# Södertälje kommun

## Granskning av hanteringen av skyddade personuppgifter

Building a better working world

# Innehållsförteckning

# Sammanfattande bedömning och rekommendationer

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

Det finns ändamålsenliga styrande dokument och utformade rutiner för hanteringen av skyddade personuppgifter. Ansvarsfördelningen tydliggörs också i styrande dokument och det finns funktioner och avdelningar som fungerar stöttande och rådgivande vid hantering av skyddade personuppgifter.

Under granskningen har det emellertid inte noterats något systematiskt arbete för att implementera styrande dokument för hanteringen av skyddade personuppgifter inom den kommunala verksamheten och granskade bolag. Det sker ingen strukturerad eller dokumenterad uppföljning av hanteringen av skyddade personuppgifter.

Kunskapen om hanteringen av skyddade personuppgifter varierar mellan kontor, bolag och ansvarsnivå. Tjänstepersoner som arbetar verksamhetsnära kommer i kontakt med den praktiska hanteringen av skyddade personuppgifter genom elever och klienter. Det finns inga funktioner som har ett specifikt ansvar för arbetet med skyddade personuppgifter i likhet med Skatteverkets rekommendation att "Varje myndighet bör utse en person med ansvar för att rutiner och regler för hantering av skyddade personuppgifter efterföljs" vilket lyfts fram som en rekommendation.

Det har inte genomförts tillräcklig kompetensutveckling kring skyddade personuppgifter. Inom respektive kontor och bolag finns behov av ökad medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter. Det saknas en lärprocess uppbyggd av erfarenheter och riskbedömningar inom och mellan respektive kontor och bolag.

Det finns inte några kontors- eller bolagsspecifika riskanalyser kring hanteringen av skyddade personuppgifter. I flertalet riskanalyser och internkontrollplaner berörs hanteringen av personuppgifter, dock inte specifikt skyddade personuppgifter, inom ramen för informationssäkerhetsarbetet. Granskningen ser positivt på arbetet med informationssäkerhet men saknar en separat hantering av skyddade personuppgifter. Bedömningen är att varken kommunen eller bolagen analyserat risken för röjning av skyddade personuppgifter.

Det finns inte ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns inget automatiskt sätt att samla personuppgiftsincidenter på koncernövergripande nivå utan manuell handläggning. Verksamheterna kan inte koda incidenten som ett skyddat personuppgiftsärende. Det sker ingen systematisk uppföljning och analys över verksamhetens egna personuppgiftsincidenter som ligger till grund för verksamhetsutveckling.

**Utifrån granskningens iakttagelser rekommenderas kommunstyrelsen och Telge AB att:**

- Ta fram en övergripande riskanalys för röjning av skyddade personuppgifter, det skulle gynna den interna kontrollen och medvetenheten hos medarbetarna då allvarlighetsgraden vid röjning av skyddade personuppgifter är hög.

- Säkerställa enhetlig hantering av personuppgiftsincidenter genom att öka medarbetares kännedom om riktlinjer och rutiner.

**Utifrån granskningens iakttagelser rekommenderas granskade nämnder och bolag att:**

- Genomföra risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter och vid behov låt inkludera i internkontrollplanerna.
- Genomföra obligatoriska utbildningar för personal avseende hanteringen av skyddade personuppgifter.
- Överväga inrättandet av "compliancefunktion/-er", det vill säga en funktion som ansvarar för att bestämmelser och interna verksamhetsprinciper, som exempelvis riktlinjer, rutiner och anvisningar, följs och följs upp.
- Säkerställa en ändamålsenlig nivå av uppföljning samt att avvikelsehanteringen avseende skyddade personuppgifter stärks.

# 1. Inledning

## 1.1. Bakgrund

Den som är utsatt för hot kan i vissa fall få skyddade personuppgifter. Från 2011 till 2021 har personer i Sverige med skyddade personuppgifter fördubblats från drygt 12 000 personer till knappt 24 000 personer. Den 1 januari 2019 skärptes lagstiftningen i syfte att öka skyddet för hotade och förföljda personer.

Personer med skyddade uppgifter riskerar allvarliga problem om kommunens nämnder/kontor och bolag röjer skyddade uppgifter. Kommun och bolag bör därför ha säkra rutiner och riktlinjer för att säkerställa korrekt hantering av dessa uppgifter. Det är väsentligt att arbetssätt och metoder är välkända hos samtliga medarbetare då i princip samtliga kan komma i kontakt med skyddade personuppgifter via kundkontakter eller som kollega.

Revisionen har beslutat genomföra en fördjupad granskning av kommunens och några av dess bolags arbete med rutiner, kunskapsspridning och säkerhetsfrågor vad gäller hanteringen av skyddade personuppgifter.

