Kommunrevisorerna granskar

Kommunens hantering av skyddade personuppgifter

2023-12-14

UMEÅ KOMMUN

Angående granskningen

Revisionsuppdraget är ett kommunalt förtroendeuppdrag och revisorerna är direkt ansvariga inför kommunfullmäktige och därmed indirekt inför medborgarna genom den representativa demokratin. Revisionen har uppdrag att granska de verksamheter som styrelser, nämnder och kommunala bolag bedriver.

I formell mening är varje revisor en egen myndighet, men i det praktiska revisionsarbetet sker arbetet gemensamt.

Ytterst syftar revisionen till att undersöka om verksamheten bedrivs i enlighet med uppställda mål och på ett från ekonomisk synpunkt tillfredsställande sätt.

- Revisorernas uppdrag regleras i kommunallag, aktiebolagslag, god revisionssed, ägardirektiv och reglemente.
- Revision ska utföras på ett oberoende sätt.
- Revisorerna genomför grundläggande granskning, granskning av delårsrapport och årsredovisning och fördjupade granskningar.

Revisorerna ska därför objektivt, opartiskt och sakligt, självständigt granska den verksamhet som styrelse, nämnder och beredningar bedriver. Revisorerna ska också bedöma om de förtroendevalda ledamöterna i nämnder och styrelser har tillräcklig styrning och kontroll över verksamhetens ekonomi, prestationer och kvalitet.

Revisorernas uttalanden och bedömningar finns i revisionsberättelser och granskningsrapporter. En ambition i revisorernas arbete är att deras rekommendationer i samband med granskning ska kunna användas av verksamheterna för att åstadkomma effekter i deras förbättringsprocess.

Kontaktuppgifter

Om kommunrevisorernas uppdrag

kommunrevisionen@umea.se

Ordförande i kommunrevisionen

Ewa Miller, ordförande
ewa.miller@umea.se

Umeå kommun

Granskning av kommunens hantering
av skyddade personuppgifter

Building a better working world

Innehåll

1. Sammanfattande bedömning och rekommendationer

Revisorerna har gett det sakkunniga biträdet från EY i uppdrag att granska kommunens hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur kommunen säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade. Detta har avsett skyddade personuppgifter för såväl anställd personal som för kommuninvånare. Granskningen har omfattat kommunstyrelsen, gymnasie- och vuxenutbildningsnämnden, för- och grundskolenämnden, individ- och familjenämnden, fritidsnämnden samt kulturnämnden.

Vår sammanfattande bedömning är att kommunstyrelsen och de granskade nämnderna inte har säkerställt att skyddade personuppgifter inte röjs till obehöriga.

Respektive verksamhet har vidtagit diverse åtgärder i sitt löpande arbete för att förhindra röjning av skyddade personuppgifter. Detta är delvis inom det ordinarie sekretessarbetet som omfattar alla kommuninvånare, men även riktade åtgärder. Inom ramen för det riktade arbetet har verksamheterna på eget initiativ och i varierande grad upprättat rutinbeskrivningar och processer för hanteringen av skyddade personuppgifter. Dessa utgör ett värdefullt stöd i sammanhanget, men vi noterar att de endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter och vår bedömning är att de har utrymme för utveckling. Vi bedömer det därtill vara aktuellt att göra en översyn av det stora antalet rutinbeskrivningar. Vi har också identifierat förbättringsområden i hanteringen av skyddade personuppgifter, däribland striktare behörighetsbegränsningar i IT-system och mindre manuell hantering.

Det finns ingen kommunövergripande styrning inom området och de granskade nämnderna har inte heller beslutat om egna styrdokument. Vår bedömning är att även med hänsyn till Umeå kommuns styrmodell är en politiskt beslutad strategisk inriktning inom området nödvändig. Varken kommunstyrelsen eller de granskade nämnderna har gjort någon uppföljning inom området avseende exempelvis enheternas arbetsrutiner, kompetensutveckling eller avvikelsehantering. Det har heller inte genomförts risk- och konsekvensanalyser avseende röjning av skyddade personuppgifter inom ramen för internkontrollarbetet. Således bedömer vi att kommunstyrelsen och granskade nämnder inte har säkerställt att ett ändamålsenligt arbete bedrivs.

Det genomförs ingen systematisk och kommunövergripande fortlöpande kompetensutveckling inom området och det finns inget särskilt utrymme för rutinförankring. Enheterna genomför själva en viss rutinförankring och kompetensutveckling genom att löpande behandla frågan internt på möten och i enstaka fall genom andra riktade kompetensutvecklingsinsatser. Vår bedömning är dock att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid. Det skulle stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn vilket enligt oss är den största risken i hanteringen av skyddade personuppgifter.

Avvikelser avseende skyddade personuppgifter behandlas i samma process som andra personuppgiftsincidenter. Då incidenter avseende skyddade personuppgifter inte särskiljs från andra personuppgiftsincidenter finns en risk att förutsättningarna för uppföljning av incidenter, särskilt från nämndernas sida, blir sämre.

Kommunstyrelsen rekommenderas att:

- Upprätta och anta ett kommunövergripande styrdokument för hanteringen av skyddade personuppgifter. Ett sådant styrdokument, exempelvis i form av en riktlinje, bör omfatta inriktningen för arbetet både kommunens kunder och dess medarbetare på en strategisk nivå.

Utifrån granskningens iakttagelser rekommenderar vi kommunstyrelsen och samtliga granskade nämnder att:

- Upprätta risk- och konsekvensanalyser specifikt avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.
- Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Tydliggör riktlinjen i verksamhetsnära rutiner/instruktioner.
- Genomföra regelbundna utbildningar för samtliga medarbetare som hanterar skyddade personuppgifter, exempelvis som en del av ett årshjul. Överväg också att på en övergripande nivå informera samtliga medarbetare om skyddade personuppgifter.
- Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning.
- Skyndsamt implementera krypterad e-post genom tjänsten Säker digital kommunikation i hela kommunen.
- Stärk arbetsrutinerna för användandet av internposten vid hantering av skyddade personuppgifter.
- Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.
- Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.

Utifrån granskningens iakttagelser rekommenderar vi individ- och familjenämnden att:

- Säkerställa att nämnden inte lagrar filer med sekretessmarkerad information på ett sätt som kan strida mot GDPR.

2. Inledning

2.1 Bakgrund

Den som är utsatt för hot kan i vissa fall få skyddade personuppgifter. Antalet personer i Sverige med skyddade personuppgifter har de senaste åren ökat. Mellan åren 2011 och 2023 har antalet personer med skyddade personuppgifter ökat från drygt 12 000 personer till drygt 28 000 personer.[1] Den 1 januari 2019 trädde lagändringar i kraft med syfte att öka skyddet för hotade och förföljda personer.

Jämställdhetsmyndigheten publicerade under år 2022 en rapport (2022:10) där flera våldsutsatta kvinnor intervjuades. 86 kvinnor ingick i urvalet. Av dessa uppgav tre av fyra att de någon gång fått sina skyddade personuppgifter röjda. Hälften av de intervjuade kvinnorna har flyttat minst en gång på grund av röjda uppgifter. Flera kvinnor berättar att deras personuppgifter röjts av till exempel socialtjänsten och andra myndigheter.

Personer med skyddade personuppgifter kan drabbas av mycket allvarliga risker och problem om kommuners verksamheter inte har en ändamålsenlig kontroll över uppgifterna. Kommuner måste därför ha tydliga riktlinjer och kontroller för att hantera skyddade personuppgifter. Det är av väsentlighet att sådana rutiner är välkända bland samtliga medarbetare då i princip samtliga kan komma i kontakt med en person som har skyddade personuppgifter.

Umeå kommuns revisorer har i sin riskanalys för 2023 identifierat hanteringen av skyddade personuppgifter som ett angeläget område för fördjupning och beslutat att genomföra en fördjupad granskning. Lekmannarevisorerna genomför motsvarande granskning i Umeå vatten och avfall AB (inklusive Vakin) samt i Umeå Energi AB.

2.2 Syfte och revisionsfrågor

Granskningen syftar till att bedöma huruvida kommunen säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt bedöma om kommunens rutiner är ändamålsenliga och tillämpas. Granskningen avser skyddade personuppgifter för såväl anställd personal som för kommuninvånare.

I granskningen besvaras följande revisionsfrågor:

- Finns ändamålsenliga styrande dokument och rutiner för hantering av skyddade personuppgifter?
    - Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?
- Har kommunen säkerställt tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?
- Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?
- Har kommunen på ett ändamålsenligt sätt analyserat och bedömt risken för att skyddade personuppgifter röjs?
    - Har den enskilda individens perspektiv beaktats?

[1] SVT, "Kraftig ökning av skyddade personuppgifter", hämtad 2023-12-05.

- Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits med utgångspunkt i dessa analyser?
- Har kommunen vidtagit ändamålsenliga åtgärder för att minska risken för röjning av skyddade personuppgifter och följs detta upp av berörda nämnder?
- Finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter?
    - Hur tillvaratas erfarenhet från avvikelser?

2.3 Ansvariga nämnder och avgränsningar

Granskningen avser kommunstyrelsen, gymnasie- och vuxenutbildningsnämnden, för- och grundskolenämnden, individ- och familjenämnden, fritidsnämnden samt kulturnämnden. Av de kommunala bolagen granskas Umeå vatten och avfall AB (inklusive Vakin) samt i Umeå Energi AB inom ramen för lekmannarevisionen.

2.4 Metod och genomförande

Granskningen baseras på dokumentstudier och intervjuer med berörda tjänstepersoner. Samtliga intervjuade funktioner och granskade underlag framgår av källförteckningen.

Granskningen har följt god revisionssed och har kvalitetssäkrats internt, bland annat genom avstämning mot revisionsfrågor, faktagranskning och strukturerad dokumentation. Utöver intern kvalitetssäkring har samtliga intervjuade haft möjlighet att komma med synpunkter på rapportutkastet, detta för att säkerställa att revisionsrapporten bygger på korrekta uttalanden.

2.5 Revisionskriterier

Med revisionskriterier avses bedömningsgrunder som används i granskningen för analyser, slutsatser och bedömningar. Revisionskriterierna kan hämtas från lagar och förarbeten eller interna regelverk beslutade av fullmäktige/bolagsstämmor. Kriterier kan också ha sin grund i jämförbar praxis eller erkänd teoribildning. I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Kommunallagen (2017:725)
- Offentlighets- och sekretesslagen (2009:400)
- Folkbokföringslagen (1991:481)
- Folkbokföringsfördordning (1991:749)
- SFS 2018:695 Lag om ändring i folkbokföringslagen
- Socialtjänstlagen (2001:453)
- Av fullmäktige antagna styrdokument eller relevanta riktlinjer
- COSO-ramverket för intern kontroll
- Best practice kring bedömning av rutiner och intern kontroll vid hantering av skyddade personuppgifter

Dessa beskrivs närmare i bilaga samt löpande i rapporten.

3. Kontrollmiljö

Kontrollmiljö består exempelvis av etiska värderingar, ledarskapsresurser och ansvarsfördelning inom organisationen. Kontrollmiljö utgör en betydande del av den kultur som finns i organisationen: Är de anställda medvetna om det interna regelverket? Kan de lyfta etiska frågor? Hur agerar de i avsaknad av regler? Här är ledningens riskhanteringsfilosofi, styrprinciper, integritet och etiska värderingar viktiga. Utöver organisationskultur består kontrollmiljön även av styrdokument. En ändamålsenlig kontrollmiljö är avgörande för att minska riskerna vid hantering av skyddade personuppgifter.

3.1 Respektive nämnd är personuppgifts- och informationssäkerhetsansvariga inom sitt verksamhetsområde

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. Personuppgiftskoordinator är ett rådgivande och samordnande stöd till verksamhetens ledning i verksamhetens interna informationssäkerhetsarbete kopplat till personuppgiftshantering. I enlighet med EU:s dataskyddsförordning och nationell dataskyddslagstiftning ska varje nämnd också utse ett dataskyddsombud.

