STRÄNGNÄS KOMMUN
KOMMUNREVISIONEN

Revisionsskrivelse 2022-06-15

För yttrande till: Kommunstyrelsen, socialnämnden, barn- och utbildningsnämnden
För kännedom till: Kommunfullmäktige

Granskning kommunens hantering av skyddade personuppgifter

EY har på uppdrag av kommunrevisionen i Strängnäs kommun granskat hur kommunen säkerställer att uppgifter som rör personer med skyddade personuppgifter inte röjs till obehöriga. Den sammanfattande bedömningen är att kommunstyrelsens, socialnämndens samt barn- och utbildningsnämndens rutiner inte är helt ändamålsenliga.

Det finns verksamhetsspecifika riktlinjer, rutiner och anvisningar för hanteringen av personer med skyddade personuppgifter. Det finns dock behov av utförligare kommunövergripande och verksamhetsspecifika beskrivningar baserat på inventerade riskmoment. Vissa styrande dokument är utformade på ett sätt som inte motsvarar det stöd som personal efterfrågar.

Det finns risker av allmän karaktär som gäller hela kommunen, däribland extern och intern kommunikation med myndigheter och privatpersoner. Det finns även brister i avvikelsehanteringen, i informationsspridning av riktlinjer, rutiner och anvisningar till medarbetare samt ett behov av tydligare rutiner för hanteringen av anställdas situation. Vidare finns kontorsspecifika risker unika för varje situation.

Risken för röjning av skyddade personuppgifter har inte bedömts och värderats utifrån risk- och konsekvensanalys varför kommunstyrelsen eller granskade nämnder därmed inte genomfört relevanta kontrollåtgärder. Styrelse och nämnder följer inte upp och kontrollerar att rutinerna efterlevs. Det sker ingen aggregering eller systematisering av avvikelser för att åtgärda brister kopplat till hanteringen av skyddade personuppgifter.

Granskningen besvarar fyra revisionsfrågor. I nedanstående tabell framgår huruvida revisionsfrågorna bedöms vara helt, delvis eller ej uppfyllda.

Helt uppfyllt	
Delvis uppfyllt	
Ej uppfyllt	

Revisionsfråga	Bedömning
Har kommunen analyserat risken för att skyddade personuppgifter röjs i kommunens verksamheter?	
Har kommunen vidtagit åtgärder för att minska risken?	
Finns det ett avvikelsehanteringssystem som omfattar dessa avvikelser?	
Finns det kommunövergripande anvisningar och rutiner för hantering av personer med skyddade personuppgifter?	

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen, socialnämnden samt barn- och utbildningsnämnden att:

- Upprätta risk- och konsekvensanalys avseende hantering av skyddade personuppgifter och inkludera i internkontrollplanen.
- Genomför obligatoriska utbildningar för samtliga medarbetare *och* förtroendevalda med utgångspunkt i tillämpning av styrande dokument.
- Säkerställ en strukturerad uppföljning av tillämpning av styrande dokument.
- Genomför återkommande penetrationstester av hanteringen av skyddade personuppgifter.
- Stärk avvikelsehanteringen och uppföljningen avseende skyddade personuppgifter.

Kommunstyrelsen rekommenderas att:

- Upprätta en kommunövergripande riktlinje samt ett specifikt styrdokument avseende medarbetare med skyddade personuppgifter.

Revisorerna önskar svar på vilka åtgärder som kommer att vidtas, inklusive tidsplanering, med anledning av vad som framkommit i granskningen och de rekommendationer som lämnas. Svar önskas senast 2022-09-30.

På uppdrag av Strängnäs kommuns revisorer

Jens Persson
Ordförande kommunrevisionen

Stefan Behrnetz
Vice ordförande

Granskningsrapport 2022
Genomförd på uppdrag av revisorerna

Strängnäs kommun

Granskning av kommunens hantering av skyddade personuppgifter

Building a better working world

Innehållsförteckning

Sammanfattande bedömning och rekommendationer

Granskningens syfte är att bedöma hur kommunen säkerställer att uppgifter som rör personer med skyddade personuppgifter inte röjs till obehöriga. Vår sammanfattande bedömning är att granskad styrelse och nämnders rutiner inte är helt ändamålsenliga.

Det finns verksamhetsspecifika riktlinjer, rutiner och anvisningar för hanteringen av personer med skyddade personuppgifter. Dessa styrande dokument bedöms i huvudsak vara utförliga och omfattar nödvändiga beskrivningar av hanteringen av personer med skyddade personuppgifter. Vi noterar att det dock inte finns några kommunövergripande rutiner för hantering av personer med skyddade personuppgifter, däribland med avseende på medarbetare. Det finns behov av utförligare kommunövergripande och verksamhetsspecifika beskrivningar baserat på inventerade riskmoment. Vissa styrande dokument är utformade på ett sätt som inte motsvarar det stöd som personal efterfrågar.

Det finns risker av allmän karaktär som gäller hela kommunen, däribland extern och intern kommunikation med myndigheter och privatpersoner. Det finns även brister i avvikelsehanteringen, i informationsspridning av riktlinjer, rutiner och anvisningar till medarbetare samt ett behov av tydligare rutiner för hanteringen av anställdas situation. Vidare finns kontorsspecifika risker unika för varje situation.

Vi uppmärksammar kompetens och kunskapsspridning som särskilda utvecklingsområden. Medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter bör stärkas genom obligatoriska utbildningar och informationsspridning då mänskliga faktorn identifierats som risk i hanteringen av skyddade personuppgifter.

Risken för röjning av skyddade personuppgifter har inte bedömts och värderats utifrån risk- och konsekvensanalys varför kommunstyrelsen eller granskade nämnder därmed inte genomfört relevanta kontrollåtgärder. Styrelse och nämnder följer inte upp och kontrollerar att rutinerna efterlevs. Det sker ingen aggregering eller systematisering av avvikelser för att åtgärda brister kopplat till hanteringen av skyddade personuppgifter.

Det är en brist att penetrationstester av IT-systemen inte utförs, vilket bör ske för att identifiera sårbarheter och skadekonsekvenser.

Utifrån granskningens iakttagelser rekommenderar vi kommunstyrelsen, socialnämnden samt barn- och utbildningsnämnden att:

- Upprätta risk- och konsekvensanalys avseende hantering av skyddade personuppgifter och inkludera i internkontrollplanen.
- Överväg obligatoriska utbildningar för samtlig personal med utgångspunkt i tillämpning av styrande dokument.
- Överväg "compliancefunktion/-er" med ansvar för strukturerad uppföljning av tillämpning av styrande dokument.
- Genomför penetrationstester av IT-system och digitala rutiner.
- Stärk avvikelsehanteringen och uppföljningen avseende skyddade personuppgifter.

Kommunstyrelsen rekommenderas att:

- Upprätta en kommunövergripande riktlinje samt ett specifikt styrdokument avseende medarbetare med 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.

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 rutinerna är välkända 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

Granskningens syfte har varit att bedöma hur kommunen säkerställer att uppgifter som rör personer med skyddade personuppgifter inte röjs till obehöriga. Svaren på revisionsfrågorna ska uppfylla granskningens syfte, det vill säga 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?
- Har kommunen vidtagit åtgärder för att minska risken?
- Finns det ett avvikelsehanteringssystem som omfattar dessa avvikelser?
- Finns det kommunövergripande anvisningar och rutiner för hantering av personer med skyddade personuppgifter? Hur görs de kända för medarbetare?

1.3. Ansvariga nämnder

Granskningen avser kommunstyrelsen, socialnämnden samt barn- och utbildningsnämnden.