## 1.2. Syfte och revisionsfrågor

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

I granskningen besvaras följande revisionsfrågor:

- Har kommunen/bolagen analyserat risken för att skyddade personuppgifter röjs?
- Har kommunen/bolagen vidtagit åtgärder för att minska risken för röjning av skyddade personuppgifter?
- Finns styrande dokument och rutiner för hantering av skyddade personuppgifter?
- Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?
- Finns ett tillräckligt stöd för medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter?
- Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?
- Har kommunen/bolagen tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?
- Finns avvikelsehanteringssystem som omfattar skyddade personuppgifter?
- Hur tillvaratas erfarenhet från avvikelser?
- Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits?
- Råder det samsyn inom Södertälje kommun och dess bolag kring hur skyddade personuppgifter ska hanteras?

## 1.3. Ansvariga nämnder

Granskningen avser kommunstyrelsen, socialnämnden samt utbildningsnämnden. Av de kommunala bolagen granskas Telge AB, Telge Bostäder AB och Telge Energi AB.

## 1.4. Metod och genomförande

Granskningen baseras på genomgång och granskning av styrande dokument och annan dokumentation samt intervjuer med företrädare för kommunens säkerhetsavdelning, IT-avdelning, HR-enhet samt med chefer inom utbildningskontor, socialkontor samt verkställande direktörer. En enkät har skickats ut till samtlig personal inom granskade nämnder och bolag i syfte att undersöka tillämpning av rutinbeskrivningar och styrdokument.

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

## 1.5. Revisionskriterier

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

- Kommunallagen
- Offentlighets- och sekretesslagen
- Folkbokföringslagen
- Folkbokföringsförordning
- SFS 2018:684 Lag om ändring i folkbokföringslagen
- Socialtjänstlagen
- Skollagen
- Av fullmäktige antagna styrdokument eller relevanta riktlinjer
- Ägardirektiv

Dessa beskrivs närmare i kapitel 2 och 4.

# 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 i Sverige dubblerats från drygt 12 000 till knappt 24 000 personer. Enligt Skatteverket utgörs dessa till 59 procent av kvinnor.

Vanligast förekommande är sekretessmarkering, som är den minst ingripande formen av skydd, med 82 procent av ärendena medan skyddad folkbokföring, som är ett starkare skydd, utgör 18 procent.

Antalet personer med skyddade personuppgifter motsvarar ca 0,22 procent av befolkningen och matematiskt motsvarar det ca 220 invånare och ett tiotal anställda. Siffrorna är inte exakta men visar att det statistiskt handlar om ett fåtal individer. Konsekvensen vid felaktig röjning av dessa personuppgifter kan emellertid vara mycket allvarlig för var och en.

Jämställdhetsmyndigheten har på regeringsuppdrag genomfört kunskapshöjande insatser gällande våldsutsatta personer som lever med skyddade personuppgifter med fokus på kvinnor och barn. I en delrapport[1] intervjuas 86 kvinnor och 15 barn om deras erfarenheter. Närmare tre fjärdedelar av de intervjuade uppger att deras identitet har röjts.

I rapporten konstateras att det i många fall handlar om kvinnor och barn som tvingats flytta på grund av våld och hot från närstående man och att målgruppen är extra utsatt. I princip samtliga kvinnor i Jämställdhetsmyndighetens intervjustudie har fått skyddade personuppgifter röjda av myndigheter.

## 2.3. Det finns omfattande lagstiftning som skyddar individen

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

### 2.3.1 Sekretessmarkering är den vanligaste och minst ingripande formen av skydd

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

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

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

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

Sekretessmarkeringen gäller ofta i två år och kan förlängas.

### 2.3.2 Skyddad folkbokföring ger starkare skydd än sekretessmarkering

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

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

### 2.3.3 Fingerade personuppgifter är den starkaste och mest ingripande formen av skydd

Fingerade uppgifter betyder att personen använder andra personuppgifter än de verkliga. Detta medför dock inte någon rättslig förändring av personens namn eller andra förhållanden. Kopplingen mellan den verkliga och den fingerade identiteten är sekretessbelagd. Med den nya identiteten kan personen vara öppen med sina personuppgifter utan risk att bli hittad.

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

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

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

## 2.4. Offentlighets- och sekretesslagen reglerar utlämning av allmänna handlingar

Offentlighets- och sekretesslagen (OSL) innehåller bestämmelser för hur myndigheter ska registrera, lämna ut och hantera allmänna handlingar.

Det finns också regler om tystnadsplikt och förbud att lämna ut allmänna handlingar.

