Örebro kommun

Granskning av kommunens hantering av skyddade personuppgifter

Building a better working world

Building a better working world

Innehållsförteckning

Sammanfattande bedömning och rekommendationer

Granskningen syftar till att bedöma hur kommunen säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade. Vår sammanfattande bedömning är att det förekommer brister i kommunens hantering av skyddade personuppgifter.

Det finns ändamålsenliga styrande dokument och rutiner för hanteringen av skyddade personuppgifter på kommunövergripande nivå samt vissa lokala rutiner som förvaltningarna tagit fram. Utöver centrala och lokala rutiner har inga specifika åtgärder vidtagits för att minska risken för röjning av skyddade personuppgifter. Vi bedömer vidare att ansvarsfördelningen tydliggörs i de styrande dokumenten men att berörda nämnder inte fullt omhändertagit sitt ansvar inom informationssäkerhetsarbetet och hanteringen av skyddade personuppgifter. Vi ser det som en brist att *Instruktionen för hantering av personuppgiftsincidenter* inte är välkänd inom kommunen och att det inte finns en enhetlig hantering av personuppgiftsincidenter. Vi har under granskningen inte noterat något arbete för att sprida antagna riktlinjer och policys inom kommunen.

Säkerhetsavdelningen kan involveras för att bistå vid riskanalyser för medarbetare med skyddade personuppgifter om verksamheterna önskar det stödet. I en sådan process beaktas hotbilden och individens enskilda perspektiv. Dock sker detta endast på begäran av verksamheten och inte systematiskt, vilket vi skulle rekommendera.

Kommunstyrelsen har delvis säkerställt en tillräcklig uppföljning och kontroll av informationssäkerhetsarbetet, det sker dock ingen specifik uppföljning eller kontroll av hanteringen av skyddade personuppgifter. Det finns inget ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns inget automatiskt sätt att samla personuppgiftsincidenter på kommunövergripande nivå utan manuell handpåläggning. Vi bedömer det även som en brist att verksamheterna inte kan koda incidenten som ett skyddat personuppgiftsärende.

Vår bedömning är att det inte genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter. Medvetandegrad och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning.

Informationssäkerhetsfrågan lyfts vid ett flertal tillfällen, för olika nämnder, i riskanalyserna. De risker som identifierats har en indirekt koppling med hanteringen av skyddade personuppgifter, det finns ingen risk med direkt bäring på individer med skyddade personuppgifter.

Utifrån granskningens iakttagelser rekommenderar vi kommunstyrelsen att:

- Säkerställa en enhetlig hantering av personuppgiftsincidenter inom hela kommunorganisationen genom att öka medarbetares kännedom om riktlinjer och rutiner.
- Genomföra risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter och vid behov låt inkludera i internkontrollplanerna.
- Prioritera att genomföra obligatoriska utbildningar för samtlig personal avseende hanteringen av skyddade personuppgifter utifrån bestämmelser i styrande dokument.
- Överväga inrättandet av "compliancefunktion/-er", det vill säga en funktion som

ansvarar för att bestämmelser och interna verksamhetsprinciper, som exempelvis riktlinjer, rutiner och anvisningar, följs och följs upp.

- Säkerställa en ändamålsenlig nivå av uppföljning och att avvikelsehanteringen avseende skyddade personuppgifter stärks

1. Inledning

1.1. Bakgrund

Stadsrevisorerna har i sin riskanalys för 2022 identifierat hanteringen av skyddade personuppgifter som ett angeläget område för fördjupning och beslutat att genomföra en granskning. Det är en angelägen uppgift för samhället att ge skydd till de personer som riskerar att utsättas för olika typer av brott, hot och förföljelse och därav lever med skyddad identitet. I många av kommunens verksamheter ingår hantering av personuppgifter, liksom för kommunens egen personal. Det är viktigt att säkerställa att skyddade personuppgifter inte röjs då det kan leda till allvarliga konsekvenser för den enskilde. Om skyddade personuppgifter hanteras på felaktigt sätt kan det även leda till att kommunen tvingas erlägga skadestånd eller sanktionsavgift.

1.2. Syfte och revisionsfrågor

Granskningen syftar till att bedöma hur kommunen säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade.

I granskningen besvaras följande revisionsfrågor:

- Har kommunen analyserat risken för att skyddade personuppgifter röjs på ett ändamålsenligt sätt?
  - ✓ Har den enskilda individens perspektiv beaktats?
- Har kommunen vidtagit ändamålsenliga åtgärder för att minska risken för röjning av skyddade personuppgifter och följs detta upp av berörda nämnder?
- 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?
- Finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter?
  - ✓ Hur tillvaratas erfarenheter från avvikelser?
- Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits med utgångspunkt i dessa analyser?

1.3. Ansvariga nämnder

Granskningen avser kommunstyrelsen, förskolenämnden, grundskolenämnden, gymnasienämnden och socialnämnden.

1.4. Metod och genomförande

Granskningen baseras på genomgång av och granskning av styrande dokument och annan upprättad dokumentation samt intervjuer med företrädare för kommunens säkerhetsavdelning, juridikenhet, digitaliseringsavdelning, HR-enheten samt chefer och medarbetare inom socialförvaltningen och utbildningsförvaltningen. Antalet intervjuer uppgår till 17 personer.

Bedömningar, slutsatser och rekommendationer utgår från den samlade bilden av styrande dokument som inventerats och jämförts med hur representanter för kommunens verksamheter i intervjuer beskriver och uppfattar förutsättningarna att hantera skyddade personuppgifter.

1.5. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som används i granskningen för analyser, slutsatser och bedömningar. Revisionskriterierna utgörs huvudsakligen av:

- Kommunallagen (2017:725)
- Offentlighets- och sekretesslagen (2009:400)
- Folkbokföringslag (1991:481)
- Folkbokföringsförordning (1991:749)
- SFS 2018:684 Lag om ändring i folkbokföringslagen (1991:481)
- Socialtjänstlagen (2001:453)
- Skollagen (2010:800)
- Av kommunfullmäktige antagna styrdokument

Dessa beskrivs närmare i kapitel 2 och 3.

2. Utgångspunkter för granskningen

2.1. Kommunallagen (2017:725)

Kommunstyrelsen ska enligt 6 kap. 1 § kommunallagen (KL) leda och samordna förvaltningen av kommunens angelägenheter och ha uppsikt över övriga nämnders verksamhet. Av 6 kap. 11 § KL framgår att styrelsen ska följa de frågor som kan inverka på kommunens utveckling och ekonomiska ställning.

Av 6 kap. 6 § KL framgår 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.