Vidare är varje nämnd ansvarig för informationssäkerheten inom sitt verksamhetsområde vilket innebär att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta innebär att den som är ansvarig för en viss verksamhet – avdelning, enhet, process, projekt och så vidare – också är ansvarig för informationssäkerheten inom verksamhetsområdet. Informationssäkerhetsarbetet leds och samordnas av en informationssäkerhetssamordnare. Denne ansvarar bland annat för:

- att kommunens styrande dokument inom området är aktuella,
- att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet,
- kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom kommunen, till exempel 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,

Kommunens 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. I kommunstyrelsens ledningsfunktion ingår att leda, samordna och utöva tillsyn gällande det kommunövergripande informationssäkerhetsarbetet.

För ytterligare beskrivning av kommunstyrelsens och nämndernas ansvarsområden inom granskningsområdet enligt beslutade reglementen hänvisar vi till bilaga 3.

3.2 Skyddade personuppgifter ska hanteras utifrån särskilda rutiner och regler

Umeå kommuns *Informationssäkerhetspolicy*[2] styr kommunens informationssäkerhetsarbete med syfte att säkerställa hanteringen av verksamhetens information, och är därmed av relevans för hanteringen av skyddade personuppgifter. Av policyn framgår att Umeå kommun aktivt arbetar för att skydda informationstillgångar för att den alltid skall vara konfidentiell, riktig och tillgänglig.

Konfidentiell information får inte nås eller avslöjas för någon obehörig. Riktig information innebär att information inte får obehörigen förändras, inte av misstag och inte på grund av funktionsstörning. Tillgänglig information innebär att informationen går att nå av behörig användare när det behövs och i rätt omfattning.

Målet med Umeå kommuns informationssäkerhetsarbete är att:

- all personal har tillräckliga kunskaper om informationssäkerhet i förhållande till sina arbetsuppgifter,
- informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man,
- informationssäkerhetsarbetet ska bedrivas med tyngdpunkt på risk- och sårbarhetsanalyser samt förebyggande aktiviteter.

Kommunen ska bedriva ett systematiskt informationssäkerhetsarbete med målet att skapa ett ledningssystem för informationssäkerhet. Ett ledningssystem för informationssäkerhet 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. Under 2020 påbörjades arbetet med att etablera ett ledningssystem för informationssäkerhet, som ska vara infört 2027. Viktiga komponenter som får konsekvenser på kommunens hantering av skyddade personuppgifter är informationsklassning, riskanalyser och konsekvensbedömningar av informationstillgångar samt utbildning och uppföljning. Respektive förvaltning ansvarar för att etablera tillräckliga resurser och skapa förutsättningar för att skapa ett ledningssystem för informationssäkerhet.

Därutöver finns *Riktlinjer för informationssäkerhet Umeå kommun,*[3] som kompletterar informationssäkerhetspolicyn med mer detaljerad information och regler för hur information får hanteras inom kommunen. Riktlinjerna gäller för alla verksamheter i Umeå kommun. Riktlinjerna gäller inte för kommunens bolag, utan dessa beslutar om informationssäkerhetspolicy och riktlinjer för informationssäkerhet inom den egna verksamheten. Kommunens riktlinjer för informationssäkerhet utvecklas i kapitel fem.

3.3 Styrande dokument och enhetsspecifika rutinbeskrivningar

3.3.1 Det saknas ett kommunövergripande styrdokument för hanteringen av skyddade personuppgifter

Det finns inget kommunövergripande styrdokument för hantering av skyddade personuppgifter. Intervjuade hänvisar i stället till informationen om hanteringen av hög sekretessinformation som framgår av riktlinjerna för informationssäkerhet. Vid intervjuer har

[2] Fastställd av kommunfullmäktige, reviderad 2013-06-17.

[3] Fastställd av kommunstyrelsen 2021-12-07.

avsaknaden av ett kommunövergripande styrdokument för hanteringen av skyddade personuppgifter bland annat hänvisats till Umeå kommuns styrmodell, där ansvaret i hög grad är delegerat till respektive nämnd och att det inte sker någon central uppföljning av nämndernas arbete med informationssäkerhet. Enligt intervjuade har det inte funnits diskussioner om att upprätta ett kommunövergripande styrdokument specifikt för hanteringen av skyddade personuppgifter.

Rutinen *Hantering av kandidat med skyddade personuppgifter i rekryteringsprocessen*[4] beskriver den processen i detalj. Det finns även en rutin, *Skyddade personuppgifter anställning och lön*[5], som beskriver hantering vid anställning samt lön- och supportärenden för personer med skyddade personuppgifter. Därtill finns ett anställningsunderlag för anonymitetsskyddad anställning i form av en blankett innehållandes uppgifter om anställningen och personen.

I föreskriften *Användning av personuppgifter i form av bilder, filmer, namn och kontaktuppgifter i kommunens kommunikation*[6] beskrivs hur kommunen använder personuppgifter vid kommunikation. Personuppgifter som används i kommunens kommunikation kan till exempel vara bilder och filmer med identifierbara människor, namn och kontaktuppgifter samt information i löpande text. Vad gäller medarbetare och förtroendevalda ska en bedömning ske i samtliga fall om personerna är sekretesskyddade och om det är nödvändigt att använda aktuella personuppgifter vid respektive kommunikationsinsats. Om det finns sekretesskydd eller om användning inte är nödvändig ska personuppgifterna inte användas.

Det finns information om hanteringen av skyddade personuppgifter tillgänglig på kommunens intranät. Denna inkluderar information om olika typer av skyddade personuppgifter och rekommendationer om hur skyddade personuppgifter bör hanteras. Bland annat framgår posthantering till personer med skyddade personuppgifter. Utöver vad som anges av riktlinjerna för informationssäkerhet framgår att:

- En riskbedömning ska göras från fall till fall då behovet av vilka uppgifter som behöver särskilt skydd varierar.
- Den personuppgiftsansvarige bör begränsa åtkomsten till de skyddade personuppgifter till ett fåtal personer.
- Den personuppgiftsansvarige bör tillse att skyddade personuppgifter inte okontrollerat sprids mellan olika verksamhetssystem som utbyter data. Detta då det är viktigt att skyddade personuppgifter inte sprids till ett system med sämre säkerhet. Den personuppgiftsansvarige är skyldig att vidta lämpliga säkerhetsåtgärder (med hänsyn till den riskbedömning som gjorts avseende behandlingen).
- All personal som kommer i kontakt med skyddade personuppgifter måste få kunskap om de regler och rutiner som gäller.

Intervjuade inom stadsledningskontoret påtalar också att de bistår med råd och stöd till verksamheterna genom att exempelvis svara på inkomna frågor vid behov. Det har inte skett i någon stor utsträckning.

[4] Godkänd av HR-direktör, reviderad 2023-02-12.

[5] Godkänd av lönechef 2022-04-05.

[6] Fastställd av kommunfullmäktige 2018-05-28.

3.3.2 De granskade nämnderna har inte beslutat om styrdokument för hanteringen av skyddade personuppgifter

De granskade nämnderna har inte beslutat om några styrdokument inom området. Förvaltningarna har dock tagit fram egna rutinbeskrivningar. I tabellen nedan redogörs ett utdrag av förvaltningarnas upprättade rutinbeskrivningar.[7]

Ansvarig enhet	Godkänd av	Rutinbeskrivning
Utbildningsförvaltningen	Bitr. utbildningsdirektör	*Rutin för elever med skyddade personuppgifter i UGS* (Umeå kommuns gymnasieskolor)
Utbildningsförvaltningen	Bitr. utbildningsdirektör	*Handlingsplan för elev med skyddade personuppgifter*
Utbildningsförvaltningen	Utbildningsdirektör	*Kvarskrivning*
Utbildningsförvaltningen	Bitr. utbildningsdirektör	*Rutin för hantering av skyddade personuppgifter i för- och grundskola*
Utbildningsförvaltningen	Administrativ chef gymnasieskola	*Administrativ hantering av elever med skyddade personuppgifter UGS* (Umeå kommuns gymnasieskolor)
Utbildningsförvaltningen	Utbildningsdirektör	*Sekretessmarkering*
Utbildningsförvaltningen	Utbildningsdirektör	*Skyddade personuppgifter – Vad verksamheterna bär tänka på*
Utbildningsförvaltningen	Enhetschef administration vuxenutbildning	*Rutin – Elev med skyddade personuppgifter* (Centrum för vuxenutbildning)
Stöd- och omsorgsförvaltningen	Framgår ej	*Treserva lathund – Skyddade personuppgifter*
Stöd- och omsorgsförvaltningen	SAS, MAS och MAR	*Behörighetsbeställning Treserva, anställd med skyddade personuppgifter*
Stöd- och omsorgsförvaltningen	SAS	*Åtkomst till och särskilt skydd av uppgifter i Treserva*
Stöd- och omsorgsförvaltningen	Systemförvaltningsledningen	*Rutin för behörigheter till Externa utförare LSS- Prator*
Stöd- och omsorgsförvaltningen	Framgår ej	*Skyddad identitet – bemanning stöd och omsorg*
Stöd- och omsorgsförvaltningen	Bitr. verksamhetschef myndighetsutövning & verksamhetschef utredning äldre	*Skyddade personuppgifter*
Stöd- och omsorgsförvaltningen	Individ- och familjenämnden	*Riktlinje för Individ- och familjenämndens arbete med våld i nära relationer och hedersrelaterat våld*
Stöd- och omsorgsförvaltningen	Bitr. Verksamhetschef Myndighetsutövning	*Våld i nära relation*
Stöd- och omsorgsförvaltningen & Utbildningsförvaltningen	Utbildningsdirektör & verksamhetschef myndighet	*Samverkansrutin mellan socialtjänst och grundskola samt gymnasieskola, ungdomar placerade i familjehem eller HVB*

[7] Tabellen är inte fullständig. Det finns ytterligare detaljerade rutinbeskrivningar som rör hanteringen av skyddade personuppgifter, exempelvis i olika IT-system.

Stöd- och omsorgsförvaltningen	Bitr. Verksamhetschef myndighetsutövning	*Personakt och dokumenthantering IFN*
Stöd- och omsorgsförvaltningen	Bitr. Verksamhetschef myndighetsutövning	*LVU – ansökan om vård samt omedelbart omhändertagande*
Kulturförvaltningen	Enhetschef Umeå stadsbibliotek	*Skyddade personuppgifter*
Kulturförvaltningen	Urax (Bibliotekssamarbetet inom Umeå kommun)	*Gemensamma regler för Umeåregionens folkbibliotek*

Fritidsförvaltningen har inte upprättat någon arbetsrutin för hanteringen av skyddade personuppgifter.

Rutinbeskrivningarna benämns på flera olika sätt, exempelvis rutiner/instruktioner och regler/föreskrifter och olika funktioner har fastställt dokumenten. Utifrån *Riktlinjer för styrande dokument*[8] ska policy eller regler/föreskrifter beslutas av kommunfullmäktige och beskriver kommunens olika regelverk som måste följas vid genomförande och/eller handläggning med mera. Vissa regler/föreskrifter kan beslutas av nämnd. En riktlinje ska beslutas av nämnd och stödjer organisationen så att den bedriver sin verksamhet på rätt sätt. Genomförandeplaner, handlingsplaner och rutiner/instruktioner ska beslutas på tjänstepersonnivå. En rutin/instruktion är en detaljerad beskrivning av hur olika aktiviteter/processer ska handläggas eller genomföras. Frågeställningarna "Hur och av vem" besvaras av rutiner/instruktioner. De upprättas på olika nivåer och fastställs av chef.

Av genomförda intervjuer framkommer flera anledningar till att de granskade nämnderna inte har beslutat om några styrdokument inom området. Däribland med hänvisning till kommunens riktlinjer för styrande dokument, där verksamheterna beskriver de upprättade rutinbeskrivningarna som rutiner/instruktioner och därför ska beslutas på tjänstepersonnivå. Flertalet intervjuade inom förvaltningarna upplever att nämnden lämpligen inte bör besluta om en riktlinje för arbetet i frågan då området är verksamhetsnära. Nuvarande rutinbeskrivningar har upprättats på en verksamhetsnära nivå genom ett behov utifrån identifierade brister i arbetssätt av de tjänstepersoner som kommer i kontakt med skyddade personuppgifter. De har således inte upprättats utifrån genomförd riskanalys eller på uppdrag av ansvarig nämnd eller förvaltningsledning.