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

Sekretessen gäller uppgift om en enskilds

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

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

# 3. Redovisning av enkät

Som en del av granskningen har det genomförts en enkätundersökning, se bilaga 2 för sammanställning. I avsnittet nedan inkluderas inte alla frågor som ställdes i enkäten utan endast ett representativt urval. Enkäten skickades ut via mejl till samtliga medarbetare inom de kontor och bolag som granskats. Av de 4 459 mottagarna svarade 645 personer vilket är en svarsfrekvens på 14,5 procent. Granskningen har inte gjort någon bortfallsanalys. Trots den procentuellt låga andelen svar är det över sexhundra som svarat vilket gör att granskningen väljer att analysera svaren, se "3.2. Sammanfattande analys".

Tabellen nedan redovisar antalet utskick, svar och svarsfrekvens, fördelat mellan kontor och bolag samt den spridningen av respondenter i förhållande till antalet svar, ej i förhållande till kontorets/bolagets storlek.

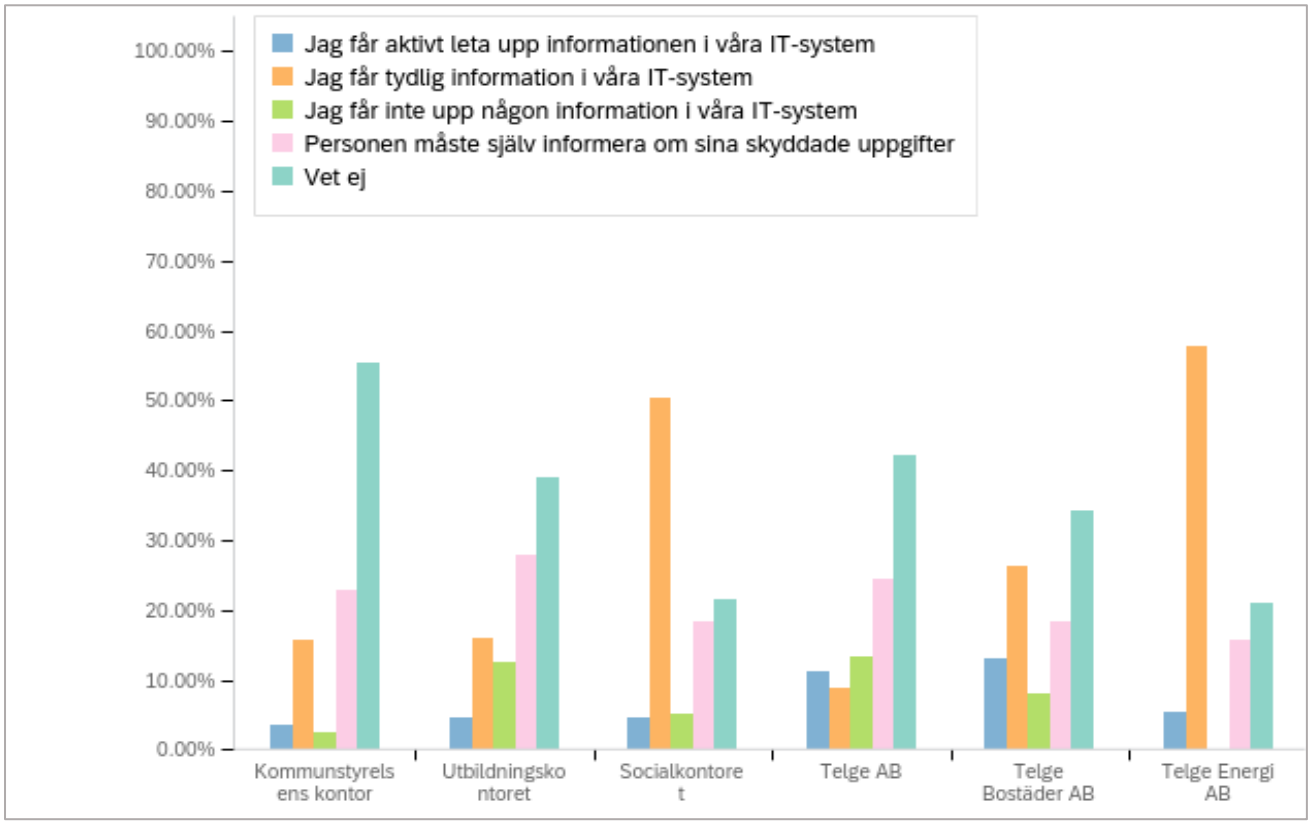
| Kontor/bolag | Antal utskick | Antal svar | Svarsfrekvens per kontor/bolag | Spridning av respondenter mellan kontor/bolag |
|---|---|---|---|---|
| **Kommunstyrelsens kontor** | 207 | 73 | 35,2% | 11,32 % |
| **Utbildningskontoret** | 3178 | 311 | 9,7 % | 48,22 % |
| **Socialkontoret** | 732 | 173 | 23,6 % | 26,82 % |
| **Telge AB** | 94 | 37 | 39,3 % | 5,74 % |
| **Telge Bostäder AB** | 162 | 34 | 20,9 % | 5,27 % |
| **Telge Energi** | 86 | 17 | 19,7 % | 2,64 % |

