Granskningsrapport 3/2022
Genomförd på uppdrag av revisorerna

Haninge kommun

Granskning av kommunens hantering av skyddade personuppgifter

Building a better working world

Innehållsförteckning

Sammanfattande bedömning och rekommendationer

EY har på uppdrag av de förtroendevalda revisorerna i Haninge kommun granskat om kommunstyrelsen, grund- och förskolenämnden, gymnasie- och vuxenutbildningsnämnden samt socialnämnden har säkerställt att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om stadens rutiner och interna kontroll avseende detta område är ändamålsenliga och tillräckliga. Vår sammantagna bedömning är att kommunstyrelsen och granskade nämnders rutiner och interna kontroll inte är helt ändamålsenliga.

Av granskningen framkommer att kommunstyrelsen kritiseras för att inte ta ett samlat grepp över hanteringen av skyddade personuppgifter vilket resulterar i att det finns organisatoriska brister. Det politiska intresset kring IT- och informationssäkerhet har ökat på ett övergripande plan, men risken för röjning av skyddade personuppgifter har inte inkluderats i tillräcklig utsträckning. Det illustreras exempelvis genom att en kommunövergripande identifierad risk för år 2022 är "Personuppgiftsbehandling enligt GDPR". Risken finns med i samtliga styrelse/nämnders internkontrollplaner. Risken för röjning av skyddade personuppgifter inkluderas specifikt i grund- och förskolenämndens samt gymnasie- och vuxenutbildningsnämndens internkontrollplaner för 2021. Risken för hanteringen av skyddade personuppgifter har dock inte behandlats i kommunstyrelsens eller socialnämndens internkontrollplaner.

Inom kommunens verksamheter finns en rad kommunövergripande och verksamhetsspecifika riktlinjer, rutiner och anvisningar vad gäller hanteringen av skyddade personuppgifter. Av granskningen framkommer att det finns flera riktlinjer och rutiner i kommunen som saknar styrkraft och relevans till följd av att de inte uppdateras i enlighet med exempelvis ny lagstiftning. De beskrivs antingen vara väldigt övergripande eller väldigt detaljerade. Det uppges därför finnas behov att inventera, uppdatera och samordna de rutiner som finns i syfte att stärka arbetet med skyddade personuppgifter. Vi ser en risk i att det finns för många riktlinjer, rutiner och anvisningar som riskerar att skapa förvirring bland personalen och försämrad styrkraft i dokumenten. Flertalet av dessa riktlinjer, rutiner och anvisningar är inte antagna och beslutade av kommunstyrelse/nämnd med hänvisning till kommunens policy för styrdokument. Vi anser därför att framtagna styrande dokument dels bör inventeras, dels bör fastställas av relevant beslutsnivå för att öka dess styrkraft.

Vidare uppmärksammar kompetensutveckling och kunskapsspridning som ett särskilt utvecklingsområde. Det finns i viss utsträckning utbildningar om GDPR men dessa inkluderar emellertid inte specifikt hanteringen av skyddade personuppgifter vilket vi anser vara en brist. Skyddade personuppgifter bör särbehandlas och medvetandegraden och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning av riktlinjer och rutiner. Detta också varför den mänskliga faktorn genomgående identifierats som den största risken i hanteringen av skyddade personuppgifter.

Granskningen visar att respektive förvaltning har upprättat verksamhetsspecifika arbetsrutiner för hanteringen av skyddade personuppgifter. Däribland hanteringen av skyddade elever, brukare och anställda i kommunens verksamhetssystem, hanteringen av e-post, kommunikation och en riskbedömning över den enskildas hotbild inom skola och socialtjänst. Utbildningsförvaltningen upprättar en individuell handlingsplan per elev/brukare vilket överensstämmer med Skolverkets rekommendationer. Social- och äldreförvaltningen upprättar inte en individuell handlingsplan. Granskningen visar att det finns anledning att vidta fler och skarpare åtgärder då det finns risker inom respektive förvaltning och verksamhetsområde som inte inkluderats i tillgängliga anvisningar.

Slutligen anser vi det vara en brist att det inte går att kategorisera avvikelser som avser skyddade personuppgifter utan manuell hantering. Vi bedömer vidare att det saknas

systematik för att åtgärda brister kopplat till hanteringen av skyddade personuppgifter i tillräcklig utsträckning.

Utifrån granskningens iakttagelser rekommenderar vi kommunstyrelsen, grund- och förskolenämnden, gymnasie- och vuxenutbildningsnämnden samt socialnämnden att:

- Inventera, uppdatera och samordna tillgängliga riktlinjer, rutiner och anvisningar.
- Överväga att genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt praktisk hantering av vardagssituationer där skyddade personuppgifter förekommer.
- Genomföra penetrationstester och systematiska loggkontroller av IT-system och rutiner för att identifiera sårbarheter och skadekonsekvenser vid intrång samt att obehöriga inte kan få tillgång till skyddade personuppgifter.
- Stärka avvikelsehanteringen och uppföljningen avseende skyddade personuppgifter.

Kommunstyrelsen och socialnämnden rekommenderas att:

- Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter och vid behov låt inkludera i internkontrollplanerna.

Kommunstyrelsen rekommenderas att:

- Överväga att inom ramen för det övergripande internkontrollansvaret ange risken för röjning av skyddade personuppgifter och inkludera denna i samtliga internkontrollplaner eller i det dagliga arbetet med intern kontroll.
- Anta övergripande styrande dokument för hanteringen av skyddade personuppgifter.
- Överväga en ”compliancefunktion” med ansvar för strukturerad uppföljning av tillämpning av styrande dokument avseende skyddade personuppgifter.

1. Inledning

1.1. 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 2021 har antalet personer med skyddade personuppgifter ökat från drygt 12 000 personer till knappt 24 000 personer, vilket motsvarar en ökning med 100 procent. Den 1 januari 2019 trädde lagändringar i kraft med syfte att öka skyddet för hotade och förföljda personer.

Jämställdhetsmyndigheten publicerade nyligen 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 de röjts på grund av att information om kvinnornas personuppgifter har röjts från till exempel socialtjänsten och andra myndigheter.

Personer med skyddade personuppgifter kan drabbas av allvarliga problem om kommunens verksamheter av misstag lämnar ut uppgifterna. Kommunen bör därför ha rutiner och riktlinjer för att hantera skyddade personuppgifter. Det är av väsentlighet att rutinen är välkänd bland samtliga medarbetare då i princip samtliga kan komma i kontakt med en person som har skyddade personuppgifter.

Revisionen har utifrån ovanstående beslutat att en fördjupad granskning ska göras av kommunens arbete med rutiner, kunskapsspridning och säkerhetsfrågor vad gäller hanteringen av skyddade personuppgifter.

1.2. Syfte och revisionsfrågor

Granskningen syftar till att bedöma hur kommunen säkerställer att uppgifter som rör personer med skyddade personuppgifter inte röjs till obehöriga. Svaren på revisionsfrågorna ska uppfylla granskningens syfte, dvs. utgöra underlag för bedömningen om kommunens rutiner är ändamålsenliga och efterlevs i organisationen.