1.4. Metod och genomförande

Granskningen bygger på dokumentgranskning och intervjuer. Intervjuer har genomförts med företrädare för kommunens säkerhetsenhet, HR-avdelning samt chefer och medarbetare inom utbildningskontoret och socialkontoret. Intervjuade funktioner och granskade underlag framgår av källförteckningen.

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"
- Socialtjänstlagen (2001:453)
- Skollagen (2010:800)
- Av fullmäktige antagna styrdokument eller relevanta riktlinjer

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. Omräknat till Strängnäs kommun motsvarar det uppskattningsvis ca 84 invånare och ca 5 anställda. Siffrorna är inte exakta men visar att det rent statistiskt är ett fåtal individer. Konsekvensen vid felaktig röjning av skyddade personuppgifter kan emellertid vara mycket allvarlig för var och en av dessa.

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 att flytta på grund av våld och hot från närstående man och att målgrupperna är extra utsatta. Att leva med skyddade personuppgifter försvårar hela livssituationen för våldsutsatta kvinnor och barn med stor ekonomisk utsatthet, boende och barnens skolgång. Många

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

upplever att efter att skyddade personuppgifter beviljats avtar - eller till och med upphör - samhällets stöd. I princip samtliga kvinnor i Jämställdhetsmyndighetens intervjustudie har fått sina 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 också 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. Skatteverket vidareförmedlar post till personer med sekretessmarkering. 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 eller intyg 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 ett starkare skydd än sekretessmarkering

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

Skyddad folkbokföring medges för person som av särskilda skäl kan antas bli utsatt för brott, förföljelser eller allvarliga trakasserier på annat sätt, om åtgärden med hänsyn till den enskildes förmåga och övriga förutsättningar kan antas tillgodose behovet av skydd. Skyddad folkbokföring kan kombineras med andra skyddsåtgärder som exempelvis

kontaktförbud om det bedöms lämpligt utifrån den enskildes specifika situation. Skyddad folkbokföring medges efter ansökan från den enskilde. För barn under 18 år får ansökan enbart göras av en vårdnadshavare om 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 i och med att 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.

2.5. Patientdatalagen ökar patientsäkerheten med bibehållet skydd för den personliga integriteten

Patientdatalagens syfte är att öka patientsäkerheten med bibehållet skydd för den personliga integriteten. Här finns bestämmelser om hur vårdgivare ska behandla personuppgifter inom hälso- och sjukvården och hur patientjournal ska föras. Lagen kompletteras av föreskrifter och allmänna råd samt handbok från Socialstyrelsen.

Patientdatalagen och Socialstyrelsens författning om journalföring och behandling av personuppgifter i hälso- och sjukvården ställer krav på unik identifiering av både patienter och personal i vårdgivarnas informationssystem som innehåller patientuppgifter. Vårdgivare behöver därför rutiner för hur skyddade personuppgifter ska hanteras.

Dokumentation av olika åtgärder i journalen kan vara avgörande för patientsäkerheten. Dokumentationen är även viktig som underlag för rättsintyg för att bedöma om ett brott har begåtts eller inte.

3. Organisation och ansvar

Ingen styrelse eller nämnd har ett utpekat ansvar för hanteringen av skyddade personuppgifter i Strängnäs kommunen. Respektive styrelse/nämnd är personuppgiftsansvarig för de personuppgifter som de behandlar i sin verksamhet. Varje styrelse/nämnd kan potentiellt komma i kontakt med personer som har skyddade personuppgifter, både i form av patienter/klienter/elever samt medarbetare. Ansvarsområdena skiljer sig dock mellan styrelse/nämnderna och de har således inte samma ansvar för kommunens hantering av personuppgifter. Nedan redogörs de granskades ansvarsområden och tjänstemannaorganisation kring hantering av skyddade personuppgifter.

3.1. Kommunstyrelsens ansvar och organisation

Kommunstyrelsen är kommunens ledande politiska förvaltningsorgan. Styrelsen har ett helhetsansvar för kommunens verksamheter, utveckling och ekonomiska ställning. Enligt kommunstyrelsens reglemente[2] ska styrelsen leda kommunens verksamhet genom att utöva en samordnad styrning och leda arbetet med att ta fram styrdokument för kommunen. Kommunstyrelsen ska ha fortlöpande uppsikt över övriga nämnders verksamhet, löpande följa upp hur den interna kontrollen hanteras i nämnderna samt att det finns en god intern kontroll inom sitt eget verksamhetsområde.

Vidare har styrelsen ett kommunövergripande ansvar för säkerhetsfrågor samt kommungemensamma informations- och kommunikationssystem. Kommunstyrelsen är arkivmyndighet och personuppgiftsansvarig för de personuppgifter som styrelsen behandlar i sin verksamhet. Kommunstyrelsen ansvarar dessutom för kommunens kontaktcenter och kommunens juristfunktion.

Slutligen är kommunstyrelsen anställningsmyndighet för all personal inom

[2] KS/2030:513-003.

kommunförvaltningen, och är därmed ansvarig för kommunens personalpolitik och för frågor som rör förhållandet mellan kommunen som arbetsgivare och dess arbetstagare.

Förvaltningen i Strängnäs kommun är organiserad i kontor och avdelningar. Kommundirektören är förvaltningens högsta tjänsteperson. Under kommunstyrelsen finns fem avdelningar; kansliavdelningen, HR-avdelningen, ekonomiavdelningen kommunikationsavdelningen samt IT- och digitaliseringsavdelningen.

Kommunstyrelsens internkontrollplan för 2022 omfattar inte risker vid hantering av skyddade personuppgifter. Det omnämns heller inte i styrelsens verksamhetsplan för 2022.

3.2. Socialnämndens ansvar och organisation

Socialnämnden fullgör kommunens uppgifter enligt bland annat socialtjänstlagen (2001:453), hälso- och sjukvårdslagen (2017:30) samt patientdatalagen (2008:355). Nämnden ska tillse att verksamheten bedrivs i enlighet med de föreskrifter som anges i lagar och förordning, de mål och riktlinjer som fullmäktige har bestämt och bestämmelserna i nämndens reglemente.[3]

Socialnämnden ska med uppmärksamhet följa utvecklingen inom sina egna verksamhetsområden, vara personuppgiftsansvarig för de personuppgifter som nämnden behandlar i sin verksamhet samt fortlöpande se över och vid behov reformera sitt regelverk.

Socialkontoret leds av en socialchef.[4] Kontorsledningsgrupper består utöver socialchef av en verksamhetscontroller, medicinskt ansvarig sjuksköterska (MAS), socialt ansvarig samordnare (SAS) samt verksamhetschefer för områdena individ- och familjeomsorg, funktionshinderomsorg, hemsjukvård, myndighetsavdelningen, äldreomsorg samt administration och digitalisering.

Socialnämndens internkontrollplan för 2022 omfattar inte risker vid hantering av skyddade personuppgifter. Det omnämns heller inte i nämndens verksamhetsplan för 2022.

3.3. Barn- och utbildningsnämndens ansvar och organisation

Barn- och utbildningsnämnden fullgör huvudsakligen kommunens uppgifter enligt skollagen (2010:800) där 26 kap. berör behandling av personuppgifter. Nämnden ska tillse att verksamheten bedrivs i enlighet med de föreskrifter som anges i lagar och förordning, de mål och riktlinjer som fullmäktige har bestämt och bestämmelserna i nämndens reglemente.[5]

Barn- och utbildningsnämnden ska med uppmärksamhet följa utvecklingen inom sina egna verksamhetsområden, vara personuppgiftsansvarig för de personuppgifter som nämnden behandlar i sin verksamhet samt fortlöpande se över och vid behov reformera sitt regelverk.

