns tillgängligt och fungerar som avsett. Kontinuitetshantering för IT är därför en viktig del i informationssäkerhetsarbetet för att minimera negativa konsekvenser vid allvarliga IT-relaterade incidenter eller avbrott. Syftet är att efter ett större avbrott så snabbt som möjligt återgå till normalläge och att konsekvenserna för verksamheten ska vara så små som möjligt, både under och efter avbrottet.

Detta innebär att det för objekt med höga skyddskrav avseende tillgänglighet måste finnas en beredskap för hur man hanterar avbrott – s.k. avbrottsplaner. Objektägare IT ansvarar för att IT mässiga avbrottsplaner finns på plats för att snabbast möjligt få igång normal IT-funktionalitet. Planerna motsvarar de krav som finns för objekt.
Verksamheten ansvarar för ej IT-mässig reservplan för att upprätthålla verksamhet.
Avbrottsplaner ska vara relaterade till incidenthanteringen och den övergripande krisplan som ska finnas på IT (se avsnitt D8). En viktig säkerhetsåtgärd för att skapa och bibehålla hög tillgänglighet är säkerhetskopiering (se avsnitt D5).

Målsättningen är att kontinuitetshantering ska utvecklas i hela Umeå kommun och på sikt ingå i ett ledningssystem för informationssäkerhet (se avsnitt B4)

D10 Granskning och kontroll

Riktlinjer för granskning och kontroll	
D 10.1	Kritiska delar i IT-miljön som stödjer objekt med **höga skyddskrav** ska regelbundet övervakas och granskas för att sårbarheter och brister ska upptäckas.
D 10.2	Vid osäkerhet gällande säkerhetsförhållanden skall de IT-säkerhetsmässiga förutsättningarna ses över och lyftas till systemförvaltningen.
D 10.3	Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, till exempel förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart
D 10.4	Rapportering av större sårbarheter och brister ska ske till IT-säkerhetsansvarig. IT-säkerhetsansvarig avgör om informationssäkerhetsrådet behövs informeras.
D 10.5	Revision av hela eller stora delar av IT-miljön ska göras minst vartannat år. Innan granskning eller revision kan ske ska följande beaktas: • Behov på åtkomst till system och data inför granskning eller revision ska avtalas med objektägare • Omfattningen av tekniska aktiviteter för granskning eller revision ska beskrivas för- och godkännas av IT-resursens ägare. • Aktiviteter vid granskning eller revision begränsas om möjligt till skrivskyddad åtkomst av program och data • Granskning som kan påverka tillgänglighet bör utföras under servicefönster eller vid sådan tidpunkt då påverkan på verksamheten är så liten som möjligt • All åtkomst vid granskning eller revision ska övervakas och loggas

Granskning av IT-säkerhet för IT-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Sådan granskning kan till exempel vara skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester. Särskilt viktigt är det att genomföra kontroll och granskning av kritiska delar av IT-miljön som direkt eller indirekt stöder system med höga skyddsvärden, samt införande av nya IT-lösningar.

Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, till exempel förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till IT-säkerhetsansvarig och i förekommande fall till informationssäkerhetsrådet.

Revision av hela eller delar av IT-miljön ska göras minst vartannat år. Revision eller mätning av Umeå kommuns informationssäkerhet i stort kan även omfatta IT-miljön.

Revisionshistorik Riktlinjer för informationssäkerhet

Datum	Version	Ändring i korthet	Ändrat av
2020-04-01	1.0	Första utkast	Beatrice Fossmo
2020-10-22	1.1	Ändringar enligt synpunkter från kommunjurist, dataskyddsorganisation, förvaltningsledare, VIT-grupp, SäkArk-råd (IT), stadsarkivarie	Beatrice Fossmo
2021-03-30	1.2	Ändringar efter översyn från IT ledningsgrupp	Beatrice Fossmo
2021-05-17	1.3	Ändringar efter översyn Digitaliseringsråd, Informationsarkitekt	Beatrice Fossmo
2021-10-06	2.0	Riktlinjer fastställs	Beatrice Fossmo
	A 1.2	Bytt formulering *från ”i O365”* till ”elektroniskt i systemet”	Beatrice Fossmo
2021-10-08	A.3.12, A 3.13	Förtydligat formuleringar kring mejl, att det avser O365 mejl.	Beatrice Fossmo
	A 4.1, A 4.2	Hanteras *(ist f skickas)*	Beatrice Fossmo
	A 5.15, A 5.19	Förtydligat att Känslig Sekretess (Gul) och Hög Sekretess (Röd) information får inte lagras i OneDrive, SharePoint Online eller Google Drive (Utbildning) av juridiska skäl	Beatrice Fossmo
	Fig 3	Förtydligat informationssäkerhetssamordnarens roll i framtagandet, ändrat till Beslutas av kommunstyrelsen *(ist f*	Beatrice Fossmo

		Stadsdirektör)	
2025-02-11	Sid 5 Dispenser och undantag Sid 42 Informationssäkerhetsråd	Raderat stycket Dispenser och undantag. Raderat punkt om dispenser och undantag.	Hanna Öberg
2025-03-18		Ver.2.1 Fastställd av Kommunstyrelsen (ändringar daterade 25-02-11)	

UMEÅ KOMMUN

Tjänsteskrivelse
2026-08-31

Tekniska nämnden

Diarienr: TN-2026/00691

Remiss AI-styrning: Policy för AI och Riktlinje för AI-användning

Förslag till beslut
Tekniska nämnden beslutar

att skicka förslag till Policy för AI och Riktlinje för AI-användning på remiss till kommunens nämnder och bolag enligt remisslista.

Ärendebeskrivning
Artificiell intelligens (AI) skapar nya möjligheter att utveckla verksamheter, stärka kvaliteten och frigöra tid för mänskliga möten. Samtidigt ställer användningen krav på ansvar, transparens, informationssäkerhet och rättssäkerhet.

För att skapa ett gemensamt förhållningssätt har Umeå kommun tagit fram förslag till en policy för AI och en riktlinje för AI-användning. Policyn beskriver de övergripande principerna för AI-användning i kommunens nämnder och bolag medan riktlinjen konkretiserar hur principerna ska tillämpas i nämnder och verksamheter.

Förslagen innebär bland annat att AI ska sätta människan i centrum, användas lagligt och etiskt samt stödja mänskliga beslut utan att ersätta mänskligt ansvar. Riktlinjen ställer krav på ett proportionerligt och riskmedvetet arbetssätt, där AI inte får tas i bruk innan lagligheten har fastställts och relevanta risker har bedömts och hanterats. Krav på riskbedömning, dokumentation, kontroll, uppföljning och mänsklig tillsyn anpassas efter användningens påverkan.

Transparens och ansvar hanteras genom krav på att det ska vara möjligt att förstå när och hur AI används, hur ett AI-system har påverkat ett resultat eller beslut samt vem som ansvarar för användningen. Nämnderna ska ha överblick över de AI-system som används, säkerställa dokumentation och registrering samt följa upp användningen löpande. Vid upphandling och utveckling tillämpas kommunens ordinarie styrning för bland annat upphandling, IT, informationssäkerhet och dataskydd.

Tjänsteskrivelse

Dnr: TN-2026/00691

Styrdokumenten utgör grunden i kommunens styrning av AI. Nästa steg är att komplettera styrningen med verksamhetsnära stöd och rutiner som vägleder medarbetare i frågor kring tillämpningen av AI. Arbetet sker inom kommunens ordinarie styrning för digital omställning och informationssäkerhet, där DoIT samordnar arbetet tillsammans med samverkansobjektet AI- och datadriven kommun. Bilagan Tillämpning av styrning för AI och styrkedja beskriver hur styrkedjan hänger ihop.

Tekniska nämnden föreslås besluta att skicka förslagen på remiss till kommunens nämnder och bolag. Inkomna remissvar utgör underlag för den fortsatta beredningen inför slutligt antagande av styrdokumenten.

Beslutsunderlag

Policy för AI - för remiss. Bilaga.
Riktlinje för AI-användning - för remiss. Bilaga.
Tillämpning av styrning för AI och styrkedja. Bilaga.
Instanser för remiss. Bilaga.

Checklista för handläggning av ärenden inför politiska beslut anses inte tillämpbar.

Beredningsansvariga

Hannes Fries, verksamhetsutvecklare, Digital omställning och IT
Stefan Boström, controller, Ekonomi och styrning

Beslutet ska skickas till

Kommunens nämnder och bolag enligt lista.

Svaren ska vara TNdiarium till handa senast 2026-12-18.

UMEÅ KOMMUN

Riktlinje för AI-användning

Beslutad av:	**Diarienummer:**	**Datum, paragraf för beslut:**	**Dokumentet styr:**
[Nämnd/styrelse]	[XXXX]	[20XX-XX-XX, § XX]	[Xxx]
Dokumenttyp:	**Giltighetstid:**	**Dokumentansvarig:**	
Riktlinje	[20XX-XX-XX]	[Nämnd/förvaltning/verksamhet	

Innehåll

Bakgrund

Artificiell intelligens (AI) innebär stora möjligheter för innovation och effektivisering av kommunens verksamheter. Utvecklingen går snabbt och AI blir successivt en naturlig del av många yrkesroller och arbetssätt i offentlig sektor. Samtidigt ställer den ökade användningen krav på ett medvetet och strukturerat förhållningssätt till hur AI används.

Riktlinjen utgör en gemensam ram för användning av AI i kommunens verksamheter och skapar förutsättningar för trygghet, förtroende samt en laglig och rättssäker användning.

Riktlinjen stödjer kommunens arbete i linje med nationella och europeiska mål för AI i offentlig sektor. Sveriges nationella AI-strategi betonar att AI ska bidra till ökad effektivitet, kvalitet, samhällsnytta och innovation, medan EU:s AI-förordning ställer krav på ett riskbaserat förhållningssätt där användning som kan påverka individers rättigheter omfattas av högre krav på styrning, transparens och mänsklig tillsyn.

Syfte

Riktlinjen ger en gemensam inriktning för hur AI ska prövas, utvecklas, införas och användas samt stödjer nämnder i deras ansvar för styrning, riskhantering och regelefterlevnad.

Omfattning och avgränsning

Riktlinjen omfattar Kommunstyrelse och kommunens nämnder.

Lagar och krav

Riktlinjen tydliggör ansvar och bidrar till att AI-användning sker i enlighet med gällande lagstiftning, såsom Cybersäkerhetslagen, Dataskyddsförordningen (GDPR), Offentlighets- och sekretesslagen (OSL), Kommunallagen (KL) och EU:s AI-förordning.

Begrepp och definitioner

Med AI avses i denna riktlinje samma definition som i *Policy för AI*. Därutöver används följande begrepp, med utgångspunkt i EU:s AI-förordning:

Allmänt tillgängliga AI-system: Publika AI-tjänster som erbjuds av externa leverantörer och där kommunen har begränsad insyn och kontroll över systemets uppbyggnad, databehandling och användning, jämfört med kommunförvaltade AI-system.

Anpassade AI-system (kommunförvaltade AI-system): AI-system som är upphandlade, anpassade eller egenutvecklade för kommunens verksamheter och som förvaltas under kommunens ansvar.

Ansvarsfördelning

Tekniska nämnden

Ansvarar enligt reglemente för att leda och samordna kommunens gemensamma arbete med digitalisering och digital transformation. Nämnden ansvarar även för att initiera och samordna revidering av dessa riktlinjer.

Kommunstyrelsen

Ansvarar enligt reglemente för att leda, samordna och utveckla det kommungemensamma arbetet med informationssäkerhet som ger stöd för arbetet med AI.

Nämnder

Respektive nämnd ansvarar enligt reglemente för digitala tjänster och informationssystem som stödjer verksamheten, informationssäkerheten samt sin information, dess förvaltning och användbarhet. Nämnden ska säkerställa att AI-användning inom det egna ansvarsområdet sker i enlighet med relevant lagstiftning och att nödvändiga bedömningar görs inför införande och användning av AI-system. Nämnden ansvarar även för att medarbetare har kännedom om gällande regler, att det finns rutiner för hur AI-system får användas i det dagliga arbetet samt att användare har tillräcklig kunskap och utbildning för att använda AI-system på ett korrekt sätt.

Tillämpning av AI-policyn

Avsnitten nedan konkretiserar principerna i *Policy för AI* och beskriver hur de ska tillämpas i kommunens förvaltningar vid införande av nya AI-system och vid uppföljning av befintlig användning.

1. AI sätter människan i centrum (Princip 1)

AI ska användas för att skapa nytta för invånare och verksamheter genom att stödja och stärka mänskliga beslut och arbetssätt. AI är ett stöd i arbetet och ersätter inte mänskligt ansvar. Särskild hänsyn ska tas när AI används som stöd till bedömningar eller beslut som rör enskilda invånare. Beslut som får konsekvenser för enskilda får inte fattas enbart genom automatiserade system utan mänsklig kontroll, om inte lagstöd finns.

För kommunens nämnder innebär det att:

- Säkerställa att AI används som stöd för mänskliga bedömningar och att ansvar för beslut alltid ligger hos en människa.

2. Ansvarsfull och etisk användning (Princip 2-3)

Användning av AI ska följa gällande lagstiftning, respektera grundläggande rättigheter och bidra till att förtroende, rättssäkerhet och personlig integritet upprätthålls. Upphovsrätt ska beaktas vid användning av AI.

För kommunens nämnder innebär det att:

- Tydliggöra ansvar för användning och resultat samt säkerställa att AI kan granskas och frångås vid felaktiga resultat.
- Nämnden ska säkerställa att användare av AI-system har tillräcklig kunskap för att använda dem korrekt och upptäcka när resultat behöver ifrågasättas.

3. Proportionerlig och riskmedveten användning (Princip 4)

All användning av AI i kommunen ska präglas av en försiktighetsprincip. AI ska användas stegvis och kontrollerat och får inte tas i bruk innan lagligheten fastställts och relevanta risker har bedömts och hanterats.

Användningen ska stå i proportion till dess påverkan på invånare, verksamhet och rättssäkerhet. Ju större påverkan, desto högre krav ställs på förberedelser, kontroll, uppföljning och mänsklig tillsyn.

Vid prövning, införande och användning av AI ska kommunens ordinarie processer för riskhantering tillämpas. Informationsrelaterade risker ska bedömas enligt kommunens modell för informationsklassning och riskvärdering, inklusive risker kopplade till rättssäkerhet, diskriminering, sekretess, informationssäkerhet och dataskydd.

För kommunens nämnder innebär det att:

- Säkerställa att AI-användning riskbedöms innan införande, enligt kommunens modell.
- Anpassa nivå av kontroll, uppföljning och mänsklig tillsyn utifrån AI-användningens påverkan.
- Bedöma och hantera relevanta risker, exempelvis kopplade till diskriminering, informationssäkerhet och dataskydd.

- Följa upp AI-användning löpande och säkerställa att den används som stöd och inte ersätter mänskligt omdöme.

4. Transparens och kommunikation (Princip 5)

Transparens och tydlig kommunikation kring användning av AI är en förutsättning för förtroende, insyn och rättssäkerhet. Det ska vara möjligt att förstå när AI används, i vilket sammanhang och på vilket sätt AI-system har påverkat ett resultat, en bedömning eller ett beslut. Nämnderna ska ha kännedom om vilka AI-system som används inom verksamheten och att dessa finns registrerade i kommunens register över system.

För kommunens nämnder innebär det att:

- Tydliggöra när och hur AI används i verksamheten.
- Säkerställa att AI-system som påverkar enskilda kan förklaras och granskas.
- Säkerställa rutiner för dokumentation av AI-användning.
- Informera tydligt enskilda när AI används i ärenden som rör dem och hur AI-stöd har påverkat handläggning, bedömningar eller beslut.
- Säkerställa överblick över AI-system i verksamheten och att de är dokumenterade och registrerade.

5. Hållbar och samordnad användning av AI (Princip 6)

Användning av AI i Umeå kommun ska bidra till en långsiktigt hållbar och ändamålsenlig användning av kommunens resurser. AI-system ska därför planeras, införas och förvaltas med utgångspunkt i verksamheternas behov, kommunens digitala helhet och förmågan till långsiktig kvalitet snarare än kortsiktiga eller isolerade lösningar.

AI-utveckling och införande ska ske i linje med kommunens gemensamma styrning för digitalisering och i samspel med samverkansobjekten, som utgör kommunens modell för att samordna behov, prioriteringar och lösningar över organisations- och verksamhetsgränser.

Vid upphandling, utveckling eller väsentlig vidareutveckling av AI-system ska kommunens ordinarie styrning för upphandling, IT, informationssäkerhet och dataskydd tillämpas. Samråd ska ske med Digital omställning och IT för att säkerställa en samordnad och långsiktigt hållbar digital helhet.

För kommunens nämnder innebär det att:

- Utgå från verksamhetens behov vid användning av AI och bidra till långsiktig kvalitet samt effektiv resursanvändning.
- Se till att AI-system harmoniserar med kommunens IT-miljö, styrning och möjliggör samverkan .
- Tillämpa ordinarie styrning vid upphandling, utveckling och användning av AI .
- Samråd med Digital omställning och IT.
- Samråd med dataskyddsombudet om personuppgifter ska behandlas.

Uppföljning av riktlinjen

Riktlinjen följs upp inom ramen för det kommungemensamma arbetet med AI för att säkerställa aktualitet i förhållande till teknik, lagstiftning och kommunens *Plan för digital omställning* och andra styrdokumentet på området.

Relaterade styrdokument

Denna riktlinje ska tillämpas i samverkan med följande styrdokument:

- **Plan för digital omställning 2025–2028** (Beslutad av KF).
- **Informationssäkerhetspolicy för Umeå kommun** (Beslutad av KF).
- **Riktlinjer för informationssäkerhet, Umeå kommun** (Beslutad av KS).
- **Policy för informationsförvaltning** (Beslutad av KF).

UMEÅ KOMMUN

Policy för AI

Beslutad av:	Diarienummer:	Datum, paragraf för beslut:	Dokumentet styr:
Kommunfullmäktige	[XXXX]	[20XX-XX-XX, § XX]	[Xxx]
Dokumenttyp:	**Giltighetstid:**	**Dokumentansvarig:**	
Policy	[20XX-XX-XX]	[Nämnd]	

Innehåll

Bakgrund

Artificiell intelligens (AI) används i Umeå kommun för att förstärka, utveckla och effektivisera våra verksamheter samt frigöra tid för mänskliga möten. AI utgör en strategisk tillgång för att möta framtidens välfärdsutmaningar. Med AI avses AI-system enligt EU:s AI-förordning:

> *"ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, drar slutsatser härledda från den indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras"*

I kommunens verksamheter kan AI t ex användas för automatiserad fakturahantering, AI som analyserar skolresultat, AI-stöd för att upptäcka risker i socialtjänsten, chattbotar för invånarservice och AI som maskerar personuppgifter i dokument.

För att upprätthålla förtroende och tillit ska AI utvecklas och användas för att skapa trygghet och nytta för invånare, verksamheter och näringsliv på ett ansvarsfullt, etiskt och hållbart sätt.

Syfte

Syftet med AI-policyn är att tydliggöra ansvar och övergripande ramar för användning och utveckling av AI inom och för Umeå kommun och hela kommunkoncernen, inklusive kommunala bolag. Policyn gäller för kommunkoncernen och alla som är verksamma i kommunkoncernen t ex anställda, arvoderade och konsulter.

Lagstiftning och andra styrande dokument

Befintlig lagstiftning som reglerar användandet av bland annat AI omfattar:

- Cybersäkerhetslagen
- Dataskyddsförordningen (GDPR)
- Offentlighets- och sekretesslagen (OSL)
- Kommunallagen (KL)
- EU:s AI-förordning (AI Act, 2024, 2026)
- Etik- och integritetsprinciper enligt DIGG och SKR

Befintliga kommunala styrdokument och riktlinjer inkluderar:

- Plan för digital omställning 2025-2028
- Riktlinjer för informationssäkerhet
- Policy för informationsförvaltning
- Policy för informationssäkerhet

Avgränsningar

Policyn omfattar Umeå kommunkoncern. Den kommunala koncernen består av kommunfullmäktige, kommunstyrelse, kommunens nämnder och förvaltningar samt helägda kommunala bolag. I gemensamma nämnder, delägda bolag och andra associationsformer verkar kommunen för att policyn ska tillämpas i tillämpliga delar. Vad som är tillämpliga delar ska avgöras utifrån ägarförhållandena, verksamhetens art och omständigheterna i övrigt.

Principer för AI-användning

Principerna beskriver Umeå kommunkoncerns gemensamma förhållningssätt till användning av AI, ska vara vägledande för hela kommunkoncernen och konkretiseras i riktlinjer för AI-användning.

Princip 1. Användningen av AI sätter människan i centrum

Användningen av AI ska bidra till nytta för invånare och verksamheter genom att stödja och stärka mänskliga beslut och arbetssätt. Som verktyg ska AI bidra till ökad kvalitet i kommunala tjänster.

Princip 2. Säker, laglig och etisk användning av AI

AI ska användas i enlighet med lagstiftning och med respekt för grundläggande rättigheter. Användningen ska skydda integritet och motverka diskriminering och oönskade snedvridningar.

Princip 3. Människan är alltid ansvarig

AI ska användas som stöd, men ansvar för beslut, bedömningar och resultat ligger alltid hos ansvarig beslutsfattare.

Princip 4. Proportionerlig och riskmedveten användning

AI ska användas i proportion till risk och påverkan. Ju större konsekvenser, desto högre krav på riskbedömning, dokumentation och kontroll.

Princip 5. Transparent användning

Det ska vara tydligt och möjligt att förstå när och hur AI har använts och hur det kan ha påverkat beslut eller bedömningar.

Princip 6. Smart och hållbar resursanvändning

AI ska bidra till en effektiv och ansvarsfull användning av tid, kompetens, energi och naturresurser. Genom att använda AI på ett klokt sätt kan utrymme skapas för mer värdeskapande mänskligt arbete.

Ansvar

Tekniska nämnden ansvarar för att leda, samordna och utveckla det kommungemensamma arbetet med AI samt tillhandahålla gemensamma ramar och stöd.

Kommunstyrelsen ansvar för att leda, samordna och utveckla det kommungemensamma arbetet med informationssäkerhet som ger stöd för arbetet med AI.

AI-utveckling i Umeå kommun sker både kommungemensamt och verksamhetsnära. Den kommungemensamma styrningen ska stödja och möjliggöra respektive nämnds samt bolags ansvar att inom sitt verksamhetsområde identifiera behov, kravställa, prioritera och följa upp AI-användning i enlighet med kommunens gemensamma styrning.

Revidering av policyn

Policyn ska ses över årligen och vid behov revideras om det sker väsentliga förändringar i lagstiftning, teknik eller kommunens arbetssätt med AI. Tekniska nämnden ansvarar för att initiera revideringen, i samverkan med berörda nämnder och kommunala bolag. Förslag till revidering fastställs av kommunfullmäktige.

UMEÅ KOMMUN

Styrning av artificiell intelligens i Umeå kommun

Artificiell intelligens (AI) skapar nya möjligheter att utveckla verksamheter, stärka kvaliteten och frigöra tid för mänskliga möten. Samtidigt ställer användningen krav på ansvar, transparens, informationssäkerhet och rättssäkerhet.

För att skapa ett gemensamt förhållningssätt har Umeå kommun tagit fram en policy och en riktlinje för AI. Policyn beskriver de övergripande principerna för AI-användning i kommunens nämnder och bolag medan riktlinjen konkretiserar hur principerna ska tillämpas i kommunens nämnder och verksamheter.

Styrdokumenten utgör grunden i kommunens styrning av AI. Nästa steg är att komplettera styrningen med stöd och rutiner som vägleder medarbetare i frågor om exempelvis AI-verktyg, informationshantering, riskbedömning och införande av AI.

Arbetet sker inom kommunens ordinarie styrning för digital omställning och informationssäkerhet. Digital omställning och IT (DoIT) samordnar arbetet tillsammans med samverkansobjektet Datadriven kommun för att säkerställa en gemensam och långsiktigt hållbar utveckling

Styrkedjan beskriven

AI-policy: Beskriver kommunens gemensamma principer och övergripande inriktning för AI.

Exempel: Risker med AI ska identifieras och hanteras innan AI-system används.

Riktlinje för AI: Konkretiserar policyn och tydliggör ansvar, krav och arbetssätt för nämnder och verksamheter.

Exempel: Verksamheten ska säkerställa att AI-system används på rätt sätt och att riskbedömningar genomförs och följs upp.

Verksamhetsnära stöd: Ger praktisk vägledning om AI-system, information, riskbedömning, metoder och utbildning.

Exempel: Vilka AI-system får användas? Vilken information får hanteras? Hur genomförs en riskbedömning?

Användning i verksamheten: Omsätter styrningen till trygg och värdeskapande användning av AI i vardagen.

Exempel: Vad får jag använda AI till och vad behöver jag vara särskilt försiktig med?

Instanser för remiss:

Policy och riktlinjer

- Kommunstyrelsen
- Kommunstyrelsens och Kommunfullmäktiges utskott
- Byggnadsnämnden
- Miljö- och hälsoskyddsnämnden
- Fritidsnämnden
- Kulturnämnden
- För- och grundskolenämnden
- Gymnasie- och vuxenutbildningsnämnden
- Personalnämnden
- Tekniska nämnden
- Individ- och familjenämnden
- Äldrenämnden
- Valnämnden

Policy

- UKF via Marcus Larsson

Svaren ska vara TNdiarium till handa senast 2026-12-18.

UMEÅ KOMMUN

Tjänsteskrivelse
2026-06-23

Tekniska nämnden

Diarienr: TN-2026/00549

Yttrande Motion 11/2026: Umeå kommun behöver styra sin AI innan implementering

Förslag till beslut

Tekniska nämnden beslutar

att föreslå kommunfullmäktige att anse motion 11/2026, Umeå kommun behöver styra sin AI innan implementering, besvarad med hänvisning till att motionens intentioner i huvudsak omhändertas genom förslagen till policy för AI och riktlinje för AI-användning.

Ärendebeskrivning

Motion 11/2026 väcker frågor om hur Umeå kommun ska styra användningen av artificiell intelligens. Motionärerna yrkar bland annat på krav på mänsklig bedömning, tydliga gränser för användningen, överblick över kommunens AI-system, konsekvensanalyser före införande, fackligt inflytande, efterlevnad av EU:s AI-förordning, löpande tillsyn, invånardelaktighet samt begränsningar för hur data får användas.

Kommunen har tagit fram förslag till en kommungemensam policy för AI och en tillhörande riktlinje för AI-användning. Avsikten är att styrdokumenten ska beslutas gå på nämndsremiss i september 2026. Policyn anger övergripande principer och ansvar, medan riktlinjen konkretiserar hur AI ska prövas, införas, användas och följas upp.

Förslagen innebär bland annat att AI ska sätta människan i centrum, användas lagligt och etiskt samt stödja mänskliga beslut utan att ersätta mänskligt ansvar. Beslut som får konsekvenser för enskilda får inte fattas enbart genom automatiserade system utan mänsklig kontroll, om inte lagstöd finns.