I granskningen besvaras följande revisionsfrågor:

- Har kommunen analyserat risken för att skyddade personuppgifter röjs i kommunens verksamheter? Sker någon informationsinhämtning från relevanta instanser inom civilsamhället?
- Följer kommunstyrelsen och nämnderna upp den interna kontrollen rörande hanteringen av skyddade personuppgifter?
- Har kommunen vidtagit åtgärder för att minska risken?
- Finns det kommunövergripande och förvaltningsspecifika anvisningar och rutiner för hantering av personer med skyddade personuppgifter? Hur görs de kända för medarbetare och vilken utbildning ges?
- Finns det ett avvikelsehanteringssystem som omfattar skyddade personuppgifter?

1.3. Granskade nämnder

Granskningen avser kommunstyrelsen, grund- och förskolenämnden, gymnasie- och vuxenutbildningsnämnden samt socialnämnden.

1.4. Metod och genomförande

Granskningen har genomförts genom dokumentstudier och intervjuer med företrädare för IT-avdelningen, HR-avdelningen, kommunens jurister och dataskyddssamordnare, samt

med chefer och andra tjänstepersoner inom social- och äldreförvaltningen och utbildningsförvaltningen. Intervjuade funktioner och granskade underlag framgår av källförteckning.

1.5. 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. 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)
- SFS 2018:684 Lag om ändring i folkbokföringslagen (1991:481)
- Patientdatalagen (2008:355)
- Skatteverket "Folkbokföring – sekretessmarkerade personuppgifter" samt "Viktigt för myndigheter att tänka på för att systemet med markering för skyddad folkbokföring och sekretessmarkering ska fungera"
- Av fullmäktige antagna styrdokument eller relevanta riktlinjer

Dessa beskrivs närmare i kapitel 2.

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 200 invånare och ett tiotal anställda i Haninge 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.

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.

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.

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.

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) ersatte sekretesslagen 2009 i syfte att göra den mer lättförståelig och lättillämpad. Lagen 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. En patients hälsotillstånd eller personliga förhållanden är exempel på vad som skyddas av sekretess.

Utöver de tre skyddsformerna (sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter) finns en särskild generell sekretessbestämmelse som gäller 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. Riskanalys och intern kontroll

Ingen styrelse eller nämnd har ett utpekat ansvar för hanteringen av skyddade personuppgifter i Haninge kommun. Respektive styrelse/nämnd är personuppgiftsansvarig för de register och andra behandlingar av personuppgifter som sker i dess verksamhet.

Varje styrelse/nämnd kan potentiellt komma i kontakt med personer som har skyddade personuppgifter, både i form av brukare, elever samt medarbetare. Ansvarsområdena skiljer sig dock mellan styrelse/nämnderna och därmed också hanteringen av personuppgifter.

Kommunstyrelsen har dock ett helhetsansvar för kommunens verksamheter, utveckling och ekonomiska ställning och ska se till att den kommunala verksamheten bedrivs i enlighet med kommunens vision, strategiska mål och vad fullmäktige i övrigt har beslutat. Enligt kommunstyrelsens reglemente[1] ska styrelsen leda kommunens verksamhet genom att utöva en samordnad styrning och leda arbetet med att ta fram styrdokument för kommunen.

Enligt riktlinjer till reglementet för intern kontroll[2] har kommunstyrelsen det övergripande ansvaret att se till att en god internkontroll upprätthålls i den kommunala verksamheten. Kommunstyrelsen ansvarar att en organisation kring intern kontroll upprättas i kommunen samt att förvaltningsövergripande riktlinjer och regler upprättas.

Nämnderna har det yttersta ansvaret för den interna kontrollen inom sina respektive verksamhetsområden. I dessa ingår att tillse att en organisation upprättas för den interna kontrollen, att nämndspecifika regler antages för den interna kontrollen och att internkontrollplaner tas fram som bygger på risk- och väsentlighetsanalyser.

3.1. Styrningen över hanteringen av skyddade personuppgifter uppvisar vissa brister

Bland annat med anledning av nationella och internationella säkerhetshot, däribland den uppmärksammade IT-attacken mot Kalix kommun, har det politiska intresset kring IT- och informationssäkerhet ökat i kommunen. Det avser dock IT-säkerhet på ett övergripande plan och inte risken för röjning av skyddade personuppgifter. Det upplevs därför inte att styrelse och granskade nämnder i tillräcklig grad uppmärksammar respektive förvaltnings hantering av skyddade personuppgifter. En möjlig orsak anges vara att styrelse och granskade nämnder uppfattar det som en teknisk/ickepolitisk fråga som professionerna tar hand om och/eller att de litar på att förvaltningarna hanterar personuppgiftsfrågorna och informerar om avvikelser vid behov.

Vidare beskrivs att kommunstyrelsen inte tar ett samlat grepp över hanteringen av skyddade personuppgifter. Det finns ett antal riktlinjer och rutiner i respektive förvaltning men dessa saknar till viss del styrkraft och relevans då de inte samordnas. Det beskrivs vara otydligt vem eller vilka i organisationen som ska vara ansvariga för hanteringen av exempelvis skyddade personuppgifter. Av intervjuer i respektive förvaltning framkommer att det i viss utsträckning saknas central styrning från kommunstyrelseförvaltningen. I syfte att effektivisera och uppnå en ändamålsenlig organisation för att hantera skyddade personuppgifter finns en önskan om att kunna fördela ansvaret nedåt i organisationskedjan till lämplig nivå utifrån tydligt uppställda mål.

[1] KS 2021-00485.
[2] KS 2015/570.

Sammantaget beskrivs den bristfälliga styrningen öka riskerna för att arbetet med skyddade personuppgifter blir eftersatt och att risken för röjning av skyddade personuppgifter ökar.

3.2. Enstaka internkontrollplaner omfattar risker vid hantering av skyddade personuppgifter

En kommunövergripande identifierad risk för år 2022 är "Personuppgiftsbehandling enligt GDPR". Risken finns med i samtliga styrelse/nämnders internkontrollplaner. Kontrollansvaret åligger enheten för demokratistöd inom kommunstyrelseförvaltningen och sker genom stickprov på efterlevnad av riktlinjer. Uppföljning sker i årsrapporterna. Risken rör framför allt *känsliga personuppgifter*.

Känsliga personuppgifter definieras i artikel 9 i Dataskyddsförordningen; "Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning". Det rör sig således inte om skyddade personuppgifter.

I grund- och förskolenämndens samt gymnasie- och vuxenutbildningsnämndens internkontrollplaner för 2021 inkluderades dock risken för röjning av skyddade personuppgifter specifikt. Kontrollmålet var att kontrollera om förvaltningens rutiner för skyddade personuppgifter följs. I nämndernas respektive årsredovisning för 2021 presenterades resultatet.

I rapporten beskrivs att kontrollmålet har följts upp genom en enkät till förskole- och grundskolerektorer. 12 grundskolor och fem förskoleområden har svarat. Inkomna svar visar att det finns en god kännedom i verksamheterna om rutinerna och att de följs. Flertalet rektorer har uttryckt att rutinerna är bra och tydliga. Några önskemål om förtydliganden i rutinerna har inkommit. Nämnden ämnar se över det under 2022.