Utbildningskontoret leds av en utbildningschef. Kontorsledningsgruppen består utöver utbildningschef av en administrativ enhetschef, en verksamhetschef för grundskola, en verksamhetschef för förskola samt elevhälsan.

Den administrativa enheten består av 13 medarbetare, däribland handläggare och

[3] KS/2020:604-003.

[4] För närvarande tillförordnad socialchef.

[5] KS/2020:616-003.

administratörer som bland annat hanterar skolplaceringar och kommer i kontakt med elever som har skyddade personuppgifter. Den centrala barn- och elevhälsan består av sex medarbetare samt nio skolsköterskor.

Barn- och utbildningsnämndens internkontrollplan för 2022 omfattar inte risker vid hantering av skyddade personuppgifter. Det omnämns heller inte i nämndens verksamhetsplan för 2022.

4. Riktlinjer med tillhörande rutiner vid hantering av personer med skyddade personuppgifter

4.1. Det saknas kommunövergripande riktlinjer med tillhörande rutiner

Strängnäs kommun saknar kommunövergripande riktlinjer med tillhörande rutiner eller anvisningar vad gäller hanteringen av skyddade personuppgifter. Det finns dokumentation som berör informationssäkerhet (informationssäkerhetspolicy), GDPR samt registerutdrag och hantering av personuppgiftsincidenter. Det finns ingen kommunövergripande riktlinje vad gäller hanteringen av medarbetare med skyddade personuppgifter.

4.2. Socialkontoret har flera riktlinjer med tillhörande rutiner och anvisningar

Socialnämnden har riktlinjer, rutiner och anvisningar för hantering av skyddade personuppgifter.

Det finns en rutin för hantering av personer med skyddade personuppgifter. Rutinen gäller för samtliga verksamheter inom socialkontoret. Rutinen beskriver bland annat genomförandet vid aktualisering och vem som ska ha behörighet till en persons akt samt när den ska avslutas. Antalet personer med tillgång bör vara begränsat. Det åligger respektive verksamhet att upprätta anvisningar anpassade till verksamhetsområdet. Rutinen har ett uppföljningsdatum för att innehållet ska kontrolleras en gång per år.

Vi har tagit del av ytterligare två anvisningar som rör hanteringen av personer med skyddade personuppgifter där en avser vård- och omsorgsutförarverksamheter. Anvisningen tydliggör vilka steg som behöver genomföras och vem som ansvarar för olika delar i hanteringen av personer med skyddade personuppgifter.

Det är enhetschefens ansvar att ta ställning till hur många i personalen som ska ha tillgång till brukarens akt. Enhetschefen informerar systemadministratör för Treserva vilka som ska ha tillgång till den digitala akten.
Tillsammans med brukare med skyddade personuppgifter rekommenderas att ett antal frågor ställs, däribland brukarens inställning till säkerhet, kontakt, hot och eventuella extra känsliga uppgifter. Det är viktigt att verksamheten inte förvarar telefonnummer eller andra kontaktuppgifter där det finns risk att obehörig kan få tillgång till uppgifterna. I genomförandeplan och journal ska endast det som är väsentligt för att genomföra uppdraget dokumenteras. Inga uppgifter om exempelvis adresser till mötesplatser med personal eller liknande ska beskrivas.

Vidare finns anvisning för beställning, justering samt avslut av behörighet till sekretesskyddade personer i verksamhetssystemet Treserva. Anvisningen förklarar och ska underlätta hanteringen av behörighet i Treserva till brukare och patienter som har någon

form av skyddade personuppgifter. Målet är att minska risken att sekretessmarkerade personuppgifter lämnas ut oavsiktligt samt begränsa antal personer som har tillgång till de skyddade uppgifterna.

Skyddade personer visas i Treserva med en hänglåssymbol. I stället för fullständigt personnummer visas sekelsiffra och de två första siffrorna i personnumret följt av ****-****Skyddad. Sekretessbehörighet har de användare som har behov av det i sin tjänst för att kunna utföra sitt arbete. Tilldelning, justering och avslut av behörighet sker manuellt via socialkontorets systemförvaltning efter godkännande av enhetschef eller gruppledare.

Vad gäller hälso- och sjukvårdsdokumentation finns riktlinje som bland annat anger ramarna för innehållet i hälso- och sjukvårdsjournalen så den uppfyller patientdatalagens intentioner beträffande innehåll. Det ska framgå vem som skriver, befattning och när anteckningen görs. Den som för patientjournal ansvarar för sina egna anteckningar. Det ska framgå om samtycke eller förmodat samtycke har getts i samband med utlämning av journalhandling, kvalitetsregister och till att legitimerad personal får tillgång till nationell patientöversikt. Enligt riktlinjen ska det finnas skriven rutin, anvisning eller checklista för journaldokumentation som beskriver bland annat hur skyddade personnummer hanteras. Det finns en anvisning som beskriver tillämpning av hälso- och sjukvårdsjournalen i verksamhetssystemet vid hantering av personer med skyddade personuppgifter.

4.3. Barn- och utbildningskontoret har flera riktlinjer med tillhörande rutiner och blanketter

Barn- och utbildningsnämnden har riktlinjer, rutiner, anvisningar, checklistor, handlingsplaner och blanketter gällande hanteringen av barn, elever och studerande med skyddade personuppgifter.

Den övergripande riktlinjen Riktlinjer för hantering av barn, elever och studerande med skyddade personuppgifter anger hur målgruppen ska hanteras i kommunen. Rektor ansvarar för att all berörd personal är informerad om riktlinjen. Rektor ansvarar även för att skyddade personuppgifter hanteras på ett korrekt sätt i verksamheten och att de barn och unga som har skyddade personuppgifter får det stöd och den utbildning som de har rätt till. Hur personuppgifter ska hanteras i detalj regleras i Rutin för barn, elever och studerande med skyddade personuppgifter.

Rutinen gäller samtliga barn- och utbildningsnämndens verksamheter. Syftet med rutinen är att barn, elever och studerande med skyddade personuppgifter i kommunen ska hanteras på samma sätt oavsett vilken enhet de sorteras under. Rutinen beskriver hela arbetsgången kring hanteringen av barn, elever och studerande med skyddade personuppgifter.

Bland annat beskrivs vikten av planering och hur den går till i praktiken, rutinen kring upprättande av en handlingsplan och blankett, hur skyddade personuppgifter förvaras, hur betygsättning går till, hur de digitala systemen ska användas, vilken information som ska delges placeringshandläggarna gällande förskola/fritids och att elever med skyddade personuppgifter ska rapporteras till SCB med sina riktiga personuppgifter. Vidare beskrivs flera praktiska detaljer som rutiner kring fotografering samt barn- och elevlistor, beredskap för akuta situationer, rutiner kring besök på biblioteket, hantering av busskort/skolkort, olovlig frånvaro, förändrade omständigheter, telefonsamtal eller förfrågan av en elev, flytt, e-post, klasslistor, utlämnande av handlingar samt vilken obligatorisk information som ska ges. Rutinen anger vidare specifika rutiner för huvudmannen.

Det finns en rad andra rutiner, anvisningar och checklistor kring hantering av elever med skyddade personuppgifter i specifika situationer. Centrala barn och elevhälsan (Elevhälsans medicinska insats, EMI) har flera. Information och rutin kring elever med skyddade personuppgifter beskriver vilka typer av skyddade personuppgifter det finns och rutinen när en elev med skyddade personuppgifter kommer till kommunen. Vidare finns Rutin och processkarta kring elever med skyddade personuppgifter. Rutinen anger bland annat journalhanteringen, hur en remiss ska skrivas, kontakt med socialtjänst samt hanteringen av tolk när elever har skyddade personuppgifter. Rutinen innehåller även processkartor över ovan nämnda hanteringar.