2.2. Om begreppet skyddade personuppgifter

Det har blivit vanligare att människor lever med skyddade personuppgifter. De senaste tio åren har antalet 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 650 invånare och ett tjugotal anställda inom Örebro kommun. Siffrorna är inte exakta men visar att det statistiskt handlar om ett begränsat antal 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[1] 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 samtliga kvinnor i Jämställdhetsmyndighetens intervjustudie har fått skyddade personuppgifter röjda av myndigheter.

2.3. 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).

2.3.1 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.

2.3.2 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.

[1] *Skyddade personuppgifter – Oskyddade personer* (Rapport 2022:10).

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.

2.3.3 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.

Det är den enskilde som ansöker om fingerade personuppgifter hos Polismyndigheten. Medgivandet får begränsas till viss tid. En person som ansöker om, eller fått medgivande att använda fingerade personuppgifter, får ansöka om medgivande även för barn som personen är vårdnadshavare för och varaktigt bor tillsammans med, om syftet är att ge skydd mot den andre vårdnadshavaren.

Myndigheter är skyldiga att lämna upplysning om en person i ett ärende om fingerade uppgifter på begäran av Polismyndigheten. Polismyndigheten har ansvar att bistå en person med fingerade personuppgifter vid kontakter med andra myndigheter samt i övrigt lämna den hjälp som krävs, om den enskildes hjälpbehov inte kan tillgodoses på annat sätt. Medgivandet upphör om den enskilde själv skriftligen anmäler hos Polismyndigheten att det inte längre behövs. Om det finns särskilda skäl kan även Polismyndigheten besluta att medgivandet ska upphöra.

Fingerade personuppgifter har inget skydd i de systemstöd som används i en region eller kommun eftersom de hanteras som vilken person som helst.

2.4. 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.

3. Styrning, organisation och uppföljning av hanteringen av skyddade personuppgifter på kommun-övergripande nivå

3.1. Det finns ett antal kommunövergripande riktlinjer som berör skyddade personuppgifter

I kommunen finns kommunövergripande policyers, riktlinjer och rutiner gällande hanteringen av skyddade personuppgifter. Dessa sammanfattas i tabellen nedan:

Riktlinje/rutin/anvisning	Kort beskrivning
"Informationssäkerhetspolicy" (Ks 412/2016)	Policyn syftar till att säkra en tillförlitlig informationshantering i en digitaliserad värld. Policyn är ett övergripande dokument som redovisar kommunens mål och inriktningar med informationssäkerhet. Policyn ska regelbundet följas upp av informationssäkerhetsansvarig och återrapporteras till kommunstyrelsen och kommundirektör.
"Dataskyddspolicy" (Ks 630/2018)	Policyn syftar till att beskriva kommunens hantering av personuppgifter på en övergripande nivå. Dokumentet fastställer även övergripande mål och intentioner för arbetet med hantering av personuppgifter. Målet för kommunen är att all behandling sker med hänsyn till den enskildes friheter och rättigheter.
"Hantering av personer med skyddade personuppgifter" (Ks 1160/2017)	Riktlinjen syftar till att säkerställa att skyddade personuppgifter hanteras på rätt sätt. Riktlinjen reglerar hantering av dokumentation, IT-stöd, kommunikation och utlämning av handlingar.
"Riktlinjer för informationssäkerhet" (Ks 267/2019)	Riktlinjen syftar till att konkretisera informationssäkerhetspolicyn med detaljerad information och regler för hur information får hanteras inom kommunen. Det fastställs att skyddade personuppgifter är konfidentiell information och ska hanteras utifrån särskilda rutiner och regler. Inom respektive system ska det finnas användarinstruktioner för bland annat hanteringen av skyddade personuppgifter.
"Riktlinjer för sociala medier i Örebro kommun" (Diarienummer saknas)	Riktlinjen syftar till att övergripande beskriva hur kommunen arbetar med sociala medier. Det fastställs att kommunen inte publicerar personuppgifter i sociala medier utan att säkerställa att berörda parter godkänner detta.
"Rutin för jobbansökningar från personer med skyddade personuppgifter" (KSF-HR4)	Rutinen syftar till att säkerställa ett gemensamt och säkert arbetssätt för hanteringen av jobbsökningar från personer med skyddade personuppgifter. Uppgifter ska hanteras med försiktighet och all kontakt ska ske på det viset som kandidaten önskar.
"Instruktion för hantering av personuppgiftsincident"	Instruktionen syftar till att tydliggöra hur tjänstepersonorganisationen ska agera när en personuppgiftsincident inträffar. Det framgår dock att instruktionen inte är välkänd inom organisationen och att den inte finns tillgänglig på kommunens intranät.

3.2. Ansvarsfördelningen för informationssäkerhetsarbetet tydliggörs i policys och riktlinjer

I *Informationssäkerhetspolicyn* redovisas roll- och ansvarsfördelningen för informationssäkerheten i kommunen. Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Ansvarig för en viss verksamhet ansvarar därav också för informationssäkerheten inom samma område. Funktioner som arbetar specifikt med informationssäkerhet stöttar övrig förvaltning i sin hantering. Det tydliggörs att kommunstyrelsen och övriga nämnder i kommunen är personuppgiftsansvariga och ansvarar för hanteringen av personuppgifter.

Styrelsen och nämnder är ytterst ansvariga, enligt *Dataskyddspolicyn*, för bland annat:

- följa gällande lagstiftning
- fastställa ändamål med behandlingar
- säkerställa att det finns ett dataskyddsombud
- ett giltigt personuppgiftsbiträdesavtal finns upprättat vid behov
- riskanalyser är dokumenterade
- säkerställa att det görs konsekvensbedömningar om behandlingar sannolikt medför en hög risk för den registrerades integritet
- säkerställa att personuppgiftsincidenter rapporteras till tillsynsmyndigheten
- tillgodose registrerades rättigheter gällande information, tillgång (utlämning), rättning, begränsning, invändning och dataportabilitet

I riktlinjen för *Hantering av personer med skyddade personuppgifter* fastställs att varje nämnd ansvarar för att kartlägga behovet av lokala rutiner. Om felaktig uppgift röjs ska det hanteras skyndsamt utifrån fastställd lokal rutin, dataskyddsombudet ska även informeras omgående.