Gymnasie- och vuxenutbildningsnämnden har likt grund- och förskolenämnden följt upp kontrollmålet med en enkät till rektorer. Av de inkomna svaren följer att det inom gymnasieskolan finns en god kännedom om rutinerna och att de följs. Inom vuxenutbildningen saknas emellertid kännedom om förvaltningens rutiner och följaktligen inte heller arbetat efter dessa. Vuxenutbildningen har dock haft egna rutiner för hantering av elever med skyddade personuppgifter. Förvaltningen uppger att befintliga rutiner kommer att ses över under 2022 för att säkerställa att de är anpassade även till vuxenutbildningen.

I socialnämndens internkontrollplan för 2022 inkluderas även risken för registrering av personuppgiftsbehandling. Det kontrolleras att de sätt som behandling av personuppgifter sker finns registrerade i kommunens förteckning för personuppgiftsbehandling. Risker vid hanteringen av skyddade personuppgifter har inte analyserats i någon internkontrollplan tidigare.

3.3. Regelbunden och löpande egenkontroll av personuppgiftsbehandling

En kommunövergripande utmaning beskrivs vara att följa upp internkontrollarbetet mer regelbundet. Kontrollmålet följs upp i årsredovisningen, men det beskrivs oftast saknas dels en efterföljande kontroll, dels en konkret åtgärdsplan för att åtgärda brister samt, om en åtgärdsplan finns, hur och när den ska följas upp.

Utöver den årliga uppföljningen av internkontrollplanerna ingår även regelbunden och löpande egenkontroll i respektive styrelse/nämnd som en del av den interna kontrollen. Av

kommunstyrelseförvaltningens rutin för att rapportera uppföljning och granskning av dataskyddsförordningen följer att nämnderna i egenskap av personuppgiftsansvariga varje år ska genomföra en egenkontroll för sitt dataskyddsarbete samt att nämnderna senast i samband med årsbokslutets upprättande efterföljande år ska rapportera resultatet från egenkontrollen till kommunstyrelsen och dataskyddsombudet. Det gäller från 2021. Egenkontrollen ska ske löpande och minst omfatta:

- De nämnd- och bolagsspecifika rutiner som finns för hanteringen av personuppgifter efterlevs och behöver inte förbättras.
    - Behövs ytterligare rutiner för att säkerställa övriga punkter?
- Alla medarbetare har fått tillräcklig utbildning.
- Konsekvensbedömningar har genomförts vid behov vid nya eller förändrade behandlingar.
- Behörigheter tilldelas och kontrollereras så att kraven på säker hantering av personuppgifter efterlevs.
- Personuppgiftsbiträdesavtal har tecknats där lagen kräver det.
    - Uppföljning sker av att underbiträdena efterlever de säkerhetskrav som ställts i biträdesavtalen.
- Relevanta åtgärder har vidtagit för att hantera brister som har orsakat personuppgiftsincidenter.

Vi noterar att kommunstyrelsen och socialnämnden inte upprättade en rapport för 2021.

I grund- och förskolenämndens samt gymnasie- och vuxenutbildningsnämndens rapporter för egenkontroll för dataskyddsarbetet under 2021 konstateras bland annat att utvecklings- och undersökningsområden har identifierats. Däribland beskrivs att gallringsrutinerna för personuppgiftsbehandlingen behöver ses över och förtydligas och att det finns behov att se över om tillräckliga säkerhetsåtgärder vidtas för personuppgiftsbehandling och att dokumentera säkerhetsåtgärderna. Vidare konstateras att det stödmaterial som finns är omfattande och kan till vissa delar vara komplext att sätta sig in i. Det beskrivs därför finnas ett behov av att löpande se över och justera rutinerna.

Rapporterna berör inte skyddade personuppgifter specifikt.

3.4. Bedömning

Av granskningen framkommer att styrelse och granskade nämnder i tillräcklig grad inte uppmärksammar respektive förvaltnings hantering av skyddade personuppgifter. Det politiska intresset kring IT- och informationssäkerhet har ökat på ett övergripande plan, men risken för röjning av skyddade personuppgifter har inte inkluderats i tillräcklig utsträckning. En möjlig orsak anges vara att styrelse och granskade nämnder uppfattar det som en teknisk/ickepolitisk fråga som professionerna tar hand om och/eller att de litar på att förvaltningarna hanterar personuppgiftsfrågorna och informerar om avvikelser vid behov. Det anser vi vara en brist.

En kommunövergripande identifierad risk för år 2022 är "Personuppgiftsbehandling enligt GDPR". Risken finns med i samtliga styrelse/nämnders internkontrollplaner. Risken för röjning av skyddade personuppgifter inkluderas specifikt i grund- och förskolenämndens samt gymnasie- och vuxenutbildningsnämndens internkontrollplaner för 2021. Risken för hanteringen av skyddade personuppgifter har inte behandlats i kommunstyrelsens och socialnämndens internkontrollplaner.

Vår uppfattning är att hanteringen av skyddade personuppgifter tämligen ofta hanteras utifrån devisen att kunskap om riskerna och dess hantering ska skötas verksamhets- och professionsnära och är inget som styrelse och nämnder kan engagera sig i. Det är

emellertid en relativt enkel metod, och ansvar, att tillse att interna kontroller finns och tillämpas samt vilka resultat dessa ger. Vi bedömer det därför vara angeläget att även kommunstyrelsen och socialnämnden behandlar risken för röjning av skyddade personuppgifter i kommande internkontrollplaner.

En kommunövergripande utmaning beskrivs vara att följa upp internkontrollarbetet mer regelbundet. Kontrollmålet följs upp i årsredovisningen. Det beskrivs dock oftast saknas dels en efterföljande kontroll, dels en konkret åtgärdsplan för att åtgärda brister samt, om en åtgärdsplan finns, hur och när den ska följas upp. Från 2021 måste nämnderna i egenskap av personuppgiftsansvariga varje år genomföra en egenkontroll för sitt dataskyddsarbete och rapportera resultatet till kommunstyrelsen och dataskyddsombudet. Skyddade personuppgifter behandlas inte i egenkontrollen. Vi bedömer det vara angeläget att skyddade personuppgifter antingen ingår i egenkontrollen av dataskyddsarbetet eller att det årligen upprättas en specifik rapport för egenkontroll av skyddade personuppgifter som följs upp följande år.

Då risken att röja skyddade personuppgifter inte bedömts och värderats utifrån risk- och konsekvensanalyser är bedömningen att kommunstyrelsen och socialnämnden inte genomfört relevanta kontrollåtgärder. Det ökar risken för röjning av skyddade personuppgifter i granskade verksamheter.

4. Styrande dokument och rutiner

4.1. Det finns en rad olika riktlinjer med tillhörande rutiner vid hantering av skyddade personuppgifter

Inom kommunens verksamheter finns en rad kommunövergripande och verksamhetsspecifika riktlinjer, rutiner och anvisningar vad gäller hanteringen av skyddade personuppgifter. Dessa sammanfattas i tabellen nedan.