Riktlinjen ställer även krav på ett proportionerligt och riskmedvetet arbetssätt. AI får inte tas i bruk innan lagligheten har fastställts och relevanta risker har bedömts och hanterats. Kraven på riskbedömning, dokumentation, kontroll, uppföljning och mänsklig tillsyn ska anpassas efter användningens påverkan. Risker kopplade till bland annat

rättssäkerhet, diskriminering, sekretess, informationssäkerhet och dataskydd ska hanteras inom kommunens ordinarie processer.

Transparens och ansvar behandlas genom krav på att det ska vara möjligt att förstå när och hur AI används, hur ett AI-system har påverkat ett resultat eller beslut samt vem som ansvarar för användningen. Nämnderna ska ha överblick över de AI-system som används, säkerställa dokumentation och registrering samt följa upp användningen löpande. Vid upphandling och utveckling ska kommunens ordinarie styrning för bland annat upphandling, IT, informationssäkerhet och dataskydd tillämpas.

Tekniska nämnden vill samtidigt framhålla att artificiell intelligens inte är en isolerad teknikfråga utan en integrerad del av kommunens samlade digitala omställning. I takt med att digitala tjänster, informationsflöden och systemstöd blir alltmer sammanlänkade ökar behovet av gemensam styrning, överblick och samordning. En långsiktigt hållbar användning av AI förutsätter därför att utveckling, införande och förvaltning sker inom ramen för kommunens gemensamma styrning för digitalisering och i enlighet med Plan för digital omställning. Detta är också anledningen till att samverkansobjekten och Digital omställning och IT (DoIT) har en viktig roll i att stödja samordning, prioritering och uppföljning över verksamhetsgränserna. Denna kommunövergripande styrning är särskilt viktig eftersom såväl tekniken som lagstiftningen på området utvecklas snabbt och kräver ett sammanhållet och kontinuerligt arbete

Tekniska nämnden bedömer att motionens huvudsakliga intentioner om mänsklig kontroll, riskhantering, transparens, ansvar och regelefterlevnad omhändertas genom den föreslagna AI-policyn och riktlinjen för AI-användning. Samtidigt skapar den föreslagna styrningen förutsättningar för en långsiktigt hållbar, kommunövergripande och samordnad utveckling av AI i takt med att teknik, verksamhetsbehov och regelverk förändras. Det bedöms därför inte vara ändamålsenligt att införa ytterligare separata styrprinciper enligt motionens yrkanden. Motionen bör därför anses besvarad.

Beslutsunderlag

Motion 11/2026: Umeå kommun behöver styra sin AI innan implementering. Bilaga.

Tjänsteskrivelse

Dnr: TN-2026/00549

Checklista för handläggning av ärenden inför politiska beslut anses inte tillämpbar.

Beredningsansvariga

Mattias Wallmark, verksamhetschef, Digital omställning och IT

Beslutet ska skickas till

KSdiarium

Umeå kommun behöver styra sin AI innan implementering

Motion till kommunfullmäktige från Arbetarpartiet

Kommunen håller på att införa artificiell intelligens i verksamheter som direkt påverkar Umeåbornas vardag. Det kan ha fördelar. Teknik kan frigöra tid, förbättra service och avlasta personal. Men det är viktigt att kommunen ser på AI inte som ett neutralt verktyg, utan något som bör styras i rätt riktning redan innan AI tas i bruk. Om ett datorprogram hjälper till att avgöra om någon får ekonomiskt bistånd, hur ett barn ska placeras eller hur en anställd presterar, då handlar det inte längre bara om effektivitet. Det handlar om makt, rättvisa och ansvar.

AI-system kan ha inbyggda fördomar utan att någon lagt dit dem medvetet. De kan systematiskt missgynna vissa grupper, som äldre, personer med funktionsnedsättning och ekonomiskt utsatta. Det är just dessa grupper som är mest beroende av kommunal service. AI-system kan fatta beslut som ingen tjänsteperson eller utvecklare kan förklara, vilket gör det omöjligt för en invånare att få en förklaring (på ett beslut) eller överklaga beslutet. Och de kan förändras över tid på sätt som ingen uppmärksammar förrän skadan redan är skedd.

Detta är ett argument för att kommunen måste ha kontroll över de system de inför och ta ansvar för dem från dag ett. När kommunen nu ska utveckla en AI-strategi är det viktigt att strategin inte bara beskriver vad tekniken ska användas till, utan också anger vad den inte får användas till, vilka värden den ska tjäna och vem som bär ansvar när något går fel. Utan sådana ramar är det budgeten och effektiviseringskraven som sätter gränserna och inte demokratin.

Yrkanden

Vi anser att de viktigaste punkterna är följande:

Rätten till en mänsklig bedömning

att det alltid måste finnas en människa som kan granska, förklara och ompröva. Ingen invånare ska behöva acceptera ett beslut som enbart fattats av ett datorprogram Det är inte en teknisk fråga utan en grundläggande rättighet.

Tydliga gränser för vad AI inte får användas till

att det utformas stoppregler. För utan sådana finns ingen gräns och en AI-strategi utan gränser är inte en styrning av teknik, det är en kapitulation inför den. En AI-strategi behöver bindande regler som anger var gränsen går.

En offentlig lista över alla AI-system i kommunen

att transparens måste vara en grundförutsättning för ansvarsutkrävning. Invånare, förtroendevalda och anställda har rätt att veta vilka system som används, vad de är till för och vem ansvarar för dem.

Konsekvensanalys innan ett system driftsätts

att kommunen, innan den börjar använda ett nytt AI-system, bör ha analyserat vilka risker det medför, för diskriminering, för rättssäkerhet och för de anställdas arbetsmiljö. Det är enklare och billigare att förebygga problem än att rätta till dem i efterhand.

Fackligt inflytande

att fackliga organisationer måste ha formellt inflytande redan i utvecklingsfasen av system som påverkar arbetsprocesser, inte bara informeras när besluten redan är fattade. De som utför arbetet vet bäst hur det fungerar i praktiken. Den kunskapen är ovärderlig när AI-system ska utvecklas och införas. Det är både demokratiskt riktigt och en förutsättning för att systemen ska fungera väl i verkligheten.

Efterlevnad av EU:s AI-förordning

att kommunens AI-strategi måste innehålla en konkret plan för inventering, riskklassning och dokumentation med ansvariga personer som har rätt expertis och kompetens för uppgiften. Delar av EU:s AI-förordning gäller redan idag. Åtta kategorier av AI-system är helt förbjudna sedan februari 2025. Alla kommuner är skyldig att veta vilka system den använder och om de uppfyller lagens krav.

Löpande tillsyn med möjlighet att stänga av system

att när ett AI-system antas av kommunen måste tydliga tidpunkter för om- och utvärdering fastställas och en namngiven ansvarig med faktiskt mandat att stänga av systemet om detta ger oönskade effekter. Ett AI-system som fungerade bra när det infördes kan orsaka skada ett år senare.

Invånarna måste vara med

att de grupper som påverkas mest av AI i kommunal service måste ges reell möjlighet att delta i hur systemen utformas och utvärderas, inte bara informeras om beslut som redan är fattade.

Data om invånare är inte en kommunal resurs att maximera

att kommunens AI-strategi måste ange tydliga begränsningar för hur data får samlas in, hur länge den lagras och vad den får användas till. Data som samlas in för ett syfte får inte användas för ett annat utan ett direkt beslut. Invånare ska veta vilken data kommunen har om dem och ha rätt att ifrågasätta hur dessa används.

Umeå kan bli en förebild för hur en kommun inför AI på ett sätt som stärker demokrati och rättvisa i stället för att undergräva dem. Men det kräver att kommunfullmäktige tar politiskt ansvar och inte bara för vad tekniken ska göra, utan för vad den ska åstadkomma för Umeåborna. Teknik ska tjäna människor. Den uppgiften kan inte delegeras till tekniken själv.

Umeå 31 mars 2026
Davis Kaza
Patrik Brännberg
Marika Atlegrim
Katarina Norlund

AP Arbetarpartiet

Vad är EU:s AI-Förordning?

EU:s AI-förordning, AI Act, är den första bindande lagen i världen som reglerar artificiell intelligens. Den gäller alla som använder AI inom EU, inklusive kommuner och myndigheter. Förordningen delar in AI-system i risknivåer. System som påverkar människors tillgång till offentliga tjänster, socialtjänst eller arbete klassas som högrisk och kräver dokumentation, riskbedömning och mänsklig tillsyn.

Sedan februari 2025 är åtta kategorier av AI system helt förbjudna i hela EU, bland annat system som betygsätter medborgare baserat på beteende och system som manipulerar människor utan deras vetskap. Kommunen är enligt förordningen en användare av AI, vilket innebär konkreta skyldigheter kring tillsyn, dokumentation och incidentrapportering oavsett om systemet är byggt internt eller köpt av en leverantör.

Denna behandling '92/26 Begäran om omfördelning inom beslutad investeringsram' har inget tjänsteutlåtande.

UMEÅ KOMMUN

Tjänsteskrivelse
2026-08-12

Tekniska nämnden

Diarienr: TN-2026/00632

Yttrande Remiss informationssäkerhetspolicy och riktlinje informationssäkerhet

Förslag till beslut
Tekniska nämnden beslutar

att lämna yttranden enligt nedan.

Ärendebeskrivning
Kommunstyrelsens näringslivs- och arbetsutskott beslutade den 5 maj att överlämna remiss av reviderad informationssäkerhetspolicy och reviderad riktlinje för informationssäkerhet till kommunens nämnder för yttrande. Teknik- och fastighetsförvaltningens personuppgiftskoordinatorer har arbetat fram ett yttrande.

Yttrande informationssäkerhetspolicy
Inledningsvis saknas upplysning om att Informationssäkerhetspolicyn är ett övergripande styrdokumentet för kommunens informationssäkerhetsarbete och omfattar all information som hanteras inom Umeå kommun. Man kan även tillägga att Informationssäkerhetspolicyn ersätter gamla Informationssäkerhetspolicy för Umeå kommun fastställda av KF 2009-04-27, version 2.

Det saknas ett avsnitt ”Syfte med informationssäkerhetsarbetet” (se Umeå kommuns mall för Policy).

Övriga synpunkter:
- Det behövs ett förtydligande gällande avgränsning om att Informationssäkerhetspolicyn gäller hela Umeå kommuns organisation inklusive eller exklusive de kommunala bolagen.
- Utgå ifrån att verksamhetsinformation ägs organisatoriskt av respektive myndighet där den ansvarige inte bara är nämnden utan även styrelse.
- Det borde finnas ett avsnitt om Ansvar och roller där det tydligt framgår vem som ansvarar för vad, utifrån t.ex. KF, KS, nämnder (bolagsstyrelserna i fall Informationssäkerhetspolicyn ska gälla dem), informationssäkerhetssamordnare, chefer, anställda förtroendevalda.

Tjänsteskrivelse

Dnr: TN-2026/00632

- Det är bra om det framkommer hur denna policy ska följas upp och revideras.

Yttrande riktlinje informationssäkerhet
Under avsnittet ”Lagar och standarder”:
Allmänna råd och föreskrifter bör flyttas ner medan lagar flyttas upp för att följa svenska regelhierarkin/rangordning: lagar först sen förordning därefter föreskrifter.
Fråga: AI-förordningen ska inte den vara med?

Beslutsunderlag

KS Protokollsutdrag. Bilaga.
Remissversion_Informationssäkerhetspolicy. Bilaga.
Remissversion_Riktlinje informationssäkerhet. Bilaga.

Checklista för handläggning av ärenden inför politiska beslut anses inte tillämpbar.

Beredningsansvariga

Teknik- och fastighetsförvaltningens personuppgiftskoordinatorer.

Beslutet ska skickas till

ksdiarium@umea.se senast den 5 oktober 2026. Ange ärendenummer KS-2026/00356 i ämnesraden.

Umeå kommun **Protokollsutdrag**

Kommunstyrelsens näringslivs- och arbetsutskott 2026-05-05

§ 172

Diarienr: KS-2026/00356

Remiss informationssäkerhetspolicy och informationssäkerhetsriktlinjer

Beslut

Kommunstyrelsens näringslivs- och arbetsutskott beslutar

att överlämna remiss av reviderad informationssäkerhetspolicy och reviderad riktlinje för informationssäkerhet till kommunens nämnder för yttrande senast 5 oktober 2026.

Ärendebeskrivning

Enligt kommunstyrelsens beslut avseende aktualitets- och relevansprövning av styrande dokument i april 2024 ska informationssäkerhetspolicy samt riktlinje för informationssäkerhet revideras.

Den reviderade informationssäkerhetspolicyn har uppdaterats utifrån ny lagstiftning på informationssäkerhetsområdet (cybersäkerhetslagen) och det förändrade omvärldsläget. Policyn syftar till att beskriva informationssäkerhetsarbetets övergripande inriktning.

Den nuvarande informationssäkerhetsriktlinjen är mycket omfattande och kommer i samband med revideringen att delas upp och omhändertas utifrån olika områden, för en tydligare och mer ändamålsenlig styrning av informationssäkerhetsarbetet.

Den reviderade riktlinjen ”systematiskt informationssäkerhetsarbete” har uppdaterats utifrån ny lagstiftning inom informationssäkerhetsområdet (cybersäkerhetslagen) och det förändrade omvärldsläget. Riktlinjen syftar till att stödja nämndernas arbete genom att beskriva och konkretisera de fokusområden som Umeå kommuns verksamheter ska arbeta med för att

uppnå ett systematiskt och riskbaserat informationssäkerhetsarbete i enlighet med lagstiftning och relevanta standarder.

Beslutsunderlag

Remissversion: Informationssäkerhetspolicy
Remissversion: Riktlinjer systematiskt informationssäkerhetsarbete

Beredningsansvariga

Jonas Andersson Wikström, säkerhetschef
Hanna Öberg, informationssäkerhetssamordnare

Näringslivs- och arbetsutskottets beslutsordning

Näringslivs- och arbetsutskottet beslutar enligt tjänsteskrivelsens förslag.

Beslut och beslutsunderlag ska skickas till

Protokoll och remisshandlingar ska skickas till samtliga nämnder.
Svar på remiss skickas till ksdiarium@umea.se senast den 5 oktober 2026. Ange ärendenummer KS-2026/00356 i ämnesraden.

UMEÅ KOMMUN

Informationssäkerhet

REMISSVERSION

Informationssäkerhetspolicy

Beslutad av: Kommunfullmäktige	**Diarienummer:** [XXXX]	**Datum, paragraf för beslut:** [20XX-XX-XX, § XX]	**Dokumentet styr:** Alla nämnder
Dokumenttyp: Policy	**Giltighetstid:** [20XX-XX-XX]	**Dokumentansvarig:** Kommunstyrelsen	

Informationssäkerhetspolicy

Umeå kommuns informationssäkerhetsarbete omfattar Umeå kommuns verksamhetsinformation och utgår från principen att var och en ska kunna lita på informationen och vara trygg med hur den hanteras.

Verksamhetsinformation omfattar all information som skapas, tas emot och förvaltas i aktiviteter under Umeå kommuns uppdrag i alla dess former, oavsett hur informationen hanteras.

All verksamhetsinformation har en informationsägare. Informationsägaren ansvarar för verksamhetsinformation ges ett tillräckligt skydd. Verksamhetsinformation ägs organisatoriskt av respektive myndighet där den ansvarige är nämnden.

Informationssäkerhetsarbetets inriktning

1. Det kommungemensamma arbetet med informationssäkerhet utformas utifrån ISO/IEC 27001 och 27002 och inriktningen i denna policy. Arbetet ska kontinuerligt utvecklas, följas upp och förbättras.
2. Informationssäkerhetsarbetet i alla nämnder ska säkerställa att informations konfidentialitet, riktighet och tillgänglighet upprätthålls.
3. Information ska erhålla rätt nivå av skydd genom ett systematiskt och riskbaserat arbetssätt.
4. Information ska skyddas genom organisatoriska, fysiska, tekniska och personalrelaterade säkerhetsåtgärder i enlighet med författningskrav och interna styrdokument.

Begrepp

Information: Kunskap om objekt, såsom fakta, händelser, saker, processer eller idéer, inklusive begrepp, som inom ett visst sammanhang har en särskild betydelse.

Informationssäkerhet: Bevarande av informationens konfidentialitet, riktighet och tillgänglighet.

Informationsägare: Person eller enhet som har ansvaret för den information som skapas och hanteras inom den egna verksamheten.

Konfidentialitet: Egenskap som innebär att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

Riktighet: Egenskap som innebär att information är korrekt och fullständig.

Säkerhetsåtgärd: Åtgärd för att bibehålla och/eller förändra risker.

Tillgänglighet: Egenskap som innebär att information är åtkomlig och användbar på begäran från ett behörigt objekt.

Verksamhetsinformation: Information som skapas, tas emot och underhålls som bevis och/eller som en tillgång av en organisation eller person för att uppfylla legala förpliktelser eller för att utföra transaktioner i verksamheten, oavsett typ av medium och format.

Relaterade styrdokument

- Riktlinjer för informationssäkerhet
- Policy för informationsförvaltning

UMEÅ KOMMUN

Informationssäkerhet

REMISSVERSION

Riktlinje informationssäkerhet

Systematiskt informationssäkerhetsarbete

Beslutad av:	**Diarienummer:**	**Datum, paragraf för beslut:**	**Dokumentet styr:**
Kommunstyrelsen	[XXXX]	[20XX-XX-XX, § XX]	Alla nämnder
Dokumenttyp:	**Giltighetstid:**	**Dokumentansvarig:**	
Riktlinje	[20XX-XX-XX]	Kommunstyrelsen	

Innehåll

Inledning

Bakgrund och syfte

Umeå kommuns informationssäkerhetsarbete omfattar Umeå kommuns verksamhetsinformation och utgår från principen att var och en ska kunna lita på informationen och vara trygg med hur den hanteras.

Ett systematiskt informationssäkerhetsarbete utgör grunden för att skydda information, upprätthålla förtroendet för organisationen och efterleva författningskrav. Ett systematiskt informationssäkerhetsarbete ökar också möjligheten att kunna stå emot och hantera störningar och avbrott kopplat till informationshanteringen.

Denna riktlinje syftar till att stödja nämndernas arbete genom att beskriva och konkretisera de fokusområden som Umeå kommuns nämnder ska arbeta med för att uppnå ett systematiskt och riskbaserat informationssäkerhetsarbete.

Lagar och standarder

Krav på informationssäkerhet utgår från gällande lagstiftning och relevanta standarder, t.ex:

- Cybersäkerhetslagen
- *Myndigheten för civilt försvars och allmänna råd om säkerhetsåtgärder och utbildning (ej beslutade)*
- *Myndigheten för civilt försvars föreskrifter om incidentrapportering och informationsskyldighet (ej beslutade)*
- Dataskyddsförordningen
- Offentlighets- och sekretesslagen
- Arkivlagen
- ISO/IEC 27001 och 27002

Angränsande styrdokument

- Informationssäkerhetspolicy
- Policy för informationsförvaltning

Omfattning och avgränsning

Denna riktlinje gäller för alla nämnder i Umeå kommun och all information som skapas, tas emot och förvaltas i aktiviteter under kommunens uppdrag i alla dess former, oavsett hur informationen hanteras.

Om det vid något tillfälle råder motsättningar mellan författningskrav och interna styrdokument har författningskrav företräde i tolkningen.

Verksamhet och information som omfattas av säkerhetsskyddslagen omfattas inte av denna riktlinje. För sådan gäller säkerhetsskyddslagen och dess relaterade författningskrav och interna styrdokument.

Begrepp och definitioner

Samtliga begrepp och definitioner är hämtade från Umeå kommuns begreppsmodell för informationsförvaltning[1].

Incident: Händelse som kan vara eller skulle kunna leda till en störning, en förlust, ett nödläge, eller en kris.

Information: Kunskap om objekt, såsom fakta, händelser, saker, processer eller idéer, inklusive begrepp, som inom ett visst sammanhang har en särskild betydelse.

Informationssystem: Uppsättning av applikationer, tjänster, informationsteknologiska tillgångar och andra informationshanteringskomponenter.

Informationssäkerhet: Bevarande av informationens konfidentialitet, riktighet och tillgänglighet.

Informationstillgång: information, och resurser som hanterar den, som är av värde för en organisation.

Informationsägare: Person eller enhet som har ansvaret för den information som skapas och hanteras inom den egna verksamheten.

Konfidentialitet: Egenskap som innebär att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

Kontinuitet: Förmåga att upprätthålla verksamhet på en i förhand bestämd nivå.

Riktighet: Egenskap som innebär att information är korrekt och fullständig.

Tillgänglighet: Egenskap som innebär att information är åtkomlig och användbar på begäran från ett behörigt objekt.

Skyddsnivå: Samling uttalade behov avseende skydd.

Systemägare: Den som äger och har ett överordnat ansvar för administration, drift och säkerhet för ett informationssystem.

Säkerhetsåtgärd: Åtgärd för att bibehålla och/eller förändra risker.

Verksamhetsinformation: Information som skapas, tas emot och underhålls som bevis och/eller som en tillgång av en organisation eller person för att uppfylla legala förpliktelser eller för att utföra transaktioner i verksamheten, oavsett typ av medium och format.

[1] Begreppsmodell informationsförvaltning — OpenDataUmea

Ansvar

Umeå kommun ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete enligt kommunens informationssäkerhetspolicy. Ansvar för informationssäkerhet följer ordinarie verksamhetsansvar. Den betyder att den som är chef för en viss verksamhet är också formellt ansvarig för informationssäkerhetsarbetet i verksamheten.

Informationsägare

All verksamhetsinformation (benämns hädanefter information i detta dokument) ska ha en utsedd informationsägare. Respektive nämnd är ytterst ansvarig för den information som hanteras i nämnden, förvaltningen och dess verksamheter. Det innebär att nämnden är informationsägare ur ett juridiskt perspektiv.

Nämnden delegerar det operativa ansvaret till förvaltningen som har det operativa ansvaret för att informationssäkerhetsarbetet bedrivs systematiskt och riskbaserat.

Som informationsägarens representant ansvarar förvaltningen och dess verksamheter för att informationssäkerhetsarbetet leds, planeras, genomförs, dokumenteras och följs upp.

Informationssäkerhetsarbetet ska integreras med befintliga sätt att leda och styra organisationen.

Systemägare

Alla informationssystem ska ha en utsedd systemägare. Respektive nämnd är ytterst ansvarig för de informationssystem som förvaltas i nämnden, förvaltningen och dess verksamheter. Det innebär att nämnden är systemägare ur ett juridiskt perspektiv.

Nämnden delegerar det operativa ansvaret till förvaltningen vilket innebär att förvaltningen har det operativa ansvaret för drift och säkerhet i de informationssystem som förvaltningen innehar.

Som systemägarens representant ansvarar förvaltningen och dess verksamheter för att säkerställa att informationssystem upprätthåller det skydd som motsvarar skyddsbehovet i den information som förekommer i informationssystemet. Skyddsnivå fastställs av informationsägaren.

För informationssystem som ingår i ett samverkansobjekt enligt Umeå kommuns samverkansmodell för digitalisering så utgör objektägaren förvaltningens representant för systemägaren.

Fokusområden i nämndernas systematiska arbete

Nedan beskrivs de områden som informationsägare och systemägare (genom dess representanter i förvaltningen och dess verksamheter) ansvarar för i arbetet med att upprätthålla ett systematiskt och riskbaserat informationssäkerhetsarbete.

Informationskartläggning

Informationsägaren ska säkerställa att all information är kartlagd och dokumenterad.

Dokumentationen ska redogöra för vilken verksamhetsprocess informationen hanteras i, vem som är informationsägare samt var informationen hanteras (t.ex. informationssystem).

Informationssäkerhetsklassning

Informationsägaren ansvarar för att arbete med informationssäkerhetsklassning genomförs och dokumenteras.

All information ska värderas avseende konfidentialitet, riktighet och tillgänglighet utifrån vilka konsekvenser ett bristande skydd kan få. Författningskrav och interna krav ska vägas in i klassningen.

Informationssäkerhetsklassning ska genomföras innan information behandlas i informationssystem.

Informationssäkerhetsklassningen ska följas upp och utvärderas vid behov men minst årligen.

Se bilaga 1 - Informationssäkerhetsklassning och skyddsnivåer.

Riskhantering

Informationsägaren ska utifrån ett allriskperspektiv identifiera, analysera och värdera risker med informationshanteringen för att få underlag för valet av lämpliga och proportionella säkerhetsåtgärder. Resultatet av informationssäkerhetsklassningen och eventuella risker som identifierats genom omvärldsbevakning används som ett ingångsvärde i riskanalysen.

Riskanalys ska genomföras innan information behandlas i informationssystem och vid förändrade hot och nya sårbarheter.

De säkerhetsåtgärder som väljs för att åtgärda identifierade risker ska dokumenteras i en åtgärdsplan. Arbetet med säkerhetsåtgärder enligt åtgärdsplanen ska följas upp utifrån identifierat behov, men minst var tredje månad.

Informationsägaren ansvarar för att arbete med riskhantering utförs och att resultatet fastställs avseende den information denne ansvarar för.

Systemägaren ansvarar för att arbete med riskhantering utförs och att resultatet fastställs avseende de informationssystem och de delar av den digitala miljön som denne ansvarar för.

Se bilaga 2 – Riskhantering.

Säkerhetsåtgärder

Informationsägaren ska säkerställa att information skyddas med lämpliga och proportionella säkerhetsåtgärder utifrån resultat från genomförda informationssäkerhetsklassningar och riskanalyser.

Informationsägaren ska involvera systemägaren i arbetet med att identifiera och hantera behov av säkerhetsåtgärder i informationssystem. Informationsägaren fastställer och kommunicerar krav på säkerhetsåtgärder i informationssystem till systemägare som har ett överordnat ansvar för informationssäkerheten i informationssystem.

Informationsägaren ska vid behov men minst årligen bedöma effektiviteten av införda säkerhetsåtgärder genom att följa upp och utvärdera deras lämplighet och proportionalitet i förhållande till externa krav, interna behov och identifierade risker.

Säkerhetsåtgärder avseende information som hanteras i informationssystem är framtagna i en kommungemensam kravkatalog. Kravkatalogen anger en miniminivå av rekommenderade säkerhetsåtgärder för informationssystem, med utgångspunkt i informationens skyddsnivå. Kravkatalogen utgår från SS-EN ISO/IEC 27002: 2022 samt gällande lagstiftning inom informationshanteringsområdet.

Informationssäkerhetsklassning ligger till grund för vilka säkerhetsåtgärder som väljs från kravkatalogen. Riskanalys ligger till grund för ytterligare säkerhetsåtgärder som behöver vidtas utifrån de åtgärdsförslag som beslutats i riskanalysen.

Informationssäkerhet i leverantörskedjan

Innan avtal upprättas med en leverantör som ska behandla kommunens information, t.ex. i ett av leverantören tillhandahållet informationssystem ska informationsägaren ha:

- Säkerställt att systemägare är utsedd.
- Genomfört en informationssäkerhetsklassning av den information som ska hanteras av leverantören och i informationssystemet.

- Identifierat och åtgärdat de risker som finns med att informationen hanteras av leverantören och i informationssystemet.
- Identifierat de krav på säkerhetsåtgärder som behöver ställas på leverantören och informationssystemet.
- Kontrollerat att tilltänkt leverantör och informationssystem uppfyller kraven på säkerhetsåtgärder och bedömt att dessa kommer att kunna uppfylla kraven under avtalstiden.