Vissa intervjuade uppger dock att det eventuellt finns ett behov av en mer övergripande riktlinje för att tydliggöra och styra arbetet med skyddade personuppgifter, i kombination med verksamhetsnära rutiner/instruktioner som beskriver praktiska detaljer kring hanteringen av skyddade personuppgifter.

Vad gäller de upprättade rutinbeskrivningarna framgår av intervjuade att intranätets sökfunktion efter rutinbeskrivningar inte är användarvänlig. Det är exempelvis svårt att hitta rutinbeskrivningarna, som kräver specifika sökord. Detta resulterar i att det är svårt att hitta rätt rutinbeskrivningar och ökar risken för felhantering av skyddade personuppgifter. Därtill finns kritik mot det stora antalet rutinbeskrivningar, vilket enligt intervjuade riskerar att skapa förvirring i stressade situationer. Till sist saknar vissa rutinbeskrivningar nödvändig information, eller innehåller skrivningar som inte efterlevs av respektive part.

[8] Fastställd av kommunstyrelsen 2017-05-16.

3.4 Det finns behov av ytterligare kompetensutveckling

Av riktlinjerna för informationssäkerhet framgår att det i informationssäkerhetssamordnarens roll bland annat ingår kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom kommunen, till exempel genom rådgivning och utforma utbildning. Chefer har dock ansvaret att delge information och erbjuda utbildning i informationssäkerhetsfrågor till sina medarbetare. Nyanställda ska via anställande chef delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet. Delgivning och utbildning ska också ges kopplat till annat ansvar som följer med rollen, till exempel informationsägarskap. Det framgår inte om specifik utbildning ska ges kopplat till hanteringen av skyddade personuppgifter. Av information om skyddade personuppgifter på kommunens intranät framkommer att all personal som kommer i kontakt med skyddade personuppgifter måste få kunskap om de regler och rutiner som gäller. Det framgår dock inte vilken funktion som ansvarig för detta.

I kommunen finns vissa kommunövergripande utbildningar som är av relevans för området. Det finns bland annat NANO-utbildningar för samtliga nyanställda kring hantering av GDPR och om informationssäkerhet. Dessa omfattar bland annat offentlighet, sekretess och vikten av att hantera personuppgifter korrekt, men inte specifik information om skyddade personuppgifter. Stadsledningskontoret ansvarar för dessa utbildningar. Det är dock varje enskild enhetschef som ska tillse att medarbetare medverkar på tillräckliga utbildningar och stadsledningskontoret gör inga kontroller av efterlevnad. Intervjuade inom stadsledningskontoret uppger att det inte finns något praktiskt hinder att inkludera hanteringen av skyddade personuppgifter i dessa utbildningar.

Respektive förvaltning hanterar kompetensutveckling av medarbetare på olika sätt. Utbildningsförvaltningen har inte några särskilda utbildningar för hanteringen av skyddade personuppgifter. Administratörer och andra berörda medarbetare som hanterar skyddade personuppgifter inom gymnasie- och vuxenutbildningsnämndens ansvarsområde informeras exempelvis via nyhetsbrev som sedan sprids till bland annat rektorer och elevhälsan. Det är dock inget uttalat ansvar utan sker på individuellt initiativ. Därutöver vilar stort ansvar på respektive rektor att informera berörd personal om tillgängliga rutiner och omvärldsbevakning inom området. Arbetsmarknad- och integrationsavdelningen, som organiseras under gymnasie- och vuxenutbildningsnämnden, har upprättat utbildningsmaterial baserat på egna samt Jämställdhetsmyndighetens erfarenheter och information från Skatteverket som samtliga medarbetare ska ta del av innan årsskiftet 2024. Samma information kommer ges fortlöpande till samtliga nyanställda.

Ingen enhet inom stöd- och omsorgsförvaltningen har regelbundna utbildningar som specifikt behandlar skyddade personuppgifter. En introduktion genomförs för alla nyanställda där det tydliggörs hur arbete ska bedrivas och var relevanta dokument går att återfinna. Skyddade personuppgifter ingår i denna introduktion. Därutöver sker diskussioner på arbetsplatsträffar och interna möten där frågan ibland behandlas, dock med varierad frekvens från enhet till enhet. Informationstillfällen om GDPR och dataskydd har förts in i årshjulet och intervjuade är öppna för att motsvarande skulle kunna införas för skyddade personuppgifter. Intervjuade hänvisar därutöver till stor noggrannhet och försiktighet vid behandling av samtliga personuppgifter utifrån gällande sekretessbestämmelser vid handläggning av ärenden eller insatser inom socialtjänst eller hälso- och sjukvård.

De medarbetare inom kulturförvaltningen som hanterar skyddade personuppgifter ska enligt intervjuade i december 2023 delta i en utbildning om skyddade personuppgifter hos

Skatteverket. I övrigt ingår hanteringen av skyddade personuppgifter vid introduktionen av nyanställda. Inom fritidsförvaltningen ingår hanteringen av skyddade personuppgifter som en del av introduktionsprogrammet för nyanställda. Därefter åligger det respektive chef att utbilda medarbetare kontinuerligt vid behov.

Intervjuade chefer på olika nivåer i förvaltningarna uttrycker önskemål om att information om och hanteringen av skyddade personuppgifter ska inkluderas i nuvarande chefsutbildning då det är ett bra forum för kompetensutveckling.

En allmän uppfattning bland de intervjuade är att arbetet med rådande arbetsrutiner fungerar bra och att medarbetare som behöver vara väl insatta i arbetet också är det. Intervjuade upplever att det finns en god kunskap om hur arbetet med skyddade personuppgifter ska bedrivas och att medarbetare kan be om hjälp vid behov.

Varken kommunstyrelsen eller de granskade nämnderna har dock gjort någon särskild uppföljning av arbetet med skyddade personuppgifter avseende kompetensutveckling och rutinförankring.

3.5 Bedömning

Vår bedömning är att det saknas ändamålsenliga styrande dokument för hantering av skyddade personuppgifter. Det finns kommunövergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen, men då dessa innehåller få skrivningar om hanteringen av skyddade personuppgifter, i kombination med att det inte finns ett beslutat kommunövergripande styrande dokument specifikt för hanteringen av skyddade personuppgifter, bedömer vi det inte vara tillräckligt. Vi noterar att det finns både kommunövergripande rutinbeskrivningar samt information om skyddade personuppgifter på kommunens intranät som berör HR-processerna. Vår bedömning är att avsaknaden av övergripande styrdokument utgör en svaghet i arbetet. Givet att det är ett område som kräver stor varsamhet och att det inte alltid finns en tillräcklig insyn i frågan på verksamhetsnivå är vår bedömning att det bör beslutas om ett övergripande styrande dokument för hanteringen av skyddade personuppgifter på en generell nivå, exempelvis som en policy fastställd av kommunfullmäktige eller som en riktlinje fastställd av kommunstyrelsen.

De granskade nämnderna har inte heller beslutat om några styrdokument inom området. Vi instämmer i att området är verksamhetsnära och att nämnderna inte bör besluta om några detaljerade rutinbeskrivningar, men vår bedömning är att de bör besluta om en riktning för arbetet. Detta är särskilt relevant med hänsyn till att det inte finns kommunövergripande styrdokument. Vi noterar att varje enhet, med undantag från fritidsförvaltningen, har upprättat egna rutinbeskrivningar för hanteringen av skyddade personuppgifter. Avdelningarnas/enheternas rutinbeskrivningar utgör ett värdefullt stöd i sammanhanget, men vi noterar att de endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter och vår bedömning är att de har utrymme för utveckling. Vi bedömer det därtill vara aktuellt att göra en översyn av det stora antalet rutinbeskrivningar.

Enheterna under de granskade nämnderna har alla liknande tillvägagångssätt för att göra rutinerna kända. Rutiner diskuteras på interna möten och arbetsplatsträffar, chefer kan uppmärksamma medarbetare på rutinerna vid behov och de diskuteras också på förekommen anledning. Rutinbeskrivningarna säkerställer delvis en tillräcklig vägledning på såväl övergripande som detaljerad nivå för kommunens medarbetare. Vi bedömer att de bör kompletteras efter genomförd risk- och väsentlighetsanalys, se bedömning i avsnitt 4.2.

Det finns inga kommunövergripande styrdokument inom området, men avdelningarna är medvetna om att de ska bedriva ett eget arbete med skyddade personuppgifter. Vi noterar att varken kommunstyrelsen eller de granskade nämnderna har genomfört någon särskild uppföljning av det arbete som bedrivs för hanteringen av skyddade personuppgifter. Med hänsyn till Umeå kommuns styrmodell och avsaknaden av övergripande styrdokument bedömer vi att det skulle finnas ett värde i att nämnderna stärker uppföljningen inom området. Vår bedömning är därför att respektive *avdelning* till viss del har tillsett tillräcklig uppföljning och kontroll av rutinbeskrivningarnas efterlevnad, men att nämnderna inte är involverade i arbetet i tillräcklig utsträckning.

Utöver rutinförankring genom interna diskussioner genomförs inte någon övergripande och systematisk kompetensutveckling specifikt för hanteringen av skyddade personuppgifter. Det finns kommunövergripande utbildningar inom exempelvis informationssäkerhet och GDPR för nyanställda som omfattar personuppgiftshantering generellt, men inte skyddade personuppgifter specifikt. Avdelningarna under de granskade nämnderna har till största del inte heller genomfört några utbildningar eller liknande kompetensutveckling för hanteringen av skyddade personuppgifter, med undantag för arbetsmarknad- och integrationsavdelningen samt kulturförvaltningen. Utifrån detta bedömer vi att det inte genomförs fortlöpande och tillräcklig kompetensutveckling kring skyddade personuppgifter.

Baserat på den begränsade kompetensutvecklingen som finns, och utvecklingsområdena i styrdokument och rutinbeskrivningarna, bedömer vi att det inte finns ett tillräckligt stöd till medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter. Då fel orsakat av den mänskliga faktorn är den största risken för röjning av skyddade personuppgifter bedömer vi det vara särskilt angeläget att stärka kontrollmiljön inom området.

4. Riskbedömningar

Riskanalys handlar om att identifiera interna och externa risker som en organisation riskerar att utsättas för. Till analysen hör också att kvantifiera hur stor sannolikhet det är att identifierad risk inträffar samt vilka konsekvenserna skulle bli för organisationen. Utifrån verksamhetens behov kan det finnas anledningar att göra riskanalyser på olika nivåer och i olika omfattning i organisationen för att hantera risker på ett ändamålsenligt sätt.

4.1 Risken för och konsekvensen av röjning av skyddade personuppgifter har inte analyserats inom ramen för internkontrollarbetet

I Umeå kommuns *Riktlinjer för intern styrning och kontroll*[9] anges de moment som ska ingå i processen för intern styrning och kontroll. Regelverket gäller för kommunens samtliga verksamhetsområden. Inledningsvis ska en riskanalys göras i syfte att identifiera omständigheter som utgör risk för att inte uppfylla de generella verksamhetskraven. Utifrån resultatet av riskanalysen ska åtgärder vidtas som är nödvändiga för att de generella verksamhetskraven med rimlig säkerhet ska uppfyllas. Den interna styrningen och kontrollen ska systematiskt och regelbundet följas upp, bedömas och avrapporteras. Riskanalysen, kontrollåtgärderna samt uppföljningen och bedömningen ska dokumenteras. Verksamheterna ska till nämnderna rapportera överenskommet underlag som nämnden behöver för att styra, genomföra och bedöma den interna kontrollen.

Risker för röjning av skyddade personuppgifter ingår inte i någon av kommunstyrelsens eller de granskande nämndernas respektive internkontrollplaner för 2023. Det finns dock risker som har identifierats som tangerar frågor kopplade till skyddade personuppgifter. Av intervju har framkommit att röjningen av skyddade personuppgifter inte har betraktats som en tillräckligt allvarlig risk att inkludera i riskanalysen. Om ett flertal incidenter skulle inträffa skulle också riskbedömningen se annorlunda ut, uppger intervjuade.