Ansvarig styrelse/nämnd	Riktlinje/rutin/anvisning	Kort beskrivning
KS	*Vägledning skyddade personuppgifter 20190101*	Beskriver vad skyddade personuppgifter är samt vad som är viktigt för myndigheter att tänka på för att systemet med markering för skyddad folkbokföring och sekretessmarkering ska fungera.
KS	*Rutiner för tillverkning av passerkort för person med skyddad identitet*	Se namn på rutin.
KS	*Rutiner för utlämning av P-tillstånd för person med skyddad identitet*	Se namn på rutin.
KS	*Posthantering för personer med skyddade personuppgifter*	Se namn på rutin.
KS	*Rutiner för hantering av medarbetare med skyddade personuppgifter*	Rutin som beskriver vad skyddade personuppgifter är och hänvisar till övriga rutiner/anvisningar.
KS	*Skyddade personuppgifter i Heroma*	Anvisning som beskriver en medarbetares sekretesskydd i verksamhetssystemet Heroma.
KS	*Anonym – Överföring från Navet*	Anvisning som beskriver hur en medarbetare överförs från Navet (Folkbokföringsregistret) som anonym till Heroma.
KS	*Hantering av ansökningar med skyddade personuppgifter*	Anvisning som beskriver hur ansökningar av personer med skyddade personuppgifter

		ska hanteras utanför rekryteringssystemet.
KS	*Så här fungerar det vad gäller Skyddade personuppgifter med sekretessmarkering, kvarskrivning och sekretess till skydd för enskild i personadministrativ verksamhet*	Se namn på rutin.
KS	*Rutin – Skyddade personuppgifter*	Anvisning som beskriver en medarbetares sekretesskydd i verksamhetssystemet Heroma
GFN & GVN	*Rutiner för hantering av elever med skyddade personuppgifter*	Övergripande rutin som beskriver vad skyddade personuppgifter är och hur elever med skyddade personuppgifter ska hanteras i förvaltningens skolor. Bilagt i rutinen finns även en handlingsplan som upprättas elev.
GVN	*Arbetsrutiner kring skyddad identitet antagning elever på Centrum Vux*	Se namn på rutin.
SN	*Rutin för att lägga upp personer med skyddad identitet i Lifecare*	Se namn på rutin. Lifecare är det huvudsakliga verksamhetssystem som social- och äldreförvaltningen använder för handläggning av ärenden.

Utöver ovan beskrivna riktlinjer/rutiner/anvisningar finns information om skyddade personuppgifter samlad på kommunens intranät.

Kommunstyrelsens "portalrutin" *Vägledning skyddade personuppgifter 20190101* anger hur personer med skyddade personuppgifter ska hanteras i kommunen. Det finns ett antal punkter som respektive myndighet i kommunen ska beakta för att systemet med markering för skyddad folkbokföring och sekretessmarkering ska fungera:

- Beakta särskilt hanteringen av skyddade personuppgifter vid utveckling av IT-stöd
- IT-stödet bör utformas så att endast ett fåtal personer med särskild behörighet har tillgång till skyddade personuppgifter
- För en handläggare som har behörighet att ta del av skyddade personuppgifter bör det på ett tydligt och enhetligt sätt framgå att uppgifterna är markerade för skyddad folkbokföring eller sekretessmarkerade
- Det bör vara möjligt att i efterhand kontrollera vilka handläggare som har tagit del av skyddade personuppgifter genom loggning
- Utforma rutiner utifrån en egen riskbedömning av de skyddade personuppgifter som myndigheten behandlar och konsekvensen av om dessa uppgifter kommer obehörig person tillhanda
- Gör en översyn av vilken information som måste anges i olika handlingar
- Det bör finnas enhetliga och säkra rutiner för att kommunicera med och om personer som har markering för skyddad folkbokföring eller sekretessmarkering
- Se till att personal som hanterar skyddade personuppgifter har goda kunskaper om vad som gäller när uppgifter har markering för skyddad folkbokföring respektive sekretessmakering
- Följ regelbundet upp att myndighetens regler och rutiner kring skyddade personuppgifter efterlevs och respekteras inom myndigheten
- Kommunikation med enskilda eller andra myndigheter

Som framgår av tabellen ovan finns en rad olika riktlinjer med tillhörande rutiner vid hanteringen av skyddade personuppgifter i kommunens olika verksamheter. Flertalet av

dessa riktlinjer, rutiner och anvisningar är inte antagna och beslutade politiskt med hänvisning till kommunens policy för styrdokument. Det finns inget uttalat politiskt intresse för just skyddade personuppgifter. Vidare beskrivs det i dagsläget finnas en rad olika riktlinjer och rutiner i kommunen som saknar styrkraft och relevans till följd av att de inte uppdateras i enlighet med exempelvis ny lagstiftning. De beskrivs antingen vara väldigt övergripande eller väldigt detaljerade. Det uppges därför finnas behov att inventera, uppdatera och samordna de rutiner som finns i syfte att stärka arbetet med skyddade personuppgifter.

4.2. Kompetensutveckling och kunskapsspridning

2018, i samband med att GDPR trädde i kraft, infördes en kommunövergripande obligatorisk utbildning om GDPR-lagstiftningens påverkan på personuppgiftsbehandlingen i kommunen. Utbildningen berör emellertid inte specifikt hantering av skyddade personuppgifter som är en mer teknisk fråga, snarare än juridisk i strikt mening. Utbildningen, som fortsatt finns tillgänglig på intranätet, är inte obligatorisk för nyanställda som påbörjat sin anställning efter införandet av GDPR. Det finns inte någon samlad bild över hur många nyanställda som har gått utbildningen. Vidare finns en obligatorisk utbildning om GDPR för nyanställda chefer.

Löneenheten utbildar samtliga nyanställda chefer om lönehanteringen ca fyra gånger per år. I utbildning ingår hanteringen av medarbetare med skyddade personuppgifter.

Utbildningsförvaltningen har en egen obligatorisk utbildning om GDPR för samtliga chefer och medarbetare. Det är en filmad föreläsning om 2x30 minuter som berör grunderna i GDPR samt vilka rutiner och stödmaterial som gäller specifikt för utbildningsförvaltningen och kommunen. Det går inte att ta del av hur många som har tagit del av utbildningen. berör emellertid inte specifikt hantering av skyddade personuppgifter.

Som konstaterats tidigare finns ett antal riktlinjer, rutiner och anvisningar men det saknas kunskap om hur många som har kännedom om de, var dem finns och hur många som har läst dem. Även här beskrivs det finnas ett behov av central samordning av utbildning och kompetensutveckling. Det beskrivs att det inom vissa verksamheter saknas en tillräcklig kunskap om riskerna och konsekvenserna vid röjning av skyddade personuppgifter.

4.3. Uppföljning och kontroll av styrande dokument och rutiner

Det finns ingen "compliancefunktion/er", det vill säga tjänsteperson/er med samordnande ansvar för att styrande dokument är relevanta, kända och tillämpade vad gäller hanteringen av skyddade personuppgifter. Det finns däremot i viss utsträckning snarlika funktioner i respektive förvaltning.