Innan leverantören påbörjar behandlingen av information ska informationsägaren godkänna informationsbehandlingen och systemägare fatta beslut om driftsättning av informationssystemet.

Incidenthantering

Informationsägaren ska säkerställa att incidenter relaterade till information och informationssystem upptäcks, rapporteras, hanteras, dokumenteras och följs upp i samverkan med systemägaren. Incidenter ska hanteras och åtgärdas skyndsamt för att minimera skador i verksamheten och för individer.

Informationsägaren ska säkerställa att informationssäkerhetsincidenter och personuppgiftsincidenter där anmälningsskyldighet finns enligt lag eller förordning, anmäls till ansvarig myndighet.

Kontinuitetshantering

Verksamhet som kommunen är skyldig att utföra enligt författning ska kunna bedrivas på en acceptabel nivå trots nedsatt funktionalitet eller allvarlig störning/avbrott i informationssystem.

Informationsägaren ska säkerställa att det finns avbrottsplaner eller kontinuitetsplaner för informationssystem som är nödvändiga för att bedriva sådan verksamhet.

Informationssäkerhetskultur och utbildning

Informationsägaren ska säkerställa att alla medarbetare har förutsättningar för att behandla information på ett säkert sätt. Alla medarbetare ska ha relevant och aktuell kunskap och kompetens för att kunna omhänderta risker vid åtkomst till information och informationssystem, utifrån sina behov.

Bilaga 1 – Informationssäkerhetsklassning och skyddsnivåer

Klassning av information görs utifrån tre olika perspektiv - konfidentialitet, riktighet och tillgänglighet. Informationen värderas utifrån vilka konsekvenser som kan uppstå om dessa perspektiv inte upprätthålls.

- **Konfidentialitet –** information ska enbart ska vara tillgänglig för den som är behörig till den.
- **Riktighet –** information ska vara korrekt och fullständig.
- **Tillgänglighet –** information ska finns tillgänglig för den som behöver den när den behöver den.

Bedömningen av vilka konsekvenser som kan uppstå om konfidentialitet, riktighet och tillgänglighet brister leder fram till att man kan avgöra skyddsnivå.

Umeå Kommun använder sig av fem skyddsnivåer vid klassning av information, se klassningsmatris.

Klassningsmatris

Skyddsnivå	Konfidentialitet	Riktighet	Tillgänglighet
5. Särskild	**K5** Information som omfattas av Säkerhetsskyddslagen. Hanteras enligt särskilda rutiner.	**R5** Information som omfattas av Säkerhetsskyddslagen. Hanteras enligt särskilda rutiner.	**T5** Information som omfattas av Säkerhetsskyddslagen. Hanteras enligt särskilda rutiner.
4. Hög	**K4** Information där förlust av konfidentialitet kan medföra allvarlig påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra allvarlig påverkan på liv och hälsa.	**R4** Information där förlust av riktighet kan medföra allvarlig påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra allvarlig påverkan på liv och hälsa.	**T4** Information där förlust av tillgänglighet kan medföra allvarlig påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra allvarlig påverkan på liv och hälsa.
3. Utökad	**K3** Information där förlust av konfidentialitet kan medföra betydande påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra betydande påverkan på liv och hälsa.	**R3** Information där förlust av riktighet kan medföra betydande påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra betydande påverkan på liv och hälsa.	**T3** Information där förlust av tillgänglighet kan medföra betydande påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra betydande påverkan på liv och hälsa.
2. Grundläggande	**K2** Information där förlust av konfidentialitet kan medföra måttlig påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra måttlig påverkan på liv och hälsa.	**R2** Information där förlust av riktighet kan medföra måttlig påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra måttlig påverkan på liv och hälsa.	**T2** Information där förlust av tillgänglighet kan medföra måttlig påverkan på förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra måttlig påverkan på liv och hälsa.
1. Låg	**K1** Information där förlust av konfidentialitet inte medför negativa konsekvenser för förmågan att upprätthålla verksamhet, bibehålla förtroende, efterleva lagstiftning eller medföra någon påverkan på liv och hälsa.	Krav finns alltid att information ska vara riktig, bedöms ej.	Krav finns alltid att information ska vara riktig, bedöms ej.

Bilaga 2 – Riskhantering

Vid en riskanalys identifieras vilka oönskade händelser som kan påverka informationshanteringen och varför de kan ske, detta formuleras som risker.

Riskerna värderas utifrån hur stor sannolikhet det är att risken inträffar och vilka konsekvenser risken kan medföra om den inträffar. Därefter identifieras vilka åtgärder som bör vidtas för att minska riskerna och vem som är ansvarig för att åtgärderna vidtas.

Umeå Kommun använder sig av fyra nivåer vid bedömning av sannolikhet och konsekvens, se riskmatris.

Utifrån riskernas värdering finns krav på att riskerna hanteras, se kriterier för riskacceptans.

Kriterier för värdering av sannolikhet och konsekvens

Sannolikhet

Sannolikhet innebär bedömningen av hur stor chans det är att en identifierad oönskad händelse inträffar. Sannolikheten bedöms utifrån fyra nivåer:

1. Osannolik/ Mycket låg
2. Mindre sannolik
3. Möjlig/ Hög
4. Sannolik/ Mycket hög/ Kan ej bedömas

Konsekvens

Konsekvens innebär bedömningen av hur det påverkar en verksamhet eller en enskild individ om en identifierad oönskad händelse inträffar. Konsekvensen bedöms utifrån fyra nivåer:

1. Ingen/ Försumbar skada
2. Måttlig skada
3. Betydande skada
4. Allvarlig skada

Riskmatris

Riskmatrisen visar hur risker värderas utifrån sannolikhet och konsekvens. Genom att multiplicera värdet för sannolikhet med värdet för konsekvens erhåller varje risk ett riskvärde.

Allvarlig 4				
Betydande 3				
Måttlig 2				
Försumbar 1				
Konsekvens/ Sannolikhet	**Osannolik**	**Mindre sannolik**	**Möjlig**	**Sannolik/kan ej bedömas**

Kriterier för riskacceptans

Tabellen visar hur beslut om att acceptera risker eller vidta åtgärder ska fattas.

Riskvärde	Riskhantering	Åtgärder	Krav på genomförande av åtgärd
Låg risk 1-2	Acceptera risk	Inga krav	Inga krav
Medelhög risk 3-6	Reducera risk	Åtgärder för att minska risk (sannolikhet eller konsekvens) ska finnas med i åtgärdsplan	Ska genomföras inom rimlig tid baserat på åtgärdens omfattning (tid, kostnad, resurser)
Hög risk 8-9	Reducera risk	Åtgärder för att minska risk (sannolikhet eller konsekvens) ska finnas med i åtgärdsplan	Ska genomföras snarast möjligt baserat på åtgärdens omfattning (tid, kostnad, resurser)
Mycket hög risk 12-16	Eliminera/undvik risk	Omfattande åtgärder för att minska risk ska finnas med i åtgärdsplan, alt. ändra förfarande helt för att undvika risken	Ska genomföras omedelbart.

UMEÅ KOMMUN

Tjänsteskrivelse
2026-08-31

Tekniska nämnden

Diarienr: TN-2026/00689

Yttrande Remiss om ändrade villkor gällande BK4 i Trafikverkets föreskrifter om bärighetsklasser TRV 2026/92928

Förslag till beslut
Tekniska nämnden beslutar

att lämna yttrande enligt nedan.

Ärendebeskrivning
Trafikverket har för avsikt att ändra villkoren i bärighetsföreskrifterna gällande BK4.
Kommunstyrelsen har överlämnat remissen till Tekniska nämnden för yttrande.

Yttrande
Villkorsändringen i Trafikverkets föreskrifter om bärighetsklass 4 med villkor berör inte kommunen direkt. Utifrån konsekvensutredningen kan ändringen medföra positiva konsekvenser för transportörer.
Umeå kommun har inget att erinra i ärendet.

Beslutsunderlag
Konsekvensutredning till förslag om ändrade villkor gällande BK4 i Trafikverkets föreskrifter om bärighetsklasser. Bilaga.

Checklista för handläggning av ärenden inför politiska beslut anses inte tillämpbar.

Beredningsansvariga
Jonas Sörlén, trafikingenjör

Beslutet ska skickas till
Sista dag för att besvara remissen är 30 september 2026.
Till trafikverket@trafikverket.se, var vänlig ange Trafikverkets diarienummer TRV 2026/92928 i yttrandet**.**

Tjänsteskrivelse

Dnr: TN-2026/00689

Kopia på nämndens protokollsutdrag inkl. yttrande skickas till ksdiarium@umea.se, märk ämnesraden med diarienummer: KS-2026/00834.

Ärendenummer
TRV 2026/92928

Dokumentdatum
2026-08-25
Sidor
1(4)

TRAFIKVERKET

Konsekvensutredning till förslag om bärighetsföreskrifter enligt förordningen (2024:183) om konsekvensutredningar

Bakgrund

Trafikverket har för avsikt att ändra villkoren i bärighetsföreskrifterna gällande BK4.

Vägar som kan klara en högre bärighetsklass än BK1 och som ingår i det upplåtna vägnätet för BK4 kan föreskrivas få BK4. Vissa vägar inom det upplåtna BK4 vägnätet klarar inte den belastning som bruttoviktstabellen för BK4 genererar. Dessa vägar villkoras med krav på fordonen avseende hjulkonfiguration i form av dubbelmonterade hjul på fordonen. Motivet till detta är att inte riskera vägkapitalet och undvika accelererande underhållskostnader. Villkorstexten är utformade på ett sätt som gör att långa fordonståg inte får färdas på de vägarna med vikter och tryck motsvarande BK4 med villkor. De fordonen ofta har 10 axlar eller fler vilket gör att slitaget inte är större med de fordonen än andra och därför borde även de omfattas av undantagen under förutsättning att vägen är öppnad för långa fordonståg.

Genom att lägga till ett stycke om detta i villkoren med krav på minst 10 axlar blir det följande förändring av villkoren.

Nuvarande lydelse:

X § Följande vägar i XX län ska tillhöra bärighetsklass 4 på följande sträckor.

Utöver vad som framgår i trafikförordningen (1998:1276) ska förande av fordon eller fordonståg vara förenade med särskilda villkor enligt följande. Motordrivna fordon med en bruttovikt som överstiger 32 ton ska ha en drivande axel som är försedd med dubbelmonterade hjul och luftfjädring eller likvärdig fjädring, eller att drivaxlarna är försedda med dubbelmonterade hjul och vikten inte överskrider 9.5 ton på någon av axlarna. För fordonskombinationer gäller dessutom att om bruttovikten överstiger 64 ton ska minst 65 procent av släpvagnens eller släpvagnarnas sammanlagda bruttovikt belastas av sådana axlar

med dubbelmonterade hjul. Fordon eller fordonståg registrerade i transportstyrelsens fordonsregister, före 2018-12-31, undantas från ovanstående villkor

Föreslagen lydelse:

X § Följande vägar i XX län ska tillhöra bärighetsklass 4 på följande sträckor.

Utöver vad som framgår i trafikförordningen (1998:1276) ska förande av fordon eller fordonståg vara förenat med särskilda villkor enligt följande. Motordrivna fordon med en bruttovikt som överstiger 32 ton ska ha minst en drivande axel som är försedd med

dubbelmonterade hjul och luftfjädring eller likvärdig fjädring, eller att drivaxlarna är försedda med dubbelmonterade hjul och vikten inte överskrider 9,5 ton på någon av axlarna. För fordonståg gäller dessutom att om bruttovikten överstiger 64 ton ska minst 65 procent av släpvagnens eller släpvagnarnas sammanlagda bruttovikt belasta axlar försedda med dubbelmonterade hjul.

Följande fordon eller fordonståg undantas från villkoren i andra stycket:

1. *Fordon som är registrerade i vägtrafikregistret senast den 31 december 2018, eller*
2. *Fordonståg som har minst 10 axlar och vars längd överstiger 25,25 meter men inte 34,5 meter, lasten inräknad, och som uppfyller villkoren enligt 4 kap. 17 f § trafikförordningen (1998:1276).*

Trafikverket har enligt 4 kap. 11 § trafikförordningen (1998:1276) mandat att meddela föreskrifter om att en allmän väg eller del av en sådan väg, som Trafikverket är väghållare för, ska tillhöra bärighetsklass 2, 3 eller 4. Med stöd av den bestämmelsen har Trafikverket meddelat följande föreskrifter som är berörda av förändringen.

Trafikverkets föreskrifter om bärighetsklasser i Blekinge län (TRVTFS 2025:31)

Trafikverkets föreskrifter om bärighetsklasser i Dalarnas län (TRVTFS 2026:9)

Trafikverkets föreskrifter om bärighetsklasser i Gotlands län (TRVTFS 2024:33), ny föreskrift föreslås träda ikraft 26-12-31, TRV 2026/20315

Trafikverkets föreskrifter om bärighetsklasser i Gävleborgs län (TRVTFS 2026:36)

Trafikverkets föreskrifter om bärighetsklasser i Hallands län (TRVTFS 2026:39)

Trafikverkets föreskrifter om bärighetsklasser i Jämtlands län (TRVTFS 2026:14), ny föreskrift föreslås träda ikraft 26-10-01, TRV 2026/43583

Trafikverkets föreskrifter om bärighetsklasser i Jönköpings län (TRVTFS 2026:16)

Trafikverkets föreskrifter om bärighetsklasser i Kalmar län (TRVTFS 2026:13)

Trafikverkets föreskrifter om bärighetsklasser i Kronobergs län (TRVTFS 2026:30), ny föreskrift föreslås träda ikraft 2027-01-01, TRV 2026/69956

Trafikverkets föreskrifter om bärighetsklasser i Norrbottens län (TRVTFS 2026:12)

Trafikverkets föreskrifter om bärighetsklasser i Skåne län (TRVTFS 2026:2), ny föreskrift föreslås träda ikraft 27-01-01, TRV 2026/60839

Trafikverkets föreskrifter om bärighetsklasser i Stockholms län (TRVTFS 2026:6), ny föreskrift föreslås träda ikraft 27-01-01, TRV 2026/28512

Trafikverkets föreskrifter om bärighetsklasser i Södermanlands län (TRVTFS 2022:32), ny föreskrift föreslås träda ikraft 26-09-14, TRV 2025/18298

Trafikverkets föreskrifter om bärighetsklasser i Uppsala län (TRVTFS 2026:21)

Trafikverkets föreskrifter om bärighetsklasser i Värmlands län (TRVTFS 2026:11), ny föreskrift föreslås träda ikraft 26-12-01, TRV 2026/49765

Trafikverkets föreskrifter om bärighetsklasser i Västerbottens län (TRVTFS 2026:32), 365 genom Lycksele (gästväg till E12) justeras

Trafikverkets föreskrifter om bärighetsklasser i Västernorrlands län (TRVTFS 2026:17)

Trafikverkets föreskrifter om bärighetsklasser i Västmanlands län (TRVTFS 2026:7)

Trafikverkets föreskrifter om bärighetsklasser i Västra Götalands län (TRVTFS 2026:42)

Trafikverkets föreskrifter om bärighetsklasser i Örebro län (TRVTFS 2026:22)

Trafikverkets föreskrifter om bärighetsklasser i Östergötlands län (TRVTFS 2026:20)

Beskrivning av aktuellt läge och vad Trafikverket vill uppnå

Långa fordonståg kan idag inte färdas på vägar som har BK4 med villkor. Om långa fordonståg som har minst 10 axlar tillåts färdas på dessa vägar under förutsättning att vägen är upplåten för långa fordonståg minskar antalet transporter totalt. Detta då de kan lasta mer per färd och på så sätt öka effektiviteten av sina transporter utan att slitaget ökar på vägen.

Om föreslaget om ändrade villkor inte kommer till stånd så kommer de vägar som har BK4 med villkor inte att kunna nyttjas av långa fordonståg, vilket innebär att vägarna inte utnyttjas maximalt.

Alternativa lösningar

En alternativ lösning är att bygga om alla vägar som har BK4 med villkor så att de klarar BK4 men det kräver stora statsningar vilket det inte finns avsatta medel för i dagsläget.

Det finns inga andra realistiska lösningar för att uppnå syftet med förslaget.

Vilka som berörs av regleringen

De näringsidkare som har fordonstyper som kan nyttja de utökade lastmöjligheterna gynnas av föreskriften. Övriga trafikanter gynnas av de minskade antalet tunga transporter totalt i landet.

Kostnader och andra konsekvenser

De särskilda villkoren gäller för motordrivna fordon och fordonsekipage med en samlad bruttovikt över 64 ton som är registrerade i vägtrafikregistret efter 2018-12-31. Genom att även låta långa fordonståg färads på fler vägar som har bärighetstsbegränsningen BK4 med villkor under förutsättning att de är upplåtna för långa fordonståg ökar framkomligheten för de fordonenen och de totala antalet transporter minskar.

Föreskrifterna förväntas inte påverka konkurrensförutsättningarna mellan olika företag då alla får samma förändring.

Dock kan det finnas företag som påverkas beroende på exempelvis verksamhet, storlek och lokalisering. Trafikverkets bedömning är att konsekvenserna av föreskriftsändringarna inte är så pass omfattande att utredning av hur många företag som påverkas är nödvändig.

Förslaget bedöms inte påverka företagens administrativa förutsättningar i någon större utsträckning.

TRAFIKVERKET

Överrensstämmelse med EU-rätten

Förslaget är av nationell karaktär och överensstämmer med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.

Ikraftträdande och informationsinsatser

Föreskrifterna föreslås träda i kraft den *2026-12-01*. Det är angeläget att de nya villkoren ikraftträder snarast för att nyttan ska tillgodogöras.

Information om BK4 och gällande regelverk finns på Trafikverkets hemsida: Regelverk BK4

Trafikverkets bedömning är att särskilda informationsinsatser inte behövs eftersom förändringen av föreskrifterna kommuniceras i och med denna remiss.

Föreskrifterna kungörs i Svensk trafikföreskriftssamling, STFS som finns i den rikstäckande databasen, RDT.

UMEÅ KOMMUN

Tjänsteskrivelse
2026-08-31
Tekniska nämnden

Diarienr: TN-2026/00690

Yttrande Remiss av förslag till ändring i bestämmelserna om texthöjd och bård för varningsskyltar

Förslag till beslut
Tekniska nämnden beslutar

att lämna yttrande enligt nedan.

Ärendebeskrivning
Den 1 september 2023 trädde Transportstyrelsens föreskrifter (TSFS 2023:36 och 2023:37) om färd med bred och lång odelbar last i kraft. Föreskrifterna innehöll bland annat nya bestämmelser för varningsskyltars dimensioner och textstorlek, samt en övergångsbestämmelse som tillät äldre skyltar fram till den 31 juli 2025. Samma bestämmelser för skylt- och textstorlek infördes även i de allmänna råden i TSFS 2024:16 och 2024:17, vilka kunde tillämpas från den 19 april 2024.
När övergångsbestämmelsen upphörde att gälla uppmärksammades en otyd-lighet i hur bestämmelserna om textstorlek ska tolkas. Det kan dels tolkas som att det är den första versalens höjd som ska vara 0,17 meter, dels som att det är typsnittets totala höjd som ska vara 0,17 meter. Avsaknaden av rättspraxis skapar osäkerhet för tillverkare, transportföretag och förare. Det försvårar även polisens och bilinspektörers arbete vid vägkantskontroller, vilket riskerar att leda till en oenhetlig rättstillämpning. Otydligheten med-för dessutom ekonomiska konsekvenser för aktörer som investerat i produkter som nu är svåra att sälja. Det finns därför skäl att se över bestäm-melserna.
Kommunstyrelsen har överlämnat remissen till Tekniska nämnden för yttrande.

Yttrande
Umeå kommun har inget att erinra i ärendet.

Beslutsunderlag
remissmissiv-tsf-2025-113. Bilaga.
konsekvensutredning-tsf-2025-113. Bilaga.
foreskriftsforslag-bred-odelbar-last. Bilaga.

Tjänsteskrivelse

Dnr: TN-2026/00690

foreskriftsforslag-lang-odelbar-last. Bilaga.
forfattningsforslag-allmanna-rad-bredd. Bilaga.
forfattningsforslag-allmanna-rad-langd. Bilaga.

Checklista för handläggning av ärenden inför politiska beslut anses inte tillämpbar.

Beredningsansvariga

Jonas Sörlén, trafikingenjör

Beslutet ska skickas till

Sista dag för att besvara remissen är 9 oktober 2026.
Till TRV, vag@transportstyrelsen.se ange diarienummer TSF 2025-113 i svaret.
Kopia på nämndens protokollsutdrag inkl. yttrande skickas till ksdiarium@umea.se, märk ämnesraden med diarienummer: KS-2026/00835.

Transportstyrelsens författningssamling

TRANSPORT STYRELSEN

TSFS 20[År]:[Nr]

Utkom från trycket
den [Välj ett datum]

Föreskrifter om ändring i Transportstyrelsens föreskrifter och allmänna råd (TSFS 2023:37) om färd med lång odelbar last;

VÄGTRAFIK

beslutade den [Välj ett datum].

Transportstyrelsen föreskriver[1] med stöd av 4 kap. 17 b § trafikförordningen (1998:1276) i fråga om styrelsens föreskrifter och allmänna råd (TSFS 2023:37) om färd med lång odelbar last

dels att 17 och 18 §§ ska ha följande lydelse,

dels att det ska införas en ny bilaga, bilaga 4, av följande lydelse.

17 § Varningsskyltarna ska ha utseende och text enligt figur 1 eller figur 2 och

1. gul botten som är retroreflekterande,
2. en 5,5 centimeter bred röd bård som, i sin helhet, antingen är fluorescerande, retroreflekterande eller både fluorescerande och retroreflekterande,
3. text med teckensnittet Tratexsvart, och
4. text där bokstäverna har den höjd som anges i tabell 1 i bilaga 4.

Trots första stycket 4 får bokstävernas höjd vara större än vad som anges i tabell 1 i bilaga 4. Samtliga bokstäver ska då ökas proportionerligt till varandra i höjd och bredd och texten ska ha samma utseende som framgår av Figur 1 eller 2. Avståndet mellan bokstäverna och bården ska vara minst 2,0 centimeter, med undantag av bokstaven g. Ingen del av bokstaven g får inkräkta på den röda bården.

Figur 1

[1] Se Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

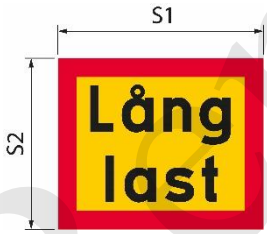
TSFS 20[År]:[Nr]

Figur 2

18 § Varningsskyltarna ska ha följande storlekar.

Skyltar med en rad	Figur 1	S1 ska vara minst 1,2 meter och S2 ska vara minst 0,4 meter. Förhållandet mellan bredd och höjd ska vara 3:1.
Skyltar med två rader	Figur 2	S1 ska vara minst 0,6 meter och S2 ska vara minst 0,5 meter.

Figur 1



Figur 2

Ikraftträdande och övergångsbestämmelser

1. Denna författning träder i kraft den…

2. Varningsskyltar med storlek 50x60 centimeter får användas till och med den 1 mars 2030 även om avståndet mellan bokstäverna och den röda bården är mindre än 2,0 centimeter. Ingen del av bokstäverna får dock inkräkta på bården.

3. Varningsskyltar med bård bredare än 5,5 centimeter får användas till och med den 1 mars 2030.

TSFS 20[År]:[Nr]

På Transportstyrelsens vägnar

JOEL SMITH

Pär Ekström
(Väg och järnväg) vägnar

Utgivare: Kristina Nilsson, Transportstyrelsen, Norrköping ISSN 2000-1975

Bilaga 4

Tabell 1. Höjd för respektive bokstav på varningsskyltar med texten ”Lång last”.

Tecken	Höjd i cm
L	13,6
å	14
n	10
g	13,7
l	13,6
a	10,1
s	10,1
t	13,6

Transportstyrelsens författningssamling

TRANSPORT STYRELSEN

TSFS 20[År]:[Nr]

Utkom från trycket
den [Välj ett datum]

Beslut om ändring i Transportstyrelsens allmänna råd (TSFS 2024:16) om undantag för färd med breda fordon och fordon med bred odelbar last;

VÄGTRAFIK

beslutade den [Välj ett datum].

Transportstyrelsen beslutar[1] i fråga om styrelsens allmänna råd (TSFS 2024:16) om undantag för färd med breda fordon och fordon med bred odelbar last

dels att nuvarande bilaga ska betecknas bilaga 1,

dels att 15, 16, 19, 22, 23, 32 och 33 ska ha följande lydelse

dels att det ska införas en ny bilaga, bilaga 2, av följande lydelse.

15 Fordon eller fordonståg vars bredd överstiger 260 centimeter är försedda med varningslyktor och utmärkta med andra lyktor, breddmarkeringsskyltar, varningsskyltar och reflexer på det sätt som framgår av 16, 19–21 och 24.

Skyltar, lyktor och reflexer är i ett sådant skick att de kan upptäckas och förstås av andra trafikanter. Breddmarkeringsskyltar och varningsskyltar är väl synliga framifrån och bakifrån.

Skyltarna är belysta vid färd under mörker, i skymning eller gryning och i övrigt när det är påkallat av väderleken eller andra omständigheter. Breddmarkeringsskyltar på EG-mobilkran och motorredskap är inte belysta.

I figur 1 i bilaga 1 finns exempel på hur last som i sidled skjuter ut utanför fordonet bör märkas ut för att vara väl synliga framifrån och bakifrån.

16 På fordon vars bredd utan last överstiger 260 centimeter är breddmarkeringsskyltar placerade på fordonets yttre kanter.

På fordon med last som i sidled skjuter ut utanför fordonet är breddmarkeringsskyltarnas yttersta kanter i horisontell riktning inte placerade innanför lastens yttersta kant. I lastens längdriktning är skyltarna placerade före eller på den del av lasten som medför att den tillåtna bredden överskrids.

Skyltarna är normalt placerade högst 2,0 meter över körbanan.

I figur 1 i bilaga 1 finns exempel på lämplig placering av breddmarkeringsskyltarna i horisontell riktning.

[1] Se Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

I figur 2 i bilaga 1 finns exempel på lämplig placering av skyltarna i lastens längdriktning.

19 Plåtar, skivor, byggplattor och andra liknande tunna lastenheter är utöver breddmarkeringsskyltar framtill och baktill försedda med en skylt eller motsvarande på de delar av lasten som medför breddöverskridande. Den har växelvis reflekterande röd och vit färg och en synlig yta på minst 250 centimeter².

Första stycket gäller inte om breddmarkeringsskyltarna placeras intill den utstickande lasten. Vad som avses med intill den utstickande lasten framgår av figur 2 i bilaga 1.

22 Varningsskyltarna har utseende och text enligt figur 1 eller figur 2 och

1. gul botten som är retroreflekterande,
2. en 5,5 centimeter bred röd bård som, i sin helhet, antingen är fluorescerande, retroreflekterande eller både fluorescerande och retroreflekterande,
3. text med teckensnittet Tratexsvart, och
4. text där bokstäverna har den höjd som anges i tabell 1 i bilaga 2.