Bland intervjuade finns därutöver en samlad bild av att risken för röjning av skyddade personuppgifter diskuteras internt inom de olika verksamheterna och att riskanalyser genomförs kontinuerligt i det dagliga arbetet, dock inte inom ramen för internkontrollarbetet. Bland annat är hanteringen av skyddade personuppgifter en fråga som oftast ingår i risk- och skyddsbedömningar avseende upphandling och implementering av specifika verksamhetssystem samt i kommunens systematiska informationssäkerhetsarbete. Likaså genomförs individuella risk- och skyddsbedömningar vid anställning av medarbetare och vid kontakt med klienter/elever som har skyddade personuppgifter. Det innefattar bland annat en kartläggning av hotbild och hur kommunikation med den enskilde ska ske. Framtagandet av vissa rutinbeskrivningar har därutöver föregåtts av en informell risk- och väsentlighetsanalys.

I kommunstyrelsens riskanalys finns en identifierad risk under kontrollområde ”Säkerhet och beredskap” som lyder ”Risk för negativ verksamhetspåverkan om det finns brister i kommunens systematiska informationssäkerhetsarbete”. Sannolikheten för att händelsen inträffar bedöms vara möjlig och konsekvensen för verksamheterna bedöms vara allvarlig, vilket resulterar i att risken rekommenderas att hanteras. Risken ingår därför i kommunstyrelsens internkontrollplan 2023 och kontrollmomentet är ”Kontroll av att information i prioriterade IT-system är säkerhetsklassificerad”. Kontrollmetoden är kontroll av

[9] Fastställd av kommunfullmäktige 2011-09-26.

att prioriterade IT-system är informationsklassade med avseende på konfidentialitet, riktighet och tillgänglighet. Ansvarig är avdelningschef för administration och innovation och återrapportering till kommunstyrelsen ska ske under tertial 2 och 3. Vid granskningens tidpunkt framgår inte om kontrollen genomförts.

2021 genomförde HR-avdelningen en genomgripande riskanalys avseende hantering av skyddade personuppgifter inom avdelningens verksamhetsområden, det vill sägen utanför internkontrollplanen. Riskanalysen omfattade identifiering och analys av risker i Umeå kommuns HR-processer kopplat till hanteringen av personer med skyddade personuppgifter. Därutöver analyserades säkerheten i de verksamhetssystem som används. Riskanalysen resulterade i ett antal risker, konsekvenser, åtgärder och rekommendationer. Riskanalysen har enligt intervjuade resulterat i en säker hantering av skyddade personuppgifter inom kommunens HR-processer.

Risken för och konsekvenserna av röjning av skyddade personuppgifter har inte ingått i individ- och familjenämndens internkontrollplan år 2023. Däremot finns en risk inom kontrollområdet informationssäkerhet. Den identifierade risken är "Brister i skyddet av personuppgifter", och riskvärdet är 9 av 16. Beskrivna åtgärder för att reducera risken är genomlysning av personuppgifter som behandlas utanför avsedda verksamhetssystem, säkerställa skyddet för de personuppgifterna samt löpande informations- och utbildningsinsatser. Vid intervjuer framgår att identifierade risker är hanterade i delar av individ- och familjenämndens verksamhetsområden. Dock kvarstår arbetet i två verksamhetsområden.

Risken för och konsekvenserna av röjning av skyddade personuppgifter eller risk för brister i informationssäkerhetsarbetet har inte ingått i förskole- och grundskolenämndens, gymnasie- och vuxenutbildningsnämndens, fritidsnämnden eller kulturnämndens internkontrollplaner år 2023. Förskole- och grundskolenämnden samt gymnasie- och vuxenutbildningsnämnden har dock gjort medvetna satsningar på GDPR och personuppgiftsbehandling efter att risken ingick i 2022 års internkontrollplaner. Däribland har GDPR-organisationen stärkts med fler personuppgiftskoordinatorer samt en utredare tillika personuppgiftssamordnare under ledning av utbildningsförvaltningens jurist.

4.2 Bedömning

Kommunstyrelsen och de granskade nämnderna har i det formella internkontrollarbetet inte analyserat risken för att skyddade personuppgifter röjs, vilket vi bedömer är en brist. Skyddade personuppgifter ingår inte i kommunstyrelsens eller någon av de granskade nämndernas internkontrollplaner och har inte ingått i de formella risk- och väsentlighetsanalyserna. Vi noterar dock att HR-avdelningen har genomfört en riskanalys kring hanteringen av skyddade personuppgifter i HR-processerna, samt att avdelningarna har analyserat risker kring hantering av skyddade personuppgifter inom informationssäkerhetsområdet och vid individuella risk- och skyddsbedömningar. Intervjuade menar att frågan har behandlats internt vid möten och på arbetsplatsträffar och vår bedömning är att det finns en riskmedvetenhet i enheterna. Med hänsyn till de allvarliga konsekvenser som en röjning av skyddade personuppgifter kan få ser vi dock att hela processen kring hanteringen av skyddade personuppgifter åtminstone bör utvärderas i risk- och väsentlighetsanalys. Detta kan också stärka kommunstyrelsens och nämndernas insyn och uppföljning inom området.

Vi bedömer att säkerhetsfrågor kopplade till skyddade personuppgifter har analyserats och trygghetsskapande åtgärder vidtagits. Bedömningen bygger på de risk- och

skyddsbedömningar avseende potentiella säkerhetsrisker som görs i anslutning till hantering av medborgare eller medarbetare med skyddade personuppgifter, bland annat av verksamhetssystem och genom kartläggning av hotbild hos den enskilde. Därigenom beaktas den enskilda individens perspektiv.

5. Kontrollaktiviteter – Nämndernas rutiner och arbetssätt

Åtgärder eller "kontrollaktiviteter" utgörs av de aktiviteter som en organisation företar för att minska eller eliminera risker. Kontrollaktiviteter anges ofta i en internkontrollplan och syftar då till att följa upp att verksamhetens kontroller fungerar ändamålsenligt (se avsnitt 4.1). Verksamhetens åtgärder/kontroller finns ofta integrerade i processer och kan se olika ut, till exempel inom ramen för dataskyddsarbetet/informationssäkerhetsarbetet, stöd och behörighet i IT- och verksamhetssystem, interna och externa kommunikationskanaler samt hanteringen av medarbetare med skyddade personuppgifter. Gemensamt är att aktiviteterna syftar till att reducera risker.

5.1 Information med hög sekretess ska informationsklassas

Informationsklassning är en grundläggande komponent i kommunens informationssäkerhetsarbete. Umeå kommun har antagit en egen modell för informationsklassning.[10] Modellen utvecklas i kommunens riktlinjer för informationssäkerhet. Det finns fyra klasser för hur känslig informationen är och hur den får spridas: öppen, begränsad, känslig sekretess samt hög sekretess. Olika regler för spridning och hantering av information gäller för de olika klasserna. För information och uppgifter som omfattas av hög sekretess gäller en mycket begränsad åtkomstbehörighet och minimal spridning. Uppgifterna kräver ofta strikt manuell hantering och ska så långt det är möjligt hållas borta från digitala miljöer. Exempel på uppgifter som omfattas av hög sekretess är skyddade personuppgifter då sådan information kan medföra fara för liv och hälsa eller samhällsskada om den hamnar i fel händer. Skyddade personuppgifter ska därför hanteras utifrån särskilda rutiner och regler. Sådana rutiner och regler ska finnas med i användarinstruktioner.[11] I riktlinjerna för informationssäkerhet rekommenderas medarbetarna fråga respektive chef om den egna verksamheten har särskilda rutiner för skyddade personuppgifter. Som konstaterats i avsnitt 3.3.2 finns för de flesta verksamheterna framtagna rutinbeskrivningar för skyddade personuppgifter, men påvisar samtidigt brister.

Av riktlinjerna för informationssäkerhet framgår därutöver att 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 skyddade 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. Denna uppfattning bekräftas av genomförda intervjuer.

IT-system klassas enligt KLASSA-metoden.[12] Enligt KLASSA finns det fem olika risknivåer som IT-systemet klassificeras utifrån:

- (0) Försumbar skada.

[10] Modellen baseras på Sveriges nationella modell för informationsklassning som är utgiven av MSB och SIS, men har anpassats till kommunens behov.

[11] 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.

[12] För att förenkla kommuners och regioners genomförande av informationsklassningen har SKR tagit fram verktyget KLASSA. KLASSA består av tre delar: informationsklassning, handlingsplan och upphandlingskrav.

- (1) Måttlig skada.
- (2) Betydande skada.
- (3) Allvarlig skada.
- (4) Synnerligen allvarlig skada.[13]

Utifrån KLASSA:s fem olika risknivåer klassificeras informationen som hanteras i de olika IT-systemen och vilka skyddsåtgärder som kan användas för att uppfylla skyddskraven för de olika aspekterna. Informationstypen kategoriseras sedan utifrån krav på dess konfidentialitet, riktighet och tillgänglighet. Skyddade personuppgifter nämns i riktlinjerna som ett exempel på en informationstyp som klassas i den högsta risknivån (3) allvarlig skada enligt alla tre krav. Exempel på olika typer av skyddsåtgärder som kan användas enligt klassningen illustreras i tabellen nedan.

Informationstyp	Konfidentialitet	Riktighet	Tillgänglighet
Höga skyddskrav (3)	Kryptering vid lagring och överföring. Stark inloggning.	Stark autentisering genom två-faktors autentisering, exempelvis SITHS-kort, BankID eller Freja e-id.	Spegling av databas, daglig säkerhetskopiering. Loggning av användares aktiviteter i system är obligatorisk.

Tabell 1. Olika typer av skyddsåtgärder i IT-system av information som klassas i den högsta risknivån.

Av intervjuer framgår också att det finns utvecklingspotential i kommunens informationsklassning av de verksamhetsprocesser som respektive verksamhet arbetar med, och inte bara av själva informationen i IT-system. Exempelvis kan ett IT-system vara informationsklassat och säkert för hanteringen av skyddade personuppgifter, medan den praktiska hanteringen som sker utanför systemet inte är riskbedömt och därför vara osäkert. Det utrycks önskemål att verksamhetsperspektivet ska integreras bättre i kommunens arbete att bedriva ett systematiskt informationssäkerhetsarbete genom att implementera ett ledningssystem för informationssäkerhet. Arbetet är enligt intervjuade fortfarande i ett tidigt skede och har i vissa nämnder fortskridit längre än i andra.

5.2 Behandling av skyddade personuppgifter i kommunens IT- och verksamhetssystem samt tillhörande processer

För att erhålla spårbarhet och möjliggöra incidentutredningar samt för att upptäcka avvikelser från legala eller interna regelverk övervakas och loggas system 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. Processer och rutiner för loggning ska följas upp och dokumenteras. Av intervjuer framgår att loggkontroller genomförs med varierande frekvens från system till system och mellan olika förvaltningar och enheter. Ansvaret vilar på respektive nämnd. Inom vissa enheter sker systematiska loggkontroller kvartals- eller månadsvis som en del av det systematiska informationssäkerhetsarbetet. Inom andra enheter sker loggkontroller på begären men är mycket ovanligt. Få loggkontroller sker specifikt för att upptäcka brister i hanteringen av skyddade personuppgifter, men möjligheten finns vid behov. Exempelvis vid en eventuell personuppgiftsincident kopplat till skyddade personuppgifter där loggkontroller användas som verktyg uppger intervjuade.

[13] Information som regleras av säkerhetsskyddslagstiftning.

Utbildningsförvaltningen genomför stickprovskontroller av loggar på vem som sökt och tittat på personer med skyddade personuppgifter.

Styrning av åtkomst är grundläggande för att skydda information och IT-resurser. Grundprincipen i Umeå kommun 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. Inom vissa områden kan man behöva ha (teknisk) behörighet till en stor mängd information. Inom exempelvis vård och omsorg, där annan personal än den ordinarie snabbt kan behöva ha åtkomst till information i akuta situationer, ersätts teknisk åtkomstkontroll av regelstyrd åtkomstkontroll. Det innebär att det finns regler som säger att en person 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.

I riktlinjerna för informationssäkerhet framgår inte om informationstypen skyddade personuppgifter omfattas av begränsad behörighetstilldelning. Av information om skyddade personuppgifter på intranätet framgår dock att den personuppgiftsansvarige bör begränsa åtkomsten till de skyddade personuppgifter till ett fåtal personer. Antalet personer definieras inte ytterligare. Av intervjuer framgår att respektive förvaltning och enhet dels har olika tekniska möjligheter att begränsa behörigheten till information om skyddade personuppgifter i verksamhetssystemen, dels har valt att begränsa behörigheten i olika utsträckning. Med andra ord går det i vissa system att tekniskt styra behörigheten till en viss handläggare, medan det i andra system där detta inte är möjligt, går att utse en eller flera handläggare som hanterar alla ärenden med skyddade personuppgifter.