I kommunstyrelseförvaltningen finns en kommunjurist tillika dataskyddsombud. I arbetsbeskrivningen ingår att svara på övriga förvaltningars frågor som rör juridik och dylikt, däribland juridiska frågor kopplat till skyddade personuppgifter, och inte framtagandet av styrande dokumentation.

Inom utbildningsförvaltningen finns sedan årsskiftet 2022 en nyinrättad grupp i bestående av två jurister tillika utredare som har ett samordnande uppdrag för dataskyddsfrågor och juridisk rådgivning. I uppdraget ingår även säkerställa att styrande dokument är uppdaterade och tydliga etcetera. Det finns en gemensam maillåda vid namn "Skoljuristerna" där samtlig skolpersonal kan ställa frågor som rör dataskydd och juridik bland annat. Det förekommer frågor som rör skyddade personuppgifter.

I social- och äldreförvaltningen finns en förvaltningsjurist/dataskyddskoordinator. Funktionen liknar de roller som finns inom utbildningsförvaltningen.

4.4. Bedömning

Inom kommunens verksamheter finns en rad kommunövergripande och verksamhetsspecifika riktlinjer, rutiner och anvisningar vad gäller hanteringen av skyddade personuppgifter. Av granskningen framkommer att det finns flera olika riktlinjer och rutiner i kommunen som saknar styrkraft och relevans till följd av att de inte uppdateras i enlighet med exempelvis ny lagstiftning. De beskrivs antingen vara väldigt övergripande eller väldigt detaljerade. Det uppges därför finnas behov att inventera, uppdatera och samordna de rutiner som finns i syfte att stärka arbetet med skyddade personuppgifter. Vi ser en risk i att det finns för många riktlinjer, rutiner och anvisningar som riskerar att skapa förvirring bland personalen och försämrad styrkraft i dokumenten.

Flertalet av dessa riktlinjer, rutiner och anvisningar är inte antagna och beslutade av kommunstyrelse/nämnd med hänvisning till kommunens policy för styrdokument. Vi anser det vara viktigt att principiella styrdokument antas av kommunstyrelse eller ansvarig nämnd. Mer rutinbeskrivande dokument lämpar sig för chefsbeslut. För tillräcklig styrkraft fordras hur som helst en tydlig hierarki bland styrdokumenten. Vi anser därför att framtagna styrande dokument dels bör inventeras, dels bör fastställas av relevant beslutsnivå för att öka dess styrkraft.

Vi uppmärksammar kompetensutveckling och kunskapsspridning som ett särskilt utvecklingsområde. Det finns i viss utsträckning utbildningar om GDPR men dessa inkluderar emellertid inte specifikt hanteringen av skyddade personuppgifter vilket vi anser vara en brist. Skyddade personuppgifter bör särbehandlas och medvetandegrad och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning av riktlinjer och rutiner, inte minst med tanke på dess omfattning. Detta också varför den mänskliga faktorn genomgående identifierats som den största risken i hanteringen av skyddade personuppgifter.

Vidare saknas en funktion som arbetar särskilt med att säkerställa att styrande dokument är kända och tillämpade, ofta kallad "compliancefunktion". Skatteverket har i "Folkbokföring – sekretessmarkerade personuppgifter", en vägledning för andra myndigheter, bland annat utryckt: "Varje myndighet bör utse en person med ansvar för att rutiner och regler för hantering av skyddade personuppgifter efterföljs." Då en kommun består av flera myndigheter kan det alltså finnas motsvarande funktion per nämnd, men även centralt under kommunstyrelsen. Vi menar att detta bör övervägas då det i dagsläget till viss del saknas en övergripande strategi eller inriktning för arbetet med skyddade personuppgifter.

5. Flera åtgärder har vidtagits för att hantera skyddade personuppgifter

5.1. IT- och verksamhetssystem

Primärt ligger personuppgiftsskyddet i personuppgiftsavtalen (PuB-avtal) IT-enheten har med respektive leverantör som behandlar personuppgifter för dess räkning och som ska skyddas i enlighet med GDPR. Av granskningen framgår att kommunen har PuB-avtal med flertalet upphandlade leverantörer.

I kommunens IT-handbok anges att bland annat sekretessbelagd information och känsliga personuppgifter som regel endast ska hanteras inom dokument- och ärendehanteringssystemet eller i annat verksamhetsspecifikt system enligt gällandet lagstiftning. Vid upphandling av ett nytt verksamhetssystem skall en informationsklassning göras av den information som skall lagras i det nya verksamhetssystemet inför eller som en del av upphandlingar. Det görs med stöd från enheten för trygghet och säkerhet i

kommunstyrelseförvaltningen. IT-enheten har dock inte mandat att säga nej vid upphandling av ett verksamhetssystem och det förekommer dessutom enligt uppgift att system upphandlas utan IT-enhetens vetskap. I gymnasiet används exempelvis ett omfattande antal system utan att IT-enheten eller utbildningsförvaltningen har kännedom om samtliga system. Det finns också system som inte är informationssäkerhetsklassade utifrån SKR:s verktyg KLASSA, utan genom kommunens egna, mindre avancerade, informationsklassningssystem vilket beskrivs vara en kvarleva från tidigare år. Utvecklingen går mot en mer central styrning bland annat i syfte att IT-enheten ska få större uppsikt över aktuella system.

Vidare anges i IT-handboken att ingen information av känslig karaktär (däribland personuppgifter) får skickas med vanlig e-post eller lagras i Microsoft Outlook utan skall, om informationen måste skickas med e-post, skickas med hjälp av krypterad e-post (SecureMailbox).

Sårbarhetsscanningar/penetrationstester, det vill säga tester som identifierar vilka sårbarheterna är och hur stor skada de kan orsaka, genomförs med viss frekvens men inte kontinuerligt. En sårbarhetsscanning genomfördes under våren 2022. Då kontrollerades säkerheten i verksamhetssystemen, det vill säga om en obehörig användare kunde ta sig in i ett verksamhetssystem utan lösenord. Resultatet visade att det finns möjlighet för obehöriga att ta sig in i system via andra personers konton. Felen upptäcktes via varningssignaler. Det beskrivs finnas förbättringar att göra kopplat till de brister som scanningen uppvisade. Det har inte gjorts sårbarhetsscanningar/penetrationstester med anledning av skyddade personuppgifter.

Loggkontroller, det vill säga kontroll av att bland annat bestämmelserna om sekretess efterlevs och att ingen otillbörlig användning av verksamhetssystemet sker, genomförs regelbundet i vissa verksamhetssystem. Dock inte specifikt kopplade till skyddade personuppgifter. Det finns inte en gemensam logglösning utan sker i olika system utifrån olika rutiner. IT-enheten genomför loggkontroller med anledning av hantering av personuppgifter, däribland i Microsoft Office 365-miljön, regelbundet.

Social- och äldreförvaltningen utför systematiska loggkontroller av verksamhetssystemet Lifecare IFO, Lifecare VoO och Appva regelbundet. Syftet är att säkerställa att ingen användare obehörigen tillskansar sig uppgifter och information om klienter eller kunder som de inte har behörighet till. Loggkontroller på vilka klienter eller kunder som slumpvis utvalda användare tagit del av tas därför en gång per kvartal. I verksamhetssystemet Appva granskas huruvida slumpmässigt utvalda användare fortfarande är i tjänst i enlighet med systemuppgifterna. Loggkontroller med anledning att upptäcka eventuell röjning av skyddade personuppgifter har inte gjorts.