Istället för första stycket 4 kan bokstävernas höjd vara större än vad som anges i tabell 1 i bilaga 2. Samtliga bokstäver ökas då proportionerligt till varandra i höjd och bredd och texten har samma utseende som framgår av Figur 1 eller 2. Avståndet mellan bokstäverna och bården är minst 2,0 centimeter.

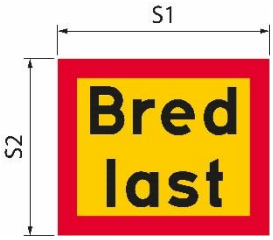
Figur 1

Figur 2

23 Varningsskyltarna har följande storlekar.

Skyltar med en rad	Figur 1	S1 är minst 1,2 meter och S2 är minst 0,4 meter. Förhållandet mellan bredd och höjd är 3:1.
Skyltar med två rader	Figur 2	S1 är minst 0,6 meter och S2 är minst 0,5 meter.

Figur 1



Figur 2

32 Varningsskyltarna har utseende och text enligt figur 1 och

1. gul botten som är retroreflekterande,
2. en 5,5 centimeter bred röd bård som, i sin helhet, antingen är fluorescerande, retroreflekterande eller både fluorescerande och retroreflekterande,
3. text med teckensnittet Tratexsvart, och
4. text där bokstäverna har den höjd som anges i tabell 2 i bilaga 2.

Istället för första stycket 4 kan bokstävernas höjd vara större än vad som anges i tabell 2 i bilaga 2. Samtliga bokstäver ökas då proportionerligt till varandra i höjd och bredd och texten har samma utseende som framgår av Figur 1. Avståndet mellan bokstäverna och bården är minst 2,0 centimeter, med undantag av bokstaven g. Ingen del av bokstaven g får inkräkta på den röda bården.

Figur 1

33 Varningsskyltarna har följande storlek.

S1 är minst 1,2 meter och S2 är minst 0,4 meter (figur 1). Förhållandet mellan bredd och höjd är 3:1.

Figur 1

På Transportstyrelsens vägnar

JOEL SMITH

Pär Ekström
(Väg och järnväg)

Utgivare: Kristina Nilsson, Transportstyrelsen, Norrköping ISSN 2000-1975

Bilaga 2

Tabell 1. Höjd för respektive bokstav på varningsskyltar med texten ”Bred last”.

Tecken	Höjd i cm
B	13,6
r	10
e	10,2
d	13,7
l	13,6
a	10,1
s	10,1
t	13,6

Tabell 2. Höjd för respektive bokstav på varningsskyltar med texten ”Varning”.

Tecken	Höjd i cm
V	13,6
a	10,1
r	10
n	10
i	14
n	10
g	13,7

Transportstyrelsens författningssamling

TRANSPORT STYRELSEN

TSFS 20[År]:[Nr]

Utkom från trycket
den [Välj ett datum]

Beslut om ändring i Transportstyrelsens allmänna råd (TSFS 2024:17) om undantag för färd med långa fordon, fordonståg eller lång odelbar last;

VÄGTRAFIK

beslutade den [Välj ett datum].

Transportstyrelsen beslutar[1] i fråga om styrelsens allmänna råd (TSFS 2024:17) om undantag för färd med långa fordon, fordonståg eller lång odelbar last

dels att nuvarande bilaga ska betecknas bilaga 1,

dels att 8, 25, 26, 30, 39, och 40 ska ha följande lydelse,

dels att det ska införas en ny bilaga, bilaga 2, av följande lydelse.

8 Undantag för transport av last som skjuter ut mer än 5,0 meter bakom centrum på fordonstågets sista axel bör endast medges om fordonståget är längre än 35,0 meter. Vad som avses med 5,0 meter bakom centrum av sista axeln framgår av figur 1 i bilaga 1.

25 Varningsskyltarna har utseende och text enligt figur 1 eller figur 2 och

1. gul botten som är retroreflekterande,
2. en 5,5 centimeter bred röd bård som, i sin helhet, antingen är fluorescerande, retroreflekterande eller både fluorescerande och retroreflekterande,
3. text med teckensnittet Tratexsvart, och
4. text där bokstäverna har den höjd som anges i tabell 1 i bilaga 2.

Istället för första stycket 4 kan bokstävernas höjd vara större än vad som anges i tabell 1 i bilaga 2. Samtliga bokstäver ökas då proportionerligt till varandra i höjd och bredd och texten har samma utseende som framgår av Figur 1 eller 2. Avståndet mellan bokstäverna och bården är minst 2,0 centimeter, med undantag av bokstaven g. Ingen del av bokstaven g får inkräkta på den röda bården.

[1] Se Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

TSFS 20[År]:[Nr]

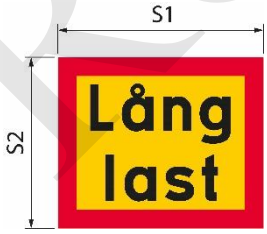
Figur 1

Figur 2

26 Varningsskyltarna har följande storlekar.

Skyltar med en rad	Figur 1	S1 är minst 1,2 meter och S2 är minst 0,4 meter. Förhållandet mellan bredd och höjd är 3:1.
Skyltar med två rader	Figur 2	S1 är minst 0,6 meter och S2 är minst 0,5 meter.

Figur 1



Figur 2

30 Lyktorna och reflexerna är placerade högst 2,0 meter bakom lastens framkant. Avståndet mellan lyktor respektive reflexer på samma sida är högst 6,0 meter. De bakersta lyktorna och reflexerna är placerade längst bak på lasten om den skjuter ut bakom fordonet (figur 2 i bilaga 1).

39 Varningsskyltarna har utseende och text enligt figur 1 och

1. gul botten som är retroreflekterande,

2. en 5,5 centimeter bred röd bård som, i sin helhet, antingen är fluorescerande, retroreflekterande eller både fluorescerande och retroreflekterande,

3. text med teckensnittet Tratexsvart, och

4. text där bokstäverna har den höjd som anges i tabell 2 i bilaga 2.

Istället för första stycket 4 kan bokstävernas höjd vara större än vad som anges i tabell 2 i bilaga 2. Samtliga bokstäver ökas då proportionerligt till varandra i höjd och bredd och texten har samma utseende som framgår av Figur 1. Avståndet mellan bokstäverna och bården är minst 2,0 centimeter, med undantag av bokstaven g. Ingen del av bokstaven g får inkräkta på den röda bården.

Figur 1

40 Varningsskyltarna har följande storlek.

S1 är minst 1,2 meter och S2 är minst 0,4 meter (figur 1). Förhållandet mellan bredd och höjd är 3:1.

Figur 1

På Transportstyrelsens vägnar

JOEL SMITH

Pär Ekström
(Väg och järnväg)

Utgivare: Kristina Nilsson, Transportstyrelsen, Norrköping ISSN 2000-1975

Bilaga 2

Tabell 1. Höjd för respektive bokstav på varningsskyltar med texten ”Lång last”.

Tecken	Höjd i cm
L	13,6
å	14
n	10
g	13,7
l	13,6
a	10,1
s	10,1
t	13,6

Tabell 2. Höjd för respektive bokstav på varningsskyltar med texten ”Varning”.

Tecken	Höjd i cm
V	13,6
a	10,1
r	10
n	10
i	14
n	10
g	13,7

TRANSPORT STYRELSEN

Missiv

Datum
2026-08-20

Dnr/Beteckning
TSF2025-113

Enligt sändlista

Remiss

Förslag till ändring av bestämmelser om texthöjd och bård för varningsskyltar

De ändringar som föreslås gäller;

- Transportstyrelsens föreskrifter och allmänna råd (TSFS 2023:36) om färd med bred odelbar last,
- Transportstyrelsens föreskrifter och allmänna råd (TSFS 2023:37) om färd med lång odelbar last,
- Transportstyrelsens allmänna råd (TSFS 2024:16) om färd med breda fordon och fordon med bred odelbar last, samt
- Transportstyrelsens allmänna råd (TSFS 2024:17) om färd med långa fordon, fordonståg eller lång odelbar last.

Välkommen att ta del av Transportstyrelsens förslag.

Bakgrund till förslaget

Den 1 september 2023 trädde Transportstyrelsens föreskrifter (TSFS 2023:36 och 2023:37) om färd med bred och lång odelbar last i kraft. Föreskrifterna innehöll bland annat nya bestämmelser för varningsskyltars dimensioner och textstorlek, samt en övergångsbestämmelse som tillät äldre skyltar fram till den 31 juli 2025. Samma bestämmelser för skylt- och textstorlek infördes även i de allmänna råden i TSFS 2024:16 och 2024:17, vilka kunde tillämpas från den 19 april 2024.

När övergångsbestämmelsen upphörde att gälla uppmärksammades en otydlighet i hur bestämmelserna om textstorlek ska tolkas. Det kan dels tolkas som att det är den första versalens höjd som ska vara 0,17 meter, dels som att det är typsnittets totala höjd som ska vara 0,17 meter. Avsaknaden av rättspraxis skapar osäkerhet för tillverkare, transportföretag och förare. Det försvårar även polisens och bilinspektörers arbete vid vägkantskontroller, vilket riskerar att leda till en oenhetlig rättstillämpning. Otydligheten medför dessutom ekonomiska konsekvenser för aktörer som investerat i

Transportstyrelsen
Väg och järnväg
Box 267, 781 23 Borlänge
Besöksadress
Jussi Björlings väg 19, Borlänge

Telefon 0771-503 503
Telefax 0243-152 74

transportstyrelsen.se
vag@transportstyrelsen.se

Pär Ekström
Trafikant
Trafikantregler
par.ekstrom@transportstyrelsen.se
010-495 55 13

produkter som nu är svåra att sälja. Det finns därför skäl att se över bestämmelserna.

Förslagets innehåll i korthet

Detta föreskriftsarbete är avgränsat till att endast omfatta bestämmelser på varningsskyltar som gäller höjd på bokstäver samt den röda bårdens egenskaper och bredd. Utöver detta görs vissa mindre redaktionella ändringar.

Förslaget innebär i huvudsak följande:

- **Minsta höjd och möjlighet till större bokstäver**: Det införs en reglerad minsta höjd på bokstäver. Det blir tillåtet att göra bokstäverna proportionellt större så länge avståndet mellan bokstäverna och den röda bården är minst 2,0 centimeter.
- **Bårdegenskaper**: Det blir möjligt att använda material med fler och andra egenskaper på den röda bården än enbart fluorescerande.
- **Fast bårdbredd**: Den röda bården på varningsskyltar ska alltid vara 5,5 centimeter bred oavsett om skylten har den reglerade minimistorleken eller om den gjorts större.
- **Nya bilagor med bokstävernas höjd**: Det läggs till nya bilagor i respektive författning där minsta höjden för varje bokstav framgår.
- **Övergångsbestämmelser**: För att mildra de ekonomiska konsekvenserna för berörda aktörer föreslås det i föreskrifterna övergångsbestämmelser för vissa skyltar. Bestämmelsen gäller tre efter att föreskrifterna trätt i kraft.

Förslagen förväntas ge tillverkare, transportföretag och tillsynsmyndigheter goda förutsättningar att avgöra om en varningsskylt uppfyller gällande krav.

Föreskriftsförslagen planeras träda i kraft den 2027-03-01.

Förslaget i sin helhet samt konsekvensutredning finns publicerat tillsammans med detta missiv på Transportstyrelsens webbplats:

https://www.transportstyrelsen.se/sv/om-oss/dina-rattigheter-lagar-och-regler/lagar-och-regler/remisser/

Synpunkter

Ni ges härmed tillfälle att lämna synpunkter på förslaget och konsekvensutredningen. Synpunkterna ska vara Transportstyrelsen tillhanda senast den 2026-10-09. Vänligen ange vårt diarienummer TSF 2025–113 i svaret.

Synpunkterna ska vara skriftliga och skickas till:

vag@transportstyrelsen.se

eller till

Transportstyrelsen
Box 267
781 23 Borlänge

Transportstyrelsen kommer att sammanställa och kommentera de remissynpunkter som kommer in, och därefter publicera sammanställningen och kommentarerna på hemsidan. Remissynpunkter som innehåller sekretessbelagda uppgifter eller personuppgifter kommer dock inte att publiceras.

Kontaktpersoner

Om ni har frågor med anledning av remissen är ni välkomna att kontakta:

Pär Ekström, utredare,
E-post: par.ekstrom@transportstyrelsen.se

Kristofer Elo, utredare,
E-post: kristofer.elo@transportstyrelsen.se

Med vänlig hälsning

Pär Ekström och Kristofer Elo
Utredare

Sändlista

Abkati
AC Märkesprodukter AB
ALFAB
Alf Pettersson AB
Blinkfyrar
Försvarsmakten
Gotlands kommun
Göteborgs Stad
Haparanda kommun
Huzells tunga delar
Kalmar kommun
Karlstads kommun
Lastfordonsgruppen
Luleå kommun
Malmö Stad
Maskinentreprenörerna
Mobilkranföreningen
Momenthia AB
Mora kommun
PG Tech
Polismyndigheten
Reklam//Skyltservice
SKR
Skyltstället
Sternhammar
Stockholms Stad
Sundsvalls kommun
Svenska Fordonsbranschen
Sveriges åkeriföretag
Swedol
Trafikverket
Transportarbetareförbundet
Transportföretagen
Umeå kommun
VTI – Statens väg- och transport-forskningsinstitut
Wärnevalls Transport AB
Åklagarmyndigheten
Örnsköldsviks kommun
Östersunds kommun
3M

TRANSPORT STYRELSEN

Konsekvensutredning

Datum
2026-08-20

Dnr/Beteckning
TSF 2025-113

Handläggare
Pär Ekström
Väg och järnväg
Trafikant
Trafikantregler

Konsekvensutredning av ändrade bestämmelser om texthöjd och bård för varningsskyltar

Transportstyrelsens förslag:

Att föreskrifter och allmänna råd om bokstävernas höjd på varningsskyltar ska förtydligas i föreskrifterna TSFS 2023:36, 2023:37 och de allmänna råden TSFS 2024:16 och 2024:17. Förslaget innebär att det införs en minsta höjd på bokstäverna, med utgångspunkt att höjden på den första versalens ska vara 13,6 centimeter, samt en undantagsbestämmelse om att bokstäverna får göras större. Dock inte större än att avståndet mellan bokstäverna och den röda bården är mindre än 2,0 centimeter.

Att föreskrifter och allmänna råd om den röda bården på varningsskyltar i ovan nämnda författningar inte begränsas till att vara enbart fluorescerande, utan att den även kan vara retroreflekterande eller både fluorescerande och retroreflekterande. Vidare begränsas bårdens bredd till att alltid vara 5,5 centimeter bred även när en varningsskylt görs större än de föreskrivna minimimåtten.

Att det i föreskrifterna införs två övergångsbestämmelser. Den första gäller för varningsskyltar med måtten 50x60 centimeter och text i två rader. Sådana skyltar får användas ytterligare tre år efter att föreskrifterna trätt i kraft även om avståndet mellan bokstäver och den röda bården som understiger 2,0 centimeter. Den andra övergångsregeln gäller för varningsskyltar vars storlek är större än dagens föreskrivna minimimått, och där bården, på grund av den större storleken – enligt nu gällande bestämmelser – gjorts bredare än 5,5 centimeter. Skyltar med sådan större bårdbredd får användas ytterligare tre år efter att föreskrifterna trätt i kraft.

Vidare föreslår vi nya bilagor till ovan nämnda författningar där minimihöjden för respektive bokstäver anges.

I övrigt föreslås några mindre redaktionella justeringar som inte ändrar något i sak, till exempel att begreppet ”skyltar” i vissa bestämmelser ändras till ”varningsskyltar”.

A. Allmänt

1. Bakgrund

Mellan åren 2018 och 2023 arbetade Transportstyrelsen med att ta fram två nya föreskrifter om färd med bred respektive lång odelbar last. De nya föreskrifterna trädde i kraft den 1 september 2023. En av de ändringar som beslutades var att fastställa storlekarna på varningsskyltar då denna tidigare endast var *rekommenderad*. Med varningsskyltar avses dessa skyltar.

Enligt de äldre, nu upphävda, föreskrifterna skulle texten på varnings-skyltarna vara utförd i svart med typsnittet Tratex och ha en teckenhöjd om 170/124 millimeter (versaler/gemener). I de nya, nu gällande föreskrifterna framgår att texten ska vara i teckensnittet Tratexsvart med textstorlek 0,17 meter.

I de nya föreskrifterna fanns även en övergångsbestämmelse som gjorde det möjligt att använda varningsskyltar enligt äldre bestämmelser till och med den 31 juli 2025.

Parallellt med ovan nämnda föreskriftsarbete arbetade myndigheten även med att ta fram två nya allmänna råd om; ”undantag för färd med breda fordon och fordon som transporterar bred odelbar last” samt ”undantag för färd med långa fordon och fordon som transporterar lång odelbar last”. Dessa allmänna råd riktar sig till de statliga väghållarna (Trafikverkets regioner) och de kommunala väghållarna när de prövar ansökningar om undantag för fordon, som vid färd på väg som inte är enskild är bredare eller längre än vad som enligt trafikförordningen (1998:1276) är tillåtet.

Även de nya allmänna råden ändrades i flera delar. För att harmonisera med de nya föreskrifterna togs bland annat begreppet ”*rekommenderad”* bort när det gäller storleken på varningsskyltar samt att lydelsen för textstorlek harmoniserades med lydelserna i de nya föreskrifterna.

De allmänna råden beslutades den 5 april 2024 och utkom från trycket den 19 april samma år. Eftersom allmänna råd inte har något ikraftträdande datum kunde de tillämpas från den 19 april.

Kraven att bården ska vara röd och fluorescerande är samma i både de nya och äldre föreskrifterna och allmänna råden.

1.1 Avgränsning

Detta föreskriftsarbete är avgränsat till att endast omfatta bestämmelser om höjd på bokstäver samt den röda bårdens egenskaper och bredd på varningsskyltar i TSFS 2023:36, 2023:37, TSFS 2024:16 och 2024:17.

Arbetet omfattar inte ändrade storlekar på skyltarna eller ändringar som möjliggör användning av skyltar från andra nordiska länder. Det omfattar inte heller ändringar av skyltar i Transportstyrelsens föreskrifter och allmänna råd (TSFS 2010:139) om vägtransportledare. Utöver ändringar som rör höjd på bokstäver och den röda bården har även vissa mindre redaktionella ändringar gjorts.

2. Undersökning upplevelse av texthöjd

För att bedöma lämpliga texthöjder på varningsskyltar genomfördes en enkel undersökning. Syftet var att ta reda på vid vilket avstånd som text med olika höjd kan ses och förstås. Storleken på de skyltar som användes vid försöket hade, med undantag för en av de tvåradiga skyltarna som var 60x70 centimeter, de föreskrivna minimistorlekarna, det vill säga 120x40 centimeter för skyltar med text i en rad och 50x60 centimeter för skylt med text i två rader. Höjden på textens första versal var antingen 13,6 eller 17,0 centimeter.

Eftersom dessa varningsskyltar – till skillnad från vägmärken som är fast monterade i infrastrukturen – är placerade på fordon som normalt kan färdas i 80 kilometer i timmen, gjordes bedömningen att en mötande trafikant behöver kunna upptäcka, läsa och förstå skyltens budskap på ett avstånd av minst 100 meter. Vid ett möte med andra fordon som också färdas i 80 kilometer i timmen minskar avståndet mellan dem med cirka 44 meter per sekund.[1] Ett läsavstånd på 100 meter innebär därmed att trafikanterna har drygt 2,2 sekunder på sig från det att skylten blir läsbar till dess att fordonen möts.

Inför undersökningen bedömdes denna tidsmarginal vara ett absolut minimum. Marginalen ska inte bara täcka den rent kognitiva processen att uppfatta och förstå budskapet, utan även ge föraren tillräcklig tid att reagera och hinna anpassa sin körning – till exempel genom att sänka hastigheten eller placera fordonet säkert på vägbanan – inför mötet med den breda eller långa transporten.

Hur undersökningen genomfördes och resultatet av studien finns beskrivet i rapporten ”Studie om läsbarhet beroende av texthöjd på varningsskyltar”,

[1] Avståndsminskningen beräknas genom den relativa hastigheten (80 km/h + 80 km/h = 160 km/h). För att omvandla kilometer i timmen till meter per sekund divideras summan med 3,6 (160/3,6 ≈ 44,4 m/s).

vilken är diarieförd hos Transportstyrelsen i ärende TSF 2025-113 med handlingsnummer 5.

2.1 Resultat

Resultatet av undersökningen visar att en höjd på den första versalen på 13,6 centimeter är tillräcklig för att uppnå god synbarhet på avstånd upp till 100 meter. Även om undersökningen indikerar en viss positiv tendens för ökad synbarhet vid 17,0 centimeter, är skillnaden inte statistiskt säkerställd. Resultatet innebär därmed att den lägre höjden uppfyller kraven för läsbarhet, men att det saknas skäl att begränsa höjden uppåt.

2.2 Slutsatser

Utifrån undersökningens resultat drar vi slutsatsen att en versalhöjd på 13,6 centimeter är en tillräcklig minimihöjd för att säkerställa god syn- och läsbarhet på avstånd upp till 100 meter. Då den observerade förbättringen vid 17,0 centimeter inte är statistiskt säkerställd, bedöms 13,6 centimeter uppfylla funktionskraven. Det saknas därmed skäl för en övre begränsning av versalhöjden med avseende på läsbarheten.

3. Vad är problemet eller anledningen till regleringen?

3.1 Olika tolkning av begreppet textstorlek

I samband med att övergångsbestämmelserna i föreskrifterna TSFS 2023:36 och 2023:37 upphörde att gälla den 31 juli 2025, uppmärksammades myndigheten på tolkningsproblem gällande bestämmelsen om textstorlek. Det visade sig att bestämmelserna kan tolkas på olika sätt, vilket har skapat en osäkerhet i branschen.

Dagens lydelse tolkas dels som att det är versalernas höjd som ska vara 17 centimeter, dels som att det är typsnittets totala höjd som ska vara 17 centimeter. Om typsnittets höjd är 17 centimeter blir versalernas höjd cirka 13,6 centimeter och gemenernas höjd cirka 10 centimeter.

Denna otydlighet skapar problem för både skylttillverkare och transportföretag då det råder tveksamhet kring om de varningsskyltar som företag tillverkat faktiskt uppfyller föreskrifternas villkor eller villkoren i en medgiven dispens. Detta i sin tur leder till att transportföretagen är osäkra på vilka skyltar som ska införskaffas, och slutligen att de förare som utför transporter av odelbara laster har svårt att avgöra om de skyltar som används vid en transport uppfyller gällande krav.

För att poliser och bilinspektörer vid vägkantskontroller ska kunna kontrollera att bestämmelserna efterlevs är det avgörande att dessa är tydliga. De tolkningsproblem som tillverkare, transportföretag och förare upplever med nuvarande lydelse rörande textstorlek bedöms även försvåra

kontrollverksamheten, då det är svårt att bedöma om en textstorlek på en varningsskylt uppfyller gällande krav. Detta kan i sin tur skapa både en rättsosäkerhet och en oenhetlig rättstillämpning.

För de som utför transporter av odelbar last är det, oaktat om färden sker med stöd av föreskrifterna eller en medgiven dispens från väghållare, en förutsättning för transporten att samtliga villkor är uppfyllda. I annat fall är det trafikförordningens (1998:1276) bestämmelser om största tillåtna bredd eller längd som gäller. Den som överskrider dessa bestämmelser kan enligt 14 kap. 3 § trafikförordningen dömas till penningböter. Storleken på böterna anges i bilaga 1, tabell 3.19 och 3.21 i Riksåklagarens föreskrifter (1999:178) om ordningsbot för vissa brott. Om en bred eller lång transport även omfattar ett viktundantag, och villkoren i dispensen inte är uppfyllda, riskerar även ägaren av fordonet att åläggas en överlastavgift enligt lagen om överlastavgift (1972:435).

Det är olyckligt att förare riskerar böter och företag påförs överlastavgifter på grund av otydliga bestämmelser, särskilt om de haft för avsikt att följa dessa. Därför är det viktigt att föreskrifter och allmänna råd är tydliga så att de som tillämpar dem får tillräckliga förutsättningar att göra rätt.

Otydligheten kring textstorleken har även lett till att vissa tillverkare, importörer och försäljningsställen av varningsskyltar har investerat medel i produkter som de nu inte får sålda, vilket leder till negativa ekonomiska konsekvenser för dessa.

Hösten 2025 publicerade Transportstyrelsen information på sin webbplats för att förtydliga vad som avses med en textstorlek på 0,17 meter. Denna information uppnådde dock inte det avsedda syftet, utan ledde i stället till fler tolkningsfrågor och en ökad otydlighet bland aktörerna. Det finns heller ingen rättspraxis på området som kan ge juridisk vägledning i hur gällande bestämmelser ska tolkas.

Mot bakgrund av detta finns det skäl att se över de bestämmelser som reglerar textstorleken på varningsskyltar.

3.2 Svårt att övervaka textstorlek

Som nämnts i avsnitt 3.1 är det otydligt hur bestämmelser om textstorleken på varningsskyltar ska tolkas. Tillämpas tolkningen att det handlar om typsnittets höjd på 17 centimeter finns det utmaningar med att mäta på en framtagen fordonskylt om texten har rätt storlek, utan att översätta detta till höjden av versaler till 13,6 centimeter. Detta försvårar kontroll både av den som ska kontrollera om en bred eller lång transport uppfyller villkoren för att få utföra transporten och även för de som utför en sådan transport.

Med dagens bestämmelser går det inte utan ett ritningsprogram, eller särskilda kunskaper att avgöra om man uppfyller kraven eller inte. Detta försvårar även kontrollen för Polisen som ska övervaka bestämmelserna.

Mot bakgrund av dessa svårigheter behöver föreskrifterna och de allmänna råden ses över för att det ska bli tydligt om vad som gäller.

3.3 Brist på utrymme

Tillämpas tolkningen att versalers höjd ska vara 17 centimeter uppstår problem för varningsskyltar med text på två rader med ytterdimensionerna 50x60 centimeter. Texten får då inte plats på den gula bakgrundsytan och behöver gå över den röda bården. Detta minskar konstrasten mellan den svarta texten, den gula bakgrunden och den röda bården.

Den minskade kontrasten leder till försämrad synbarhet och läsbarhet av texten, vilket i sin tur påverkar hur snabbt andra trafikanter kan uppfatta, tolka och förstå budskapet på varningsskyltarna.

Mot bakgrund av detta behöver föreskrifterna och de allmänna råden ses över.

3.4 Fluorescerande röd bård

Enligt både äldre och nu gällande föreskrifter och allmänna råd är det krav på att den röda bården på varningsskyltarna ska vara av ett fluorescerande material, vilket är ett krav som funnits åtminstone sedan 1991.[2]

Bestämmelser om utformning av röd bård finns bland annat på fordonsskyltar som används för att märka ut fordonståg som är längre än 25,25 meter. Den röda bården ska på dessa skyltar vara retroreflekterande.[3] Det finns därför skäl att harmonisera bestämmelser som rör egenskaper på den röda bården på varningsskyltar som används vid transporter av odelbara laster med skyltar som används på fordonståg som är längre än 25,25 meter.