Fritidsförvaltningen och kulturförvaltningen har inga behörighetsbegränsningar. De hänvisar huvudsakligen till att det endast är ett fåtal handläggare som hanterar ärenden med skyddade personuppgifter, och att de därför inte har identifierat ett behov av striktare behörighetsbegränsningar. Verksamhetssystemen inom utbildningsförvaltningen är behörighetsstyrda till ansvarig administrativ personal. Inom stöd- och omsorgsförvaltningen finns goda möjligheter att begränsa behörigheten i nuvarande verksamhetssystem. Det skiljer sig dock från enhet till enhet hur strikta behörighetsbegränsningarna är. Detta då enhetschefen måste beställa behörighet av systemförvaltningen vilket resulterar i ökad administration. De praktiska arbetsrutinerna för att rätt handläggare ska få behörighet brister enligt intervjuade. Nämnden har upphandlat ett nytt verksamhetssystem, med bättre möjligheter att styra behörighetsbegränsningen, som ska implementeras under 2024.

Vidare framgår av riktlinjerna att uppgifter som kategoriseras med hög sekretess endast ska 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. Av de granskade verksamheternas verksamhetssystem har merparten en tydlig funktion för sekretessmarkering. Vissa system kräver dock mer manuell hantering än andra, samt saknar möjligheten att behörighetsbegränsa åtkomsten till skyddade personuppgifter, vilket uppges öka risken för felhantering orsakad av den mänskliga faktorn. Vissa system saknar helt en tydlig funktion för sekretessmarkering i kombination med avsaknad av möjligheter till behörighetsbegränsning. Exempelvis kan arbetsmarknads- och integrationsavdelningen nyligen implementerade verksamhetssystem inte användas vid hantering av skyddade personuppgifter, då säkerheten inte kan garanteras. Avdelningen har därför valt att hantera skyddade personuppgifter manuellt utanför systemet. Intervjuade

påpekar risker med hanteringen, men har säkerställt ett tillräckligt skydd genom att utbilda samtliga medarbetare, och så gott det går säkrat den manuella hanteringen.

Intervjuade inom stadsledningskontoret påtalar brister i delar av kommunens fillagring av sekretessmarkerad information. I dagsläget lagrar individ- och familjenämnden samt äldrenämnden avsiktligt sekretesskyddad information i en molntjänst vilket enligt intervjuade kan strida mot GDPR och offentlighets- och sekretesslagen. Det har också hänt att andra nämnders verksamheter lagrat sekretesskyddad information eller känsliga personuppgifter i molntjänster i strid med lag och kommunens interna regler.

Enligt riktlinjerna för informationssäkerhet får skriftligt material som innehåller hög sekretessinformation 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. Som tidigare beskrivits hanteras viss information innehållandes skyddade personuppgifter utanför systemen på papper. När dessa inte är inlåsta i kassaskåp finns risk att de lämnas framme på skrivbord eller dylikt. Intervjuade uppger dock att det finns en stor medvetenhet att inte lämna papper framme och att risken för den typen av röjning är låg. Därtill finns få öppna kontorslandskap i kommunens lokaler.

Vid fysisk posttjänst ska dubbla förslutna brev (internpostkuvert och kuvert) användas för intern information och rekommenderade försändelser ska användas om externbrev innehåller hög sekretessinformation. Flera enheter tar av och till emot fysisk post. Post som ska till dessa kommer in till receptionen och fördelas sedan internt. Dessutom skickas vissa underlag med kommunens internpost. Flera intervjuade har uppgett en osäkerhet kring vilka rutiner som finns kring postgången och om post som innehåller känsliga personuppgifter hanteras med större försiktighet. Intervjuade har nämnt att viktig post från person med skyddade personuppgifter har försvunnit i den interna postgången mellan det att posten kom in till receptionen och sedan skulle fördelas till verksamheten. Rutinerna har delvis stärkts utifrån identifierade risker, däribland har vissa enheter slutat använda internposten. Intervjuade påpekar att den interna posthanteringen kan utgöra en ökad risk för röjning av skyddade personuppgifter.

Vad gäller informationsöverföring ska kommunikation med höga skyddskrav alltid krypteras och kommunicerande parter ska identifieras på ett säkert sätt. Av riktlinjerna framkommer att fax är ett väldigt osäkert kommunikationssätt. Fax används dock fortfarande inom vissa enheter i kommunen. Kommunen håller på att ersätta bland annat faxen med Säker digital kommunikation, som erbjuder en lösning att skicka krypterad e-post. Lösningen skulle införas 2022, men är dock inte införd än. Av intervjuer framgår att behovet av Säker digital kommunikation är mycket stort, särskilt inom utbildningsförvaltningen och stöd- och omsorgsförvaltningens verksamheter som kommunicerar mycket med varandra. Stöd- och omsorgsförvaltningen driver processen att införa lösningen. Vid granskningens tidpunkt är upphandlingen klar och verktyget ska enligt plan implementeras under 2024 i hela kommunen. Intervjuade vittnar om en stor frustration att införandet dröjt.

Om mejl inkommer som innehåller information med hög sekretess ska denna genast flyttas till verksamhetssystem. Mejlet ska inte besvaras eller vidarebefordras i samma mejlkonversation. Meddelandet ska raderas från e-postklienten. Inkommande mejl innehållandes information med hög sekretess ska genast överföras till verksamhetssystem, varpå meddelandet ska raderas från e-postklienten. Intervjuade uppger att det finns en stor medvetenhet om rutinerna att inte svara på mejl innehållandes information med skyddade personuppgifter. Vi noterar dock att riktlinjerna för informationssäkerhet inte omfattar rutiner för kommunikation

med externa parter per telefon. Den informationen framgår dock av flertalet verksamheters rutinbeskrivningar. Intervjuade uppger även avseende detta att det finns en stor medvetenhet att inte uppge information om personer när en privatperson ringer, eller motringa när en extern myndighet ringer. Dock framhävs också behovet av att ytterligare förtydliga dessa rutiner och kontinuerligt sprida informationen till samtliga medarbetare, även de som sällan kommer i kontakt med skyddade personuppgifter. Risken för röjning av skyddade personuppgifter beskrivs vara som störst vid extern kommunikation i olika former.

Kritiska delar i IT-miljön som hanterar objekt med höga skyddskrav ska regelbundet övervakas och granskas för att sårbarheter och brister ska upptäckas. Sådan granskning kan till exempel vara skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester. Ett penetrationstest identifierar svagheter i systemen och utvärderar säkerhetsnivåer. 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. Penetrationstester har inte genomförts med anledning av risken för röjning av skyddade personuppgifter i kommunens verksamhetssystem.

5.3 Hantering av skyddade personuppgifter i kommunens HR-processer

Utifrån tidigare beskrivna genomförda riskanalys för hantering skyddade personuppgifter i kommunens HR-processer finns upprättade rutinbeskrivningar. Vid rekrytering ombeds personer med skyddade personuppgifter via Umeå kommuns hemsida att inte söka jobbet via systemet, utan i stället kontakta rekryterande chef på berörd enhet och skicka ansökan via papperspost. Därefter ansvarar rekryterande chef eller rekryteringskonsult för den fortsatta hanteringen under rekryteringsprocessen. Ansökan ska hanteras manuellt. Om kandidaten blir anställd ska rekryterande chef ringa rekryteringssupporten och meddela vem som är anställd, detta för avslut och arkivering av rekryteringsärendet. Uppgifterna får inte skickas med e-post. All kommunikation med kandidater med skyddade personuppgifter ska i största möjliga utsträckning ske muntligen. Vid digital referenstagning används ett upphandlat system. Då systemet inte har stöd för personer med skyddade personuppgifter rekommenderas att digital referenstagning inte används. Detta för att systemet inte kan säkerställa att enbart rekryterande chef/rekryteringsgrupp får tillgång till informationen, vilket kan innebära en risk att informationen sprids av misstag om handlingarna begärs ut. Det finns också rutiner som omfattar anställning och lön för den anställda med skyddade personuppgifter.

HR-avdelningen har inte några rutiner för hur det vardagliga arbetet inom verksamheterna ska hanteras avseende medarbetare med skyddade personuppgifter. Ansvaret åligger respektive förvaltning och dess personalchefer. Inom respektive förvaltning beslutas frågor som rör den praktiska hanteringen av personalchef och rekryterande chef i samverkan med den enskilde medarbetaren som har skyddade personuppgifter. Av intervju har framkommit att verksamheterna har liknande perspektiv på hur medarbetare med skyddade personuppgifter ska hanteras. I stort utgår detta från att medarbetare själva får bestämma exempelvis om det vill medverka i bild som används internt och hur många som ska känna till att de har skyddade personuppgifter. Inom vissa enheter sker en säkerhetsbedömning kring konsekvenserna att ha personen anställd, exempelvis om denne kan överföra en hotbild till andra anställda eller elever/klienter. Intervjuade känner sig generellt sett trygga med den praktiska hanteringen av anställda som har skyddade personuppgifter, men uppger att stort ansvar vilar på medarbetaren själv samt rekryterande chef. Vissa enheter har aldrig haft en anställd med skyddade personuppgifter och kan därför inte svara på om rutiner eller vilka rutiner som finns för ändamålet.

Ett relativt vanligt förekommande problem är att de anställda med skyddade personuppgifter inte själva förstår vissa komplikationer det innebär att ha skyddade personuppgifter och därför agerar oaktsamt. Ett annat problem som intervjuade inom HR-avdelningen beskriver är att vara anställd chef i kommunen och ha skyddade personuppgifter. En anställd som har skyddade personuppgifter har inte samma möjligheter att använda vissa av kommunens digitala systemstöd som andra medarbetare då säkerheten inte kan garanteras, exempelvis ärendeportalen. Den anställda måste i stället gå via dennes chef som får göra en anmälan. Detta medför komplikationer för en chef som har skyddade personuppgifter då denne inte kan göra anmälningar i ärendeportalen exempelvis. Den största risken i HR-processerna beskrivs finnas när den rekryterande chefen skickar det manuella anställningsunderlaget via kommunens internpost till HR-avdelningen. Arbetsrutinen ses över enligt intervjuade.

5.4 Bedömning

Vår sammantagna bedömning är att kommunstyrelsen och de granskade nämnderna inte har vidtagit tillräckliga åtgärder för att minska risken för röjning av skyddade personuppgifter. Vi noterar dock att respektive avdelning har vidtagit ett antal olika åtgärder, även om vi också bedömer att det samtidigt finns utrymme för förbättringar som presenteras nedan. Vi bedömer det vara särskilt angeläget att kommunstyrelsen och granskade nämnder följer upp vidtagna åtgärder.

Av de granskade nämndernas verksamhetssystem har merparten en tydlig funktion för sekretessmarkering, även om vissa system kräver mer manuell hantering än andra. Vi bedömer det finnas risker att samtliga system inte har en funktion för sekretessmarkering, då det medför risker att hantera skyddade personuppgifter utanför systemet. Detta då manuell hantering av skyddade personuppgifter ställer exceptionella krav på noggrannhet och riskmedvetenhet samt ökar risken för felhantering orsakad av den mänskliga faktorn.

Respektive förvaltning och enhet har dels olika tekniska möjligheter att begränsa behörigheten till information om skyddade personuppgifter i verksamhetssystemen, dels har valt att begränsa behörigheten i olika utsträckning. Vi bedömer det finns betydande risker med att samtliga avdelningar inte har strikta behörighetsbegränsningar till sekretessbelagda ärenden, både i och utanför systemen. Detta då vi bedömer det vara angeläget att minimera antalet personer som hanterar skyddade personuppgifter.

Intervjuade inom stadsledningskontoret påtalar brister i individ- och familjenämnden samt äldrenämndens fillagring av sekretessmarkerad information, genom lagring i en molntjänst. Då detta kan strida mot GDPR och offentlighets- och sekretesslagen bedömer vi det vara en brist som bör åtgärdas skyndsamt.