Utbildningskontoret har inte genomfört loggkontroller i verksamhetssystemen.

5.2. Medarbetare med skyddade personuppgifter

Löneenheten inom HR-avdelningen ansvarar för att anställningen av en person med skyddade personuppgifter läggs upp korrekt i kommunens personalsystem. Som beskrivits tidigare finns ett antal rutiner/anvisningar för hanteringen av medarbetare med skyddade personuppgifter. Rutinerna har utformats utifrån Skatteverkets och SKR:s stödmaterial och gäller samtliga medarbetare som finns registrerade i kommunens lön- och personalsystem. Rutinerna uppdateras löpande utifrån regler och avtal. Vid varje uppdatering informeras löneenhetens personal på så kallade lönemöten.

HR-avdelningen får information om att kommunen ska anställa en person med skyddade personuppgifter via personen själv vid anställningsförfarandet eller via Skatteverkets folkbokföringsregister. De HR- och lönesystem som används är anpassade för att kunna

hantera medarbetare med skyddade personuppgifter. Framtagna rutiner omfattar hanteringen av medarbetare med skyddade personuppgifter i verksamhetssystemen.

Medarbetarens hotbild dokumenteras inte i en handlingsplan likt kommunens skolor gör med elever som har skyddade personuppgifter. HR-avdelningen rådfrågas av respektive förvaltning om hur medarbetaren ska hanteras vid anställning. Huvudprincipen är att så få som möjligt, exempelvis närmaste chef, ska ha vetskap om vilka anställda som har skyddade personuppgifter.

5.3. Utbildningsförvaltningen har vidtagit verksamhetsspecifika åtgärder

Skolorna kommer i kontakt med skyddade personuppgifter vid inskrivningen. När vårdnadshavare eller myndig elev ansöker om plats i skola uppmärksammas kommunen om vilken typ av skyddade personuppgifter som är aktuella via vårdnadshavaren/myndig elev. Uppgifterna kan också hämtas från Skatteverket en gång i veckan. Det finns vid granskningens tidpunkt inga planer att göra det oftare, exempelvis dagligen. Det är rektorn respektive förskolechefen som ansvarar för att skyddade personuppgifter hanteras på ett korrekt sätt i verksamheten.

I kommunen används Extens som "huvudsystem". I Extens syns endast namn, personnummer och familjebild på eleven. Elever med skyddade personuppgifter registreras inte på någon enhet utan flyttas till en skyddad klass. Antalet handläggare med tillgång till den skyddade klassen är begränsad. Den fysiska elevakten med de riktiga personuppgifterna förvaras fysiskt i ett kassaskåp på respektive skola. Det finns inga uppgifter om exakt hur många personer som har tillgång till det låsta kassaskåpet.

Handläggare på utbildningsförvaltningen informerar skolan och meddelar att eleven plockas bort från förskolans/skolans/fritidshemmets register. Inga uppgifter om elever med skyddade personuppgifter överförs från Extens till andra system. Detta innebär att eleverna inte kommer med på klasslistor, placeringslistor eller andra i övrigt förekommande listor och system. Det går att skapa ett aliaskonto om vårdnadshavaren vill att elevens personuppgifter ska vara fingerade. I kommunen används Unikum som lärplattform. Inga elever med skyddade personuppgifter släpps in i systemen under eget namn. Elever och vårdnadshavare får ett fiktivt namn och personnummer som de kan logga in med.

Vid inskrivning håller rektorn (och eventuell handläggare) i ett planeringssamtal med vårdnadshavaren (eller eleven om denne är myndig). Syftet med samtalet är att klargöra hur elevens situation ser ut och att utforma en handlingsplan för eleven där vårdnadshavare/elev tar ställning till frågor som till exempel hur sjukanmälan, skolutflykter och fotografering ska hanteras. En vanligt förekommande situation är att vårdnadshavaren underskattar behovet av elevens skydd i skolans miljöer. Optimalt ur skolans synpunkt vore att varje elev skulle ha maximalt skydd enligt handlingsplanen. I och med att det är upp till vårdnadshavaren att fatta beslut om denna är det vanligt att eleven inte får nödvändigt skydd. Exempelvis vill vårdnadshavaren, trots att eleven har skyddade personuppgifter, tillåta eleven finnas med i skolkataloger eller gruppfotografier. Situationen beskrivs vara svår för skolorna att hantera då de inte kan garantera tillräckligt skydd för eleven i skolans miljöer i utan att frångå vårdnadshavarens vilja. Vårdnadshavaren/myndig elev skriver inte under handlingsplanen och den följs inte upp årligen.

I samband med intervju identifierades risk när barn har skyddade personuppgifter på grund av hot från en av föräldrarna. Denne förälder kan fortfarande vara vårdnadshavare och besitta rätt att ta del av uppgifter som rör barnet. Båda vårdnadshavarna har laglig rätt att få kallelser till bokförd hemadress. Det finns en "lucka i lagen" som är svår att undvika. I vissa fall, när det inte framkommer av handlingsplanen, saknar skolorna kunskap om att den andra vårdnadshavaren är hotet som eleven ska skyddas från. I förekommande fall

kontaktas socialtjänsten som kan besitta ytterligare information om eleven, varefter samverkan etableras mellan skolan och socialtjänsten.

Tillgängliga riktlinjer och rutiner beskrivs huvudsakligen vara ändamålsenliga. Dock framkommer av intervjuer att de till viss del är ofullständiga. Däribland saknas bland annat information om intern och extern kommunikation. Med andra ord hur telefonsamtal om var en elev befinner sig med exempelvis anhöriga eller utomstående ska hanteras samt om hur extern kommunikation med andra myndigheter ska hanteras. Det beskrivs vara en brist.

5.4. Social- och äldreförvaltningen har vidtagit verksamhetsspecifika åtgärder

Socialnämnden eller social- och äldreförvaltningen har inte upprättat någon egen riktlinje/rutin för hanteringen av brukare med skyddade personuppgifter, utan följer den kommunövergripande riktlinjen som kommunstyrelsen har beslutat om.

Inom social- och äldreförvaltningen används verksamhetssystemet Lifecare. Systemet läser in alla personuppgifter från Skatteverket veckovis. Skyddade personuppgifter markeras med en röd markering. De kan också läggas in manuellt då brukaren med skyddade personuppgifter tar kontakt med socialtjänsten. Då vilar ansvaret på socialtjänsten att utreda hur vidare kontakt ska etableras utifrån en riskbedömning då det i systemet inte framkommer någon "hushållsbild", det vill säga vilka fler i hushållet som har skyddade personuppgifter. Riskbedömningen baseras bland annat på anledning till hotet, hur hotet ser ut idag samt vilka uppgifter som är känsliga. Det åligger brukaren att informera socialtjänsten vid förändrad hotbild. Det upprättas inte en handlingsplan, utan kontakten bygger på muntlig kontakt med socialsekreteraren vid ett första möte som sedan ska journalföra uppgifterna.