Därutöver finns blanketter och handlingsplaner som används vid hanteringen av elever med skyddade personuppgifter.

4.4. Bedömning

Hanteringen av personer med skyddade personuppgifter ska följa särskilda krav. Identiteten hos den som lever skyddad får inte röjas av misstag. Kommunen bör därför ha en eller flera riktlinjer med tillhörande rutiner för att hantera skyddade personuppgifter. Det är av väsentlighet att rutinerna är välkända bland samtliga medarbetare då i princip alla kan komma i kontakt med personer med skyddade personuppgifter.

Vi noterar att ingen av granskade internkontrollplaner omfattar risker förknippade med skyddade personuppgifter. Risken att röja skyddade personuppgifter har inte bedömts och värderats av granskad styrelse och nämnder baserat på inventerade riskmoment och med stöd av eventuella avvikelser. Att så inte sker uppfattas av oss som en brist.

Dokumentgranskningen visar att det saknas en kommunövergripande riktlinje som beskriver hanteringen av skyddade personuppgifter, däribland hanteringen av medarbetare med skyddade personuppgifter. Vi kan konstatera att det strider mot kommunstyrelsens reglemente. Socialkontoret och utbildningskontoret har antagit verksamhetsspecifika riktlinjer, rutiner och anvisningar på eget initiativ, exempelvis efter genomförd riskanalys i en specifik enhet, som beskriver hanteringen av skyddade personuppgifter. Vi bedömer att upprättade dokument i huvudsak är utförliga och behandlar ändamålsenliga beskrivningar av hanteringen av personer med skyddade personuppgifter.

Vi ser dock ett behov av en kommunövergripande riktlinje som även behandlar hanteringen av medarbetare. Detta för att sätta fokus på denna angelägna fråga samt öka kommunstyrelsens styrkraft och samordning. Därutöver ser vi en risk i att det inom utbildningskontorets verksamheter finns för många riktlinjer, rutiner och anvisningar som riskerar att skapa förvirring bland personalen och försämrad styrkraft i dokumenten. Vidare konstaterar vi att flertalet styrande dokument inte är politiskt antagna, vilket riskerar att ytterligare försvaga dokumentens styrkraft.

5. Iakttagelser utifrån genomförda intervjuer

5.1. Kommunstyrelsen har inte tagit ett övergripande ansvar för hanteringen av skyddade personuppgifter

Då det saknas kommunövergripande dokumentation kring hur skyddade personuppgifter ska hanteras finns heller inga rutiner för hur frågan ska hanteras, påtalar intervjuad nämndsekreterare/dataskyddssamordnare. Ansvarsfördelningen beskrivs vara otydlig och skapar därför inte gynnsamma förutsättningar. Det finns rutiner vad gäller hanteringen av

GDPR som "spiller över" på informationssäkerhet och hanteringen av skyddade personuppgifter. GDPR-arbetet uppfattas dock olika i kommunen. Det beskrivs av intervjuad nämndsekreterare/dataskyddssamordnare inte vara prioriterat och vad gäller informationssäkerhetsarbetet beskrivs det finnas en omognad i organisationen. Intervjuad kommunjurist tillika dataskyddsombud beskriver att de rutiner som finns är förlegade och att det inte har upprättats nya inom området sedan genomförda omorganisationer. Däremot har det gjorts krafttag i organisationen där data skyddssamordnare har införts, men att dessa inte har tid för sitt uppdrag. Intervjuad kanslichef delar inte uppfattningen om att GDPR- och informationssäkerhetsarbetet är nedprioriterat.

I kommunen tillämpas en förvaltningsstyrningsmodell som baseras på Pm3 för förvaltning av IT-baserade system. Pm3-modellen möjliggör styrning utifrån ett tvärfunktionellt perspektiv där respektive kontor/avdelning hanterar och förvaltar sina egna verksamhetssystem, där bland annat skyddade personuppgifter hanteras. I varje verksamhet finns en objektägare (kontorschef) över de objekt som förvaltas samt en dataskyddssamordnare.

Intervjuad nämndsekreterare/dataskyddssamordnare kritiserar den decentraliserade organisationen för att vara i startgroparna där GDPR och informationssäkerhetsarbetet inte ges tillräcklig uppmärksamhet. Bland annat påtalas att kompetensen är otillräcklig. Vidare beskrivs att det inte ges någon uppmärksamhet från politisk håll kring GDPR och informationssäkerhetsfrågor i kommunen, trots att respektive styrelse och nämnd är personuppgiftsansvarig för respektive styrelses/nämnds verksamhet. Att GDPR och informationssäkerhet inte får tillräcklig uppmärksamhet och fokus beskrivs vara en bidragande orsak till att det inte finns antagna riktlinjer eller beskrivna rutiner kring hanteringen av skyddade personuppgifter. Ett konkret exempel som nämns är avsaknaden av säker och krypterad e-post, trots att frågan har diskuterats under lång tid.

Kommunens arbete med informationssäkerhet har dock intensifierats, däribland genom att erbjuda utbildningar till de olika kontoren. Däremot finns en osäkerhet bland personalen vad man får och inte får göra, vilket beskrivs kräva arbete för att alla ska känna sig trygga med hanteringen av personuppgifter. Skyddade personuppgifter har inte aktualiserats i detta sammanhang. Penetrationstester ur ett förövarperspektiv, det vill säga test för att identifiera vilka sårbarheterna är och hur stor skada de kan orsaka, används för att kontrollera att systemen är säkra. Penetrationstester i syfte att kontrollera sårbarenheten i hanteringen av skyddade personuppgifter har inte genomförts.

Eventuella personuppgiftsincidenter rapporteras i det kommunövergripande ärende- och dokumenthanteringssystemet LEX. I och med att respektive styrelse och nämnd är personuppgiftsansvarig ansvarar de för att rapportera avvikelser vad gäller skyddade personuppgifter. Det lyfts fram i intervju att det saknas anvisning över var avvikelser för skyddade personuppgifter ska registreras och avvikelser har inte påträffats i LEX. Avvikelser vad gäller skyddade personuppgifter går emellertid inte att sortera från övriga personuppgiftsincidenter utan att utföra en hantering.

Vid eventuell röjning av personuppgifter åligger det styrelsen/nämnderna att rapportera det till Integritetsskyddsmyndigheten (IMY). Övriga ärenden rapporteras i KIA. Det finns ingen kommunövergripande compliancefunktion, det vill säga en funktion som ansvarar för att bestämmelser och interna verksamhetsprinciper, som exempelvis riktlinjer, rutiner och anvisningar, följs. Det finns således ingen samlad bild över antalet avvikelser vad gäller skyddade personuppgifter och osäkerheten kring hur de ska registreras utgör en osäkerhetsfaktor kring om det förekommer eller inte.

Kontaktcenter finns i kommunhusets entré. Där jobbar åtta samhällsvägledare som ger information, vägledning och svar på kommuninvånares frågor. Det går att ställa frågor via e-post, telefon eller i samband med fysiskt besök. Kontaktcenter fungerar även som stöd åt kansliavdelningen i administrativa frågor. Då socialkontorets reception har begränsade öppettider fungerar även kontaktcenter som reception för socialkontoret.

Att kontaktcenter övertagit socialkontorets reception beskrivs resultera i problem då de inte har tillgång till samma information i syfte att på ett ändamålsenligt sätt skydda personer med skyddade personuppgifter. Exempelvis saknar de behörighet att se var möten äger rum vilket gör att samhällsvägledarna måste ställa många frågor till den besökande brukaren. Det ökar risken för att skyddade personuppgifter kan komma på tal.