Kommunen fattade för ett par år sedan beslutet att införa tjänsten Säker digital kommunikation, en lösning att skicka krypterad e-post med. Tjänsten är vid granskningens tidpunkt inte införd, men ska implementeras 2024. Av intervjuer framgår att behovet av Säker digital kommunikation är mycket stort, särskilt inom utbildningsförvaltningen och stöd- och omsorgsförvaltningens verksamheter som kommunicerar mycket med varandra. Vi delar den uppfattningen och bedömer därför det vara mycket angeläget att Säker digital kommunikation implementeras skyndsamt i hela kommunen. Detta då risken för röjning av skyddade personuppgifter är som störst vid intern och extern kommunikation i olika former.

Dessutom skickas vissa underlag med kommunens internpost, där intervjuade beskriver att viktig post innehållandes uppgifter om personer med skyddade personuppgifter har

försvunnit. Vi bedömer det vara en brist att internposten används vid hantering av skyddade personuppgifter och att arbetsrutinerna därför bör stärkas.

De granskade nämnderna, med undantag för förskole- och grundskolenämnden samt gymnasie- och vuxenutbildningsnämnden, har inte gjort loggkontroller för att upptäcka suspekta användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser kopplat till risken för röjning av skyddade personuppgifter. Vi bedömer att respektive nämnd årligen bör genomföra systematisk anomalianalys av loggar – att avvikande beteendemönster i verksamhetssystemen uppmärksammas automatiskt och därefter analyseras – med anledning av risken för röjning av skyddade personuppgifter. Detta särskilt med anledning av att det i samtliga system inte finns begränsad behörighetstilldelning.

De granskade nämnderna har därtill inte övervakat och granskat verksamhetssystem som hanterar skyddade personuppgifter för att upptäcka sårbarheter och brister, däribland genom så kallade penetrationstester. Penetrationstester kan användas på många sätt för att identifiera brister vid hantering av skyddade personuppgifter, däribland säkerheten i IT-systemen och de arbetsrutiner som finns beskrivna i respektive förvaltnings rutinbeskrivningar. Vi bedömer det vara angeläget att rutiner för penetrationstester implementeras inom respektive granskad nämnds verksamhetsområden.

6. Avvikelsehantering

6.1 Det går inte att särmarkera personuppgiftsincidenter som rör hanteringen av skyddade personuppgifter

Kommunens riktlinjer för personuppgiftsincidenthantering[14] beskriver hantering och ansvaret för att undvika, upptäcka, anmäla och utreda personuppgiftsincidenter. Respektive nämnd ska upprätta ett dokument som beskriver den praktiska hanteringen. Ansvaret att anmäla en personuppgiftsincident åligger personuppgiftsansvarig nämnd, ansvaret för att utreda personuppgiftsincidenter ingår i verksamhetsansvaret och samordnas av personuppgiftskoordinator inom respektive nämnd. Incidenten ska rapporteras via ett verktyg som nås genom intranätet. Vid användning av IT-verktyget för anmälan får inga känsliga personuppgifter eller sekretesskyddade uppgifter anges. Närmaste chef ska också meddelas vid anmälan. Om det är sannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter ska händelsen anmälas till tillsynsmyndigheten (IMY). Det tydliggörs också att den drabbade ska informeras utan dröjsmål i dessa situationer.

Respektive nämnd har olika arbetsrutiner för rapportering av incidenter som skett inom nämndens verksamhetsområde och de åtgärder som vidtagits. Fritidsnämnden fattade exempelvis 2018 ett beslut om att fritidsnämnden kvartalsvis ska informeras om de incidenter som skett. Inom individ- och familjenämnden ska personuppgiftsincidenter som anmälts till IMY läggas som anmälningsärende till nämnd i samband med att ärendet diarieförs. Inom för- och grundskolenämnden samt gymnasie- och vuxenutbildningsnämnden deltar GDPR-utredare tillika personuppgiftssamordnare på nämndsmöte vid återkoppling av inträffade och anmälda incidenter. Från och med februari 2024 kommer återrapporteringen ske genom en skriftlig årsberättelse till båda nämnderna gällande det GDPR-arbete som bedrivits på förvaltningen, samt förslag på åtgärder som behöver vidtas utifrån identifierade händelser och beslut från IMY. Där ingår eventuella incidenter som involverar personer med skyddade personuppgifter. Kulturnämnden informeras av personuppgiftsincidenter varje tertial, dock inte med särskilt fokus på skyddade personuppgifter.

Av kommunstyrelsens riktlinjer för informationssäkerhet framgår att alla medarbetare har skyldighet att rapportera informationssäkerhetsincidenter eller brister som misstänkts kunna medföra negativ påverkan på Umeå kommuns informationssäkerhet. Det kan till exempel röra sig om:

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

Informationssäkerhetssamordnare sammanställer en incidentrapport en gång per år som rapporteras till stadsdirektörens ledningsgrupp och berörda verksamheter.

[14] Godkänd av respektive nämn.

Individ- och familjenämnden kan därutöver rapportera missförhållanden enligt lex Sarah. Brott mot sekretesslagen och brister i dokumentation är ett exempel på missförhållanden som kan rapporteras enligt lex Sarah som berör skyddade personuppgifter.

Det går inte att särmarkera personuppgiftsincidenter som rör hanteringen av skyddade personuppgifter. Intervjuade beskriver att incidenter avseende skyddade personuppgifter hanteras inom ramen för den ovan beskrivna ordinära avvikelsehanteringen för personuppgiftsincidenter. Flertalet intervjuade påtalar en risk för underrapportering av personuppgiftsincidenter, däribland de som rör skyddade personuppgifter. Orsaken till att det inte har rapporterats några avvikelser vad gäller skyddade personuppgifter är inte känd. Det är enligt intervjuade osäkert om det betyder att det inte finns avvikelser eller om rutinen att anmäla sådana ärenden inte förmedlats i tillräcklig utsträckning. Det kan således inte likställas med att avvikelser inte inträffat, enbart att inga uppmärksammats.

I intervjuer uppges också att det preventiva arbetet är en viktig del i incidenthanteringsprocessen. För att framtida incidenter ska kunna förhindras på ett effektivt sätt måste rotorsaken till en incident utredas. Dels måste den direkta orsaken till incidenten analyseras, dels måste även de bakomliggande orsakerna klarläggas. Det framgår ingen specifik arbetsprocess för uppföljningen och det förebyggande arbetet.

6.2 Bedömning

Vi bedömer att det inte finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns ingen egen process för avvikelser gällande skyddade personuppgifter. I kommunen finns en central process för hanteringen av personuppgiftsincidenter och avvikelser avseende skyddade personuppgifter hanteras i denna process. Av upprättade riktlinjer och rutiner för personuppgiftsincidenter framgår inte någon särskild information om skyddade personuppgifter. Vår bedömning är att det behöver tydliggöras att incidenter med skyddade personuppgifter måste hanteras särskilt varsamt och skyndsamt, givet de möjliga konsekvenserna av en röjning. Det bör även inkluderas i styrande dokumentation som rör hanteringen av skyddade personuppgifter. Då incidenter avseende skyddade personuppgifter inte på något sätt särskiljs från övriga personuppgiftsincidenter är vår bedömning även att det finns begränsade förutsättningar för uppföljning inom området, vilket riskerar få konsekvensen att erfarenheter från avvikelser inte tillvaratas.

7. Svar på revisionsfrågor

Fråga	Svar
Finns ändamålsenliga styrande dokument och rutiner för hantering av skyddade personuppgifter? o *Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?*	Nej. Det finns kommunövergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen, men kommunstyrelsen har inte beslutat om något styrande dokument för hantering av skyddade personuppgifter specifikt. De granskade nämnderna har inte beslutat om styrande rutiner, men enheterna under de granskade nämnderna har tagit fram arbetsrutiner utifrån det egna upplevda behovet. Dessa utgör ett värdefullt stöd i sammanhanget, men vi noterar att de endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter. Styrdokument saknas inom området. Upprättade arbetsrutiner görs i huvudsak kända genom interna möten och arbetsplatsträffar inom verksamheterna. Skyddade personuppgifter diskuteras i huvudsak på förekommen anledning, exempelvis vid avvikelse. I dessa sammanhang förankras, och vid behov, stärks arbetsrutinerna. Ingen av de granskade nämnderna har genomgång av rutiner för hantering av skyddade personuppgifter som ett återkommande moment i exempelvis ett årshjul.
Har kommunen säkerställt tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?	Nej. Det finns inga styrdokument inom området, men respektive enhet är medvetna om att de ska bedriva ett eget arbete med skyddade personuppgifter. Varken kommunstyrelsen eller de granskade nämnderna har genomfört någon uppföljning av det arbete som bedrivs för hanteringen av skyddade personuppgifter. I praktiken genomförs förankring av rutiner av verksamheterna själva, men detta följs inte upp från nämnden eller kommunens ledning.
Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?	Nej. Utöver rutinförankring genom interna diskussioner genomförs inte någon övergripande och systematisk kompetensutveckling specifikt för hanteringen av skyddade personuppgifter. Det finns kommunövergripande utbildningar inom exempelvis informationssäkerhet och GDPR för nyanställda som omfattar personuppgiftshantering generellt, men inte skyddade personuppgifter specifikt. Avdelningarna under de granskade nämnderna har till största del inte heller genomfört några utbildningar eller liknande kompetensutveckling för hanteringen av skyddade personuppgifter, med undantag för arbetsmarknad- och integrationsavdelningen samt kulturförvaltningen.
Har kommunen på ett ändamålsenligt sätt analyserat och bedömt risken för att skyddade personuppgifter röjs? o *Har den enskilda individens perspektiv beaktats?*	Nej. Skyddade personuppgifter ingår inte i kommunstyrelsens eller någon av de granskade nämndernas internkontrollplaner och har inte ingått i de formella risk- och väsentlighetsanalyserna. Vi noterar dock att HR-avdelningen har genomfört en riskanalys kring hanteringen av skyddade personuppgifter i HR-processerna, samt att avdelningarna har analyserat risker kring hantering av skyddade personuppgifter inom informationssäkerhetsområdet och vid individuella risk- och skyddsbedömningar. Ja. Genom de individuella risk- och skyddsbedömningar avseende potentiella säkerhetsrisker som görs i anslutning till hantering av medborgare eller medarbetare med skyddade personuppgifter, bland

	annat av verksamhetssystem och genom kartläggning av hotbild hos den enskilde, beaktas den enskilde individens perspektiv.
Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygg-hetsskapande åtgärder vidtagits med utgångspunkt i dessa analyser?	Delvis. Kommunstyrelsen och de granskade nämnderna har inte själva genomfört några analyser inom området. De har inte heller tillsett att säkerhetsfrågor analyseras och åtgärder vidtas av enheterna. Däremot görs individuella risk- och skyddsbedömningar avseende potentiella säkerhetsrisker på enhetsnivå i anslutning till hantering av medborgare eller medarbetare med skyddade personuppgifter.
Har kommunen vidtagit ändamålsenliga åtgärder för att minska risken för röjning av skyddade personuppgifter och följs detta upp av berörda nämnder?	Nej. Varken kommunstyrelsen eller de granskade nämnderna har säkerställt att åtgärder har vidtagits för att minska risken för röjning av skyddade personuppgifter. Enheterna har dock på eget initiativ vidtagit ett antal olika åtgärder, även om det också samtidigt finns utrymme för förbättringar. Enheternas rutiner medför ett antal gynnsamma åtgärder, men det finns brister. I granskningen framgår potentiella förbättringsområden per granskad nämnd och kommunstyrelsen.
Finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter? o *Hur tillvaratas erfarenhet från avvikelser?*	Nej. Kommunen har en gemensam och dokumenterad process för hanteringen av personuppgiftsincidenter. Avvikelser avseende hanteringen av skyddade personuppgifter ingår i detta system. Det finns dock inget eget särskilt system för att hantera incidenter med skyddade personuppgifter, vilket försvårar möjligheten till uppföljning och att tillvarata erfarenheter från avvikelser. Varje enskild enhet följer upp och tillvaratar erfarenheter från avvikelser. Det saknas instruktioner för hur det ska gå till. I praktiken sker tillvaratagandet av erfarenhet genom interna diskussioner på respektive verksamhets interna möten och arbetsplatsträffar.