Kommunens dataskyddsombud ansvarar för följande uppgifter:

- informera och ge råd till personuppgiftsansvariga
- övervaka efterlevnad av personuppgiftsbehandlingar
- ge råd vid riskanalyser och assistera med konsekvensbedömningar
- vara kontakt för registrerade och tillsynsmyndighet
- samarbeta och begära förhandsråd av tillsynsmyndighet vid behov

Vid intervju anges att det finns ett Dataskyddsombud utsedd för samtliga nämnder och majoritetsägda bolag som inte har tillräckliga resurser för att genomföra samtliga uppgifter som faller på rollen. Ombudet anges främst arbeta reaktivt och inte förebyggande. Under 2018 utsågs GDPR kontaktpersoner inom förvaltningarna som dataskyddsombudet kallade till informationsmöten. Kontaktpersonerna skulle sedan föra informationen vidare till förvaltningen samt fånga upp eventuella oklarheter. Samarbetet med GDPR kontaktpersonerna är inte aktivt i dagsläget.

Intervjupersoner anger att kunskapen om ansvarsfördelningen gällande informationssäkerheten i vissa avseenden brister. Det finns en övergripande förståelse för ansvarsfördelningen i kommunen men konsekvenser som bristande informationssäkerhet kan leda till är inte lika välkända vilket gör att vikten av ansvaret förbises.

3.3. Digitaliseringsutvecklingen är prioriterad men informations-säkerhetsarbetet behöver komma i kapp

Det finns en förståelse inom kommunen för att arbetet med informationssäkerhet är viktigt, det uppges även finnas stöd från politiken som enligt intervjupersoner vill öka informationssäkerheten i kommunen för att undvika externa intrång i system och påverkanskampanjer, vilket blivit reala risker till följd av en ostabil omvärld. Verkställandet får dock ingen verklig prioritet. En förutsättning för fungerande informationssäkerhet är ändamålsenliga verksamhetssystem. För att utveckla verksamhetssystemen krävs resurser och kunskap vilket de lokala förvaltningarna inte alltid besitter/prioriterar och enligt uppgift har även IT avdelningen knappa resurser gällande informationssäkerhetsarbetet vilket innebär att frågan inte prioriteras. Digitaliseringsavdelningen är en stöttande funktion gentemot förvaltningarna men de kan inte driva utvecklingen när nämnden har huvudansvaret för systemen och informationssäkerheten.

Kunskapen om hanteringen av skyddade personuppgifter anges vara högre än andra delar av informationssäkerhetsarbetet till följd av ny lagstiftning och uppgifternas känsliga karaktär. Intervjupersoner anser dock att det inte finns tillräcklig guidning eller stöd för chefer gällande hur skyddade personuppgifter ska hanteras. Arbetet med GDPR anges inte vara fullt utvecklat i kommunen och det finns inget etablerat arbetssätt för hur tjänstepersoner ska hantera skyddade personuppgifter.

Vid intervju anges att Örebro kommun har en underutvecklad informationssäkerhet och arbetssätt som inte utvecklas i takt med digitaliseringen. När kommunens verksamheter digitaliseras ökar kravet på informationssäkerhet eftersom mer information finns digitalt. Digitaliseringsutvecklingen anges vara för snabb för att informationssäkerhetsarbete ska hinna med. Det är ett politiskt fokus att öka kommunens digitaliseringsmognad men den utvecklingen kräver ökade resurser och långsiktigt perspektiv, vilket försvårar genomförandet.

Systemen som används i kommunen är inte integrerade, om en uppgift ändras i exempelvis HR-systemet kommer det inte automatiskt ändras i de andra systemen. Kommunen arbetar inte med förflyttning av data utan varje system fungerar självständigt. Det finns vissa system som har koppling till varandra samt andra myndigheter men det finns ingen gemensam hantering.

3.4. Det förekommer medarbetare med skyddade personuppgifter i kommunen

Om en medarbetar inom kommunen har skyddade personuppgifter krävs det att medarbetarens kollegor och överordnande har kunskap om hanteringen av skyddade personuppgifter. Medarbetaren får i systemen välja ett användarnamn i stället för sina personuppgifter som behörighetstillgång. I ett av kommunens system måste dock medarbetaren ange sitt riktiga namn, den informationen är skyddad och det krävs behörighet för att få tillgång till det riktiga namnet i systemet. Medarbetaren ger kommunen sitt muntliga medgivande att använda sitt riktiga namn i systemet. Det faller på medarbetaren att informera närstående chef och HR att hen har skyddade personuppgifter, om kommunen inte får informationen kan de inte agera i enlighet med bestämmelserna. Medarbetaren är delaktig i utformningen av skyddet i kommunens verksamhet och system. Intervjuperson anger att antalet medarbetare med skyddade personuppgifter ökar.

Säkerhetsavdelningen kan involveras vid hanteringen av en medarbetare med skyddade personuppgifter om den lokala verksamheten söker stöd. De deltar då vid genomförandet av riskanalyser över medarbetarens hotbild. Det som analyseras är eventuella hot- och våldssituationer som kan uppstå samt vilka åtgärder som kan tillämpas för att undvika samt hantera dessa situationer. Det analyseras även vilka kollegor som bör känna till att medarbetaren har skyddade personuppgifter.

Vid rekrytering krävs vissa kontaktuppgifter som telefonnummer och personnummer, dock anges namn inte vara nödvändigt. Intervjupersoner upplever att det finns stöd vid hanteringen av skyddade personuppgifter vid rekrytering men att stödet främst gäller den praktiska hanteringen i verksamhetssystem. Det finns andra situationer som kan uppstå på arbetsplatsen kopplat till medarbetare med skyddade personuppgifter där chefer efterfrågar stöd.

3.5. Det sker ett centralt uppföljningsarbete gällande informationssäkerheten och dess status

Örebro kommun arbetar med ledningssystem för informationssäkerhet (LIS) som säkerställer ett systematiskt arbete. En gång om året sedan 2020 går informationssäkerhetsstrategen igenom ledningssystemet för att identifiera eventuella brister och förbättringsåtgärder, genomgången sammanställs i en rapport som föredras för kommundirektören och kommunstyrelsen. Utifrån bristerna samt de rekommenderade åtgärderna som identifieras vid genomgången tas en handlingsplan för informationssäkerhet fram. Vi har tagit del av *Handlingsplan för informationssäkerhet 2019*, *Handlingsplan för informationssäkerhet 2020–2021* och *Handlingsplan för informationssäkerhet 2022–2023* som samtliga är antagna av kommundirektören.

I *Ledningens genomgång av LIS, 2022*, görs bedömningen att kommunen har en låg mognadsgrad gällande att skydda information som sekretess och känsliga personuppgifter. I rapporten sammanfattas även informationssäkerhetsincidenter som uppstår under verksamhetsåret, under 2021 rapporterades 26 personuppgiftsincidenter varav 19 rapporterades till Integritetsskyddsmyndigheten. Det finns ingen sammanställning för personuppgiftsincidenter under 2020 men under 2019 diarieförde s ca 50 incidenter varav ett trettiotal rapporterats till myndigheten. En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, röjning eller ändring av personuppgifter. Antalet informationssäkerhetsincidenter som är inrapporterade anges vara låg och det bedöms finnas ett mycket stort mörkertal. Rapporten fastställer även att det saknas en kontinuerlig sammanställning och uppföljning av personuppgiftsincidenter inom kommunen.