Det finns en e-tjänst för ansökan om ekonomiskt bistånd och vid löpande ansökningar. Det finns också möjlighet att, utöver att etablera kontakt via telefon, etablera kontakt med socialtjänsten genom att lämna in en ansökan exempelvis genom papper i receptionen eller via post. Det beskrivs vara en risk därför att det är ett fysiskt papper med information som inte ska hanteras av obehöriga personer. En sårbarhet är hanteringen av de fysiska personakterna. Hantering av fysiska personakter ställer högre krav på respektive socialsekreterare och det finns större risker för att obehöriga får tillgång till känsliga uppgifter, däribland skyddade personuppgifter.

Åtkomst till personakten i verksamhetssystemet Lifecare kräver särskild behörighet. Samtliga socialsekreterare kan få behörighet förutsatt att man är involverad i ärendet som handläggare. Inloggning kräver tvåfaktorsautentisering. Behörigheten beskrivs vara omfattande.

E-post kan skickas med krypterad e-post genom tjänsten säkra meddelanden. Det finns möjlighet att fortsatt använda fax. Det är dock endast domstolarna som skickar fax. Både den interna och externa kommunikationen framställs som riskområden där felhantering kan resultera i röjning av skyddade personuppgifter orsakad av den mänskliga faktorn.

Inom socialtjänstens verksamheter finns en vana att hantera känsliga personuppgifter där alla personuppgifter behandlas med varsamhet och med sekretess i åtanke. Dessutom styrs socialtjänstens verksamhet i hög utsträckning av offentlighet- och sekretesslagstiftning och samtliga socialsekreterare har fått utbildning om hanteringen av sekretess och personer med skyddade personuppgifter under utbildningen. Dock framställs att det finns en osäkerhet kring hanteringen av skyddade personuppgifter till följd av avsaknaden av nedtecknade rutiner och introduktion vid nyanställning. Det lyfts också fram ett behov av specifika arbetsgrupper för klienter med skyddade personuppgifter.

5.5. Bedömning

Respektive förvaltning har upprättat verksamhetsspecifika arbetsrutiner för hanteringen av skyddade personuppgifter. Däribland hanteringen av skyddade elever, brukare och anställda i kommunens verksamhetssystem, hanteringen av e-post, kommunikation och en riskbedömning över den enskildas hotbild inom skola och socialtjänst. Utbildningsförvaltningen upprättar en individuell handlingsplan per elev/brukare vilket överensstämmer med Skolverkets rekommendationer. Vi noterar dock att handlingsplanen inte signeras av vårdnadshavare/myndig elev. Vidare följs inte handlingsplanen upp kontinuerligt vilket vi anser vara ytterligare en brist som bör åtgärdas. Social- och äldreförvaltningen upprättar inte en individuell handlingsplan. Det gör inte heller HR-avdelningen per anställd med skyddade personuppgifter. Vår bedömning är att HR-avdelningen och social- och äldreförvaltningen bör upprätta en individuell handlingsplan inom respektive verksamhet.

Det finns risker av allmän karaktär som gäller hela kommunen, däribland extern och intern kommunikation med andra myndigheter och privatpersoner, hanteringen av fysiska personakter samt brister i informationsspridning av riktlinjer, rutiner och anvisningar. Vidare finns verksamhetsspecifika risker som är unika för varje uppkommen situation. Det finns dessutom risker inom respektive förvaltning och verksamhetsområde som inte inkluderats i tillgängliga anvisningar.

Granskningen visar att det varken har gjorts penetrationstester eller loggkontroller med anledning av risken för röjning av skyddade personuppgifter. Penetrationstester utförs för att identifiera vilka sårbarheterna är och hur stor skada intrång kan orsaka. Penetrationstester kan användas på många sätt för att identifiera brister vid hantering av skyddade personuppgifter, däribland säkerheten i IT-systemen och alla de rutiner som finns beskrivna i respektive nämnds riktlinjer, rutiner och anvisningar. Loggkontroller är ytterligare ett effektivt verktyg att säkerställa att obehöriga inte får tillgång till skyddade personuppgifter. Däremot uppmärksammar vi att det regelbundet sker både penetrationstester/sårbarhetsscanningar och loggkontroller i kommunens verksamhetssystem. Vi bedömer dock att det är av särskilt vikt att det utförs med anledning av risken för röjning av skyddade personuppgifter framgent.

6. Avvikelsehanteringssystem

Röjning av personuppgifter ska rapporteras i KIA (informationssystem för arbetsmiljö), kommunens incidentrapporteringssystem. Ansvarig chef ska sedan samråda med dataskyddsombudet om en eventuell till integritetsskyddsmyndigheten (IMY) inom 72 timmar. Skyddade personuppgifter måste hanteras manuellt. I KIA rapporteras en personuppgiftsincident under kategorin 'säkerhet'. Detta medför bland annat att personuppgiftsincidenter blandas med bråk på en skola exempelvis. Det ska åtgärdas framgent, då skolorna kommer att anmäla incidenter i ett annat system och bara hantera incidenter kopplade till arbetsgivaren/arbetstagaren i KIA medan incidenter kopplade till elever hanteras frånskilt KIA. Detta är något som social- och äldreförvaltningen redan har hanterat.

Av granskningen framgår att det råder osäkerhet hur kring en personuppgiftsincident, framför allt en röjning av skyddade personuppgifter, ska rapporteras. Det framhålls bland annat att det saknas vetskap om att det finns en samlad rutin över hur en personuppgiftsincident ska rapporteras.

Som ett led i grund- och förskolenämndens samt gymnasie- och vuxenutbildningsnämndens egenkontroll för dataskyddsarbetet har samtliga inrapporterade incidenter under 2021 analyserats. Under 2021 har fem incidenter anmälts i KIA varav två har anmälts till IMY. IMY har inte vidtagit några åtgärder med anledning av

anmälningarna. I fyra av incidenterna har en individs personuppgifter spridits till obehöriga. Orsaken i samtliga fall bedöms vara den mänskliga faktorn. De två incidenterna som anmälts till IMY rör känsliga personuppgifter. Ingen av incidenterna rör skyddade personuppgifter.

6.1. Bedömning

Enligt vår bedömning finns det brister i avvikelsehanteringen. Det är viktigt att kommunen har en god intern kontroll över den egna verksamheten med system för att identifiera, rapportera, åtgärda och följa upp avvikelser och risker i ett lärande syfte. Det är en brist att det inte går att kategorisera avvikelser som avser skyddade personuppgifter utan manuell hantering. Vi bedömer vidare att det saknas systematik för att åtgärda brister kopplat till hanteringen av skyddade personuppgifter i tillräcklig utsträckning. Uppföljningsarbetet av avvikelser bör prioriteras.