I kontaktcenter kan vårdnadshavare fylla i blankett med information om barn med skyddade personuppgifter. Blanketten skickas till utbildningskontoret i sekretessmarkerade kuvert som placeras i ett annat kuvert enligt rutinen för postgång. Överlag hanterar dock inte kontaktcenter personuppgifter, varken bland brukare, elever eller anställda. Om problem uppstår vänder de sig till respektive kontor som äger frågan.

Vad gäller de anställda så finns idag ett antal med skyddade personuppgifter. Kriget i Ukraina och påföljder i Sverige har resulterat i en risk- och konsekvensanalys där inventering av systemstöd, säkerhetsskydd, rutiner kring hantering av personuppgifter i e-post med mera genomförts. Frågorna beskrivs ha arbetats igenom noggrant men att det inte finns en riktlinje för hanteringen av medarbetare med skyddade personuppgifter beskrivs vara bristfälligt.

HR- och lönesystemet hanteras i Visma där skyddade personuppgifter särmarkeras. Systemet är kopplat till Skatteverket som uppdaterar data löpande. Vid anställningsförfarandet uppdateras Visma mot Skatteverkets folkbokföringsregister och uppdateras om någon har skyddade personuppgifter. Vid sökande av tjänst kan den sökande ange skyddade personuppgifter i rekryteringssystemet. I övrigt beskrivs att Visma fungerar ändamålsenligt. Vid behov söks i loggarna för att se vem som har registrerat i systemet men inga loggar över vem som gjort sökning i systemet.

Behovet beskrivs som störst i utbildningsinsatser till personalen. En i intervju identifierad risk är hanteringen av medarbetar- och lönesamtal som idag sker analogt där anteckningar förs på papper (Microsoft Word). Anställningsavtalen finns både digitalt och analogt men ska enligt intervjuade bli digitala efter sommaren 2022. Det genomförs för tillfället en förstudie i syfte att digitalisera alla personakter. Idag skrivs de ut och förvaras i säkerhetsarkivet. Det beskrivs vara en brist som ökar risken för felhantering orsakad av mänskliga faktorn.

5.2. Socialnämnden är van att hantera känsliga personuppgifter

Under intervjuerna framhålls att det finns en trygghet i socialkontorets riktlinjer och rutiner vad gäller hanteringen av skyddade personuppgifter och att dessa upplevs ändamålsenliga. 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. Utbildningsbehovet ser dock olika ut inom socialtjänsten beroende på hur mycket personuppgifter som hanteras.

Det finns inga speciella utbildningar som inkluderar hanteringen av skyddade personuppgifter. Det finns dock annan typ av utbildning som rör informationssäkerhet och hanteringen av personuppgifter utifrån speciallagstiftningen GDPR. Säkerhetsenheten har i närtid kommunicerat kring klassningen i informationssäkerhet utifrån KLASSA. Vidare anordnade kommunjuristen en utbildning under hösten 2021 som berörde personuppgifter, sekretess, skydd etcetera. Det finns också utbildningar för handläggarna inom utredningsenheten för barn och vuxna som rör våld i nära relationer som inkluderar skyddade personuppgifter.

Under intervjuerna framkommer en önskan om utbildningsinsatser specifikt vad gäller skyddade personuppgifter ur flera perspektiv. Allmänt uttrycks ett behov av att öka medvetenheten kring skyddade personuppgifter och vilka risker som föreligger vid felhantering.

De rutiner och specifika anvisningar kring hanteringen av skyddade personuppgifter som socialkontoret har antagit bygger inte på genomförd risk- och sårbarhetsanalys. Någon sådan har inte genomförts vad gäller skyddade personuppgifter. Däremot har skyddade personuppgifter klassats med hjälp av SKR:s informationsklassningsverktyg KLASSA. Tf. socialchef beskriver att socialkontoret utifrån klassa-arbetet kommer att arbeta med risk- och konsekvensanalyser av skyddade personuppgifter specifikt. I dagsläget har kontoret inte kommit tillräckligt långt i processen. Särskilt poängteras att det interna arbetet i organisationen har kommit längre än det externa i bemärkelsen att rutiner och anvisningar finns på plats, men att det finns ytterligare riskbedömningar att göra genom att penetrationstesta systemet inklusive kontorets rutiner med dess tillhörande anvisningar.

Ett ändamålsenligt systemstöd är en förutsättning för att kunna hantera skyddade personuppgifter på ett betryggande sätt. Kommunen har upphandlat systemstödet Treserva. Systemet används av socialkontoret bland annat gällande individ- och familjeomsorg, äldreomsorg, funktionshinder samt kommunal hälso- och sjukvård. På socialförvaltningen finns tre systemförvaltare som har till uppgift att underhålla verksamhetssystemet så att det fungerar ändamålsenligt för handläggarna. Systemförvaltarna har möjlighet att anpassa systemet efter kontorets processer och utredningar så länge det följer Socialstyrelsens krav och regler. De ansvarar också för alla behörigheter och för supporten.

Systemet är ett av de största tillgängliga på marknaden och fungerar i allmänhet bra enligt intervjuade. Vid intervjuerna har det dock framkommit att det finns vissa brister. En är att det uppstår dataprogramfel vid exempelvis uppdateringar. Buggar (fel) upptäcks framförallt av handläggarna själva. Handläggarna kontaktar då systemförvaltarna som i sin tur kontaktar Treserva och de åtgärdar inom ett par veckor. Buggar som rör personuppgifter har identifierats. En avvikelse gällde att systemet inte hade uppdaterats med information om att en förälder förlorat vårdnadskap, varefter det kommunicerades information om barnet till föräldern som förlorat vårdnadskapet via ett brev. Avvikelsen inträffade för ca tre månader sedan. I detta fall var barnets identitet inte skyddad.

En potentiell risk gäller behörigheten till systemet. Den framtagna rutinbeskrivningen för tilldelande av behörighet till personer med sekretesskyddade uppgifter beskrivs vara välfungerande men en risk är antalet personer som har full behörighet till samtliga ärenden. Totalt gäller det upp till tio personer på socialkontoret som har full behörighet, däribland mottagningsenheten och samtliga systemförvaltare. Den fulla behörigheten beskrivs vara nödvändig i och med att utökad behörighet till handläggare måste kunna beviljas. Med full

behörighet följer ett stort ansvar och kräver en medvetenhet om att det råder nolltolerans mot att vara inne i ärenden i onödan. Systemförvaltarna kan också behöva gå in i ett ärende när handläggaren behöver support eller när upprättad behörighet inte fungerar. Fördelen är att datasystemfel upptäcks, nackdelen är att det inte görs systematiska kontroller vilka ärenden systemförvaltarna har varit i samt att systemförvaltarna då får information om personer med skyddade personuppgifter. Det är dessutom svårt för systemförvaltarna att förklara varför de har varit inne i respektive ärende i och med att det ibland inte går att spåra orsaken. Ansvaret som åläggs systemförvaltarna är således stort.

En del av den interna kontrollen omfattar behörigheten till ärenden i Treserva. I systemet finns en kontrollfunktion som genomför analyskontroller av behörigheten två gånger per år av fem slumpmässigt utvalda medarbetare vid ett slumpmässigt datum. Syftet med stickprovskontrollerna är att tillse att en handläggare inte varit inne i fel ärende. I dessa kontroller framkommer information om vem som har varit inne i respektive ärende och när. Om en brukare begär ut sin logg framkommer samma information. Likaså vid misstanke eller indikation på felhantering av handläggare.