Varje år genomför samtliga förvaltningar en självskattning av informationssäkerheten inom verksamheten. Under 2022 samlades även en del grundläggande information in från alla förvaltningar och presenterades i *Ledningens genomgång av LIS, 2022*. Se tabellen nedan:

Grundläggande information	Utfall
Hur många informationssäkerhetsincidenter har ni haft under 2021?	0
Hur många personuppgiftsincidenter har förvaltningen haft under 2021?	26

Hur många personuppgiftsincidenter är rapporterade till IMY?	19
Hur många riskanalyser rörande informationssäkerhet är genomförda under 2021?	15
Förvaltningen har en utsedd kontaktperson för dataskyddsfrågor?	56 %
Förvaltningen har en informationshanteringsplan som är uppdaterad 2020 eller 2021?	33 %
Förvaltningen har tillräckliga kunskaper inom informationssäkerhet?	33 %
Förvaltningen får tillräckligt sakkunnigt stöd i arbetet med Informationssäkerhet?	56 %

I Ledningens genomgång genomförs även en översikt av kommunens system och hur god informationssäkerheten är inom systemen. Det framgår att knappt något av de granskade systemen klarar av att hantera sekretessbelagd information eller känsliga personuppgifter i enlighet med gällande lagstiftning.

Ett annat sätt att följa upp informationssäkerheten är kontroll av loggar. I verksamhetssystem skapas loggar över vilka användare som är inne i systemen och vad dom gör i systemen. Intervjupersoner anger att det i dagsläget inte förekommer någon systematisk uppföljning och kontroll av loggarna för att säkerställa att endast behöriga medarbetare har tillgång till systemen. Intervjupersoner anger att det kan förekomma kontroller av loggar vid uppmärksammade incidenter men arbetet blir därav reaktivt. Den bristande kontrollen över behörigheterna i systemen är kända inom verksamheten och något som ska utredas.

3.6. Vår bedömning

Vår bedömning är att det finns ändamålsenliga styrande dokument och utformade rutiner för hanteringen av skyddade personuppgifter. Vi bedömer vidare att ansvarsfördelningen tydliggörs i de styrande dokumenten men att granskade nämnder inte fullt omhändertagit sitt ansvar inom informationssäkerhetsarbetet och hanteringen av skyddade personuppgifter. De lokala verksamheternas ansvarsområden är omfattande och innehåller flera frågor, det är vår bedömning att informationssäkerhetsarbetet inte prioriterats av förvaltningarna.

Digitaliseringsavdelningen ska fungera som en stödfunktion till de lokala verksamheterna som i sin tur ansvarar för att utveckla och driva informationssäkerhetsfrågorna, om förvaltningen inte väljer att utveckla arbetet har IT inget mandat att skynda på utvecklingen. En ökad förståelse gällande eventuella konsekvenser av bristande informationssäkerhetsarbete skulle kunna leda till ökat fokus på säkerhetsfrågorna.

Vi ser det som en brist att *Instruktionen för hantering av personuppgiftsincidenter* inte är välkänd inom kommunen och att det inte finns en enhetlig hantering av personuppgiftsincidenter. Vi har under granskningen inte noterat något arbete för att sprida antagna riktlinjer och policys inom kommunen.

Säkerhetsavdelningen kan involveras för att bistå vid riskanalyser för medarbetare med skyddade personuppgifter om verksamheterna önskar det stödet. I en sådan process beaktas hotbilden och individens enskilda perspektiv. Dock sker detta endast på begäran av

verksamheten och inte systematiskt, vilket vi skulle rekommendera.

Vid intervjuer framgår att vissa arbetsuppgifter som tillfaller dataskyddsombudet enligt lagstiftning samt interna styrdokument inte genomförs då arbetsbelastningen är för hög. Det krävs mer resurser för att säkerställa regelefterlevnad och ett ändamålsenligt arbete med personuppgiftshantering.

Arbetet för att digitalisera och effektivisera kommunens verksamheter är prioriterat, dock innebär ett ökat fokus på digitalisering en ökad utmaning inom den digitala informationssäkerheten. Det finns ett flertal identifierade brister i kommunens egna uppföljningar av informationssäkerheten som indikerar att kommunen behöver prioritera arbetet med informationssäkerhet och system som kan hantera sekretessbestämmelser.

Vår bedömning är att kommunstyrelsen delvis säkerställt en tillräcklig uppföljning och kontroll av informationssäkerhetsarbetet, det sker dock ingen specifik uppföljning eller kontroll av hanteringen av skyddade personuppgifter. Det finns en medvetenhet inom organisationen att informationssäkerhetsarbetet brister. Vi bedömer det som positivt att digitaliseringsavdelningen formulerar handlingsplaner utifrån identifierade brister vid ledningens genomgång. För att säkerställa att kommunen arbetar ändamålsenligt med informationssäkerhet krävs ett större engagemang från verksamheterna och mer resurssatta åtgärder.

4. Det förekommer delvis lokala rutiner och arbetssätt vid hantering av skyddade personuppgifter

I riktlinjen *Hantering av personer med skyddade personuppgifter* fastställs att *"arbetsrutiner ska finnas där det finns behov av dem för att säkra hanteringen av skyddade personuppgifter"*.

Nedan redogörs för berörda nämnders hantering av skyddade personuppgifter samt eventuella lokala rutiner.

- **Förskolenämnden och grundskolenämnden**

År 2016 genomfördes en granskning av grundskolenämndens hantering av personuppgifter på uppdrag av stadsrevisionen. Den sammanfattande bedömningen var att nämnden inte säkerställt att obehöriga inte kan komma åt personuppgifter som hanteras i skolan. Risken att personuppgifter sprids på ett oönskat sätt bedömdes som hög och nämnden hade inga egna riktlinjer för hanteringen av personuppgifter. Nämnden bedömdes även brista i sin kontroll över tillämpade IT-system.

Vid intervju uppges personalen inom utbildningsverksamheten ha varierad kunskap om hur barn och unga med skyddade personuppgifter ska hanteras. Vissa skolor har mer kontakt med elever som har skyddade personuppgifter vilket ökar kunskapen. Förvaltningens verksamhetssystem anges försvåra hanteringen då det är omständligt och svårhanterligt.