Från tillverkare har det även framförts synpunkter på kraven för varningsskyltarnas utformning. Man menar att tillverkningsprocessen försvåras med krav både på fluorescerande egenskaper (den röda bården) och retroreflekterande egenskaper (den gula bakgrunden).

Mot bakgrund av detta ser vi skäl att se över vilka egenskaper den röda bården ska ha.

[2] Se Bilaga 1 Vägverkets författningssamling VVFS 1991:5
[3] Se 11 § Transportstyrelsens föreskrifter och allmänna råd (TSFS 2025:17) om tekniska krav på fordonståg med längd över 25,25 meter

3.5 Bårdbredd

Enligt nu gällande bestämmelser ska den röda bården vara 5,5 centimeter bred. Om en varningsskylt görs större än de föreskrivna minimimåtten, ska bårdens bredd ökas proportionellt i motsvarande grad. Syftet med den röda bården är att skapa en tydlig avgränsning och hög kontrast mot skyltens gula bakgrund.

Den tvåradiga varningsskylten ska enligt nu gällande bestämmelser vara *minst* 50x60 centimeter. Den tillåts dock göras större. Till skillnad från skyltar med text i en rad finns det för skyltar med text i två rader inga krav på ett visst bredd- och höjdförhållande. Dessa skyltar kan därför till exempel göras med måtten 60x70 centimeter. Om den breddgående och den höjdgående bården på en skylt med sådana mått ändras proportionerligt i förhållande till en skylt som har måtten 50x60 centimeter kommer den breddgående och den höjdgående bården få olika bredd, vilket inte är önskvärt.

Mot bakgrund av detta ser vi skäl att se över bestämmelserna som säger att bårdens bredd ska öka om storleken på en varningsskylt görs större.

4. Vad ska uppnås?

Det som ska uppnås är att bestämmelserna ska vara praktiskt användbara, juridiskt tydliga och lätta att tillämpa för samtliga berörda aktörer. Hur detta ska uppnås för respektive förslag framgår under regleringsalternativen.

4.1 Textstorlek

Syftet med ändrade bestämmelser om textstorlek på varningsskyltar är att undanröja nuvarande osäkerhet om hur dagens bestämmelser ska tolkas. Genom att införa tydliga och mätbara krav ska en ökad rättssäkerhet och förutsägbarhet uppnås och därigenom bidra till att bestämmelserna blir tydligare och lättare att förstå för de som ska tillämpa och övervaka dessa. Detta förväntas därmed leda till en god regelefterlevnad, vilket förväntas bidra till hög trafiksäkerhet och god synbarhet för varningsskyltarna. Vidare ska ändringen säkerställa en effektiv tillsyn och kontroll genom att ge Polismyndigheten och bilinspektörer vid vägkantskontroller ett objektivt och enkelt mått att förhålla sig till. Detta säkerställer en enhetlig rättstillämpning oavsett vem som gör kontrollen.

4.2 Bårdegenskaper

Förslaget ska möjliggöra teknikutveckling och användning av modernare och mera hållbara material, vilket bidrar till att garantera en tillräcklig synbarhet och bibehållen hög trafiksäkerhet vid fordonsmöten.

4.3 Bårdbredd

Syftet med ändringen att säkerställa en enhetlig visuell identitet på varningsskyltar och samtidigt eliminera behovet av komplexa proportionalitetsberäkningar vid förstoring av vissa skyltar med text i två rader. Detta ska leda till bättre förutsättningar för en mer kostnadseffektiv och standardiserad tillverkningsprocess utan att det påverkar trafiksäkerheten negativt.

5. Vilka är lösningsalternativen?

5.1 Effekter om ingenting görs?

Dagens krav på textstorlek

Om vi inte ändrar bestämmelserna om textstorlek kommer föreskrifterna och de allmänna råden att tolkas på olika sätt vilket innebär en fortsatt osäkerhet om vad som gäller. Det leder även till en bristande rättssäkerhet om vad som gäller då bestämmelserna är svåra att övervaka.

Dagens krav på bårdegenskaper

Om vi inte ändrar dagens krav om att den röda bården ska vara fluorescerande kommer möjligheten att använda andra material inte vara tillåtet. Harmoniseringen mot andra fordonsskyltar som ska ha en bård som är retroreflekterande kommer inte att ske. Vi möjliggör inte heller för tillverkarna att använda andra material med andra egenskaper än fluorescerande.

Dagens krav på bårdbredd

Om vi inte tar bort kravet på att den röda bårdens bredd (5,5 centimeter) ska ökas proportionerligt när skyltar med text i två rader görs större kommer bredden på den breddgående och den höjdgående bården för vissa skyltar med text i två rader att vara olika bred, vilket inte är önskvärt.

5.2 Alternativ som inte innebär reglering

Eftersom de problem som beskrivs ovan har sitt ursprung i bestämmelsernas nuvarande utformning, ser vi inget annat alternativ än att ändra föreskrifterna och de allmänna råden i de delar som nämnts. Inga andra åtgärder bedöms kunna lösa de identifierade bristerna utan att de föreslagna regeländringarna genomförs.

Textstorlek

För att minska tolkningsutrymmet vad gäller textstorlek på varningsskyltar finns inga alternativ som inte innebär någon form av reglering.

Bårdegenskaper

Om inga åtgärder vidtas kommer det nuvarande kravet på att den röda bården på varningsskyltar måste vara fluorescerande att ligga kvar oförändrat. Det innebär att det även fortsättningsvis inte är möjligt att

använda andra material och tekniska egenskaper på bården, även om dessa skulle uppfylla tillräckliga krav och vara ändamålsenliga.

Bårdbredd
Om inga föreskriftsändringar sker kommer varningsskyltar med text i två rader (exempelvis i formatet 60x70 centimeter) även fortsättningsvis att resultera i olika bredd på den horisontella och vertikala bården. Det innebär att skyltarnas visuella utformning förblir oenhetlig, vilket strider mot den princip om enhetlighet som finns för vägmärken i vägmärkesförordningen (2007:90). Det finns inga alternativ som löser denna problematik utan en ändring i bestämmelserna.

5.3 Regleringsförslag

Under detta avsnitt beskriver vi vårt regleringsförslag.

Minsta höjd på bokstäver
Förslaget innebär att varje bokstav i texten ska ha en fastställd minimihöjd. Vilken höjd som gäller framgår av en ny bilaga. Vi ändrar därmed författningstexten så att vi inte längre använder begreppet ”textstorlek”, utan istället reglerar höjden på respektive bokstav. Enligt bilagan ska höjden på den första versalen vara 13,6 centimeter. De höga gemenerna har ungefär samma höjd som den första versalen, medan de låga gemenerna uppgår till cirka 10 centimeter.

Vi föreslår även en undantagsbestämmelse som medger att bokstäverna kan göras större än de fastställda måtten i bilagan. För att bokstäverna inte ska komma för nära den röda bården – som då skulle försämra synbarheten – får den inte göras större än att ett avstånd på minst 2,0 centimeter bibehålls mellan bokstav och bård. Detta krav gäller dock inte för den nedre ”kroken” på bokstaven ”g” för varningsskyltar med text ”Lång last” och ”Varning”. Ingen del av den bokstaven får oavsett inkräkta på bården.

Oavsett om nuvarande bestämmelser tolkas som att höjden på den första versalen ska vara antingen 13,6 eller 17,0 centimeter, innebär förslaget att befintliga skyltar får fortsätta användas. Det enda undantaget är varningsskyltar med formatet 50x60 centimeter med text i två rader, där bokstäverna hamnar för nära den röda bården om tolkningen på 17 centimeters versalhöjd tillämpas. För att de som investerat i sådana skyltar inte ska förbjudas att använda dessa med detsamma föreslås en övergångsbestämmelse. Läs mer under rubriken ”Övergångsbestämmelser” nedan.

Bårdegenskaper
Regleringsförslaget innebär att bården får vara både fluorescerande och retroreflekterande, eller en kombination av båda egenskaperna. Bården ska i

sin helhet ha ett enhetligt utförande, vilket innebär att dess egenskaper ska vara identiska på bårdens samtliga sidor.

Bårdbredd
Regleringsförslaget innebär att den röda bården på varningsskyltar alltid ska vara 5,5 centimeter bred, oavsett om skylten har den reglerade minimistorleken eller är större. Därmed slopas det nuvarande kravet på att både bårdens bredd och textens storlek måste öka när en skylt görs större. För att de som har investerat i befintliga skyltar ska få fortsätta använda dem föreslås en övergångsbestämmelse (läs mer under rubriken ”Övergångsbestämmelser” nedan).

Övergångsbestämmelser
För att möjliggöra fortsatt användning av skyltar i storleken 50x60 centimeter med text i två rader, där första versalen är 17 centimeter och tecknen sitter närmare den röda bården än 2,0 centimeter, föreslås det i föreskrifterna en övergångsbestämmelse som medger att sådana skyltar får användas ytterligare tre år efter att föreskrifterna trätt i kraft. Denna övergångsbestämmelse omfattar dock inte varningsskyltar där en bokstav, eller en del av en bokstav, inkräktar på den röda bården.

I föreskrifterna föreslås även en övergångsbestämmelse för de varningsskyltar som i dag används. Det gäller skyltar som överstiger de föreskrivna minimimåtten och som därför – enligt nuvarande krav – har en bårdbredd som är större än 5,5 centimeter. Det innebär att även dessa skyltar får användas ytterligare tre år efter att föreskrifterna trätt i kraft.

5.4 Regleringsalternativ

Under detta avsnitt förklarar vi vilka regleringsalternativ som har övervägts och vad de innebär.

13,6 centimeters höjd på bokstäver
Alternativet innebär att höjden på den första versalen ska vara 13,6 centimeter och att samtliga bokstäver ska utformas enligt en bilaga där höjden för varje enskild bokstav specificeras. Detta alternativ liknar det liggande förslaget, men med skillnaden att det saknar undantag som tillåter större bokstäver.

Myndighetens läsbarhetsundersökning visar att en versalhöjd på 13,6 centimeter ger tillräcklig synbarhet, men att en versalhöjd på 17,0 centimeter ger något bättre synbarhet. Detta alternativ skulle innebära att skyltar där den första versalen är 17,0 centimeter blir förbjudna att använda, vilket i sin tur skulle kräva en övergångsbestämmelse.

Vi väljer att inte gå vidare med detta alternativ eftersom avsaknaden av ett undantag skulle förbjuda befintliga skyltar med en versalhöjd på 17,0

centimeter. Det är inte heller motiverat att förbjuda dessa skyltar då de har en bevisat bättre synbarhet.

17,0 centimeters höjd på bokstäverna

Alternativet innebär att höjden på den första versalen ska vara 17,0 centimeter och att samtliga bokstäver ska utformas enligt en bilaga där höjden för varje enskild bokstav specificeras. Detta alternativ skulle innebära att de skyltar som tillverkats enligt tolkningen att den första versalen ska vara 13,6 centimeter blir förbjudna att använda. Även med detta alternativ skulle det därför krävas en övergångsbestämmelse.

Vår läsbarhetsundersökning visar att en versalhöjd på 13,6 centimeter ger en tillräcklig synbarhet. Eftersom denna höjd uppfyller kraven på hög trafiksäkerhet ser vi inga skäl att förbjuda dessa skyltar.

För tvåradiga skyltar med måtten 50x60 centimeter innebär kravet på en fast versalhöjd på 17,0 centimeter att alternativet inte är genomförbart i praktiken. Texten får helt enkelt inte plats utan att inkräkta på den röda bården, såvida man inte samtidigt minskar avståndet mellan bokstäverna. Att justera teckenavståndet innebär dock att man frångår typsnittets originalutförande, vilket direkt motverkar syftet med en enhetlig reglering.

Att tvinga fram ett utbyte till en fast storlek på 17,0 centimeter är därför inte motiverat, och vi väljer att inte gå vidare med detta alternativ.

Retroreflekterande bård

Detta alternativ innebär att nuvarande krav på fluorescerande röd bård tas bort och ersätts med ett tvingande krav på retroreflekterande bård. En sådan förändring innebär att branschens befintliga skyltar måste bytas ut. För att mildra de ekonomiska konsekvenserna skulle en övergångsbestämmelse krävas. Det har inte heller visats att nuvarande bestämmelse med fluorescerande bård medför några problem i praktiken.

Alternativet bedöms medföra stora administrativa och ekonomiska bördor för branschen. Eftersom det saknas ett påvisat problem är alternativet inte proportionerligt, och vi väljer att inte gå vidare med detta alternativ.

5.5 Andra ändringar som undersökts

Under arbetet har nedanstående regleringsalternativ undersökts men inte bedömts vara motiverade att gå vidare med.

Byte av typsnitt

Ett alternativ som övervägts är att ersätta typsnittet Tratexsvart med ett annat typsnitt, exempelvis ett typsnitt där versaler och gemener har en enhetlig höjd. Syftet skulle vara att förenkla föreskrifterna genom att endast behöva ange en enhetlig höjdangivelse för samtliga bokstäver.

Vi har valt att inte gå vidare med detta alternativ av flera skäl. För det första förvaltas Tratexsvart av staten (Transportstyrelsen och Trafikverket), vilket garanterar att typsnittet förblir stabilt över tid. Om ett externt, kommersiellt, typsnitt skulle användas riskerar myndigheterna att förlora kontrollen över tecknens utformning, exempelvis om ägaren ändrar typsnittets design eller licensvillkor.

För det andra ska det enligt svensk rättspraxis inte medföra immaterialrättsliga kostnader[4] för enskilda eller företag att efterleva tvingande bestämmelser. Att kräva ett skyddat typsnitt skulle tvinga skylttillverkare att köpa licenser, vilket strider mot principen om att regelverk ska kunna tillämpas utan kostnad för medborgaren.

Slutligen är Tratexsvart specifikt framtaget för god läsbarhet i trafikmiljö. Att införa ett nytt typsnitt på varningsskyltar skulle bryta den visuella enhetligheten på svenska vägar, vilket riskerar att försämra igenkänningen. Eftersom ett krav på licensbelagda typsnitt vid efterlevnad av tvingande regler inte bedöms vara förenligt med svensk rättspraxis, är alternativet varken rättssäkert eller motiverat att gå vidare med.

Sammanfattningsvis bedöms ett byte av typsnitt medföra oskäliga kostnader för branschen och skapa en osäkerhet i regleringen. Dessutom saknas vetenskapligt stöd för att ett annat typsnitt skulle ge bättre läsbarhet i trafiken än det beprövade Tratexsvart. Med hänsyn till de negativa konsekvenserna för både rätts- och trafiksäkerheten väljer vi att inte gå vidare med detta alternativ.

Endast versaler

Ett alternativ som övervägts är att text på varningsskyltar ska skrivas med enbart versaler. Vi har dock valt att inte gå vidare med detta alternativ av följande skäl.

Trafik- och läsforskning visar att ord skrivna med gemener eller blandad versal/gemen ofta känns igen snabbare än ord skrivna enbart med versaler.[5] Detta beror på att gemener skapar mer karakteristiska ordformer genom bokstäver med varierande höjd, exempelvis ”d”, ”l” och ”t”. Ord skrivna med enbart versaler får en mer enhetlig form, vilket gör dem svårare att särskilja på längre avstånd.[6] I en trafikmiljö, där föraren har begränsad tid att uppfatta ett budskap, är snabb igenkänning av information avgörande.

När en trafikant befinner sig i en komplex trafiksituation är den kognitiva belastningen hög. Studier visar att läshastigheten sjunker med cirka 10–20

[4] Kostnader för användning av annans skyddade egendom, exempelvis licensavgifter för att få använda ett upphovsrättsligt skyddat typsnitt eller varumärke.
[5] Vergara-Martínez, Perea & Leone-Fernandez (2020), *Neuropsychologia*, 146, 107556.
[6] FHWA, *Handbook for Designing Roadways for the Aging Population*, kap. 7.

procent när texter skrivs med enbart versaler.[7] Genom att använda en kombination av versaler och gemener underlättas informationsintaget, vilket minskar den tid föraren behöver ta blicken från vägen.

Huvudprincipen för det svenska vägvisningssystemet (med typsnittet Tratex) är att använda gemener för att maximera läsbarheten. Att använda enbart versaler på varningsskyltar för transporter av odelbara laster skulle bryta mot enhetligheten och frångå det system som trafikanter i Sverige är vana vid att läsa.

Genom att behålla gemener – med undantag för en inledande versal – säkerställer vi att budskapet uppfattas så snabbt och effektivt som möjligt. Detta bedömer vi är en av de viktigaste faktorerna för att varningsskylten ska fylla sitt syfte, varför vi valt att inte gå vidare med detta alternativ.

Funktionsbaserade krav

Funktionsbaserade regler är bestämmelser som anger *vad* som ska uppnås, men inte exakt *hur* det ska göras. Detta tillvägagångssätt ger den enskilde större flexibilitet. Till exempel att kunna välja tekniska lösningar, men det ställer också högre krav på att man själv kan påvisa och bevisa att ett krav är uppfyllt. I starkt handlingsdirigerande bestämmelser, till exempel trafikregler – vilka ska kunna kontrolleras av Polis och bilinspektör vid vägkantskontroll eller i domstol – kan dock funktionsbaserade regler vara olämpliga då behovet av tydlighet och kontrollerbara bestämmelser väger tyngre än fördelarna med teknisk flexibilitet.

Alternativet med funktionsbaserade krav har dock övervägts på så sätt att dagens nuvarande detaljkrav skulle ersättas med funktionsbaserade krav. Ett funktionsbaserat krav för bokstävernas höjd på varningsskyltar skulle till exempel innebära att hela texten ska vara läsbar på ett visst minsta avstånd. I Danmark har man en sådan reglering som anger att en skylt ska kunna läsas på ett avstånd av 30 meter.[8] Även om myndigheten strävar efter att i möjligaste mån ha funktionsbaserade regler har vi valt att inte gå vidare med det alternativet av följande skäl.

Ett krav på läsbarhet på ett visst avstånd innebär en hög grad av subjektivitet[9] samt att läsbarheten även påverkas av yttre faktorer som ljusförhållanden, väder och den enskilde betraktarens synförmåga. Eftersom dessa faktorer ständigt varierar, saknas det fasta parametrar för vad som utgör en godkänd skylt. Det blir därför svårt att på förhand veta om en skylt

[7] Holmqvist, K. & Wartenberg, C. (2005). *The role of shape in the recognition of road signs*. Lund University Cognitive Studies, 123. Lund: Lunds universitet.
[8] Se bilaga 2 punkten 10 i Bekendtgørelse om særtransport, BEK nr 635 af 31/05/2023
[9] Avser att en bedömning vilar på enskilda personers uppfattning och förutsättningar (t.ex. synförmåga) samt yttre omständigheter (t.ex. ljus- och väderförhållanden)

uppfyller gällande krav vid ett specifikt tillfälle. Avsaknaden av mätbara och förutsebara mått innebär dessutom att kraven inte går att kontrollera på ett objektivt och rättssäkert sätt.

För polisen och andra tillsynsmyndigheter skulle ett sådant förslag göra det mycket svårt att genomföra en objektiv och enhetlig kontroll vid vägkanten. Utan fastställda mått och typsnitt saknas objektiva kriterier för att avgöra om en överträdelse har skett. Ett funktionsbaserat krav i detta fall skulle därmed även medföra en bristande rättssäkerhet.

En funktionsbaserad regel skapar även en osäkerhet som kan leda till olika bedömningar i olika delar av landet och beroende på vilken polis eller bilinspektör som ska kontrollera att det funktionsbaserade kravet är uppfyllt.

Vi bedömer att tydlighet och förutsebarhet i detta fall väger tyngre än den flexibilitet som funktionsbaserade krav innebär. Mot bakgrund av de svårigheter som identifierats vid tillämpning och övervakning, bedömer vi att funktionsbaserade krav inte är lämpliga för denna typ av reglering.

6. Vilka är berörda?

De som i första hand påverkas av förslaget är tillverkare, importörer och försäljare av varningsskyltar. Det rör sig om relativt få företag som kan vara små, medelstora och stora.

I andra hand påverkas transportföretag som utför transporter av odelbar last med stöd av föreskrifter eller dispenser. För dessa är det avgörande att skyltarna uppfyller villkoren i föreskrifterna eller i en medgiven dispens för att få utföra transporten. Enligt Trafikverket hanterade verket år 2023 drygt 30 000 dispensansökningar. Där framgår även att Sveriges kommuner handlägger och beslutar cirka 15 000 dispensärenden per år.[10] Dessa ärenden påverkas sannolikt av de föreslagna ändringarna av de allmänna råden. Majoriteten av dessa ärenden omfattar företag. Det kan dock förekomma att privatpersoner ansöker om en transportdispens. Vad gäller företag kan det handla om allt från små enmansföretag, till medelstora och stora företag. När det gäller våra föreskrifter om färd med odelbar last kan dessa tillämpas av såväl företag, privatpersoner, föreningar med mera. Enligt Transportföretagen finns det cirka 13 600 transportföretag i Sverige med omkring 62 000 heltidsanställda. Hur många av dessa företag som tillämpar föreskrifterna är mycket svårt att fastställa.

[10] Rapport, Hantering av transportdispenser – Redovisning av regeringsuppdrag, Trafikverket år 2024, TRV 2022/143756

I tredje hand påverkas Polisen i sin övervakning av trafik, då tydliga bestämmelser är en förutsättning för att kunna kontrollera regelefterlevnaden.

7. Vilka konsekvenser medför regleringen?

7.1 Företag

(X) **Regleringen bedöms inte få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Samtliga konsekvenser för företagen beskrivs därför under 7.1.**

( ) **Regleringen bedöms få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför ingen beskrivning under 7.1 utan samtliga konsekvenser för företagen beskrivs under avsnitt C.**

Tillverkare av skyltar

För tillverkare av varningsskyltar bedöms regleringsförslagen medföra tydligare förutsättningar och en trygghet i att de produkter som tillhandahålls uppfyller gällande krav för att få användas i trafik. De nya föreskrifterna och allmänna råden öppnar upp för båda de tidigare förekommande tolkningarna av textstorlek. Undantaget är varningsskyltar i storleken 50x60 centimeter där den första versalen har en höjd på 17 centimeter samt de skyltar med en bård som är bredare än 5,5 centimeter.

I övrigt säkerställs genom den föreslagna regleringen att tillverkarnas befintliga sortiment och tillverkningsmetoder resulterar i tillåtna skyltar. Detta innebär i sin tur att tillverkarna kan fortsätta använda befintliga mallar, verktyg och produktionslinjer utan behov av nyinvesteringar eller omställningskostnader. Förslaget motverkar därmed kapitalförstöring, eftersom äldre skyltar i lager – som inte uppfyller dagens gällande bestämmelser – blir tillåtna att säljas enligt de nya bestämmelserna.

Vidare minskar de administrativa kostnaderna eftersom osäkerheten kring hur de tekniska kraven ska omsättas i produktion försvinner. Då inga aktörer tvingas till kostsamma justeringar är förslaget konkurrensneutralt och bedöms inte medföra några negativa ekonomiska konsekvenser för berörd bransch.

Sammantaget bedöms föreslagna regleringsalternativ utgöra sådana regelförenklingar som stabiliserar marknadsvillkoren för samtliga berörda tillverkare över tid.

Återförsäljare av skyltar

I likhet med vad som gäller för tillverkare, bedöms regleringsförslagen medföra en ökad trygghet för återförsäljare av varningsskyltar på så sätt att de produkter som lagerhålls och säljs uppfyller gällande krav för att få

användas i trafik. De nya reglerna omfattar båda de tidigare tolkningarna av textstorlek. Detta säkerställer att återförsäljarnas befintliga lager består av skyltar som är tillåtna att använda. Därmed kan återförsäljare sälja slut på nuvarande lager utan risk för att sitta på osäljbara produkter eller behöva hantera reklamationer till följd av otydliga bestämmelser. Förslaget motverkar på så sätt kapitalförstöring i hela distributionskedjan. Vidare innebär regleringsförslagen att återförsäljare kan ge säkra besked till sina kunder om att skyltarna är förenliga med gällande trafikregler, vilket underlättar försäljningsprocessen och minskar administrativa kostnader.

Förslagen medför att varningsskyltar som inte uppfyller de nya kraven måste bytas ut på sikt. Under den treåriga övergångsperiod kan dock befintliga skyltar fortfarande säljas, vilket ger återförsäljare möjlighet att ställa om och införa nya produkter som uppfyller kraven. Vi bedömer att majoriteten av de varningsskyltar som säljs i dag uppfyller de föreslagna kraven. Sammantaget bedöms förslagen över tid stabilisera marknadsvillkoren och säkerställa tillgängligheten av varningsskyltar.

Användare av skyltar

För användare av varningsskyltar bedöms regleringsförslagen medföra en ökad tydlighet och trygghet vid framförande av fordon i trafik. Genom att regleringsförslagen omhändertar både de tidigare förekommande tolkningarna av textstorlek och bårdens egenskaper, säkerställs att de skyltar som redan används på fordonen är tillåtna. För användarna innebär detta att inga investeringar i nya skyltar krävs för att möta de tekniska kraven, vilket förhindrar onödiga kostnader för den enskilde näringsidkaren.

Förslaget eliminerar även risken för osäkerhet hos förare och företag vid kontroll utmed väg, då det blir tydligt att båda utförandena är förenliga med gällande bestämmelser. Vidare underlättas inköp av ny utrustning då användare kan kontrollera att de skyltar som finns på marknaden uppfyller kraven för att få användas i trafik.

De som idag använder varningsskyltar med text i två rader och med ytterdimensionerna 50x60 centimeter kommer att behöva byta ut dessa om bokstäverna är närmare bården än 2,0 centimeter. Detta gäller även de som använder skyltar som har större ytterdimensioner än de föreskrivna minimimåtten på grund av att bården har gjorts bredare än 5,5 centimeter. För att minska konsekvenserna för användarna föreslår vi övergångs-bestämmelser som tillåter fortsatt användning av sådana skyltar ytterligare tre år efter att föreskrifterna trätt i kraft.

Sammantaget innebär förslaget en förenkling som säkerställer att användarna kan fortsätta sin verksamhet utan avbrott eller behov av kostsamma materialbyten.

7.2 Enskilda

Enskilda bedöms inte påverkas nämnvärt av förslagen. De gånger enskilda påverkas är det i egenskap av trafikanter som möter fordon som transporterar breda eller långa odelbara laster. Även om förslagen syftar till att trafikanterna ska ges goda och tillräckliga förutsättningar att upptäcka och förstå texten på varningsskyltar, bedöms förslagen inte medföra några direkta konsekvenser för medborgarna som helhet.

7.3 Staten, regioner eller kommuner

Trafikverket
Trafikverket påverkas i den del myndigheten hanterar ansökningar om undantag från trafikförordningens (1998:1276) bredd- och längdbestämmelser för färder i mer än en kommun.

I de fall Trafikverket väljer att följa våra allmänna råd behöver de göra interna ändringar i sina stödjande och styrande dokument så att dessa stämmer överens med de ändrade allmänna råden. Om råden följs kommer detta medföra vissa administrativa kostnader. Kostnaden kan komma att bestå av ändringar av beslutsmallar, uppdateringar av IT-system, och uppdatering av information på sina webbsidor. För detta bedöms att Trafikverket behöva cirka 80 timmars arbete.