Stockholm den 14 december 2023

David Leinsköld
Verksamhetsrevisor, EY

Bilaga 1. Källförteckning

Intervjuade funktioner

- Personuppgiftskoordinator IT (Teknik- och fastighetsförvaltningen)
- IT-infrastrukturspecialist (Teknik- och fastighetsförvaltningen)
- Informationssäkerhetssamordnare (Stadsledningskontoret)
- Kommunjurist (Stadsledningskontoret)
- Redovisningschef (Stadsledningskontoret)
- Processledare reskontraprocesserna (Stadsledningskontoret)
- Förhandlingschef (Stadsledningskontoret, HR-avdelningen)
- Förvaltningsledare lön, (Stadsledningskontoret, HR-avdelningen)
- Lönekonsult (Stadsledningskontoret, HR-avdelningen)
- Lönekonsult Stadsledningskontoret, (HR-avdelningen)
- HR-strateg (Stadsledningskontoret, HR-avdelningen)
- Arbetsmiljöstrateg (Stadsledningskontoret, HR-avdelningen)
- HR-konsult rekrytering (Stadsledningskontoret, HR-avdelningen)
- HR-konsult/teamledare (Stadsledningskontoret, HR-avdelningen)
- Fritidsdirektör (Fritidsförvaltningen)
- Personuppgiftskoordinator/nämndsekreterare (Fritidsförvaltningen)
- Personuppgiftskoordinator/IT-samordnare (Fritidsförvaltningen)
- Bidragshandläggare (Fritidsförvaltningen)
- Verksamhetschef fritid unga (Fritidsförvaltningen)
- HR-chef kultur och fritid (Fritidsförvaltningen)
- Verksamhetschef Bibliotekschef (Kulturförvaltningen)
- Verksamhetsutvecklare (Kulturförvaltningen)
- Verksamhetschef Kulturskolan (Kulturförvaltningen)
- Verksamhetssamordnare (Kulturförvaltningen)
- Utbildningsdirektör (Utbildningsförvaltningen)
- Områdeschef förskola (Utbildningsförvaltningen)
- Områdeschef grundskola åk F-6 (Utbildningsförvaltningen)
- Områdeschef grundskola åk 7-9 (Utbildningsförvaltningen)
- Administrativ chef på pedagogiska placeringsenheten förskola/grundskola (Utbildningsförvaltningen)
- Utvecklingsledare IT förskola/grundskola (Utbildningsförvaltningen)
- Utbildningsjurist GDPR förskola/grundskola (Utbildningsförvaltningen)
- Kanslichef (Utbildningsförvaltningen)
- Nämndsekreterare och koordinator förskola/grundskola (Utbildningsförvaltningen)
- Utbildningsjurist GDPR gymnasium/vux (Utbildningsförvaltningen)
- Skoladministratör gymnasiet (Utbildningsförvaltningen)
- Verksamhetsutvecklare/arbetsmarknadskonsulent/personuppgiftskoordinator (Utbildningsförvaltningen, Arbetsmarknad- och integrationsavdelningen)
- Utvecklingsledare (Utbildningsförvaltningen, Arbetsmarknad- och integrationsavdelningen)
- Koordinator/Systemförvaltare (Stöd- och omsorgsförvaltningen, Systemförvaltning)
- Systemförvaltare (Stöd- och omsorgsförvaltningen, Systemförvaltning)
- Personuppgiftskoordinator (Stöd- och omsorgsförvaltningen)
- Socialsekreterare (Stöd- och omsorgsförvaltningen, Mottagningsenheten)
- Socialsekreterare (Stöd- och omsorgsförvaltningen, Mottagningsenheten)

- Enhetschef personlig assistans (Stöd- och omsorgsförvaltningen, Funktionshinderomsorg)
- Enhetschef personlig assistans (Stöd- och omsorgsförvaltningen, Funktionshinderomsorg)
- Enhetschef boendestöd (Stöd- och omsorgsförvaltningen, Funktionshinderomsorg)
- Socialsekreterare boendestöd (Stöd- och omsorgsförvaltningen, Funktionshinderomsorg)
- Enhetschef familjehemscentrum (Stöd- och omsorgsförvaltningen, Individ- och familjeomsorg)
- Socialsekreterare (Stöd- och omsorgsförvaltningen, Individ- och familjeomsorg)
- Enhetschef beroendeenheten, alkohol och drogmottagningen och bosocial enhet (Stöd- och omsorgsförvaltningen, Individ- och familjeomsorg)
- Behandlingschef Bryggan stödboende (Stöd- och omsorgsförvaltningen, Individ- och familjeomsorg)
- Enhetschef bemanning stöd och omsorg (Stöd- och omsorgsförvaltningen)
- Verksamhetsutvecklare bemanning stöd och omsorg (Stöd- och omsorgsförvaltningen)
- Socialt ansvarig samordnare (SAS) (Stöd- och omsorgsförvaltningen)
- Verksamhetsassistent (Stöd- och omsorgsförvaltningen, Myndighetsövning)
- Socialsekreterare barn och unga (Stöd- och omsorgsförvaltningen, Myndighetsövning)
- Socialsekreterare vuxna (Stöd- och omsorgsförvaltningen, Myndighetsövning)

Granskad dokumentation

- Informationssäkerhetspolicy för Umeå kommun (KF 2013-06-17)
- Riktlinjer för informationssäkerhet Umeå kommun (KS 2021-12-17)
- Användning av personuppgifter i form av bilder, filmer, namn och kontaktuppgifter i kommunens kommunikation (DNR KS-2018/00378)
- Hantering av kandidat med skyddade personuppgifter i rekryteringsprocessen (2023-02-12)
- LP-04.20 Skyddade personuppgifter anställning och lön
- Riktlinjer för intern styrning och kontroll (DNR KS000559/2011)
- Handledning – intern styrning och kontroll (KS 2019-12-19)
- Kommunstyrelsen riskinventering, riskvärdering och internkontrollplan 2023
- För- och grundskolenämnden internkontrollplan 2023
- Gymnasie- och vuxenutbildningsnämnden internkontrollplan 2023
- Individ- och familjenämnden internkontrollplan 2023
- Fritidsnämnden internkontrollplan 2023
- Kulturnämnden internkontrollplan 2023
- Rutin för personuppgiftsincident inom fritidsnämndens verksamhet (2021-10-14)
- Gemensamma regler för Umeåregionens folkbibliotek (2022-01-10)
- Skyddade personuppgifter, Kulturförvaltningen (2023-01-26)
- Policy för informationsförvaltning (KS-2023/00270-5)
- Anställningsunderlag för anonymitetsskyddad anställning, HR-avdelningen
- Att hantera offentlighet, tystnadsplikt och sekretess inom Umeå kommun (2020-12-29)
- Riktlinjer för personuppgiftsincidenthantering (FGN 2018-10-25 §80, GVN 2018-10-24 §75)
- Instruktion för handhavande av sekretessbelagda handlingar (KS-2018/00905-1)
- Riktlinjer för personuppgiftsincidenthantering (FN-2018/00336)
- Skyddade personuppgifter, Treserva förvaltning (2018-01-10)

- Behörighetsbeställning Treserva, anställd med skyddade personuppgifter (2022-05-12)
- Rutin för behörigheter till Externa utförare LSS – Prator (2022-02-01)
- Personuppgiftsincident hos äldre- samt stöd- och omsorg (2023-04-05)
- Rapportering av missförhållanden enligt lex Sarah (2023-04-25)
- LVU-ansökan om vård samt omedelbart omhändertagande (2022-08-18)
- Personakt och dokumenthantering IFN (2023-05-11)
- Samverkansrutin mellan socialtjänst och grundskola samt gymnasieskola, ungdomar placerade i familjehem eller HVB (2022-09-01)
- Åtkomst till och särskilt skydd av uppgifter i Treserva (2019-06-19)
- Våld i nära relation (2023-10-06)
- Riktlinje för individ- och familjenämndens arbete med våld i nära relationer och hedersrelaterat våld (2023-02-22)
- Skyddade personuppgifter, myndighetsutövning stöd- och omsorgsförvaltningen (2022-10-10)
- Skyddad identitet, Bemanning stöd och omsorg (framgår ej när den är upprättad)
- Led – Personuppgiftsbehandling – Sekretess och att ge information om inskrivna personer (2023-08-29)
- Arb STA – Skyddade personuppgifter, Arbetsmarknadsavdelningen (2023-11-02)
- Rutin vid personuppgiftsincident med utredningsstöd som bilaga, utbildningsförvaltningen (2023-05-04)
- Skyddade personuppgifter – Vad verksamheten bör tänka på, Utbildningsförvaltningen (2018-06-14)
- Sekretessmarkering, Utbildningsförvaltningen (2018-06-14)
- Administrativ hantering av elev med skyddade personuppgifter UGS, Utbildningsförvaltningen (2020-01-15)
- Rutin för hantering av skyddade personuppgifter i för- och grundskola (2020-11-19)
- Rutin – Elev med skyddade personuppgifter – sekretessmarkerade, Centrum för vuxenutbildning (2023-03-22)
- Kvarskrivning, Utbildningsförvaltningen (2018-06-14)
- Handlingsplan för elev med skyddade personuppgifter (2021-06-18)
- Rutin för elever med skyddade personuppgifter i UGS, Utbildningsförvaltningen (2021-06-18)

Bilaga 2. Revisionskriterier

COSO-ramverket för intern kontroll

Det finns varken för kommuner, kommunala bolag, företag eller andra organisationer en formellt fastställd standard för hur den interna kontrollen ska hanteras. I praktiken har dock en amerikansk standard blivit dominerande: The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Målet med COSO och intern kontroll är att säkerställa att risker undviks och ge en trygghet i att organisationens mål uppfylls. COSO-modellens huvudmål är att garantera en ändamålsenlig och kostnadseffektiv verksamhet, tillförlitlig finansiell rapportering och information om verksamheten samt att lagar följs.

COSO-modellen består av fem huvudkomponenter: kontrollmiljö, riskanalys, kontrollaktiviteter, information och kommunikation samt uppföljning. Dessa perspektiv beaktas i revisionsfrågorna samt rapportens analys och bedömningar.

Kommunallagen (2017:725)

Det är enligt 6 kap. 1 § styrelsens uppgift att leda och samordna förvaltningen av kommunens angelägenheter och ha uppsikt över övriga nämnders och eventuella gemensamma nämnder. Kommunstyrelsen ska, enligt 6 kap. 2 §, uppmärksammat följa de frågor som kan inverka på kommunens utveckling och ekonomiska ställning.

Kommunallagens 6 kap. 6 § anger att nämnderna var och en inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som beslutats av kommunfullmäktige samt de föreskrifter som gäller för verksamheten. Nämnderna ska även tillse att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Om begreppet skyddade personuppgifter

Det har blivit vanligare att människor lever med skyddade personuppgifter. De senaste tio åren har antalet i Sverige dubblerats från drygt 12 000 till knappt 24 000 personer. Enligt Skatteverket utgörs dessa till 59 procent av kvinnor. Vanligast förekommande är sekretessmarkering, som är den minst ingripande formen av skydd, med 82 procent av ärendena medan skyddad folkbokföring, som är ett starkare skydd, utgör 18 procent.

Antalet personer med skyddade personuppgifter motsvarar ca 0,22 procent av befolkningen och matematiskt motsvarar det ca 240 invånare och ett tiotal anställda i Nacka kommun. Siffrorna är inte exakta men visar att det statistiskt handlar om ett fåtal individer. Konsekvensen vid felaktig röjning av dessa personuppgifter kan emellertid vara mycket allvarlig för var och en.

Jämställdhetsmyndigheten har på regeringsuppdrag genomfört kunskapshöjande insatser gällande våldsutsatta personer som lever med skyddade personuppgifter med fokus på kvinnor och barn. I en delrapport[15] intervjuas 86 kvinnor och 15 barn om deras erfarenheter. Närmare tre fjärdedelar av de intervjuade uppger att deras identitet har röjts.

I rapporten konstateras att det i många fall handlar om kvinnor och barn som tvingats flytta på grund av våld och hot från närstående man och att målgruppen är extra utsatt. I princip

[15] *Skyddade personuppgifter – oskyddade personer* (Jämställdhetsmyndigheten 2022:10).

samtliga kvinnor i Jämställdhetsmyndighetens intervjustudie har fått skyddade personuppgifter röjda av myndigheter.