Vidare har socialkontoret identifierat en svag länk i möjligheten till säker intern och extern digital informationsöverföring där risker för felhantering föreligger. Bland annat har det påpekats att det är otydligt vilka rutiner som är gällande. I dagsläget finns inte möjligheten att skicka krypterad epost. Enligt gällande rutiner ska känslig information inte kommuniceras via epost, utan via skriftlig information på papper eller med hjälp av fax. Det pågår för närvarande en upphandling om systemstöd som ska möjliggöra säker digital kommunikation via krypterad e-post. Enligt tf. socialdirektör kommer säker e-post implementeras i juni 2022. Kommunens interna verksamhetssystem Treserva uppges ge bra stöd för säker intern kommunikation.

Fax används exempelvis av mottagnings- och familjeenheten samt av utredningsenheten barn och vuxen i de fall de ska skicka anmälningar till andra kommuner eller myndigheter, däribland polisen. De tar även emot orosanmälningar via fax. Utredningsenheten för äldre och personer med funktionsnedsättning använder fax för att skicka uppdrag/beställningar till andra kommuner vid vistelser. Även sjukhus kan faxa inskrivningsmeddelanden.

Att kommunicera via fax beskrivs vara en kvarleva från förr, men att rutinen kring faxhanteringen är så säker den kan vara. Vi noterar dock att faxen står i postrummet och att det faxade papperet skrivs ut utan ytterligare särskilda säkerhetsrutiner. Kommunikation via fax av känsliga personuppgifter är särskilt riskfyllt. Det kan exempelvis resultera i en felaktig hantering i samband med faxöverföringen, till exempel att faxet går till fel nummer, vilket kan innebära att obehöriga får del av känsliga och sekretesskyddade personuppgifter såsom skyddade personuppgifter. Nuvarande rutin kan också resultera i att en obehörig handläggare av misstag blir mottagare av fax i postrummet. Enligt tf. socialchef kommer faxen, i samband med att säker e-post implementeras, skickas vidare till säkra funktionsbrevlådor som ett fåtal personer har tillgång till.

Den externa informationsöverföringen är förknippad med störst risker. Orsaken beskrivs bland annat vara att kommunen måste kommunicera med regionens systemstöd Prator vilket per automatik är riskfyllt vad gäller överföringen av känsliga personuppgifter. Vid kommunikation till andra statliga myndigheter hänvisar socialkontoret till Skatteverket i syfte att hantera känslig informationsöverföring i så begränsad utsträckning som möjligt. Vidare framställs telefonhantering av känsliga personuppgifter som ett stort riskmoment. Det avser framförallt situationer vid inkommande telefonsamtal från exempelvis medborgare. I jämförelse med verksamhetssystemen finns en ovana att hantera

personuppgifter via telefon. Det kan enligt intervjuade skapa osäkerhet och riskerna för att avvika från gängse rutiner ökar således. Det finns inga rutiner eller anvisningar för hur just inkommande telefonsamtal ska hanteras.

I situationer där exempelvis mor och barn har skyddade personuppgifter men inte fadern, som också är vårdnadshavare, beskrivs hanteringen vara särskilt känslig då det kräver en annorlunda hantering i Treserva. En handläggare måste då ha behörighet till samtliga personer för att kunna se vem som har skyddade personuppgifter och vem vårdnadshavaren är. Annars anger systemet bara "sekretess". I en situation där exempelvis barn ska skyddas från fadern måste handläggaren ha behörighet till även moderns personakt för att se att även hon har skyddade personuppgifter. Dock går det inte att se vem de är skyddade mot vilket kan leda till stor osäkerhet. Det finns enligt de intervjuade tydliga rutiner och anvisningar samt ett välfungerande systemstöd men det poängteras också att den typen av hantering kräver större försiktighet och noggrannhet i att kontrollera samtliga uppgifter, varefter risken för felhantering orsakad av den mänskliga faktorn ökar.

Personuppgiftsavvikelser hanteras på flera sätt. Avvikelser kan rapporteras i verksamhetssystemet Treserva, kommunens informationssystem om arbetsmiljö KIA, i det kommunövergripande ärende- och dokumenthanteringssystemet Lex samt genom Lex Sarah-anmälningar. I KIA kan dock inte personuppgiftsincidenter rapporteras specifikt. Vid eventuella avvikelser kan en brukare vända sig till personalen, ansvarig chef eller direkt till socialnämnden. Personal vänder sig till närmsta chef. Det går också att anmäla personuppgiftsärenden till Integritetsskyddsmyndighet (IMY).

I nuvarande systemstöd klassas skyddade personuppgifter inte som en avvikelse. Det finns däremot möjlighet att ställa in systemet så att det ska gå att särskilja avvikelser med skyddade personuppgifter. Det går att få en samlad bild över avvikelser som rör hanteringen av skyddade personuppgifter men det kräver en manuell sökning i systemet och att verksamhetschef begär ut den efterfrågade statistiken. Intervjuad systemförvaltare av Treserva uppger att det inte har skett. Det är också möjligt att rapportera risk för avvikelser.

Socialt ansvarig samordnare (SAS) på socialkontoret beskriver att det enligt hennes kännedom inte finns några rapporterade avvikelser vad gäller hanteringen av skyddade personuppgifter. Vid intervjuerna uttrycks dock att det inte med säkerhet går att konstatera att inga avvikelser kopplat till skyddade personuppgifter har ägt rum bara för att inga avvikelser rapporterats. Det kan således inte likställas med att avvikelser inte inträffat, enbart att inga uppmärksammats.

Vad gäller medarbetare med skyddade personuppgifter finns en upplevd otrygghet i hanteringen av anställd med skyddade personuppgifter då det saknas riktlinjer, rutiner eller anvisningar. Det finns en större osäkerhet kring hanteringen av eventuella medarbetare med skyddade personuppgifter än hanteringen av brukare med skyddade personuppgifter.

5.3. Barn- och utbildningsnämnden hanterar många elever med skyddade personuppgifter

Av cirka 3 000 barn- och elever i kommunen finns cirka 30 med skyddade personuppgifter. De rutiner och specifika anvisningar kring hanteringen av skyddade personuppgifter som utbildningskontoret har antagit bygger emellertid inte på någon genomförd risk- och sårbarhetsanalys. Likt socialkontoret har någon sådan inte genomförts vad gäller skyddade personuppgifter. Intervjuad utbildningschef beskriver att kontoret har konstaterat att någon riskanalys inte finns och därför gått direkt på handling och skapat rutiner utifrån olika

scenarios. Vid risk- och sårbarhetsanalys skulle frågan fått hög prioritet.

Utbildningschef beskriver att utbildningskontorets medarbetare är välinformerade, insatta och uppdaterade i kontorets riktlinjer, rutiner och anvisningar. Rutinerna har reviderats och anpassats utifrån skoladministratörernas hantering av barn och unga med skyddade personuppgifter, de beskrivs därför huvudsakligen vara ändamålsenliga. Samtidigt påtalar en intervjuad handläggare att det inte sker tillräckliga utbildningsinsatser till nyanställda vad gäller informationssäkerhet i allmänhet och hanteringen av skyddade personuppgifter i synnerhet i tillräcklig utsträckning. Det beskrivs ha fallit mellan stolarna på grund av Coronapandemin. Intervjuad efterfrågar obligatorisk utbildningstillfällen en gång per halvår.

På varje skola finns en eller flera skoladministratörer med ansvar för hanteringen av barn och unga med skyddade personuppgifter. Kännedomen om att elev har skyddade personuppgifter kommer antingen via Skatteverket i systemstödet eller via ansökan från vårdnadshavare. Eleven får då en fiktiv identitet med ett alias i verksamhetsstödet. De fysiska ansökningsblanketterna, som omfattas av sekretess eller skyddade personuppgifter, förvaras i låsta arkivskåp som gallras tre år efter avslutad placering enligt upprättad dokumenthanteringsplan. Alla inkomna handlingar som myndigheten förvarar kan begäras ut. Om så sker görs en sekretessprövning.