Polismyndigheten
Polisen påverkas generellt i dess övervakning av ändrade bestämmelser och trafikregler, vilket även gäller de nu föreslagna ändringarna. Ett av huvudsyftena med ändringarna är att bestämmelser vad gäller höjd på bokstäver och den röda bården ska bli tydligare, och att de som tillämpar bestämmelser ska ges förutsättningar att göra rätt. Därmed förväntas detta i förlängningen förenkla för poliser och bilinspektörer när de ska kontrollera om transporter av breda eller långa odelbara laster uppfyller villkoren i Transportstyrelsens föreskrifter eller i en medgiven dispens från väghållare.

Kommuner
I likhet med Trafikverket bedöms kommunerna påverkas vid handläggningen av ansökningar om undantag från trafikförordningens bestämmelser om fordons bredd och längd för färder inom den egna kommunen.

De allmänna råden bidrar till att de villkor som ställs i dispenser harmoniseras på nationell nivå, vilket underlättar handläggningen för kommunerna.

Ändringarna av de allmänna råden medför ingen förändring av kommunernas befogenheter eller skyldigheter, och påverkar inte heller deras organisation eller verksamhetsformer. Den kommunala självstyrelsen bedöms därmed inte påverkas, eftersom kommunerna fortsättningsvis har

befogenhet att besluta om undantag från trafikförordningens bestämmelser om fordons bredd och längd för färder som sker inom den egna kommunen.

Kommuner kan komma att få ökade administrativa kostnader om de väljer att följa de allmänna råden. Dessa kostnader består i så fall av ändringar i beslutsmallar, uppdateringar av IT-system, ändrade arbetssätt och rutiner samt uppdatering av information på kommunernas webbplatser.

7.4 Miljö

Förslaget bedöms medföra minimala miljömässiga konsekvenser för samhället i stort. Möjligheten att använda även äldre skyltar minskar miljöpåverkan då de tillåts att användas ytterligare tre år efter att föreskrifterna trätt i kraft. Förenklad tillverkningsprocess vad gäller den röda bården medför minskat materialspill.

7.5 Externa effekter

Förslaget bedöms inte medföra några negativa externa effekter. Utifrån vår undersökning om hur texthöjden påverkar läsbarhet på varningsskyltarna bedöms de föreslagna kraven på bokstävernas höjd vara tillräckliga för att säkerställa trafiksäkerheten. Samma bedömning görs gällande möjligheten att använda material med andra och fler egenskaper på den röda bården, samt att bårdens bredd fixeras till 5,5 centimeter oavsett skyltens storlek.

8. Sammanfattning av övervägda alternativ och varför föreslagen reglering anses vara det bästa alternativet

Detta avsnitt innehåller för- och nackdelar för förslag och alternativ för följande regleringsområdena; texthöjd, bårdegenskaper och bårdbredd. För varje regleringsområde motiveras även varför vi förespråkar vårt förslag.

8.1 Höjd på bokstäver

Minsta höjd på bokstäver – Transportstyrelsens förslag

Transportstyrelsen föreslår krav på en minimihöjd på bokstäver som förekommer på varningsskyltar. Förslaget innebär en avvägning som säkerställer god synbarhet samtidigt som det ger tillverkare, återförsäljare och användare flexibilitet att välja skyltstorlek och höjd på bokstäver. Genom att specificera höjden för varje enskild bokstav blir bestämmelser tydligare för såväl branschen som rättsvårdande myndigheter. Eftersom bokstavshöjden är konkret mätbar på plats i trafiken förenklas tillsynen. Om exempelvis en versal görs 15,0 centimeter hög (en ökning med ca 10,3 procent från minimikravet på 13,6 centimeter), ska övriga bokstäver ökas med samma procentsats.

Förslaget är en kombination av tekniska bestämmelser med ett minimimått och en mer funktionsbaserad del, vilket skapar förutsättningar för att

använda varningsskyltar med högre bokstäver. Oaktat om man tolkat dagens bestämmelser som att den första versalens höjd ska vara 13,6 eller 17,0 centimeter kommer detta förslag göra så att dessa skyltar uppfyller de föreskrivna kraven. Detta gör att de skyltar som tillverkats, och som ingen tidigare vågat använda på grund av osäkerheten om vad som gäller, nu kan säljas och tas i bruk, vilket är den största fördelen med förslaget.

Eftersom vi föreslår minimimått för tecknen på varningsskyltarna bedömer vi att trafiksäkerheten inte kommer att påverkas i någon större omfattning. De föreslagna minimimåtten bedöms göra att trafikanter hinner upptäcka och förstå varningsskyltarna på ett avstånd som bibehåller trafiksäkerheten.

Den föreslagna bestämmelsen öppnar upp för en högre bokstavshöjd och innebär en viss detaljreglering, särskilt när det handlar om höjden på bokstaven ”g” på varningsskyltar med texten ”Varning” och ”Lång last”. Denna detaljreglering kan upplevas som svårare att förstå. Vi anser dock att förslaget är en god avvägning mellan tydlighet och mer detaljerade bestämmelser. Fördelen med en detaljreglering blir dock att det är relativt enkelt att kontrollera om man uppfyller gällande krav eller inte, vilket är viktigt när det kommer till användningsregler.

En annan nackdel är att förslaget kommer medföra att vissa varningsskyltar med text i två rader som förekommer i dag inte kommer att vara tillåtna att användas i trafik. Vi bedömer dock att det rör sig om ett relativt litet antal skyltar och att det redan idag är tveksamt om dessa skyltar uppfyller de bestämmelser som förekommer i dag. Dessa varningsskyltar kommer behöva bytas ut i samband med förslaget.

Eventuella nackdelar kommer dock motverkas med en övergångs-bestämmelse som gör att dagens bestämmelser i vissa delar kan tillämpas under en övergångsperiod. Detta gör att företag ges en viss omställnings-period för att minska de ekonomiska konsekvenserna.

13,6 centimeters höjd på bokstäver

Som ett alternativ till Transportstyrelsens regleringsförslag har vi övervägt att ha en fast höjd på bokstäverna utan möjlighet att göra tecknen större. Det innebär att den inledande versalen låses till 13,6 centimeter, och att de efterföljande gemenernas höjd följer de proportioner som gäller inom typsnittet Tratexsvart med den versalhöjden.

Detta alternativ skulle över tid medföra en tydlig reglering om vad som ska gälla eftersom endast en höjd på bokstäverna i varningsskyltarna skulle vara tillåtna och bidra till att varningsskyltarna skulle få ett enhetligt utseende. Måtten – som skulle vara samma som de minimimått som vi föreslår i vårt regleringsförslag – bedöms ge varningsskyltar som i tillräcklig grad går att

upptäcka och förstås på ett tillräckligt långt avstånd för att trafiksäkerheten ska bibehållas.

En nackdel med detta alternativ är att befintliga varningsskyltar, där man tolkat dagens bestämmelser som att det är den första versalens höjd som ska vara 17,0 centimeter, inte skulle uppfylla de nya kraven och därmed behöva ersättas. Befintliga lager med sådana skyltar skulle bli osäljbara och behöva kasseras vilket skulle medföra negativa ekonomiska konsekvenser för företag i form av kapitalförstöring.

De varningsskyltar som har högre bokstäver än de som föreslås kan tydas på något längre avstånd. Att tvinga fram ett utbyte av sådana skyltar som både ger god synbarhet och innebär en betydande investering för branschen bedöms inte vara proportionerligt. Mot bakgrund av att större bokstäver inte försämrar trafiksäkerheten, saknas tillräckliga skäl för att gå vidare med detta alternativ.

En fördel med detta alternativ är att bokstäverna får plats på ett bra sätt i tvåradiga varningsskyltar med den föreskrivna minimistorleken på 50x60 centimeter. Ytterligare en fördel är att de varningsskyltar som har tagits fram med bokstavshöjder enligt detta alternativ kommer uppfylla kraven. En nackdel är dock att dessa skyltar, och andra med avvikande bokstavshöjd, inte kommer att uppfylla kraven och kan därför inte användas i trafiken.

Kontrollen av varningsskyltar med en bokstavshöjd enligt alternativet kommer vara relativt enkel eftersom höjden på varje bokstav kommer vara specificerad. Höjden på bokstäverna kan mätas på plats i trafiken och bedöms även ge tillräckligt god läsbarhet och förståelse för att anses vara trafiksäker.

Vi har valt att inte gå vidare med detta förslag då det bedöms som oproportionerligt och medför betydande ekonomiska konsekvenser i form av kapitalförstöring för branschen. Eftersom befintliga varningsskyltar med 17,0 centimeter höga versaler har något bättre synbarhet bedömer vi att det även av den anledningen saknas skäl att tvinga branschen att byta ut sådana varningsskyltar.

17 centimeters höjd på bokstäver

Som ett alternativ till vårt regleringsförslag har vi även övervägt alternativet om att ha en fast höjd på 17,0 centimeter på den första versalen. I likhet med regleringsalternativet ovan skulle det över tid medföra en tydlig reglering om vad som gäller eftersom endast en och samma höjd på bokstäverna på varningsskyltar kommer vara tillåtna. Det bidrar till att skyltar skulle få ett enhetligt utseende. Även kontrollen av bokstävernas höjd på varningsskyltar skulle vara relativt enkel då höjden på varje bokstav kommer vara specificerad.

En nackdel med detta alternativ är att befintliga varningsskyltar, där man tolkat dagens bestämmelser som att det är den första versalens höjd som ska vara 13,6 centimeter, inte skulle uppfylla de nya kraven och därmed behöva bytas ut. Befintliga lager med sådana skyltar skulle bli osäljbara och behöva kasseras vilket skulle medföra negativa ekonomiska konsekvenser för företag i form av kapitalförstöring.

Vi har valt att inte gå vidare med detta förslag då det bedöms, i likhet med förslaget ovan, medföra bristande proportionalitet och betydande ekonomiska konsekvenser i form av kapitalförstöring för branschen. Att införa en fast, tvingande höjd på 17,0 centimeter skulle göra alla befintliga varningsskyltar med en höjd på den första versalen som är 13,6 centimeter olagliga. Ett sådant krav skulle tvinga fram omfattande utbyten och leda till stora kostnader för berörda företag. Eftersom det saknas tillräckliga trafiksäkerhetsskäl för att förbjuda de lägre bokstavshöjderna, överväger de negativa ekonomiska konsekvenserna för företagen de potentiella fördelarna med en enhetlig reglering.

Varför regleringsförslaget anses vara det bästa

Vi bedömer att de föreslagna bokstavshöjderna säkerställer god läsbarhet och ger trafikanter möjlighet att uppfatta och förstå varningsskyltarna på ett trafiksäkert avstånd. Förslaget innehåller en undantagsbestämmelse som tillåter skyltar med högre bokstäver än den föreskrivna minimistorleken. Detta innebär att de skyltar som används i dag uppfyller de nya kraven, oavsett hur dagens bestämmelser tidigare har tolkats.

Förslaget säkerställer en hög trafiksäkerhet samtidigt som det ger flexibilitet och minimerar behovet av att ersätta befintliga varningsskyltar. Vissa skyltar kan dock fortfarande behöva bytas ut, till exempel tvåradiga skyltar med måtten 50x60 centimeter där den första versalen är 17,0 centimeter. För att minska de ekonomiska konsekvenserna för branschen föreslås en övergångsregel som tillåter att dessa skyltar används ytterligare tre år efter att föreskrifterna trätt i kraft. Övergångsbestämmelsen ger företag tre år att förbereda sig inför nya bestämmelser, vilket bedöms vara en skälig tid för framförhållning för att byta ut befintliga skyltar.

Sammanfattningsvis bedöms att vårt regleringsförslag uppnår det avsedda trafiksäkerhetsmålet till minsta möjliga kostnad för samhälle, företag och berörda aktörer. Detta inkluderar även administrativa kostnader.

8.2 Bårdegenskaper

Fluorescerande eller retroreflekterande röd bård – Transportstyrelsens förslag

Transportstyrelsens regleringsförslag är att egenskaperna på den röda bården – till skillnad från dagens krav på att den ska vara fluorescerande –

även får vara retroreflekterande eller en kombination av båda dessa egenskaper. Av förslaget framgår att man inte kan blanda egenskaperna på olika sidor av bården, utan egenskaperna på den röda bården ska i sin helhet vara samma.

Förslaget bedöms medföra att synbarheten blir något lägre om enbart retroreflekterande material används. Eftersom det finns krav på att skylten ska vara belyst under mörker, i skymning, eller gryning och i övrigt när det är påkallat av väderleken eller andra omständigheter bedöms synbarheten dock vara tillräcklig. Skillnaden i synbarhet mellan de olika materialens egenskaper bedöms därför vara minimal.

Förslaget innebär även att antalet valbara material ökar, och tillverkare behöver heller inte ändra sin tillverkningsprocess.

Retroreflekterande bård

Ett alternativ som övervägts är att ersätta dagens krav på att den röda bården ska vara fluorescerande med ett krav på att bården enbart får vara retroreflekterande.

Fördelarna med detta alternativ är att det bedöms förenkla tillverkningsprocessen och sänka kostnaderna för slutanvändaren.

En nackdel är att det blir förbjudet att använda fluorescerande material som, ur ett synbarhetsperspektiv, är något bättre än ett enbart retroreflekterande material. Eftersom det finns krav på att varningsskyltarna ska vara belysta vid färd under mörker, i skymning eller gryning, samt när det i övrigt påkallas av väderleken eller andra omständigheter, bedöms dock en retroreflekterande bård säkerställa en tillräcklig synbarhet för att inte äventyra trafiksäkerheten.

En annan nackdel med detta förslag är att befintliga varningsskyltar med enbart fluorescerande bård blir förbjudna att använda. Alternativet kräver därför även en övergångsbestämmelse. Ytterligare en nackdel är att tillverkare med etablerad verksamhet kommer att behöva ställa om sin tillverkningsprocess.

Att gå vidare med ett krav på enbart retroreflekterande material skulle innebära ett omotiverat förbud mot fluorescerande bårder, vilket skulle tvinga fram kostsamma utbyten av fullt fungerande varningsskyltar. Eftersom det saknas skäl att begränsa bestämmelsen till att den röda bården enbart får vara retroreflekterande väljer vi att inte gå vidare med detta alternativ.

Fluorescerande

Ett annat alternativ som övervägts är att behålla dagens krav på att den röda bården ska vara fluorescerande (nollalternativet). Fördelarna med detta är att

en god synbarhet säkerställs och att skylttillverkarna inte behöver ändra sina tillverkningsprocesser.

Nackdelen är att alternativet inte möjliggör användning av material som enbart är retroreflekterande, trots att dessa bedöms ha en tillräcklig synbarhet. En annan nackdel är att vissa fluorescerande material bleks av solen över tid och då ändrar färg från rött till orange. Enligt uppgifter som myndigheten har fått från tillverkare är livslängden för vissa fluorescerande material så kort som två år.

Varför regleringsförslaget anses vara det bästa

Vi bedömer att vårt förslag är det mest ändamålsenliga alternativet eftersom det på ett balanserat sätt förenar kraven på trafiksäkerhet med flexibilitet för marknadens aktörer. Genom att tillåta fluorescerande och retroreflekterande material samt material som både är fluorescerande och retroreflekterande skapas teknikneutrala bestämmelser som tillvaratar fördelarna från de övriga övervägda alternativen utan att medföra deras respektive nackdelar.

Att helt övergå till enbart retroreflekterande material skulle tvinga etablerade tillverkare att göra om sina produktionsprocesser. Förslaget skulle även göra dagens varningsskyltar otillåtna. Dessutom skulle förslaget kräva övergångsbestämmelser. Regleringsförslaget undviker dessa negativa konsekvenser helt genom att istället utöka antalet tillåtna material, vilket ökar valfriheten och konkurrensen på marknaden samtidigt som tillverkare som vill behålla sin nuvarande produktion kan göra det utan extra kostnader.

Nollalternativet erbjuder förvisso en optimal synbarhet genom det fluorescerande kravet. De fluorescerande egenskaperna mattas dock av över tid på grund av solblekning, vilket leder till att den röda färgen blir mer orange än röd till färgen. I kontakt med tillverkare har vi fått informationen att detta sker redan efter en så kort tid som två år.

Eftersom gällande bestämmelser redan kräver att varningsskyltarna ska vara belysta under mörker, skymning, gryning och vid dålig väderlek, bedöms ett enbart retroreflekterande material ge en fullgod tillräcklig synbarhet samtidigt som skillnaden i trafiksäkerhet under dessa förhållanden är minimal. Det valda förslaget garanterar därmed att trafiksäkerheten upprätthålls samtidigt som det öppnar upp för mer beständiga materialval, vilket förlänger skyltarnas faktiska livslängd och minskar kostnaderna för slutanvändaren.

Sammanfattningsvis innebär regleringsförslaget att problemet med det fluorescerande materialets korta livslängd löses, samtidigt som marknaden får en större flexibilitet. Eftersom det redan finns krav på att varningsskyltarna ska vara belysta vid behov är synbarheten tillräcklig,

vilket innebär att trafiksäkerheten inte äventyras. Alternativet bedöms därför vara det mest fördelaktiga.

8.3 Bårdbredd

Fast bårdbredd på 5,5 centimeter – Transportstyrelsens förslag
Vårt förslag innebär att den röda bårdens bredd alltid ska vara 5,5 centimeter även om ytterdimensionerna på varningsskylten görs större än de föreskrivna minimimåtten.

En bårdbredd på 5,5 centimeter är redan i dag bredare än vad som gäller för vissa andra fordonsskyltar. På de skyltar som används på en vägtransportledares fordon ska bården exempelvis vara 2,5 centimeter bred. För de fordonsskyltar som ska finnas baktill på fordonståg längre än 25,25 meter ska bårdens bredd vara 3,0 centimeter. En fast bårdbredd på 5,5 centimeter för de varningsskyltar som används vid transporter av odelbara laster bedöms därför vara tillräcklig för att säkerställa en god synbarhet.

En nackdel är att i de fall en varningsskylt tillverkas med större storlek än de föreskrivna minimimåtten så kommer igenkänningsfaktorn minska eftersom varningsskyltarnas utseende kommer att avvika från det utseende som framgår av figurerna i föreskrifterna. Branschen förefaller önska att använda skyltar med de föreskrivna yttre minimimåtten. Vi bedömer därför att majoriteten av de skyltar som används kommer att överensstämma med figurerna i föreskrifterna.

Dagens krav på bårdbredd
Ett alternativ som övervägts är att behålla det krav som gäller i dag, vilket innebär att den röda bårdens bredd ska ökas i motsvarande grad om en varningsskylt görs större än minimimåtten.

Fördelen med att behålla dagens gällande krav är att bestämmelser redan är kända av marknadens aktörer och att det inte krävs några omedelbara omställningar av rådande tillverkningsmetoder.

En nackdel med detta alternativ är att det – i de fall en varningsskylt gjorts större – krävs en proportionalitetsberäkning för varje enskild skyltstorlek, vilket försvårar kontrollen för såväl tillverkare, tillämpare och tillsynsmyndigheter då man ska kontrollera och veta hur bred bården ska vara för den specifika skyltstorleken. Detta driver onödigtvis upp produktionskostnaderna för varningsskyltarna. Ytterligare en nackdel visar sig i de fall en skylt förstoras asymmetriskt, exempelvis till storleken 60x70 centimeter för att rymma två textrader. Skylten uppfyller då förvisso de föreskrivna minimimåtten men är inte proportionerligt skalad, vilket medför att den röda bården får olika bredd på de horisontella och vertikala delarna. En sådan visuell avvikelse är inte önskvärd.

Varför regleringsförslaget anses vara det bästa

Vi bedömer att vårt regleringsförslag, vilket innebär att införa ett fast mått på 5,5 centimeter för den röda bårdens bredd, utgör den mest balanserade och långsiktigt ändamålsenliga lösningen. En fast bårdbredd på 5,5 centimeter är fullt tillräcklig för att säkerställa god synbarhet för varningsskyltar vid transporter av odelbara laster. Måttet är väl tilltaget i jämförelse med andra fordonsskyltar på marknaden. Det finns därmed inga trafiksäkerhetsmässiga skäl att kräva en ännu bredare bård även när en varningsskylt görs större än de reglerade minimimåtten.

Ett bibehållande av dagens krav har förvisso fördelen att bestämmelserna är kända och inte kräver omedelbara omställningar i produktionen. Nackdelarna är dock betydande då det nuvarande kravet på proportionell ökning skapar en krånglig administrativ börda då det krävs en proportionalitetsberäkning för varje specifik skyltstorlek. Detta försvårar kontrollen för tillverkare, tillämpare och tillsynsmyndigheter samt driver upp produktionskostnaderna. Den nuvarande bestämmelsen skapar dessutom visuella avvikelser vid asymmetriska förstoringar – exempelvis om en skylt med text i två rader görs i storleken 60x70 centimeter – eftersom bården då får olika bredd på de horisontella och vertikala delarna, vilket inte är önskvärt. Genom att istället införa vårt förslag med en standardiserad bårdbredd, oavsett skyltens totala storlek, underlättas tillverkningsprocessen avsevärt. Detta bidrar till en mer kostnadseffektiv, förutsägbar och enhetlig produktion utan att göra avkall på trafiksäkerheten.

9. Vilka bemyndiganden grundar sig myndighetens beslutanderätt på?

Föreskrifter om färd med bred odelbar last meddelas med stöd av bemyndigande i 4 kap. 15 § trafikförordningen, och föreskrifter om färd med lång odelbar last meddelas med stöd av bemyndigande i 4 kap. 17 b § samma förordning.

Beslut om allmänna råd kräver inget särskilt bemyndigande. Frågor om krav på fordon och bestämmelser för vägtrafik ligger inom Transportstyrelsens ansvarsområde, jämför 2 § förordningen (2008:1300) med instruktion för Transportstyrelsen.

10. Överensstämmer regleringen med eller går den utöver de skyldigheter som följer av EU-rättslig reglering eller andra internationella regler?

Transportstyrelsens förslag utgår från nationell regelgivning och vi bedömer att förslaget inte medför hinder för den fria rörligheten enligt EU-rätten.

Förslagen om ändring av både föreskrifterna och de allmänna råden innehåller bestämmelser om varningsskyltar och hur dessa ska vara

utformade. Förslagen bedöms därmed utgöra sådana tekniska regler som omfattas av krav på anmälan enligt förordningen (1994:2029) om tekniska regler. Vi avser därför att anmäla råden till kommissionen enligt gällande informationsprocedur beträffande tekniska standarder och föreskrifter i Europaparlamentets och rådets direktiv (EU) 2015/1535.

Transportstyrelsens bemyndigande och de ändringar vi föreslår bedöms inte gå utöver de skyldigheter som följer av direktivet 96/53/EG. Det finns heller inga andra internationella regler som berör detta.

Förslagen bedöms inte påverka organisatoriska krav på tjänsteutövare utöver de som finns i EU-gemensam reglering.

11. Behöver särskild hänsyn tas när det gäller tidpunkten för ikraftträdande och finns det behov av speciella informationsinsatser?

Eftersom de problem som presenteras under avsnitt 3 kvarstår utan en regeländring eller ändringar av allmänna råd behöver de föreslagna ändringarna träda i kraft så snart det är möjligt. Vi anser dock att det inte råder sådan brådska i ärendet att myndighetens behöver frångå vårt normala förfarande för att ta fram och besluta om ändringar av föreskrifter eller allmänna råd.

Myndigheten har information om gällande bestämmelser på hemsidan som behöver uppdateras i och med en uppdatering av föreskrifterna, denna uppdatering kan dock först göras efter att ändringar av föreskrifterna och allmänna råden har beslutats.

Myndigheten har deltagit vid olika webbinarium med branschföreträdare och personer från vissa av de branscher som påverkas av de föreslagna ändringarna. I samband med beslut om föreslagna ändringar kan vi informera om dessa ändringar på kommande webbinarium.

B. Transportpolitisk måluppfyllelse

Det övergripande målet för svensk transportpolitik är att säkerställa en samhällsekonomiskt effektiv och långsiktigt hållbar transportförsörjning för medborgare och näringsliv i hela landet. Under det övergripande målet finns också funktionsmål och hänsynsmål med ett antal prioriterade områden.

Funktionsmålet handlar om att skapa tillgänglighet för människor och gods. Transportsystemets utformning, funktion och användning ska medverka till att ge alla en grundläggande tillgänglighet med god kvalitet och användbarhet samt bidra till utvecklingskraft i hela landet. Samtidigt ska transportsystemet vara jämställt, det vill säga likvärdigt svara mot kvinnors respektive mäns transportbehov.

Hänsynsmålet handlar om säkerhet, miljö och hälsa. Transportsystemets utformning, funktion och användning ska anpassas till att ingen ska dödas eller skadas allvarligt. Det ska också bidra till det övergripande generationsmålet för miljö och att miljökvalitetsmålen uppnås, samt bidra till ökad hälsa.

Samtliga förslag ligger i linje med de transportpolitiska målen eftersom de syftar till att säkerställa samhällseffektiva och långsiktigt hållbara bestämmelser för tillverkare och transportörer av gods som innebär längre och bredare transporter än som annars är normalt. Genom tydligare bestämmelser och fler allmänna råd och exempel förväntas förslagen bidra till att förbättra trafiksäkerheten och framkomligheten.

10. Hur påverkar regleringen funktionsmålet?

Framkomligheten i transportsystemet påverkas alltid i olika grad av transporter, och det gäller särskilt vid transporter av last som är bredare och längre än vad som normalt är tillåtet. Förslagen bidrar till att uppfylla funktionsmålet på så sätt att dessa transporter kan utföras utan att trafiksäkerheten åsidosätts. Genom tydligare bestämmelser förväntas regelefterlevnaden öka, vilket i sin tur leder till ökad trafiksäkerhet och färre olyckor eller tillbud. Därmed förväntas förslagen bidra till en bättre tillgänglighet i transportsystemet.

11. Hur påverkar regleringen hänsynsmålet?

Tydligare bestämmelser om hur varningsskyltar ska se ut och vara utformade bedöms bidra till en ökad trafiksäkerhet. Hänsynsmålet, i den del det avser trafiksäkerhet, hälsa och miljö, bedöms därmed påverkas positivt av de föreslagna ändringarna.

C. Företag

Regleringen bedöms inte få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Samtliga konsekvenser för företag beskrivs därför under avsnitt A.7.1.

D. Sammanställning av konsekvenser

Berörd aktör	Effekter som inte kan beräknas		Beräknade effekter (tkr)	Kommentar
	Fördelar	**Nackdelar**	**+ / -**	
Företag	-Tydligare regler som gör det lättare att göra rätt. -Underlättar framtagande av varningsskyltar, kan resultera i billigare skyltar. -Minskade administrativa kostnader. -Ökad flexibilitet.	-Skyltar med text i två rader, där bokstäverna är mindre än 2,0 centimeter från den röda båden, måste bytas senast tre år efter att föreskrifterna trätt i kraft även om dess skick är bra.		
Medborgare				-Medborgare bedöms generellt inte påverkas av förslagen.
Staten m.fl.	-Tydliga regler som förenklar Polisens arbete vid vägkants-kontroll.	-Trafikverket och kommunerna kan behöva ändra mallar som används vid hantering av ansökningar om undantag.		
Externa effekter	Minskat spill vid skylttillverkning.			
Totalt				

E. Förslagets proportionalitet

De föreslagna ändringarna bedöms vara proportionerliga i förhållande till de mål som ska uppnås. Syftet med förslagen är att undanröja nuvarande tolkningsproblem och säkerställa en enhetlig tillämpning av bestämmelser för varningsskyltar.