Inom förvaltningen för förskola och skola finns en utpekad informations-säkerhetssamordnare. Funktionen har funnits i drygt ett år med intentionen att bedriva ett mer systematiskt informationssäkerhetsarbete. Rollen som

informationssäkerhetssamordnare är inte en heltidstjänst. Informationssäkerhetsarbetet anges inte vara förebyggande utan snarare reaktivt då informationssäkerhetsarbetet ska inrymmas i sedan tidigare befintlig tjänst.

Det har inte förekommit några större incidenter gällande röjning av skyddade personuppgifter. Information om elever med skyddade personuppgifter ska vara begränsad och därav finns ingen överblick av antalet elever med skyddade personuppgifter.

Nämndledamöterna anges ha förtroende för verksamheten gällande hanteringen av personuppgifter men frågan om sekretess kan även diskuteras på politisk nivå.

Det finns i nuläget inga lokala rutiner för hanteringen av skyddade personuppgifter men det pågår ett arbete med att ta fram en rutin som skolorna kan använda för att säkerställa en enhetlig hantering av ärenden med skyddade personuppgifter. Det finns en gemensam rutin för grundskola och gymnasiet gällande hantering av elever med sekretesskydd i utbildningsverksamhetens system, se nedan:

Riktlinje/rutin/anvisning	Kort beskrivning
"Rutin för hantering av elever med sekretesskydd inom grundskola/gymnasium" (inget diarienummer)	Rutinen syftar till att säkerställa en korrekt hantering av elever med sekretesskydd inom grundskola/gymnasium. Rutinen beskriver hur verksamheten ska hantera ärendet i sitt elevregister.

- **Gymnasienämnden**

Inom förvaltningen anges det finnas kunskap kring hanteringen av skyddade personuppgifter, dock behöver den allmänna kunskapsnivån höjas. Det förekommer personuppgiftsincidenter men dessa resulterar sällan i direkt skada. Inom förvaltningen finns en utpekad informationssäkerhetssamordnare. Funktionen har funnits i drygt ett år och ska bedriva ett mer systematiskt informationssäkerhetsarbete. Rollen som informationssäkerhetssamordnare är inte en heltidstjänst.

När det finns en medarbetare eller elev med skyddade personuppgifter är fokuset på individen och inte på den risk som föreläggs andra genom att vara i samma sammanhang som den utsatta. Vid utsatta situationer finns säkerhetsåtgärder som förvaltningens medarbetare kan vidta. Eftersom förvaltningen som arbetar för gymnasienämnden också hanterar kommunens försörjningsstöd finns det god kunskap inom organisationen om hur hotfulla situationer hanteras.

Riktlinje/rutin/anvisning	Kort beskrivning
"Rutin för hantering av elever med skyddade personuppgifter – Örebro kommuns Gymnasieskolor, Riksgymnasier och Gymnasiesärskola" (Gy 34/2022)	Syftet med arbetsrutinen är att säkerställa att skyddade personuppgifter hanteras på rätt sätt inom kommunen. Rutinen beskriver hur skolan ska arbeta när en elev har eller får skyddade personuppgifter. Elevens behov ska kartläggas utifrån en mall för handlingsplan. Det fastställs i rutinen att om skyddade personuppgifter röjs kvalificeras det som en personuppgiftsincident som omgående ska rapporteras till dataskyddsombudet för anmälan till Integritetsskyddsmyndigheten. Det ska ske inom 72 timmar.

Rutinen för hanteringen av elever med skyddade personuppgifter är relativt ny inom

förvaltningen och har tagits fram utifrån Skolverkets riktlinjer. I samband med framtagandet av rutinen skapades en samverkansgrupp som löpande ska uppdatera rutinen och hålla den levande.
Intervjupersoner anger att rutinen säkerställer enhetlig hantering samt medvetenhet om frågan.

Under pandemin togs även en *Rutin för användning av röst- och videosamtal i Microsoft Teams* fram, den var aktiv till 2022-06-30. Rutinen gällde för förvaltningen förskola och skola samt förvaltningen för utbildning, försörjning och arbete då samtal med känsliga personuppgifter eller sekretessuppgifter diskuteras via Teams. Rutinen tydliggjorde ansvaret för informationsbehandlingen och vilka uppgifter som får hanteras i vilka medier.

- **Socialnämnden**

Frågan om informationssäkerhet anges vara aktuell inom nämnden och förvaltningen arbetar för att säkerställa att sekretesslagstiftningen efterlevs inom verksamheten. Det anges inte finnas något särskilt fokus på hanteringen av skyddade personuppgifter. Intervjupersoner är medvetna om att arbetet med informationssäkerheter brister på olika håll.

I förvaltningens verksamhetssystem särskiljs inte den ordinarie sekretessen och skyddade personuppgifter. Inom sociala insatser är sekretessen högt prioriterad och intervjupersoner anger att systemen omhändertar den problematiken som finns vid skyddade personuppgifter automatiskt utan att särskilja ärendet. Socialtjänstens verksamhetssystem har hög skyddsklassning då systemen hanterar känsliga data. Det hanteras även en del fysisk dokumentation inom förvaltningen vilket skapar krav på fysiska lösningar för att förhindra röjningar. Förvaltningen arbetar för att kartlägga den fysiska information som finns och därefter ska informationshanteringsplaner tas fram för att säkerställa en ändamålsenlig och säker hantering. Eventuell röjning av skyddade personuppgifter ses som en stor kvalitetsbrist och klassificeras som en incident med hög allvarlighetsgrad.

Inom socialnämndens förvaltning finns en informationssäkerhetssamordnare, utvecklingschef och verksamhetsutvecklare som arbetar med informations-säkerhetsfrågorna. Ansvaret för informationssäkerheten är därav spridd inom verksamheten. Funktionerna arbetar dels med framtagandet av rapporter vid personuppgiftsincidenter, dels anmälningar till Integritetsskyddsmyndigheten.

Socialnämnden arbetar utifrån sitt kvalitetsledningssystem vilket inkluderar ett flertal rutiner och riktlinjer. Det finns inga rutiner som specifikt reglerar hanteringen av skyddade personuppgifter men det förekommer hänvisningar till skyddade personuppgifter i andra mer övergripande rutiner. Det uppges att förvaltningen använder kommunens övergripande riktlinje, information från Skatteverket samt Socialstyrelsen vid hantering av skyddade personuppgifter. Enligt intervjupersoner finns inget behov av ytterligare lokala rutiner och riktlinjer. Se lokala rutiner nedan:

Riktlinje/rutin/anvisning	Kort beskrivning
”Ansökan om skyddade personuppgifter hos skatteverket ”sekretessmarkering”	Rutinen beskriver hur socialtjänsten ska ansöka hos Skatteverket om de vill folkbokföra en person som ska ha en sekretessmarkering.
”Rutin för informationssäkerhet” (Soc 1171/2020)	Syftet med rutinen är att komplettera Örebro kommuns riktlinjer för informationssäkerhet och tydliggöra hur Socialnämndens verksamhet ska arbeta med

	informationssäkerhet. I rutinen tydliggörs bland annat att e-post och meddelanden via mobiltelefon aldrig får skickas till individer med skyddade personuppgifter.