När elev med skyddade personuppgifter börjat på en skola, alternativt redan går på skolan men får skyddade personuppgifter under studietiden, upprättas handlingsplan mellan föräldern/föräldrarna och ansvarig pedagog. I handlingsplanen anges barnets/elevens riktiga namn, efternamn och personnummer samt ett fingerat namn, efternamn och personnummer. I handlingsplanen anger vårdnadshavaren också vilket skydd barnet har och vilka specifika hot denne är utsatt för, hantering vid eventuell akut situation, information om vårdnadshavare och en rad exempel på hur skolan ska agera kring uppkomna situationer. Handlingsplanen skrivs under av vårdnadshavare och rektor och förvaras i låsta arkivskåp.

Ibland uppstår situationer då vårdnadshavare har önskemål om hantering av sitt barn som strider mot utbildningskontorets riktlinjer och rutiner. Ett exempel som återges är en vårdnadshavare som önskar att barnet med skyddade personuppgifter ska vara med på skolans klasslistor. I det konkreta exemplet kontaktades kommunjuristen för rådgivning och saken landade i lagstiftningen ger vårdnadshavaren rätt att själv bestämma. Situationen blir svårhanterlig i och med att intervjuad handläggare måste frångå kontorets antagna rutiner och riktlinjer och särbehandla en elev med skyddade personuppgifter vilket riskerar negativa följdeffekter.

Antalet personer med kännedom om att elev har skyddade personuppgifter ska begränsas till en så liten krets som möjligt. De som har kännedom är respektive rektor, pedagoger och skoladministratörer/handläggare. Intervjuad utbildningschef beskriver det vara utmaning att hålla det till en så liten krets som möjligt då personalomsättningen bland lärare är hög och det dessutom finns stor rörlighet av vikarier. Intervjuade skoladministratörer beskriver en potentiell brist i hanteringen där nuvarande rutiner inte omfattar hanteringen av timvikarier som ställer frågor om vilka elever som har skyddade personuppgifter.

Om barn eller elev med skyddade personuppgifter är frånvarande från skolan ska lärare/rektor informera administrativ personal omgående. En handläggare beskriver att rutinen är bristfällig då det kan dröja flera dagar innan de får kännedom om sådan frånvaro.

Skolchef beskriver en risk i att skolpersonal är i kontakt med många aktörer, framförallt föräldrar. Det finns situationer där föräldrar obetänksamt utrycker sig på ett sätt som innebär risk för att personuppgifter röjs. En handläggare påtalar att det ofta uppstår problematiska situationer när skolpersonal ska förhålla sig till föräldrar som har en annan uppfattning än vad riktlinjerna och rutinerna anger. Samtidigt poängteras att personalen är vana att hantera föräldrar rätt sätt men att det är en risk som inte ska underskattas.

Intern och extern kommunikation beskrivs, likt vad socialkontoret vittnar om, vara särskilt utmanande. Utbildningskontoret använder inte fax som kommunikationskanal. Post skickas med sekretessmarkerade kuvert som placeras i ett annat kuvert enligt rutinen för postgång. Vidare beskrivs det vara en brist att krypterad e-post inte finns. Ibland förekommer det att förälder skickar e-post med skyddade personnummer. Skoladministratörer hänvisar föräldrarna att ringa under vissa tider men det beskrivs allmänt svårt att komma i kontakt med föräldrar med skyddade personuppgifter då de ofta inte svarar i telefon, byter telefonnummer etcetera. Det förekommer att verksamheten skickar e-post rörande elev med skyddade personuppgifter, dock utan att avslöja namn eller personnummer. En handläggare beskriver det som problematiskt och att det strider mot rutinerna men tillämpas då telefon inte är möjligt.

Om en myndighet ringer, exempelvis Försäkringskassan eller Polisen, beskriver skoladministratörer att de ska ringa tillbaka via växeln för att försäkra sig om att inte lämna ut personuppgifter till obehöriga. Handläggare beskriver att det inte finns en sådan rutin nedtecknad och att hanteringen inte är välkänd bland samtliga medarbetare. Vidare beskrivs det som viktigt att vara extra medveten om att inte lämna ut personuppgifter vid eventuella telefonsamtal från privatpersoner, exempelvis anhöriga. Rutinerna kring intern och extern kommunikation beskrivs inte vara angivna i riktlinje eller rutin och inte vara kända bland samtlig personal. Telefonhantering beskrivs av samtliga intervjuade innebära större risker för felhantering orsakad av den mänskliga faktorn.

Vad gäller eventuella medarbetare med skyddade personuppgifter beskriver utbildningschef att det åligger respektive chef att säkerställa att personens identitet inte röjs. I rekryteringsärenden av person med skyddade personuppgifter sker dialog med personen ifråga och med HR. Då det exempelvis rör sig om lärare som ska arbeta med elever krävs även en riskbedömning utifrån eventuella hotbilder som kan överföras på arbetsplatsen. Skoladministratörer beskriver att de saknar vetskap om hur de skulle hantera en situation där en medarbetare har skyddade personuppgifter och skulle vid uppkommen situation vända sig till närmaste chef.

Enligt 2 kap. 25–26 §§ Skollagen ska elever ha tillgång till elevhälsa med medicinska, psykologiska, psykosociala och specialpedagogiska insatser. Inom elevhälsan finns skolsköterskor som kommer i kontakt och hanterar elever som har skyddade personuppgifter i journalsystemet. Samordnad verksamhetschef för elevhälsans medicinska insats (EMI) påtalar ett glapp i nuvarande rutiner. Omsättningen av elever med skyddade personuppgifter är ganska stor och det är därför viktigt att journalsystemet är uppdaterat. Skolsköterskorna får uppgift om att elev med skyddade personuppgifter börjar på en skola via rektor/skoladministratör på respektive skola men rutinerna skiljer sig mellan skolorna. I vissa skolor har det dröjt ett halvår innan centrala elevhälsan får vetskap om att eleven går på skolan.

Då eleven får ett fiktivt personnummer måste skolsköterskorna skapa en manuell journal till den skyddade eleven då det inte är möjligt att skriva en journal med ett fiktivt personnummer. Den manuella hanteringen beskrivs vara ytterligare ett riskmoment då det

ökar risken för felhantering orsakad av den mänskliga faktorn, och riskera att bli ogjort. Konsekvensen blir att den skyddade eleven inte får hälsobesök, inte kan vaccinera sig och inte kan söka sig vidare till annan vård via elevhälsan.

EMI har rapporterat ett par avvikelser utifrån brister i hanteringen av skyddade personuppgifter. En avvikelse avser att EMI inte fått vetskap om elev med skyddade personuppgifter, en avvikelse avser att brev inte skickats med rekommenderad post trots önskemål. Riktlinjerna har justerats utifrån rapporterade avvikelser.

5.4. Bedömning

Granskningen visar att det finns en rad risker inom respektive nämnds verksamhetsområden som visserligen omfattas av riktlinjer, rutiner och anvisningar men där det finns risker och situationer där det saknas rutiner. Vissa styrande dokument är utformade på ett otydligt sätt i situationer där personal efterfrågar konkreta regler och metodanvisningar.

Det finns risker av allmän karaktär som gäller hela kommunen, däribland extern och intern kommunikation med andra myndigheter och privatpersoner, avvikelsehanteringen, brister i informationsspridning av riktlinjer, rutiner och anvisningar till medarbetare och behov av tydliga rutiner för hanteringen av anställda med skyddade personuppgifter. Vidare finns kontorsspecifika risker som är unika för varje uppkommen situation.