Genom att införa övergångsbestämmelser för vissa varningsskyltar med text i två rader samt skyltar med bredare bård än 5,5 centimeter minimeras de ekonomiska konsekvenserna för berörda företag. Alternativet att inte införa en övergångsbestämmelse skulle medföra kostnader för branschen utan att tillföra en proportionerlig ökning av trafiksäkerheten.

Sammantaget bedöms förslagen ha en rimlig balans mellan krav på tydliga föreskrifter och näringslivets behov av förutsägbarhet och

kostnadseffektivitet. Förslaget bedöms inte heller gå utöver vad som är nödvändigt för att uppnå de eftersträvade förbättringarna.

F. Uppföljning och utvärdering

Ungefär två år efter övergångsperiodens slut planerar Transportstyrelsen att hålla ett uppföljningsmöte med referensgruppen för detta föreskriftsarbete. Tidsperioden väljs för utbytet av nya skyltar ska slå igenom och att de nya reglerna ska ha tillämpats över en tid. Därmed bedöms att vi då kommer att ha en god bild om hur föreskrifterna fungerar, förstås och tillämpas. Utöver samverkan med referensgruppen planeras uppföljning genom samverkan med Polismyndigheten samt Trafikverket, analys av olycksstatistik och marknadsundersökning.

Indikatorer och kriterier för uppföljning och utvärdering skulle kunna vara följande.

Vad ska uppnås?	Indikatorer	Kriterier
Ökad rättssäkerhet	Ordningsbot relaterat till transporter med stöd av föreskrifter eller medgiven dispens	Färre utfärdade ordningsböter
Tydligare bestämmelser	Frågor till myndigheten relaterat till transporter med stöd av föreskrifter eller dispens	Färre inkomna frågor
Bibehållen trafiksäkerhet	Döda och allvarligt skadad i trafiken relaterat till transporter med stöd av föreskrifter eller dispens	Oförändrat eller färre antalet döda och allvarligt skadade
Högre kostnadseffektivitet	Kostnader för varningsskyltar	Oförändrat eller lägre kostnader för att köpa fordonsskyltar
Enhetligt utseende	Använda varningsskyltar	Antalet olika varianter av varningsskyltar blir färre
	Utseende på varningsskyltar	Färre varningsskyltar som avviker från det ursprungliga utseendet

G. Samråd

En workshop genomfördes på Transportstyrelsens kontor i Örebro den 11 november 2025. På workshopen deltog företrädare från olika skylttillverkare, leverantörer av varningsskyltar, transportutförare samt branschföreträdare för Svenska Mobilkranföreningen. Sveriges Åkeriföretag var inbjuda till workshopen men meddelade att de hade fått förhinder. Dessa (och Svenska mobilkranföreningen med flera) har informerats om detta arbete via nätverket ”Dispenstransporter” som bedrivs av Trafikverket. I det nätverket ingår bland annat även Polismyndigheten, Sveriges kommuner och regioner,

Maskinentreprenörerna med flera. Vi har även haft dialog med företrädare för Trafikverket gällande de konsekvenser de föreslagna ändringarna av de allmänna råden kan medföra för dem.

Förslagen omfattas inte av någon samrådsskyldighet enligt lag eller förordning.

Om ni har några frågor med anledning av konsekvensutredningen eller synpunkter ni vill framföra får ni gärna kontakta oss:

Pär Ekström, utredare
010-495 55 13
par.ekstrom@transportstyrelsen.se

Kristofer Elo, utredare
010-495 57 71
kristofer.elo@transportstyrelsen.se

Transportstyrelsens författningssamling

TRANSPORT STYRELSEN

TSFS 20[År]:[Nr]

Utkom från trycket
den [Välj ett datum]

Föreskrifter om ändring i Transportstyrelsens föreskrifter och allmänna råd (TSFS 2023:36) om färd med bred odelbar last;

VÄGTRAFIK

beslutade den [Välj ett datum].

Transportstyrelsen föreskriver[1] med stöd av 4 kap. 15 § trafikförordningen (1998:1276) i fråga om styrelsens föreskrifter och allmänna råd (TSFS 2023:36) om färd med bred odelbar last

dels att 15, 16, 29 och 30 §§ ska ha följande lydelse,

dels att det ska införas en ny bilaga, bilaga 3, av följande lydelse.

15 § Varningsskyltarna ska ha utseende och text enligt figur 1 eller figur 2 och

1. gul botten som är retroreflekterande,
2. en 5,5 centimeter bred röd bård som, i sin helhet, antingen är fluorescerande, retroreflekterande eller både fluorescerande och retroreflekterande,
3. text med teckensnittet Tratexsvart, och
4. text där bokstäverna har den höjd som anges i tabell 1 i bilaga 3.

Trots första stycket 4 får bokstävernas höjd vara större än vad som anges i tabell 1 i bilaga 3. Samtliga bokstäver ska då ökas proportionerligt till varandra i höjd och bredd och texten ska ha samma utseende som framgår av Figur 1 eller 2. Avståndet mellan bokstäverna och bården får inte underskrida 2,0 centimeter.

Figur 1

[1] Se Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

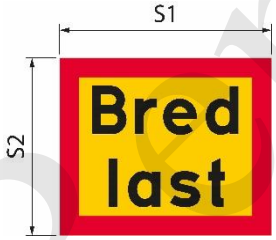
TSFS 20[År]:[Nr]

Figur 2

16 § Varningsskyltarna ska ha följande storlekar.

Skyltar med en rad	Figur 1	S1 ska vara minst 1,2 meter och S2 ska vara minst 0,4 meter. Förhållandet mellan bredd och höjd ska vara 3:1.
Skyltar med två rader	Figur 2	S1 ska vara minst 0,6 meter och S2 ska vara minst 0,5 meter.

Figur 1



Figur 2

29 § Varningsskyltarna ska ha utseende och text enligt figur 1 och

1. gul botten som är retroreflekterande,

2. en 5,5 centimeter bred röd bård som, i sin helhet, antingen är fluorescerande, retroreflekterande eller både fluorescerande och retroreflekterande,

3. text med teckensnittet Tratexsvart, och

4. text där bokstäverna har den höjd som anges i tabell 2 i bilaga 3.

Trots första stycket 4 får bokstävernas höjd vara större än vad som anges i tabell 2 i bilaga 3. Samtliga bokstäver ska då ökas proportionerligt till varandra i höjd och bredd och texten ska ha samma utseende som framgår av Figur 1. Avståndet mellan bokstäverna och bården ska vara minst 2,0 centimeter, med undantag av bokstaven g. Ingen del av bokstaven g får inkräkta på den röda bården.

Figur 1

30 § Varningsskyltarna ska ha följande storlek.

S1 ska vara minst 1,2 meter och S2 ska vara minst 0,4 meter (figur 1). Förhållandet mellan bredd och höjd ska vara 3:1.

Figur 1

Ikraftträdande och övergångsbestämmelser

1. Denna författning träder i kraft den…

2. Varningsskyltar med storlek 50x60 centimeter får användas till och med den 1 mars 2030 även om avståndet mellan bokstäverna och den röda bården är mindre än 2,0 centimeter. Ingen del av bokstäverna får dock inkräkta på bården.

3. Varningsskyltar med bård bredare än 5,5 cm får användas till och med den 1 mars 2030.

På Transportstyrelsens vägnar

JOEL SMITH

Pär Ekström
(Väg och järnväg)

Utgivare: Kristina Nilsson, Transportstyrelsen, Norrköping ISSN 2000-1975

Bilaga 3

Tabell 1. Höjd för respektive bokstav på varningsskyltar med texten ”Bred last”.

Tecken	Höjd i cm
B	13,6
r	10
e	10,2
d	13,7
l	13,6
a	10,1
s	10,1
t	13,6

Tabell 2. Höjd för respektive bokstav på varningsskyltar med texten ”Varning”.

Tecken	Höjd i cm
V	13,6
a	10,1
r	10
n	10
i	14
n	10
g	13,7

UMEÅ KOMMUN

Tjänsteskrivelse
2026-08-31

Tekniska nämnden

Diarienr: TN-2026/00692

Yttrande Remittering av promemoria: Vägval för framtiden: Justeringar av vägmärken i vägmärkesförordningen (2007:90)

Förslag till beslut
Tekniska nämnden beslutar

att lämna yttrande enligt nedan.

Ärendebeskrivning
Umeå kommun har beretts tillfälle att yttra sig över Landsbygds- och infrastrukturdepartementets remiss av promemorian Vägval för framtiden: Justeringar av vägmärken i vägmärkesförordningen (2007:90). Förslaget innebär ändringar av varningsmärken, anvisningsmärken och bommar vid järnvägskorsningar för att öka trafiksäkerheten och harmonisera reglerna internationellt. Det innehåller även en mindre, redaktionell rättelse av en felaktig paragrafhänvisning för vägmarkeringen M8 Heldragen linje.

Yttrande
Umeå kommun ställer sig positiv till de föreslagna ändringarna och har inga invändningar mot promemorians förslag.

Kommunen välkomnar att vägmärkena anpassas till internationell standard samt att trafiksäkerheten vid järnvägskorsningar stärks genom det nya anvisningsmärket E35 (”Kör genom bommen”). Att användningen av det nya märket är frivillig gör det möjligt för kommunen att prioritera resurserna där de gör mest nytta.

Eftersom äldre vägmärken får användas ända till utgången av 2041 kan utbytet ske löpande inom ramen för kommunens ordinarie drift och underhåll. Förslaget medför därför inga nya eller ökade kostnader för Umeå kommun.

Kommunen har inte heller några invändningar mot den föreslagna redaktionella rättelsen för vägmarkeringen M8.

Tjänsteskrivelse

Dnr: TN-2026/00692

Beslutsunderlag

Remissmissiv av promemorian Vägval för framtiden Justeringar av vägmärken. Bilaga.
Promemoria Vägval för framtiden - justeringar av vägmärken i vägmärkesförordningen. Bilaga.

Checklista för handläggning av ärenden inför politiska beslut anses inte tillämpbar.

Beredningsansvariga

Fredrik Öhrner

Beslutet ska skickas till

Till Landsbygds- och infrastrukturdepartementet senast den 16 oktober 2026. Svaren bör lämnas per e post till li.remissvar@regeringskansliet.se och med kopia till li.transport.remissvar@regeringskansliet.se. Ange diarienummer LI2026/01197 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Kopia på nämndens protokollsutdrag inkl. yttrande skickas till ksdiarium@umea.se, märk ämnesraden med diarienummer: KS-2026/00635

Promemoria

Vägval för framtiden: Justeringar av vägmärken i vägmärkesförordningen (2007:90)

Promemorians huvudsakliga innehåll

I promemorian föreslås att 2 kap. 5 och 12 §§, 4 kap. 6 § och 6 kap. 8 § vägmärkesförordningen (2007:90) ändras så att varningsmärket för järnvägskorsning med bommar, A35, ersätts av en ny version av märket och att det införs ett nytt anvisningsmärke, E35, som får användas vid sådana korsningar. Dessutom ändras de närmare föreskrifterna för anordning Y3 Bom som en följd av införandet av anvisningsmärket E35 och det görs även en rättelse i de närmare föreskrifterna till vägmarkering M8 Heldragen linje.

Förordningsändringarna föreslås träda i kraft den 1 januari 2027.

Innehållsförteckning

2 Förslag till förordning om ändring i vägmärkesförordningen (2007:90)

Härigenom föreskrivs att 2 kap. 5 och 12 §§, 4 kap. 6 § och 6 kap. 8 § vägmärkesförordningen (2007:90) ska ha följande lydelse.

2 kap.

5 §[1] Varningsmärken är följande.

Märke	Närmare föreskrifter
A34 Varning för kö 	Märket anger en vägsträcka där det finns risk för köbildning.
A35 Varning för järnvägskorsning med bommar 	Märket anger en korsning med järnväg eller spårväg där det finns bommar.
A36 Varning för järnvägskorsning utan bommar 	

12 §[2] Anvisningsmärken är följande.

Märke	Närmare föreskrifter
E34 Cykelgata upphör 	Märket anger att en cykelgata upphör.

[1] Senaste lydelse 2017:923.
[2] Senaste lydelse 2020:844.

E35 Kör genom bommen 	Märket anger att fordon som befinner sig mellan nedfällda bommar ska fortsätta färden genom bommen. Märket används på baksidan av anordningen Y3, bom.

4 kap.

6 §[3] Heldragna linjer är följande.

Markering	Närmare föreskrifter
M8 Heldragen linje 	Markeringen anger att bestämmelserna i 3 kap. 11 § eller 12 § fjärde stycket trafikförordningen (1998:1276) eller föreskrifter meddelade med stöd av den förordningen är tillämpliga. Heldragen linje kan vara heldragen mittlinje, heldragen körfältslinje eller heldragen kantlinje. Heldragen körfältslinje och heldragen kantlinje är enkel. Heldragen mittlinje kan vara såväl enkel som dubbel.
M9 Spärrområde 	Markeringen anger ett område där fordon inte får föras enligt 3 kap. 11 § trafikförordningen. Markeringen består av vinklade eller snedställda streck beroende på förhållandena på platsen. Del av eller hela området kan utföras i vitt.

6 kap.

8 §[4] Bommar vid korsning med järnväg eller spårväg är följande.

Anordning	Närmare föreskrifter
Y3 Bom 	Märke E35, kör genom bommen, kan vara uppsatt på anordningens baksida. Anordningens baksida får förses med texten "Kör genom bommen".

1. Denna förordning träder i kraft den 1 januari 2027.

[3] Senaste lydelse SFS 2017:923.
[4] Senaste lydelse SFS 2017:923.

2. Vägmärken och andra anordningar enligt äldre bestämmelser som till storlek eller utformning strider mot denna förordning får användas tills vidare, dock längst till utgången av år 2041. I fråga om sådana vägmärken eller anordningar gäller äldre bestämmelser, om inte Transportstyrelsen föreskriver annat.

3 Utbyte av vägmärken

I denna promemoria föreslås ändringar i vägmärkesförordningen (2007:90). För att gränsöverskridande trafik ska fungera smidigt finns det på FN-nivå en konvention som reglerar hur vägmärken och signaler ska utformas: Konvention om vägmärken och signaler. För Europa finns även en särskild överenskommelse som utgör tillägg till konventionen och ett tilläggsprotokoll om vägmarkeringar. Sverige är ansluten till alla tre. Målet med dessa rättsakter är inte full enhetlighet, men att det ska vara möjligt att känna igen vägmärken och signaler runt om i världen.

United Nations Economic Commission for Europe (FN:s ekonomiska kommission för Europa), UNECE, antog under 2025 ändringar i konventionen, överenskommelsen och tilläggsprotokollet som bl.a. innebär att det finns helt nya vägmärken och vägmärken som fått ett nytt utseende.

Transportstyrelsen har rekommenderat att Sverige inför det nya utseendet för Varningsmärke för järnvägskorsning med bommar, med den svenska benämningen A35 och ett helt nytt anvisningsmärke med uppmaningen Kör genom bommen, som föreslås få benämningen E35. Som en följd av införandet av E35 bör även de närmare föreskrifterna till anordning Y3 Bom ändras. Transportstyrelsen har även framfört att det finns en felaktig hänvisning i de närmare föreskrifterna till vägmarkering M8 Heldragen linje. Förordningsändringarna föreslås träda i kraft den 1 januari 2027.

4 Varningsmärke A35

Förslag

Nuvarande varningsmärke för järnvägskorsning med bommar A35 ska bytas ut.

Skälen för förslaget

United Nations Economic Commission for Europe (FN:s ekonomiska kommission för Europa), UNECE, har tagit fram ett nytt utseende för varningsmärket för järnvägskorsning med bommar. Det nya utseendet för märket är markant lättare att förstå. Finland har uppgett att de kommer att använda det nya utseendet. Norge och Danmark har ännu inte tagit ställning men uttryckt att det nya utseendet är tydligare. Det nuvarande varningsmärket föreslås därför bytas ut mot det varningsmärke som UNECE tagit fram. Införandet kräver en ändring i 2 kap. 5 § vägmärkesförordningen (2007:90).

5 Anvisningsmärke E35

Förslag

Nytt anvisningsmärke E35 kör genom bommen ska införas.

Skälen för förslaget

Märket är nytt och innebär en uppmaning till en trafikant som har hamnat mellan nedfällda bommar i en järnvägskorsning att köra genom bommen. Vägmärket kommer att kunna användas på baksidan på anordningen Y3 Bom och får ersätta eller komplettera den text som redan finns på många järnvägsbommar. Det blir upp till ansvarig väghållare, dvs. Trafikverket och kommunerna, att avgöra om märket ska sättas upp. Införandet kräver en ändring i 2 kap. 12 § och 6 kap. 8 § vägmärkesförordningen (2007:90).

6 Anordning Y3

Förslag

De närmare föreskrifterna till anordning Y3 Bom bör ändras så att det framgår att märke E35 får vara uppsatt på bommens baksida samt att bommens baksida får förses med texten ”kör genom bommen”.

Skälen för förslaget

Baksidan på anordning Y3 Bom får redan i dag förses med texten ”kör genom bommen”. Genom införandet av märke E35 tillkommer en möjlighet att kombinera texten med det nya märket. Det blir upp till ansvarig väghållare att bedöma när det är lämpligt att ha märke, text eller både och. Ändringen av de närmare föreskrifterna innebär att 6 kap. 8 § vägmärkesförordningen (2007:90) behöver revideras.

7 Vägmarkering M8

Förslag

De närmare föreskrifter som hänför sig till vägmarkering M8 Heldragen linje ska revideras genom att hänvisningen till 3 kap. 12 § trafikförordningen (1998:1276) ändras från tredje till fjärde stycket.

Skälen för förslaget

Transportstyrelsen har uppmärksammat att de närmare föreskrifterna till vägmarkeringen M8 hänvisar till fel stycke i 3 kap. 12 § i

trafikförordningen (1998:1276). Den korrekta hänvisningen ska vara till 3 kap. 12 § fjärde stycket i trafikförordningen.

8 Ikraftträdande och övergångsbestämmelser

Förslag

Förslagen ska träda i kraft den 1 januari 2027. Vägmärken och andra anordningar enligt äldre bestämmelser som till storlek eller utformning strider mot förordningen får användas tills vidare, dock längst till utgången av år 2041. I fråga om sådana vägmärken eller anordningar gäller äldre bestämmelser om inte Transportstyrelsen föreskriver annat.

Skälen för bedömningen

Denna förordning träder i kraft den 1 januari 2027. En ikraftträdandetidpunkt under 2027 bedöms ge ansvariga myndigheter och väghållare tillräcklig tid att anpassa rutiner, planering och informationsinsatser till de nya bestämmelserna. Samtidigt säkerställs att ändringarna kan börja tillämpas utan onödigt dröjsmål.

Det är vidare motiverat att tillåta en längre övergångsperiod för befintliga vägmärken och anordningar som inte uppfyller de nya kraven på utformning eller storlek. Utbyte av vägmärken sker i normalfallet i samband med ordinarie drift och underhåll, och att kräva ett omedelbart eller snabbt generellt utbyte skulle innebära betydande kostnader och administrativa belastningar för såväl statliga som kommunala väghållare. En övergångsperiod som sträcker sig till utgången av 2041 medger att utbytet kan ske successivt och kostnadseffektivt, utan att trafiksäkerheten påverkas negativt. Den föreslagna tidsramen innebär även att hela livslängden för redan uppsatta vägmärken kan tas till vara, vilket är förenligt med principerna om god resurshushållning och miljömässig hållbarhet. Samtidigt säkerställs att det finns en tydlig slutpunkt för övergången, vilket på längre sikt främjar en enhetlig och modern vägmiljö.

9 Konsekvenser

Bedömning

Förslaget förväntas medföra tydligare skyltning vid järnvägskorsningar med bommar, vilket kan bidra till ökad trafiksäkerhet. Förslaget innebär inga nya arbetsuppgifter i sak för Trafikverket och kommunerna, men medför ett behov av att vidta vissa åtgärder inom ramen för det befintliga väghållaransvaret. Eftersom utbytet av befintliga vägmärken kan ske i samband med ordinarie drift- och underhållsåtgärder över en

period på 15 år bedöms det inte heller medföra några ekonomiska konsekvenser för staten och kommunerna. Förslaget bedöms ha en begränsad och proportionerlig påverkan på den kommunala självstyrelsen.

Skälen för bedömningen

Nuvarande varningsmärke för järnvägskorsning med bommar A35 ska enligt förslaget bytas ut. Enligt uppgifter från Trafikverket finns det sammanlagt 3 500 sådana vägmärken på statliga, kommunala och enskilda vägar. Trafikverket uppskattar att kostnaden för att byta ut ett vägmärke är ca 13–14 000 kronor, vilket inkluderar material och arbetskostnader. Detta är en kostnad som gäller redan i dag, för alla vägmärken som byts ut fortlöpande. Det är alltså inte fråga om en kostnad som enbart tillkommer för varningsmärken för järnvägskorsning med bommar, utan beskriver de kostnader som Trafikverket och kommunerna har redan nu.

I egenskap av väghållare för det statliga vägnätet ansvarar Trafikverket för att byta skyltar på statliga och enskilda vägar, vilket innebär att Trafikverket kommer att behöva byta 1 300 respektive 950 vägmärken. Det beräknas innebära en sammanlagd engångskostnad på ca 30 miljoner kronor för Trafikverket, men det är kostnader som Trafikverket ändå skulle ha haft i och med att vägmärken behöver bytas ut återkommande på grund av att de blir slitna och tappar färg. Skillnaden nu är att i stället för att ersätta ett slitet märke med den gamla versionen av A35 ersätts det av en ny version. Det innebär att kostnaderna för Trafikverket inte går utöver de kostnader som myndigheten redan har för drifts- och underhållsåtgärder.

I egenskap av väghållare för det kommunala vägnätet ansvarar kommunerna för att byta skyltar på kommunala vägar. Enligt uppgifter från Trafikverket beräknas kostnaderna på motsvarande sätt som för kommunerna att bli ca 17 miljoner kronor för ett utbyte av 1 250 vägmärken, men eftersom utbytet kan ske i samband med ordinarie drifts- och underhållsåtgärder över en period på 15 år bedöms det inte medföra några nya kostnader för kommunerna som de inte ändå skulle ha haft. Antalet vägmärken som berörs av förslaget varierar från kommun till kommun. Utifrån uppgiften att det handlar om 1 250 vägmärken totalt som kan bytas ut under 15 år skulle det vid en jämn fördelning av underhållsåtgärder över tid bli fråga om att byta ut 80 märken varje år. Detta antal avser dessutom 290 kommuner, så i flera fall blir det inte ens fråga om att byta ut ett enda vägmärke per kommun och år, även om det givetvis kommer att finnas kommuner som har fler märken än andra. Sammantaget är bedömningen ändå att kostnaderna för förslaget kan anses vara försumbara.

Enligt förslaget får vägmärken och andra anordningar enligt äldre bestämmelser som längst användas till utgången av år 2041. Eftersom vägmärken normalt sett har en livslängd på ca 20 år kommer de allra flesta befintliga vägmärken inte behöva bytas ut under sin ordinarie användningstid.

För både Trafikverkets och kommunernas del är därför bedömningen att några extra kostnader inte kommer att uppstå som en följd av förslaget,

vilket även innebär att det inte föranleder ekonomisk kompensation till kommunerna enligt den kommunala finansieringsprincipen.

Förslaget i denna del innebär en viss påverkan på den kommunala självstyrelsen genom att kommunerna i egenskap av väghållare successivt behöver byta ut varningsmärke A35 på kommunala vägar. Syftet med regleringen är att öka trafiksäkerheten genom tydligare skyltning och förbättra igenkännbarheten av vägmärken vid järnvägskorsningar för trafikanter. Kommunerna ges samtidigt ett betydande handlingsutrymme vid genomförandet, bland annat genom en lång övergångsperiod och möjlighet att samordna utbytet med ordinarie drifts- och underhållsarbete. Inskränkningen i den kommunala självstyrelsen bedöms därför vara begränsad och inte gå utöver vad som är nödvändigt för att uppnå syftet med förslaget, i enlighet med 14 kap. 3 § regeringsformen.

Vad gäller det nya anvisningsmärket E35 kommer det att vara frivilligt för Trafikverket och kommunerna att sätta upp märket, vilket innebär att förslaget inte inskränker den kommunala självstyrelsen i detta avseende. Ändringen av de närmare föreskrifterna till anordning Y3 Bom görs som en följd av att anvisningsmärke E35 införs. Förslaget i dessa delar medför därmed inga nya skyldigheter och således inte heller några tvingande kostnader för vare sig Trafikverket eller kommunerna.

Ändringen av de närmare föreskrifter som anges till vägmarkering M8 utgör endast en redaktionell ändring som inte medför några kostnader eller andra nämnvärda konsekvenser för vare sig Trafikverket eller kommunerna.

Regeringskansliet

Remiss

2026-06-17
LI2026/01197

Landsbygds- och infrastrukturdepartementet
Transportmarknadsenheten

Remittering av promemorian Vägval för framtiden: Justeringar av vägmärken i vägmärkesförordningen (2007:90)

Remissinstanser

1. Bodens kommun
2. Borlänge kommun
3. Bräcke kommun
4. Dorotea kommun
5. Göteborgs stad
6. Hässleholms kommun
7. Höörs kommun
8. Kalmar kommun
9. Karlskoga kommun
10. Knivsta kommun
11. Kungsbacka kommun
12. Ljungby kommun
13. Mariestads kommun
14. Markaryds kommun
15. Mjölby kommun
16. Polismyndigheten
17. Rättviks kommun
18. Simrishamns kommun
19. Smedjebackens kommun

Telefonväxel: 08-405 10 00
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Herkulesgatan 17
E-post: li.registrator@regeringskansliet.se

20. Sorsele kommun
21. Sundbybergs kommun
22. Svalövs kommun
23. Svedala kommun
24. Sveriges kommuner och regioner
25. Säffle kommun
26. Timrå kommun
27. Trafikverket
28. Transportstyrelsen
29. Tranås kommun
30. Uddevalla kommun
31. Umeå kommun
32. Vara kommun
33. Ånge kommun
34. Årjängs kommun
35. Örnsköldsviks kommun

Remissvaren ska ha kommit in till Landsbygds- och infrastrukturdepartementet **senast den 16 oktober 2026**. Svaren bör lämnas per e-post till li.remissvar@regeringskansliet.se och med kopia till li.transport.remissvar@regeringskansliet.se. Ange diarienummer LI2026/01197 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i promemorian.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Promemorian kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss (SB PM 2021:1). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Maria Gelin
Departementsråd

UMEÅ KOMMUN

Tjänsteskrivelse
2026-09-04

Tekniska nämnden

Diarienr: TN-2026/00008

Aktuellt från förvaltningen september

Förslag till beslut

Tekniska nämnden beslutar
att med utgångspunkt från föredragningen ge förvaltningen i uppdrag att …….
att konstatera att inga tilläggsuppdrag läggs med utgångspunkt i föredragningen

Ärendebeskrivning

Förvaltningschefen föredrar aktuellt arbete vid förvaltningen.