4.1. Vår bedömning

Vår bedömning är att det finns vissa lokala rutiner som förvaltningarna tagit fram, vi ser positivt på den rutin/handlingsplan som gymnasieverksamheten tagit fram för hanteringen av elever med skyddade personuppgifter samt att ett liknande arbete bedrivs inom förvaltningen för förskola och grundskola. Lokala rutiner och riktlinjer ökar chansen att medarbetare inom förvaltningarna har kunskap om hanteringen av skyddade personuppgifter samt håller frågan levande inom organisationen. Utöver lokala rutiner har inga specifika åtgärder vidtagits för att minska risken för röjning av skyddade personuppgifter.

Samtliga intervjupersoner anger att det finns viss kunskap om hanteringen av skyddade personuppgifter men att kunskapen varierar bland medarbetarna. Det finns roller inom samtliga förvaltningar som arbetar löpande med informationssäkerhetsfrågor, det finns dock inget särskilt fokus på hanteringen av skyddade personuppgifter. Ökad kunskap om problematiken och hanteringen av skyddade personuppgifter minskar risken för röjning.

Vår övergripande bedömning är att det finns kännedom kring frågorna gällande informationssäkerhet och hanteringen av skyddade personuppgifter, dock finns inget prioriterat utvecklingsarbete inom systemfrågorna utan verksamheterna agerar främst reaktivt.

5. Det förekommer ingen kompetensutveckling kring skyddade personuppgifter

Det finns ingen strukturerad kompetensutveckling på kommunövergripande nivå med direkt koppling till hanteringen av skyddade personuppgifter. På kommunövergripande nivå genomförs nano-utbildningar[2] som samtliga medarbetare ska genomföra. Den nano-utbildningen som intervjupersoner lyfter fram med viss koppling till hanteringen av skyddade personuppgifter berör hanteringen av offentliga handlingar. Intervjuperson lyfter att deltagandet i nano-utbildningar är lågt trots påminnelser var tredje vecka.

Den lokala kompetensutvecklingen som erbjuds inom berörda verksamheter redovisas nedan i tabellen:

Nämnd/Styrelse	Kompetensutveckling
Kommunstyrelsen	Medarbetare vid digitaliseringsavdelningen deltar i nätverk gällande informationssäkerhet vilket möjliggör informationsutbyte och diskussion. Det anges dock att skyddade personuppgifter inte varit i fokus.
Förskolenämnden	Inom utbildningsverksamheten förekommer det individuell kompetensutveckling vilket kan involvera hanteringen av

[2] En digital inlärningsupplevelse

Grundskolenämnden	skyddade personuppgifter. Medarbetarnas individuella kompetensutveckling beslutas i samtal med chef vid medarbetarsamtal.
Gymnasienämnden	Det förekommer ingen direkt kompetensutveckling kopplat till hanteringen av skyddade personuppgifter.
Socialnämnden	Det är inte tydligt vilken typ av kompetensutveckling gällande hanteringen av skyddade personuppgifter som erbjuds. Vid nyanställning får samtliga medarbetare tillgång till kommunens övergripande rutiner och riktlinjer vilket säkerställer en viss kunskapsnivå.

Det förekommer ingen lokal kompetensutveckling gällande hanteringen av skyddade personuppgifter i någon granskad förvaltning.

Inom samtliga förvaltningar ska det finnas en utsedd informationssäkerhetssamordnare, vid tillsättning av rollen erbjuds medarbetaren intern kompetensutveckling inom informationssäkerhet. Den interna utbildningen består av totalt sju dagars fördjupad utbildning, men utbildningen berör inte specifikt hanteringen av skyddade personuppgifter. Utbildningen kan även erbjudas till andra roller i kommunen än informationssäkerhetssamordnaren.

Informationssäkerhetssamordnarna, informationssäkerhetsspecialister och informationssäkerhetsstrateg utgör deltagarna i kommunens nätverk för informationssäkerhetsarbetet. Syftet med nätverket är att diskutera nuläget, aktuella händelser och byta erfarenheter med varandra. Gruppen samlas en gång i månaden.

I *Handlingsplan för informationssäkerhet 2022–2023* framgår två delmål inom kategorin anställning och utbildning med indirekt koppling till hanteringen av skyddade personuppgifter.

Delmål C1: Inkludera informationssäkerhet i anställnings- och uppsägningsprocessen och relaterade rutiner och arbetssätt.

Delmål C2: Ta fram och etablera en utbildningsplan i informationssäkerhet för samtliga anställda och utvalda grupperingar.

Delmålen är inte genomförda vid tidpunkten för granskningen.

5.1. Vår bedömning

Vår bedömning är att det inte genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter. Medvetandegrad och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning. Inom respektive område finns behov av ökad medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter. Det saknas en lärprocess uppbyggd av erfarenheter och riskbedömningar inom och mellan respektive verksamhetsområde.

Informationssäkerhetssamordnare får introduktions-utbildning inom informationssäkerhet, vi saknar dock fokus på hantering av skyddade personuppgifter.

6. Det finns ett strukturerat system för riskanalys inom kommunen och vissa identifierade risker berör informationssäkerhetsarbetet

Det förekommer ett strukturerat riskarbete inom kommunen men inte direkt kopplat till hanteringen av skyddade personuppgifter. Inom ramen för kommunens internkontrollarbete genomför samtliga nämnder och styrelsen årligen en riskanalys som ligger till grund för nämndens tillsynsplan. Utöver det formaliserade internkontrollarbetet arbetar förvaltningarna olika med riskanalyser kopplade till hanteringen av skyddade personuppgifter, se sammanställningen i tabellen nedan:

Nämnd/ Styrelse	Riskanalys 2021	Riskanalys 2022	Övrig riskanalys
Kommun-styrelsen	I riskanalysen för 2021 identifieras risken "Bristande stöd till övriga nämnder inom informations-försörjningsområdet" och resultatet av risken kan b.la bli att personuppgifter hanteras felaktigt. Även risken "Oklart införande av Office 365 och relationen till GDPR" identifieras och konsekvensen bedöms som röjning av personuppgifter. Dessa risker inkluderades inte i styrelsens tillsynsplan för 2021.	I riskanalysen för 2022 identifieras samma risker kopplat till skyddade personuppgifter som i riskanalysen för 2021. Dessa risker inkluderades inte i styrelsens tillsynsplan för 2022.	Digitaliseringsavdelningen genomför ostrukturerade riskanalyser vid kryptering av data för att bedöma risken vid eventuell röjning. Det dokumenteras inte. Det anges även ske riskanalyser vid implementering och översyn av systemstöd. Säkerhetsavdelningen kan delta vid riskanalyser kopplat till medarbetare med skyddade personuppgifter, då analyseras individens hotbild och eventuella säkerhetsåtgärder som kan tillämpas.
Förskole-nämnden	I nämndens riskanalys finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter.	I nämndens riskanalys för 2022 identifieras "efterlevnad av GDPR" som en risk. Det anges att om GDPR inte efterlevs finns en risk att personuppgiftshanteringen strider mot lag. En annan risk som identifieras är "efterlevnad av Riktlinjer för informationssäkerhet". Dessa risker inkluderas inte i nämndens tillsynsplan.	Om det förekommer en hotbild gentemot en elev genomförs en riskbedömning av situationen i samverkan med säkerhetsavdelningen. Det inkluderar förekomsten av skyddade personuppgifter.
Grundskole-nämnden	I nämndens riskanalys finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter.	I nämndens riskanalys för 2022 identifieras "efterlevnad av GDPR" som en risk. Det anges att om GDPR inte efterlevs finns en risk att personuppgiftshanteringen strider mot lag. En annan risk som identifieras är	

		"efterlevnad av Riktlinjer för informationssäkerhet" samt "Hantering av information om elever med sekretessmarkering". Dessa risker inkluderas inte i nämndens tillsynsplan.	
Gymnasie-nämnden	I nämndens riskanalys finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter.	I nämndens riskanalys finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter.	Vid framtagandet av den interna rutinen för hantering av elever med skyddade personuppgifter genomfördes en riskanalys. I den lokala rutinen fastställs att en handlingsplan ska tas fram för elev med skyddade personuppgifter, handlingsplanen fungerar även som en typ av individuell riskanalys.
Social-nämnden	I nämndens riskanalys finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter.	I nämndens riskanalys för 2022 identifieras "risk att man inte följer rutin för informationssäkerhet" vilket kan leda till sekretessbrott. Anledningen till att risken förekommer är att rutinen inte är välkänd inom verksamheten, den mänskliga faktorn och att medarbetare väljer att ha kontakt via SMS trots att det ska undvikas. Risken bedöms vara tillräckligt allvarlig och inkluderas i nämndens tillsynsplan för 2022.	Det sker individuella riskanalyser vid förekomsten av skyddade personuppgifter, dessa är dock inte dokumenterade eller strukturerade utan sker på eget bevåg.

6.1. Vår bedömning

Informationssäkerhetsfrågan lyfts vid ett flertal tillfällen, för olika nämnder, i riskanalyserna. Kommunstyrelsen identifierar samma brister under 2021 som för 2022, risken bedöms inte vara tillräckligt hög för att inkluderas i tillsynsplanen men det är positivt att styrelsen problematiserar och uppmärksammar riskerna kopplat till personuppgifter. Socialnämnden uppmärksammar risken med att inte efterleva kommunens rutin för informationssäkerhet och risken värderas tillräckligt högt för att inkluderas i nämndens tillsynsplan. De risker som identifierats har en indirekt koppling med hanteringen av skyddade personuppgifter, det finns ingen risk med direkt bäring på individer med skyddade personuppgifter. Risken för röjning av skyddade personuppgifter har inte bedömts och värderats utifrån genomförda risk- och konsekvensanalyser.

7. Det finns inget kommunövergripande avvikelsehanteringssystem

I *Instruktion för hantering av personuppgiftsincidenter* framgår att samtliga incidenter behöver dokumenteras i kommunens ärendehanteringssystem. Under granskningen noterar vi dock att instruktionen inte är välkänd inom verksamheterna och att det inte finns ett kommunövergripande system för avvikelsehantering för personuppgiftsincidenter. Personuppgiftsincidenter rapporteras i förvaltningens lokala verksamhetssystem. Exempelvis rapporteras eventuella avvikelser inom utbildningsverksamheten där elev har skyddade personuppgifter i det ordinarie verksamhetssystemet som en personuppgifts-incident. Om det berör en medarbetare med skyddade personuppgifter rapporteras incidenten i systemet för arbetsmiljö, samma gäller för socialförvaltningen. Inom socialförvaltningen sker en löpande rapportering vid klientkontakt och system för avvikelsehantering varierar inom förvaltningen, vissa har digitala system och andra rapporterar avvikelser fysiskt.

Det sker ingen strukturerad uppföljning och analys av avvikelsehanteringen kopplat till hanteringen av skyddade personuppgifter inom någon förvaltning. Den svagaste länken i hanteringen av skyddade personuppgifter anges vara kontakten med andra myndigheter samt den mänskliga faktorn.

Intervjupersoner har viss kännedom om röjningar av skyddade personuppgifter. Det anges att organisationen inte har information om tillfällen där skyddade personuppgifter inte röjdes men kunde ha röjts på grund av bristande hantering inom kommunen.

Det sker ingen automatisk aggregering av kommunens personuppgiftsincidenter utan vid framtagandet av statistik över personuppgiftsincidenter som presenteras i *Ledningens genomgång av LIS* krävs manuell hantering av data. Digitaliseringsavdelningen kontaktar respektive förvaltning och samlar manuellt ihop statistik över antalet incidenter. Vid dokumentering av en personuppgiftsincident i de lokala verksamhetssystemen finns inget sätt att koda ärendet för att tydliggöra att det berör skyddade personuppgifter.

7.1. Vår bedömning

Vår bedömning är att det inte finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns inget automatiskt sätt att samla personuppgiftsincidenter på kommunövergripande nivå utan manuell handpåläggning. Vi bedömer det även som en brist att verksamheterna inte kan koda incidenten som ett skyddat personuppgiftsärende. Det sker ingen systematisk uppföljning och analys över verksamhetens egna personuppgiftsincidenter som ligger till grund för verksamhetsutveckling.