7. Svar på revisionsfrågor

Fråga	Svar
Har kommunen analyserat risken för att skyddade personuppgifter röjs i kommunens verksamheter? Sker någon informationsinhämtning från relevanta instanser inom civilsamhället?	**Delvis**. En kommunövergripande identifierad risk för år 2022 är "Personuppgiftsbehandling enligt GDPR". Risken finns med i samtliga styrelse/nämnders internkontrollplaner. Risken för röjning av skyddade personuppgifter specifikt har endast inkluderats i grund- och förskolenämndens samt gymnasie- och vuxenutbildningsnämndens internkontrollplaner för 2021. Risken för hanteringen av skyddade personuppgifter har inte behandlats i kommunstyrelsens och socialnämndens internkontrollplaner. Vidare måste nämnderna i egenskap av personuppgiftsansvariga årligen från 2021 genomföra en egenkontroll för sitt dataskyddsarbete och rapportera resultatet till kommunstyrelsen och dataskyddsombudet. Skyddade personuppgifter behandlas inte i egenkontrollen.
Har kommunen vidtagit åtgärder för att minska risken?	**Ja, men inte i tillräcklig utsträckning**. Respektive förvaltning har upprättat verksamhetsspecifika arbetsrutiner för hanteringen av skyddade personuppgifter. Däribland hanteringen av skyddade elever, brukare och anställda i kommunens verksamhetssystem, hanteringen av e-post, kommunikation och en riskbedömning över den enskildas hotbild inom skola och socialtjänst. Utbildningsförvaltningen upprättar en individuell handlingsplan per elev/brukare vilket överensstämmer med Skolverkets rekommendationer. Social- och äldreförvaltningen upprättar inte en individuell handlingsplan. Det gör inte heller HR-/löneenheten per anställd med skyddade personuppgifter. Det finns anledning att vidta fler och skarpare åtgärder då det finns risker inom respektive förvaltning och verksamhetsområde som inte inkluderats i tillgängliga anvisningar. Vidare visar granskningen att det varken har gjorts penetrationstester eller loggkontroller med anledning av risken för röjning av skyddade personuppgifter.
Följer kommunstyrelsen och nämnderna upp den interna kontrollen rörande hanteringen av skyddade personuppgifter?	**Delvis**. I och med att kommunstyrelsen och socialnämnden inte har inkluderat risken för röjning av skyddade personuppgifter i någon internkontrollplan kan frågan ej besvaras. Grund- och förskolenämnden samt gymnasie- och vuxenutbildningsnämnden har följt upp kontrollmålet avseende risken för röjning av skyddade personuppgifter från 2021. Kontrollmålet följdes bland annat upp genom en enkät till förskole- och grundskolerektorer.

Finns det kommunövergripande och förvaltningsspecifika anvisningar och rutiner för hantering av personer med skyddade personuppgifter? Hur görs de kända för medarbetare och vilken utbildning ges?	**Ja**. Inom kommunens verksamheter finns en rad kommunövergripande och verksamhetsspecifika riktlinjer, rutiner och anvisningar vad gäller hanteringen av skyddade personuppgifter. Av granskningen framkommer att det finns flera olika riktlinjer och rutiner i kommunen som saknar styrkraft och relevans till följd av att de inte uppdateras i enlighet med exempelvis ny lagstiftning. De beskrivs antingen vara väldigt övergripande eller väldigt detaljerade. Det uppges därför finnas behov att inventera, uppdatera och samordna de rutiner som finns i syfte att stärka arbetet med skyddade personuppgifter. Utöver tillgängliga riktlinjer/rutiner/anvisningar finns även information om skyddade personuppgifter på kommunens intranät. Kompetensutveckling och kunskapsspridning framställs dock som ett särskilt utvecklingsområde. Det finns i viss utsträckning utbildningar om GDPR men dessa inkluderar emellertid inte specifikt hanteringen av skyddade personuppgifter. Vidare saknas en funktion som arbetar särskilt med att säkerställa att styrande dokument är kända och tillämpade, ofta kallad ”compliancefunktion”.
Finns det ett avvikelsehanteringssystem som omfattar skyddade personuppgifter?	**Delvis**. På kommunens intranät finns information om rutinerna för rapportering av personuppgiftsincident. Rutinen avser rapportering av alla sorters personuppgiftsincidenter. Det finns således inte någon särskild rutin för hanteringen av eventuell röjning av skyddade personuppgifter, och det går inte att särskilja en sådan rapportering utan manuell hantering.

Haninge den 3 oktober 2022

David Leinsköld
Verksamhetsrevisor, EY

Bilaga 1: Källförteckning

Intervjuade funktioner

Kommunstyrelseförvaltningen:

- HR-chef
- IT-chef
- Kommunjurist/dataskyddsombud
- Kvalitetschef

Utbildningsförvaltningen:

- Förvaltningsjurist/utredare
- Objektspecialist IT
- Objektspecialist IT
- Rektor grundskola
- Rektor förskola
- Rektor centrum vux.

Social- och äldreförvaltningen:

- Förvaltningsjurist/dataskyddskoordinator
- IT-strateg/förvaltningsledare vård- och omsorg
- Gruppledare mottagning – Avdelningen arbete och försörjning
- Gruppledare egen försörjning – Avdelningen arbete och försörjning
- Enhetschef barnenheten – Avdelningen individ- och familjeomsorg
- Enhetschef relationsvårdsteamet – Avdelningen för individ- och familjeomsorg

Granskad dokumentation

- Reglemente för kommunstyrelsen och övriga nämnder i Haninge kommun (KS 021-00485)
- Riktlinjer till reglementet för intern kontroll (KS 2015/570)
- "Skyddade personuppgifter" (information på intranätet)
- Haninges IT-handbok – Anvisningar om hur du hanterar din IT- och telefonutrustning" (Version 1.3 2022-05-05)
- Gemensamma kontroller i internkontrollplan 2022
- Internkontrollplan 2022 Grund- och förskolenämnden
- Internkontrollplan 2022 Gymnasie- och vuxenutbildningsnämnden
- Internkontrollplan 2022 Socialnämnden
- Rutin för att rapportera uppföljning och granskning av dataskyddsförordningen (KS 2021/431)
- Grund- och förskolenämndens egenkontroll för dataskyddsarbetet under 2021
- Gymnasie- och vuxenutbildningsnämndens egenkontroll för dataskyddsarbetet under 2021
- Vägledning skyddade personuppgifter 20190101 (KS)
- Rutiner för tillverkning av passerkort för person med skyddad identitet (KS)
- Rutiner för utlämning av P-tillstånd för person med skyddad identitet (KS)
- Posthantering för personer med skyddade personuppgifter (KS)
- Rutiner för hantering av medarbetare med skyddade personuppgifter (KS)
- Skyddade personuppgifter i Heroma (KS)
- Anonym – Överföring från Navet (KS)
- Hantering av ansökningar med skyddade personuppgifter (KS)
- Så här fungerar det vad gäller Skyddade personuppgifter med sekretessmarkering, kvarskrivning och sekretess till skydd för enskild i personadministrativ verksamhet (KS)
- Rutin – Skyddade personuppgifter (KS)

- Rutiner för hantering av elever med skyddade personuppgifter (GFN & GVN)
- Arbetsrutiner kring skyddad identitet antagning elever på Centrum Vux (GVN)
- Rutin för att lägga upp personer med skyddad identitet i Lifecare (SN)
- Rutin systematisk logguppföljning (SN)