Beslutet ska skickas till

UMEÅ KOMMUN

Tjänsteskrivelse
2026-09-07

Tekniska nämnden

Diarienr: TN-2026/00009

Kurser och konferenser september

Förslag till beslut
Tekniska nämnden beslutar

att till protokollet notera att ledamöter och ersättare tagit del av information om kurser och konferenser.

Ärendebeskrivning
Kurser och konferenser inom tekniska nämndens verksamhetsområden presenteras.

Beslutsunderlag
Inga kurser har inkommit.

UMEÅ KOMMUN

Tjänsteskrivelse
2026-08-28

Tekniska nämnden

Diarienr: TN-2026/00005

Delegationsbeslut och anmälningsärenden september

Förslag till beslut
Tekniska nämnden beslutar

att godkänna redovisning av delegationsbeslut och anmälningsärenden.

Ärendebeskrivning
Redovisning av ärenden beslutade med stöd av tekniska nämndens fastställda delegationsordning samt anmälningsärenden.

Beslutsunderlag
Delegationsbeslut gatu- och parkärenden, augusti 2026
- Upplåtelse offentlig plats – tillstånd, lokala trafikföreskrifter, tillstånd/dispenser, övrigt, avgivna remissvar samt yttranden. Bilaga.

Delegationsbeslut fordonsvrak
- Lagen om flyttning av vissa fordon, augusti 2026. Bilaga.

Delegationsbeslut särskild kollektivtrafik/färdtjänst
1. Kommunal färdtjänst, augusti 2026. Bilaga
2. Riksfärdtjänst, augusti 2026. Bilaga
3. Parkeringstillstånd, augusti 2026. Bilaga.

Delegationsbeslut skador
- Anmälda skadeärenden samt beslut. Bilaga.

Delegationsbeslut fastighetsärenden
- Extern förhyrning av lokaler, beslut om antagande av konsulter, entreprenörer och leverantörer för underhålls- och investeringsobjekt inom Fastighetstekniks verksamhetsområde och igångsättningstillstånd, rivning av bebyggda fastigheter, augusti 2026. Bilaga.

Anmälningsärenden
KN Protokollsutdrag ram. Bilaga.

Tjänsteskrivelse

Dnr: TN-2026/00005

Beredningsansvariga

Ulla Nilsson, Tommy Johansson, Martin Nylander, Anna Bugaeva, Frida Herbeck, Åsa Larsson och Annika Kjellsson Lind

UMEÅ KOMMUN

Anmälan av delegationsbeslut

Rubrik/ärendemening:		Beslut på delegation under perioden …… – 2026-08-01 – 2026-08-31	
Ärendetyp	Diarienummer	Beslutsdatum	Delegat (namn och befattning)
Markupplåtelse		Se nedan	

Beskrivning av ärendet

Ärende	Sökande	Avser	Plats	Period	Beslutsdatum
MU_20260817_11106	Ellen Kapstad	Taxor och avgifter: Torghandel: Tillfällig Torghandel	Kungsgatan 53 Renmarkstorget 7	2026-08-24 – 2026-08-24 2026-08-18 – 2026-08-18 2026-09-02 – 2026-09-03	2026-08-17
MU_20260825_11157	Ingrid Larsson	Taxor och avgifter: Torghandel: Tillfällig Torghandel	Kungsgatan 53 Renmarkstorget 7	2026-09-11 – 2026-09-11	2026-08-25
MU_20260618_10891	Selbergs Produktion i Umeå AB	Taxor och avgifter: Bygg och renovering: Grundavgift	Sandbackavägen 24, 26	2026-09-01 – 2027-12-15	2026-08-10
MU_20260827_11170	Umeå kommun, Kommunikationsavd.	Markupplåtelse	Olle Fiskares Väg 13-15	2026-09-05 – 2026-09-25	2026-08-28
MU_20260826_11162	SO Larsson Maskin AB	Taxor och avgifter: Evenemang: Grundavgift	Maskinvisning, Mariehemsängarna	2026-09-04 – 2026-09-04	2026-08-31
MU_20260730_11053	Kommunistiska partiet i Umeå	Markupplåtelse	Rådhustorget, torgmöten Kommunistiska Partiet i Umeå Kungsgatan 59 Rådhusesplanaden 1	2026-08-15 – 2026-08-15 2026-08-22 – 2026-08-22 2026-08-29 – 2026-08-29 2026-09-05 – 2026-09-05 2026-09-12 – 2026-09-12	2026-08-18
MU_20260826_11164	Umeriver Swimrun	Taxor och avgifter: Evenemang: Grundavgift	Umeriver Marathonstafett, Bölesholmarna	2026-09-20 – 2026-09-20	2026-08-27

MU_20260827_11169	KARLA GONZALEZ CHAVEZ	Taxor och avgifter: Tillfällig försäljning: Arealavgift zon 2 0-5 kvm	Slöjdgatan 2 Storgatan 33, 35, 37	2026-08-28 – 2026-10-31	2026-08-27
MU_20260807_11068	Jalles TC Umeå	Taxor och avgifter: Evenemang: Grundavgift	Tegs Centralskola, Löpartävling Björkågatan 2 Bryggargatan 29-43, 34-52 Byvägen 1 Bölevägen 62 Ekvägen 2, 4 Flottargatan 3, 5, 16 Fågelstigen 3, 6, 12, 14 Kardangatan 1 Kråkbärsvägen 9, 11, 16, 18, 20 Lamellgatan 1 Målargränd 15 Norra Obbolavägen 77, 131 Skeppargatan 16 Skiljevägen 3-39, 2-34 Tegsvägen 1 Tranbärsvägen 8 Västra Strandgatan 8 Åkervägen 1-2 Ögatan 3, 5 Övägen 10, 12, 16	2026-10-10 – 2026-10-10	2026-08-28
MU_20260814_11104	Privat	Markupplåtelse	Renmarkstorget, Torgmöte Ambition Sverige Kungsgatan 52-53, 55 Renmarkstorget 7-8, 10, 12	2026-09-05 – 2026-09-05	2026-08-20

MU_20260617_10883	Umeå kommun	Markupplåtelse	Rådhustorget, beredskapsdagen Kungsgatan 54, 59 Rådhusesplanaden 1 Rådhustorget 1, 5 Västra Rådhusgatan 5, 7	2026-09-26 – 2026-09-26	2026-08-28
MU_20260824_11148	Nsm umeå AB	Taxor och avgifter: Bygg och renovering: Grundavgift	Hagaplan 9	2026-08-24 – 2026-09-30	2026-08-26
MU_20260821_11145	matias karlsson	Markupplåtelse	Renmarkstorget, litteraturvagnar Kungsgatan 53	2026-09-04 – 2026-09-05 2026-09-11 – 2026-09-12 2026-09-18 – 2026-09-19 2026-09-25 – 2026-09-26	2026-08-24
MU_20260617_10889	Umeå Teaterförening	Taxor och avgifter: Reklam, skyltar och affischer: Grundavgift	Vid befintlig anordning för banderoller vid Kungsgatan 58/65 Kungsgatan 65	2026-08-25 – 2026-09-11	2026-08-05
MU_20260819_11130	D&M Handelsbolag	Taxor och avgifter: Tillfällig försäljning: Grundavgift	Slöjdgatan 2 Storgatan 35, 37, 48	2026-08-22 – 2026-09-30	2026-08-20
MU_20260818_11117	LIBERALERNAS KOMMUNFÖRENING I UMEÅ	Markupplåtelse	Rådhustorget, Torgmöte med tal, Liberalerna Kungsgatan 59 Rådhusesplanaden 1	2026-08-17 – 2026-09-13	2026-08-20
MU_20260819_11132	Ola Ling Slöjd AB	Taxor och avgifter: Bygg och renovering: Grundavgift	Klintvägen/Köksvägen, byggetablering Klintvägen 1, 3, 9-10 Köksvägen 11 Ålderstigen 2	2026-09-08 – 2026-09-09	2026-08-20
MU_20260820_11137	Ellen Kapstad	Taxor och avgifter: Torghandel: Tillfällig Torghandel	Rådhustorget 5	2026-09-25 – 2026-09-25	2026-08-20

MU_20260820_11136	Ellen Kapstad	Taxor och avgifter: Torghandel: Tillfällig Torghandel	Rådhustorget 5	2026-09-17 – 2026-09-18 2026-09-21 – 2026-09-24	2026-08-20
MU_20260724_11036	Umeå Pastorat, kyrkogårdsförvaltn.	Taxor och avgifter: Bygg och renovering: Arealavgift zon 3	Korsningen Västerlånggatan/Kungsgatan, container Kungsgatan 21, 23 Västergatan 3, 5, 7	2026-07-24 – 2026-10-31 2027-04-01 – 2027-04-30	2026-08-17
MU_20260814_11098	Larssons Måleri AB	Taxor och avgifter: Bygg och renovering: Grundavgift	Operaplan 1, byggetablering Vasagatan 21 Västra Norrlandsgatan 19	2026-08-17 – 2026-10-31	2026-08-17
MU_20260811_11085	Privat	Markupplåtelse	Rådhustorget, tal KD Kungsgatan 59 Rådhusesplanaden 1	2026-08-18 – 2026-09-12	2026-08-11
MU_20260814_11099	Larssons Måleri AB	Taxor och avgifter: Bygg och renovering: Arealavgift zon 3	Brogatan 2A, byggetablering Brogatan 2	2026-08-17 – 2026-10-31	2026-08-14
MU_20260813_11092	Moderata samlingspartiet i AC-län	Markupplåtelse	Rådhustorget, Torgmöten inför valet, Moderaterna Kungsgatan 59 Rådhusesplanaden 1	2026-08-17 – 2026-09-12	2026-08-13
MU_20260813_11093	Moderata samlingspartiet i AC-län	Markupplåtelse	Rådhustorget, kampanjarbete utanför valstuga, Moderaterna Rådhustorget 5	2026-08-17 – 2026-09-13	2026-08-13
MU_20260806_11067	Privat	Markupplåtelse	Valaffishering, Kristdemokraterna Rådhustorget 1	2026-08-16 – 2026-09-19	2026-08-06

MU_20260729_11050	Privatperson	Markupplåtelse	Affischering, privatperson Rådhustorget 1	2026-08-16 – 2026-09-20	2026-08-05
MU_20260730_11052	Arbetarpartiet	Markupplåtelse	Valaffischering, Arbetarpartiet Rådhustorget 1	2026-08-16 – 2026-09-20	2026-08-05
MU_20260811_11084	Privat	Markupplåtelse	Rådhustorget, sammankomst vid valstuga KD Rådhusesplanaden 1 Rådhustorget 1, 5 Västra Rådhusgatan 7	2026-08-15 – 2026-09-16	2026-08-11
MU_20260728_11049	Islams Ahmadiyya Församling	Markupplåtelse	Rådhustorget, fråga en muslim Kungsgatan 59, 61, 63 Rådhusesplanaden 1-2 Rådhustorget 1, 5 Västra Rådhusgatan 7	2026-09-26 – 2026-09-26 2026-10-31 – 2026-10-31 2026-11-24 – 2026-11-24 2026-12-22 – 2026-12-22	2026-08-11

UMEÅ KOMMUN

Anmälan av delegationsbeslut

Rubrik/ärendemening:			Beslut på delegation under perioden …… – 2026-08-01 – 2026-08-31
Ärendetyp	Diarienummer	Beslutsdatum	Delegat (namn och befattning)
Lokala trafikföreskrifter		Se nedan	

Beskrivning av ärendet

Ärende	Sökande	Avser	Plats	Period	Beslutsdatum
TF_20260828_11177		förbud mot trafik med motorfordon på	Verkstadsgatan	2026-09-01 – 2026-09-25	2026-08-28
TF_20260623_10916		högsta tillåten hastighet på	ensklid väg mellan väg AC 523 och väg AC 522	2026-08-24 –	2026-08-19
TF_20250909_9528		högsta tillåten hastighet på	Anna Grönfeldts gata	2026-08-12 –	2026-08-11

DELEGATIONSBESLUT 2026-08-01--2026-08-31

UPPLÅTELSE AV OFFENTLIG PLATS

Yttrande enligt allmänna lokala ordningsföreskrifter §2, upplåta offentlig plats för hithörande ändamål och torghandel

Se ISY-Case MU

Meddela lokala trafikföreskrifter för Umeå kommun enligt TrF 10, kap 1, 3 och 14 §§ och TrF 3 kap 17 §

Meddela undantag från lokala trafikföreskrifter för Umeå kommun enligt TrF 13 kap 3, 4 och 5 §§

Se ISY-Case LTF

Beslut om transportdispens för tung och bred transport, norra timber	TN-2026/00648
Beslut om transporttillstånd gällande bred transport inom Umeå kommun TRV2026/82732	TN-2026/00651

Avtal och Ramavtal Projekt

Angivna remissvar och yttranden

Remissyttrande TEGLET 6 (Murbruksvägen 4), BN 2026-000596	TN-2026/00020
Remissvar Transportdispens TRV 2026/88084, Gävle-Umeå	TN-2026/00678
Remissvar TRV2026/72734, Kiruna-Sundsvall	TN-2026/00606
Remissvar TRV2026/81166, Grästorp-Umeå	TN-2026/00639
Remissvar TRV2026/81245, Österåker-Umeå ToR	TN-2026/00663
Remissvar TRV2026/82068, inom Umeå kommun	TN-2026/00645
Remissvar TRV2026/87752, Holmsund-Boden	TN-2026/00669
Yttrande angående transportdispens TRV2026/83806, Gällivare-.Umeå ToR	TN-2026/00662
Yttrande i ärende 2760-2025, Förslag om lokala trafikföreskrifter om busshållplats väg 661	TN-2026/00642
Yttrande om bred transport TRV2026/82375, Österåker-Säbyviken	TN-2026/00666
Yttrande om tung, bred och lång transport TRV 2026/79646, Sundsvall-Luleå ToR	TN-2026/00623

Ärendenr.	Ärendetitel	Kommentar
TN-2026/00440	Backenvägen, skadat bullerplank vid snöröjning	20260806 Avslag
TN-2026/00625	Bruksgatan, skadad postlåda vid gräsklippning	20260812 Godkänd

Observationstyp	Adress	Datum	Flyttningsgrund	Marktyp	Diarienummer
FORDONSVRAK	Kärrvägen 13A	2026-08-04	Ett fordonsvrak (2 § 1 st 7.)	Tomtmark	UK260804-134822874
FORDONSVRAK	Spårvägen 24	2026-08-05	Ett fordonsvrak (2 § 1 st 7.)	Tomtmark	UK260805-103312917
FORDONSVRAK	Spårvägen 24	2026-08-05	Ett fordonsvrak (2 § 1 st 7.)	Tomtmark	UK260805-102744292
FORDONSVRAK	Spårvägen 24	2026-08-05	Ett fordonsvrak (2 § 1 st 7.)	Tomtmark	UK260805-085310627

Umeå kommun
Click here to enter text.

Protokollsutdrag
Click here to enter text.

§ 47

Diarienr: KU-2026/00038

Sveriges depåbibliotek och lånecentral - teknisk ramjustering och fördelning av statsbidrag

Beslut

Kulturnämnden beslutar

att den del av statsbidraget från Kungliga biblioteket, som idag tillfaller Sveriges depåbibliotek och lånecentral (SDLC), tillfaller tekniska nämnden från och med 2027-01-01. Summan uppgår till 2 175 000 kronor vilket motsvarar kostnaden för lokalerna som SDLC bedriver sin verksamhet i.

att föreslå kommunstyrelsen att besluta om en teknisk ramjustering om 1 647 000 kr från tekniska nämnden till kulturnämnden, motsvarande kostnaden för de lokaler som Sveriges depåbibliotek och lånecentral (SDLC) bedriver verksamhet i, med anledning av att tekniska nämnden i stället får del av statsbidraget för lokalkostnaderna kopplat till verksamheten. Förändringen börjar gälla 2027-01-01.

Ärendebeskrivning

Under 2027 kommer Sveriges depåbibliotek och lånecentral (SDLC), en verksamhet som finansieras av Kungliga biblioteket via statsbidrag och som idag har sina lokaler på Nygatan IDUN1 samt ingår i kulturnämndens grunduppdrag att utöka sin verksamhet här i Umeå. Med utökningen kommer en ny lokalisering att tillkomma.

I samband med kommunstyrelsens beslut att avskaffa interna affärer (2015-12-01 § 361) var det den nämnd som bedrev verksamhet och stod för den externa kostnaden som erhöll den ekonomiska ramen för kostnaderna. Det gällde även statligt finansierad verksamhet. Medel för att täcka lokalkostnaden för depåbiblioteket och lånecentralen återfinns därför i tekniska nämndens budgetram medan kulturnämnden rekvirerar och erhåller statsbidrag för alla kostnader inklusive lokalkostnaden.

Kommunstyrelsen har fattat beslut om en ny princip (2021-02-09 §17) som är vägledande när det gäller hur enskilda frågor som kvarstår efter avskaffandet av interna affärer ska lösas. Av beslutet framgår att intäkter och kostnader bör följas åt så långt det är möjligt, samt att statsbidrag som berör flera nämnder ska fördelas.

Mot bakgrund av detta föreslås att den ram som tekniska nämnden fick i samband med avskaffandet av interna affärer för att täcka lokalkostnader avseende SDLC justeras till kulturnämnden. Tekniska nämnden får i stället del av det statsbidrag som kulturnämnden erhåller för verksamheten.

Kulturnämnden har en sammanhållande roll och beslutar om fördelning av statsbidrag mellan kulturnämnden och tekniska nämnden, där tekniska nämnden erhåller statsbidrag motsvarande kostnaderna för den lokal som SDLC bedriver verksamhet i. Nuvarande lokalkostnader är årligen 2 000 tkr för hyra, 15 tkr för el och 160 tkr för städ. Inför 2027 tillkommer indexreglering för hyra och el.

I samband med att SDLC utökar sin verksamhet kommer kulturnämnden att besluta om en ny fördelning av statsbidraget mellan kulturnämnden och tekniska nämnden med samma princip. Finansiering av lokalkostnader under tekniska nämnden finansieras av en del av statsbidraget och verksamhetskostnader under kulturnämnden finansieras av en del av statsbidraget. På samma sätt kommer förändringar av lokalnyttjande att medföra ett beslut om förändring av fördelning av statsbidraget. Årlig indexering av lokalkostnader kommer också att ske.

Beredningsansvariga

Peter Gustavsson, controller
Marcus Bystedt, ekonomichef

Kulturnämndens beslutsordning

Ordförande finner att nämnden beslutar i enlighet med förvaltningens förslag.

Beslutet ska skickas till
ksdiarium@umea.se

Umeå kommun
Click here to enter text.

Protokollsutdrag
Click here to enter text.

Justerares sign:

Utdraget bestyrks:

Beslutsdatum	BeslutsID	ÄrendeID	Ärendetyp	Utfall	Antal
2026-08-03	389830	457599	Färdtjänst	Bifall	1
2026-08-03	390376	457942	Färdtjänst	Avslag	1
2026-08-03	390448	456046	Färdtjänst	Bifall	1
2026-08-03	390449	458164	Färdtjänst	Bifall	1
2026-08-04	389477	457284	Färdtjänst	Avslag	1
2026-08-04	389571	457367	Färdtjänst	Återtagen ansökan	1
2026-08-04	390405	458127	Färdtjänst	Bifall	1
2026-08-04	390442	458159	Färdtjänst	Bifall	1
2026-08-04	390452	458166	Färdtjänst	Bifall	1
2026-08-04	390453	458169	Färdtjänst	Bifall	1
2026-08-04	390454	458170	Färdtjänst	Bifall	1
2026-08-05	390443	458160	Färdtjänst	Bifall	1
2026-08-05	390445	458161	Färdtjänst	Bifall	1
2026-08-05	390446	458162	Färdtjänst	Bifall	1
2026-08-05	390457	458177	Färdtjänst	Bifall	1
2026-08-05	390460	444685	Färdtjänst	Bifall	1
2026-08-06	389500	457301	Färdtjänst	Bifall	1
2026-08-06	390441	458156	Färdtjänst	Bifall	1
2026-08-06	390458	458178	Färdtjänst	Bifall	1
2026-08-06	390461	458180	Färdtjänst	Bifall	1
2026-08-06	390462	458181	Färdtjänst	Bifall	1
2026-08-06	390463	458182	Färdtjänst	Bifall	1
2026-08-10	390469	458189	Färdtjänst	Bifall	1
2026-08-10	390473	458192	Färdtjänst	Bifall	1
2026-08-10	390474	458193	Färdtjänst	Bifall	1
2026-08-10	390475	458194	Färdtjänst	Bifall	1
2026-08-11	390467	458185	Färdtjänst	Bifall	1
2026-08-11	390480	458157	Färdtjänst	Bifall	1
2026-08-11	390484	458202	Färdtjänst	Bifall	1
2026-08-12	390472	458165	Färdtjänst	Bifall	1
2026-08-12	390483	458201	Färdtjänst	Bifall	1
2026-08-12	390492	458209	Färdtjänst	Bifall	1
2026-08-12	390493	458210	Färdtjänst	Bifall	1
2026-08-13	390485	458203	Färdtjänst	Bifall	1
2026-08-14	390497	458218	Färdtjänst	Bifall	1

2026-08-17	389547	457343	Färdtjänst	Avslag	1
2026-08-17	390491	458208	Färdtjänst	Bifall	1
2026-08-17	390496	458216	Färdtjänst	Bifall	1
2026-08-18	390341	458066	Färdtjänst	Bifall	1
2026-08-18	390396	458092	Färdtjänst	Bifall	1
2026-08-18	390417	457996	Färdtjänst	Avslag	1
2026-08-18	390418	458115	Färdtjänst	Avslag	1
2026-08-18	390529	452885	Färdtjänst	Bifall	1
2026-08-18	390530	449563	Färdtjänst	Bifall	1
2026-08-19	390489	458104	Färdtjänst	Bifall	1
2026-08-19	390527	453597	Färdtjänst	Bifall	1
2026-08-20	390404	458119	Färdtjänst	Bifall	1
2026-08-20	390521	458239	Färdtjänst	Bifall	1
2026-08-20	390544	452203	Färdtjänst	Bifall	1
2026-08-20	390545	455802	Färdtjänst	Bifall	1
2026-08-21	390543	458250	Färdtjänst	Bifall	1
2026-08-21	390548	458258	Färdtjänst	Bifall	1
2026-08-21	390549	455898	Färdtjänst	Bifall	1
2026-08-21	390554	458265	Färdtjänst	Bifall	1
2026-08-24	390515	458230	Färdtjänst	Bifall	1
2026-08-24	390519	458233	Färdtjänst	Bifall	1
2026-08-24	390520	458238	Färdtjänst	Bifall	1
2026-08-24	390552	458264	Färdtjänst	Bifall	1
2026-08-24	390563	454545	Färdtjänst	Bifall	1
2026-08-25	389574	457370	Färdtjänst	Avslag	1
2026-08-25	390419	458116	Färdtjänst	Avslag	1
2026-08-25	390464	458156	Färdtjänst	Avslag	1
2026-08-25	390537	457875	Färdtjänst	Bifall	1
2026-08-25	390568	458274	Färdtjänst	Bifall	1
2026-08-25	390569	458274	Färdtjänst	Bifall	1
2026-08-25	390580	458286	Färdtjänst	Bifall	1
2026-08-26	390486	458187	Färdtjänst	Bifall	1
2026-08-26	390564	453060	Färdtjänst	Bifall	1
2026-08-26	390565	454546	Färdtjänst	Bifall	1
2026-08-26	390581	458287	Färdtjänst	Bifall	1
2026-08-27	389942	457700	Färdtjänst	Bifall	1
2026-08-27	390171	457906	Färdtjänst	Bifall	1

2026-08-27	390524	458176	Färdtjänst	Bifall	1
2026-08-27	390526	458243	Färdtjänst	Bifall	1
2026-08-27	390538	458211	Färdtjänst	Bifall	1
2026-08-27	390582	458289	Färdtjänst	Bifall	1
2026-08-27	390586	458297	Färdtjänst	Bifall	1
2026-08-27	390597	458302	Färdtjänst	Bifall	1
2026-08-27	390600	450697	Färdtjänst	Bifall	1
2026-08-28	390466	458184	Färdtjänst	Bifall	1
2026-08-28	390502	458113	Färdtjänst	Bifall	1
2026-08-28	390508	458144	Färdtjänst	Bifall	1
2026-08-28	390523	458241	Färdtjänst	Bifall	1
2026-08-28	390525	458163	Färdtjänst	Bifall	1
2026-08-28	390556	458266	Färdtjänst	Bifall	1
2026-08-31	389985	457742	Färdtjänst	Avslag	1
2026-08-31	390476	458195	Färdtjänst	Avslag	1
2026-08-31	390513	458227	Färdtjänst	Bifall	1
2026-08-31	390528	458231	Färdtjänst	Bifall	1
2026-08-31	390561	458269	Färdtjänst	Bifall	1
2026-08-31	390596	458257	Färdtjänst	Bifall	1
2026-08-31	390602	458306	Färdtjänst	Bifall	1
2026-08-31	390605	453743	Färdtjänst	Bifall	1
2026-08-04	390426	458091	Parkeringstillstånd	Bifall	1
2026-08-05	390450	458167	Parkeringstillstånd	Bifall	1
2026-08-06	390425	458137	Parkeringstillstånd	Bifall	1
2026-08-13	390451	458153	Parkeringstillstånd	Bifall	1
2026-08-17	390498	458219	Parkeringstillstånd	Bifall	1
2026-08-18	390416	458136	Parkeringstillstånd	Avslag	1
2026-08-18	390501	458224	Parkeringstillstånd	Bifall	1
2026-08-20	390477	458197	Parkeringstillstånd	Bifall	1
2026-08-20	390546	458256	Parkeringstillstånd	Bifall	1
2026-08-24	390511	458214	Parkeringstillstånd	Bifall	1
2026-08-26	390284	458025	Parkeringstillstånd	Avslag	1
2026-08-26	390394	458103	Parkeringstillstånd	Bifall	1
2026-08-27	390344	458068	Parkeringstillstånd	Avslag	1
2026-08-28	390558	458263	Parkeringstillstånd	Bifall	1
2026-08-04	390455	458171	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-05	390459	458174	Riksfärdtjänst Tillstånd	Bifall	1

2026-08-10	390470	458190	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-11	390479	458198	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-11	390488	458206	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-12	390434	458150	Riksfärdtjänst Tillstånd	Avslag	1
2026-08-12	390471	458191	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-13	390487	458205	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-17	390510	458213	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-18	390499	458223	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-18	390500	458222	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-27	390403	458125	Riksfärdtjänst Tillstånd	Avslag	1
2026-08-28	390567	458273	Riksfärdtjänst Tillstånd	Bifall	1
2026-08-31	390495	458191	Riksfärdtjänst Tillstånd	Avslag	1
2026-08-31	390595	458293	Riksfärdtjänst Tillstånd	Bifall	1
					122
Total					**122**