8. Svar på revisionsfrågorna

Fråga	Svar
Har kommunen analyserat risken för att skyddade personuppgifter röjs på ett ändamålsenligt sätt? ► Har den enskilda individens perspektiv beaktats?	Delvis. Informationssäkerhetsfrågan lyfts vid ett flertal tillfällen, för olika nämnder, i riskanalyserna. Det är positivt att kommunstyrelsen problematiserar och uppmärksammar riskerna kopplat till personuppgifter i sin riskanalys. Socialnämnden uppmärksammar risken med att inte efterleva kommunens rutin för informationssäkerhet och risken värderas tillräckligt högt för att inkluderas i nämndens tillsynsplan. De risker som identifierats har en indirekt koppling med hanteringen av skyddade personuppgifter, det finns ingen risk med direkt bäring på individer med skyddade personuppgifter.
Har kommunen vidtagit ändamålsenliga åtgärder för att minska risken för röjning av skyddade personuppgifter och följs detta upp av berörda nämnder?	Delvis. Vår bedömning är att det antagits relevanta styrdokument på kommunövergripande nivå samt vissa lokala rutiner som förvaltningarna tagit fram, vi ser positivt på den rutin/handlingsplan som gymnasieverksamheten tagit fram för hanteringen av elever med skyddade personuppgifter samt att ett liknande arbete bedrivs inom förvaltningen för förskola och grundskola. Utöver lokala rutiner har inga specifika åtgärder vidtagits för att minska risken för röjning av skyddade personuppgifter.
Finns ändamålsenliga styrande dokument och rutiner för hantering av skyddade personuppgifter? ► Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?	Ja. Vår bedömning är att det finns ändamålsenliga styrande dokument och rutiner för hanteringen av skyddade personuppgifter. Vi bedömer vidare att ansvarsfördelningen tydliggörs i de styrande dokumenten men att vissa roller inte fullt omhändertagit sitt ansvar inom informationssäkerhetsarbetet och hanteringen av skyddade personuppgifter. Vi ser det som en brist att *Instruktionen för hantering av personuppgiftsincidenter* inte är välkänd inom kommunen och att det inte finns en enhetlig hantering av personuppgiftsincidenter. Vi har under granskningen inte noterat något arbete för att sprida antagna riktlinjer och policys inom kommunen.
Har kommunen säkerställt tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?	Delvis. Vår bedömning är att kommunstyrelsen delvis säkerställt en tillräcklig uppföljning och kontroll av informationssäkerhetsarbetet, det sker dock ingen specifik uppföljning eller kontroll av hanteringen av skyddade personuppgifter. Det finns en medvetenhet inom organisationen att informationssäkerhetsarbetet brister. Vi bedömer det som positivt att digitaliseringsavdelningen formulerar handlingsplaner utifrån identifierade brister vid ledningens genomgång. För att säkerställa att kommunen arbetar ändamålsenligt med informationssäkerhet krävs ett större engagemang från verksamheterna och mer resurssatta åtgärder.
Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?	Nej. Vår bedömning är att det inte genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter. Medvetandegrad och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning. Inom respektive område finns behov av ökad medvetandegrad och kunskapsnivå kring hanteringen av

	skyddade personuppgifter. Informationssäkerhetssamordnare får introduktions-utbildning inom informationssäkerhet, vi saknar dock fokus på hantering av skyddade personuppgifter.
Finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter? ► Hur tillvaratas erfarenhet från avvikelser?	Nej. Vår bedömning är att det inte finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns inget automatiskt sätt att samla personuppgiftsincidenter på kommunövergripande nivå utan manuell handpåläggning. Vi bedömer det även som en brist att verksamheterna inte kan koda incidenten som ett skyddat personuppgiftsärende. Det sker ingen systematisk uppföljning och analys över verksamhetens egna personuppgiftsincidenter som ligger till grund för verksamhetsutveckling.
Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits med utgångspunkt i dessa analyser?	Delvis. Säkerhetsavdelningen kan involveras för att bistå vid riskanalyser för medarbetare med skyddade personuppgifter om verksamheterna önskar det stödet. I en sådan process beaktas hotbilden och individens enskilda perspektiv. Dock sker detta endast på begäran av verksamheten och inte systematiskt, vilket vi skulle rekommendera.

Örebro kommun 2022-10-20

Jan Darrell
Certifierad kommunal yrkesrevisor, EY

Sara Jansson
Verksamhetsrevisor, EY

Bilaga 1: Källförteckning

Intervjuade funktioner

- Informationssäkerhetsstrateg
- Chef för digitaliseringsavdelningen
- Förvaltningschef för förskola och skola
- Förvaltningschef för sociala insatser
- Förvaltningschef för vuxenutbildning och arbetsmarknad
- HR-direktör
- Säkerhetschef
- Systemförvaltare
- IT säkerhetsansvarig
- Informationssäkerhetsansvarig
- Informationssäkerhetssamordnare, förvaltningen för förskola och skola
- Enhetschefer och andra medarbetare inom förvaltningen för sociala insatser
- Informationssäkerhetssamordnare, förvaltningen för utbildning, försörjning och arbete
- Dataskyddsombud
- Kommunikationsdirektör

Granskad dokumentation

- Informationssäkerhetspolicy (Ks 412/2016)
- Dataskyddspolicy (Ks 630/2018)
- Hantering av personer med skyddade personuppgifter (Ks 1160/2017)
- Riktlinjer för informationssäkerhet (Ks 267/2019)
- Riktlinjer för sociala medier i Örebro kommun (Diarienummer saknas)
- Riskanalys för kommunstyrelsens egen verksamhet, 2021
- Tillsynsplan 2021, kommunstyrelsen
- Riskanalys för socialnämndens verksamheter, 2021
- Tillsynsplan 2021, socialnämnden
- Riskanalys för förskolenämnden, 2021
- Tillsynsplan 2021, förskolenämnden
- Riskanalys för grundskolenämnden, 2021
- Tillsynsplan 2021, grundskolenämnden
- Riskanalys för gymnasienämnden, 2021
- Tillsynsplan 2021, gymnasienämnden
- Handlingsplan för informationssäkerhet 2019
- Handlingsplan för informationssäkerhet 2020–2021
- Handlingsplan för informationssäkerhet 2022–2023
- Ledningens genomgång av LIS, 2020
- Ledningens genomgång av LIS, 2021
- Ledningens genomgång av LIS, 2022
- Rapport från Handlingsplan informationssäkerhet 2020–2021
- Rutin för hantering av elever med sekretesskydd inom grundskola/gymnasium (inget diarienummer)
- Rutin för hantering av elever med skyddade personuppgifter – Örebro kommuns Gymnasieskolor, Riksgymnasier och Gymnasiesärskola (Gy 34/2022)
- Ansökan om skyddade personuppgifter hos skatteverket ”sekretessmarkering”
- Rutin för informationssäkerhet (Soc 1171/2020)
- Instruktion för hantering av personuppgiftsincidenter