Det finns omfattande lagstiftning som skyddar individen

Skyddade personuppgifter är ett samlingsbegrepp för olika åtgärder som kan vidtas för att skydda personer som riskerar att utsättas för hot, våld eller förföljelse. Beroende på hotets allvarlighetsgrad finns tre grader av skydd av personuppgifter; sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter. Därutöver finns ytterligare bestämmelser om sekretess som kan aktualiseras för hotade och förföljda personer, bland annat inom offentlighets- och sekretesslagen (2009:400).

Sekretessmarkering är den vanligaste och minst ingripande formen av skydd

Sekretessmarkering är den minst ingripande formen av skydd av personuppgifter som innebär att Skatteverket gör en sekretessmarkering av enskild persons uppgifter i folkbokföringen (se 5 kap. 5 § offentlighets- och sekretesslagen [2009:400], OSL). Syftet är att förhindra att hotande eller förföljande person med hjälp av personuppgifter kan hitta och utsätta person för brott, förföljelse eller trakasserier.

Sekretessmarkeringen är dock inte ett bindande beslut, endast en indikation på att folkbokföringssekretess enligt 22 kap. 1 § OSL kan gälla för uppgifterna. Den fungerar alltså som en påminnelse eller varningssignal hos alla myndigheter om att det finns behov att göra en noggrann sekretessprövning innan personuppgifter lämnas ut.

I praktiken registrerar Skatteverket en sekretessmarkering som aviseras tillsammans med personuppgifterna till alla myndigheter som får grundläggande personuppgifter från Skatteverkets folkbokföringsverksamhet. Det är den enskilde som ansöker om sekretessmarkering hos Skatteverket. Det finns inga formella krav för att beviljas skyddsåtgärden men den enskilde behöver motivera varför den behöver sekretessmarkering med någon form av handling som stödjer att det föreligger ett aktuellt och konkret hot. Det kan till exempel vara en utredning eller ett utlåtande från Polismyndigheten eller socialtjänsten. Sekretessmarkeringen gäller ofta i två år och kan förlängas.

Skyddad folkbokföring ger starkare skydd än sekretessmarkering

Skyddad folkbokföring ger starkare skydd än sekretessmarkering och innebär att en person kan vara folkbokförd på sin gamla folkbokföringsort efter att ha flyttat. De gamla adressuppgifterna tas bort och den nya adressen registreras inte i folkbokföringen och sprids därmed aldrig till andra myndigheter. Uppgifterna om skyddad folkbokföring skickas till andra myndigheter och annan samhällsservice som personen har kontakt med, till exempel sjukvården, Försäkringskassan och kommunen. Det betyder att dessa instanser kan se att personen har skyddad folkbokföring.

Skyddad folkbokföring medges för person som av särskilda skäl kan antas bli utsatt för brott, förföljelser eller allvarliga trakasserier på annat sätt, om åtgärden med hänsyn till den enskildes förmåga och övriga förutsättningar kan antas tillgodose behovet av skydd. Skyddad folkbokföring kan kombineras med andra skyddsåtgärder som exempelvis kontaktförbud om det bedöms lämpligt utifrån den enskildes specifika situation. Skyddad folkbokföring medges efter ansökan från den enskilde. För barn under 18 år får ansökan enbart göras av den ena vårdnadshavaren i det fall syftet är att skydda från den andra vårdnadshavaren.

Fingerade personuppgifter är den starkaste och mest ingripande formen av skydd

År 2015 fanns i Sverige ungefär 160 personer med fingerade personuppgifter. Fingerade uppgifter betyder att personen använder andra personuppgifter än de verkliga. Detta medför dock inte någon rättslig förändring av personens namn eller andra förhållanden. Kopplingen mellan den verkliga och den fingerade identiteten är sekretessbelagd. Med den nya identiteten kan personen vara öppen med sina personuppgifter utan risk att bli hittad. Fingerade personuppgifter har inget skydd i de systemstöd som används i en region eller kommun eftersom de hanteras som vilken person som helst.

Offentlighets- och sekretesslagen reglerar utlämning av allmänna handlingar

Offentlighets- och sekretesslagen (OSL) innehåller bestämmelser för hur myndigheter ska registrera, lämna ut och hantera allmänna handlingar. Det finns också regler om tystnadsplikt och förbud att lämna ut allmänna handlingar.

Utöver de tre skyddsformerna (sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter) finns en särskild generell sekretessbestämmelse som gäller för vissa personuppgifter om det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs (21 kap. 3 § första stycket OSL).

Sekretessen gäller uppgift om en enskilds

- bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde stadigvarande eller tillfälligt bor,
- telefonnummer,
- e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med personen.

Sekretessen gäller även för motsvarande uppgifter om personens anhöriga. Bestämmelsen gäller oavsett sammanhang som uppgiften förekommer i.

Bilaga 3. Kommunstyrelsens och nämndernas ansvarsområden

Kommunstyrelsen

Av *Reglemente för Umeå kommuns styrelse och nämnder*[16] framgår bland annat att kommunstyrelsen styr, leder och samordnar kommunens verksamheter och ekonomi samt följer upp och rapporterar utvecklingen i kommunens verksamheter till kommunfullmäktige. Kommunstyrelsen ska samordna förvaltningen av kommunens angelägenheter och ha uppsikt över kommunens nämnder, bolag och av kommunen förvaltade stiftelser. Kommunstyrelsen ska utöva en samordnad styrning, bereda ärenden inför kommunfullmäktige och ansvara för uppföljning av att fullmäktiges beslut genomförs. Kommunstyrelsen har ansvar att leda och samordna utveckling av för kommunen strategiskt viktiga områden som ej fördelats till annan nämnd, exempelvis kommunövergripande arbete med social, ekologisk och ekonomisk hållbarhet, näringslivs- och tillväxtpolitiskt arbete samt bostads- respektive markförsörjning. Dessutom har kommunstyrelsen ett särskilt ansvar för bland annat:

- Kommunkansli, arkiv och juridik
- Arbetsgivarfrågor och lönehantering
- Ekonomi, styrning och upphandling
- Digitalisering
- Kommunikation
- Säkerhet och trygghet

För- och grundskolenämnden

För- och grundskolenämnden har ett övergripande ansvar för att alla barn folkbokförda i kommunen har tillgång till förskola och pedagogisk omsorg samt skolgång i kommunens egna eller i fristående verksamheter. Nämnden ansvarar för kommunal förskola inklusive förskolor på minoritetsspråk, pedagogisk omsorg i form av dagbarnvårdare och nattisverksamhet, förskoleklass, grundskola, anpassad grundskola och fritidshem. Nämnden ansvarar för att fördela resurser till egen verksamhet och till fristående verksamheter enligt bidrag på lika villkor. Vidare har nämnden ansvar för skolpliktsbevakning och samverkan med fristående verksamheter i egenskap av hemkommun, samt att bevilja tillstånd och genomföra tillsyn av fristående förskoleverksamheter eller pedagogisk omsorg.

För- och grundskolenämnden ansvarar för de åligganden som åvilar kommunen enligt skollagen och annan lagstiftning som rör nämndens område och inte ska fullgöras av annan. Nämnden ska verka för att skollagstiftningens mål kan uppfyllas i nämndens verksamheter. Nämnden ansvarar exempelvis för att det finns skolbibliotek, elevhälsa, studie- och yrkesvägledning samt modersmålsundervisning i nämndens verksamheter. Vidare ansvarar nämnden för myndighetsutövning enligt skollagen, för både kommunala och fristående verksamheter, exempelvis gällande skolskjuts samt interkommunala frågor. Nämnden svarar för ledning, samordning och utveckling av det kommunala skolväsendet.

[16] Fastställt av kommunfullmäktige 2022-12-19 § 297.

Gymnasie- och vuxenutbildningsnämnden

Gymnasie- och vuxenutbildningsnämnden har ett övergripande ansvar för att alla ungdomar och unga vuxna boende i kommunen har tillgång till skola i kommunens egna verksamheter eller i fristående verksamheter. Nämnden ansvarar för kommunens gymnasieskolor, anpassad gymnasieskola, Elitidrottsgymnasium (NIU- och RIG) och Riksgymnasium för rörelsehindrade (RH-gymnasium. Nämnden ska säkerställa att nämndens verksamheter ger eleverna en grund för fortsatta studier och/eller yrkesverksamhet, samt ett aktivt deltagande i samhället i övrigt. Nämnden ansvarar övergripande för ledning, samordning och utveckling av skolväsendet

Vidare har nämnden ett samlat ansvar för det kommunala aktivitetsansvaret och kommunal vuxenutbildning på grundläggande nivå, gymnasienivå och som anpassad utbildning samt svenska för invandrare (sfi). Nämnden svarar vidare för arbetsmarknad och integration, genom att tillhandahålla sysselsättningsbefrämjande åtgärder samt mottagande av vissa nyanlända invandrare för bosättning. Nämnden ska verka för att skollagstiftningens mål kan uppfyllas. Nämnden ansvarar för myndighetsutövning enligt skollagen, och svarar exempelvis för att det finns skolbibliotek, elevhälsa, studie- och yrkesvägledning samt arbetsplatsförlagt lärande (APL). Vidare ansvarar nämnden för bestämmelserna kring elevresor, interkommunala skolfrågor och modersmålsundervisning.

Individ- och familjenämnden

Individ- och familjenämndens grunduppdrag är att tillgodose behov av stöd och omsorg inom socialtjänstens lagstadgade ansvarsområde för att stärka och trygga den enskilde att leva ett självständigt liv. Socialtjänsten arbetar förebyggande för att främja jämlika levnadsvillkor. Grunduppdraget omfattar att:

- Ge stöd, omsorg och skydd till barn, unga och vuxna
- Ge stöd och service till barn, unga och vuxna med funktionsnedsättning
- Ge stöd till självförsörjning och tillgodose behov av försörjningsstöd
- Tillgodose behov av råd, stöd samt handläggning av familjerättsliga frågor
- Tillhandahålla familjerådgivning
- Erbjuda hälso- och sjukvård till personer i bostad med särskild service och under vistelsetid på daglig verksamhet
- Erbjuda hälso- och sjukvård till personer i ordinärt boende (hemsjukvård under 65 år)

Kulturnämnden

Kulturnämnden svarar för folkbibliotek, Skolbiblioteksservice, konstverksamhet, kulturskola, kvinnohistoriskt museum, kultur i skolan, kultur för seniorer, arrangemang i Väven och kommungemensamma arrangemang samt den kommungemensamma konstsamlingen.

Kulturnämnden svarar för den politiska styrningen av kommunens verksamheter såsom folkbibliotek, Skolbiblioteksservice, konstverksamhet, kulturskola, kvinnohistoriskt museum, kultur i skolan, kultur för seniorer, arrangemang i Väven och kommungemensamma arrangemang.

Utöver detta har kulturnämnden även ett ansvar för Sveriges depåbibliotek och lånecentral samt stöd till kulturföreningar, kulturfestivaler och studieförbund. Kulturnämnden fördelar stipendier och annat stöd till kulturutövare samt till samlingslokaler. Kulturnämnden svarar för

de uppgifter som åligger kommunen i enlighet med Bibliotekslag (2013:801) samt Museilag (2017:563).

Fritidsnämnden

Fritidsnämnden ansvarar för att erbjuda Umeås invånare ett rikt, jämlikt, jämställt och hållbart fritidsutbud, där barn och ungas delaktighet och möjlighet till utveckling har en särställning. Nämnden erbjuder fritidsaktiviteter och inkluderande mötesplatser, för unga liksom för vuxna med intellektuell funktionsnedsättning. Nämnden har det samlade ansvaret för handläggning av kommunens föreningsbidrag, samt ett särskilt uppdrag att stödja föreningslivet och främja det ideella engagemanget. Nämnden ansvarar för skötsel och uthyrning av idrotts- och fritidsanläggningar, både för elit- och breddidrott. I uppdraget ingår även skötsel av friluftsområden samt fiskefrämjande åtgärder. Nämnden har i uppdrag att erbjuda Umeås invånare badupplevelser, friskvård samt ansvara för simundervisning för samtliga grundskoleelever.