Vi uppmärksammar kompetens och kunskapsspridning som ett särskilt utvecklingsområde. Inom respektive kontor säger intervjuade att medvetandegraden och kunskapsnivån kring hanteringen av skyddade personuppgifter bör stärkas genom exempelvis obligatoriska utbildningar samt informationsspridning. Detta är en uppfattning vi delar då den mänskliga faktorn medför stor risk för felhantering.

Det saknas i dagsläget en lärprocess uppbyggd av erfarenheter och riskbedömningar mellan respektive kontor. Det 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.

Den externa och interna kommunikationen ska särskilt lyftas fram som utvecklingsområden då de utgör stor risk för att skyddad personuppgift röjs. Det saknas tydliga rutinbeskrivningar kring hanteringen av exempelvis telefonkontakt med privatpersoner. Vidare beskrivs rutinerna för hanteringen av kontakt med myndigheter vara bristfälliga och inte tillräckligt välkända bland samtliga medarbetare. Möjligheten till användandet av krypterad e-post finns i dagsläget inte och socialnämndens verksamheter använder i viss utsträckning fax för kommunikation vilket är särskilt riskfyllt. Det går att ifrågasätta om det överhuvudtaget är lämpligt att använda fax för att överföra personuppgifter som omfattas av bestämmelser om sekretess och tystnadsplikt. Sammantaget vittnar intervjuade om en osäkerhet som riskerar att resultera i felhantering vid extern och intern kommunikation.

Då risken att röja skyddade personuppgifter inte risk- och konsekvensanalyserats går det inte att säga att kommunstyrelsen eller granskade nämnder genomför relevanta kontrollåtgärder. Det saknas dessutom penetrationstester av IT-hanteringen 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.

Slutligen brister kommunen enligt vår bedömning 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. Vi noterar att det inte har rapporterats några avvikelser vad gäller skyddade personuppgifter men att orsaken till detta är inte känd. Det är osäkert om det betyder att det inte finns avvikelser eller om rutinen att anmäla sådana ärenden inte förmedlats i tillräcklig utsträckning. 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.

6. Svar på revisionsfrågor

Fråga	Svar
Har kommunen analyserat risken för att skyddade personuppgifter röjs i kommunens verksamheter?	**Nej**. Risken att röja skyddade personuppgifter har inte bedömts och värderats utifrån risk- och konsekvensanalyser eller med stöd av avvikelsehanteringen. Kommunstyrelsen eller granskade nämnder genomför därför inte relevanta kontrollåtgärder. Granskad styrelse och nämnder följer inte upp och kontroller att rutinerna efterlevs i kommunen. Det saknas en funktion i organisationen med detta övergripande ansvar.
Har kommunen vidtagit åtgärder för att minska risken?	**Delvis**. Kommunstyrelsen har inte antagit kommunövergripande riktlinjer som beskriver hanteringen av skyddade personuppgifter, däribland hanteringen av medarbetare. Däremot uppmärksammar vi att socialkontoret och utbildningskontoret har antagit verksamhetsspecifika riktlinjer, rutiner och anvisningar på eget initiativ, exempelvis efter genomförd riskanalys i en specifik enhet, som beskriver hanteringen av skyddade personuppgifter. Vi bedömer att upprättade dokument i huvudsak är utförliga och behandlar ändamålsenliga beskrivningar av hanteringen av personer med skyddade personuppgifter som efterföljs i respektive verksamhet. Dessa riktlinjer är inte antagna av respektive nämnd. Vidare kan vi konstatera att det finns risker och andra situationer där det saknas rutiner. Vissa styrande dokument är utformade på ett otydligt sätt i situationer där personal efterfrågar konkreta regler och metodanvisningar.
Finns det ett avvikelsehanteringssystem som omfattar dessa avvikelser?	**Nej**. Vi noterar att det inte har rapporterats några avvikelser vad gäller skyddade personuppgifter (vid sidan av de två som EMI har rapporterat) men att orsaken till detta inte är känd. Det är osäkert om det betyder att det inte finns avvikelser vid hantering av skyddade personuppgifter eller om informationen om möjligheten att anmäla sådana ärenden via kommunens avvikelsehanteringssystem inte förmedlas i tillräcklig utsträckning. Vidare går det inte att kategorisera eventuella avvikelser som avser skyddade personuppgifter utan manuell hantering. Vi bedömer vidare att eventuella avvikelser inte systematiseras och aggregeras för att åtgärda brister kopplat till hanteringen av skyddade personuppgifter i tillräcklig utsträckning.

Finns det kommunövergripande anvisningar och rutiner för hantering av personer med skyddade personuppgifter? Hur görs de kända för medarbetare?	**Nej**. Dokumentgranskningen visar att det saknas en kommunövergripande riktlinje som beskriver hanteringen av skyddade personuppgifter, däribland hanteringen av medarbetare med skyddade personuppgifter. Vi kan konstatera att det strider mot kommunstyrelsens reglemente. Kompetens och kunskapsspridning är ett särskilt utvecklingsområde. De intervjuade vittnar om att medvetandegraden och kunskapsnivån kring hanteringen av skyddade personuppgifter bör stärkas genom exempelvis obligatoriska utbildningar och informationsspridning. Det saknas en lärprocess uppbyggd av erfarenheter och riskbedömningar inom och mellan respektive verksamhetsområde.

Strängnäs den 15 juni 2022

Jan Darrell
Certifierad kommunal yrkesrevisor EY

David Leinsköld
Verksamhetsrevisor EY

Bilaga 1: Källförteckning

Intervjuade funktioner

- Kanslichef
- Nämndsekreterare/dataskyddssamordnare
- Kommunjurist/Dataskyddsombud kansliavdelningen
- Säkerhetschef
- HR-chef
- Lönechef
- Utbildningschef
- Tf. Socialchef
- Näringslivschef/Chef kontaktcenter
- Gruppledare kontaktcenter
- Handläggare/Administratör barnomsorg förskola
- Handläggare/Administratör barnomsorg förskola
- Handläggare fakturering/elevregistrering
- Handläggare grundskola
- Samordnad verksamhetschef elevhälsans medicinska insats (EMI)
- Verksamhetsutvecklare/socialt ansvarig samordnare socialkontoret
- Nämndsekreterare/GDPR-ansvarig socialkontoret
- Systemförvaltare socialkontoret

Granskad dokumentation

- Informationssäkerhetspolicy (KS/2021:90-003)
- GDPR Handbok (Dnr saknas)
- Rutin för begäran om registerutdrag (KS/2021:136-094)
- Rutin för personuppgiftsincidenter (KS/2019:492-003)
- Riktlinje för hälso- och sjukvårdsdokumentation (SN/2020:101-700)
- Rutin för hantering av personer med skyddade personuppgifter (Dnr saknas)
- Anvisning för hantering av personer med skyddade personuppgifter hälso- och sjukvård (Dnr saknas)
- Anvisning för hantering av personer med skyddade personuppgifter inom vård- och omsorg (Dnr saknas)
- Anvisning för beställning, justering samt avslut av behörighet till sekretesskyddade personer i verksamhetssystemet Treserva, Socialkontoret (Dnr saknas)
- Riktlinjer för hantering av barn, elever och studerande med skyddade personuppgifter (BUN/2018:485-003)
- Rutin för barn, elever och studerande med skyddade personuppgifter (Dnr saknas)
- Information och rutin kring elever med skyddade personuppgifter, Centrala barn och elevhälsan – Elevhälsans medicinska insats (Dnr saknas)