Utbildningskontoret står för nästan hälften av antalet svar, följt av socialkontoret och kommunstyrelsens kontor. Svarsfrekvensen för utbildningskontoret i förhållande till antalet medarbetare är dock låg, endast 9,7 procent. Slutsatserna som går att dra från enkäten är därför mest representativa för Telge AB och kommunstyrelsens kontor och minst representativa för utbildningskontoret.

## 3.1. Kunskapen om hanteringen av skyddade personuppgifter varierar

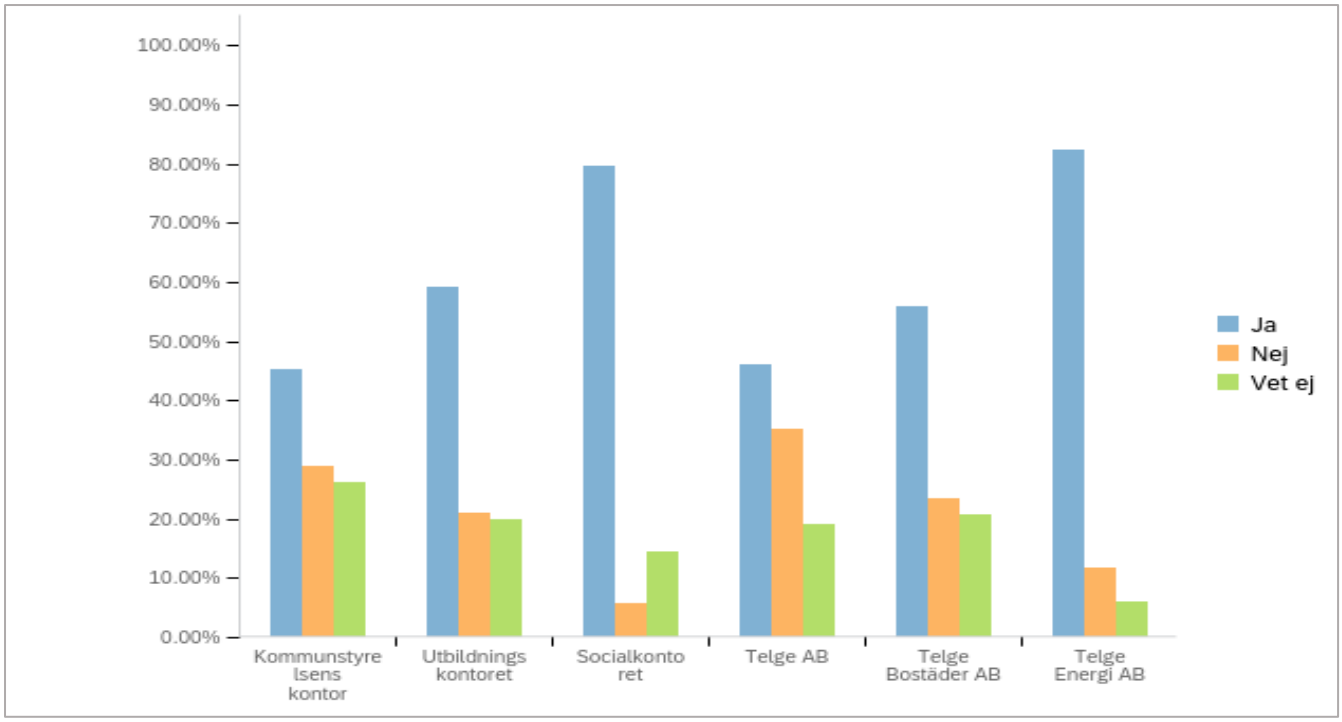
När medarbetarna i kommunen får svara på frågan om hur ofta de kommer i kontakt med personer med skyddade personuppgifter varierar svaren. Frågan hade fem svarsalternativ som sträckte sig från "aldrig" till "ofta". Majoriteten av enkätrespondenterna svarade att de väldigt sällan kommer i kontakt med skyddade personuppgifter. Det är enbart respondenter från utbildningskontoret och socialkontoret som svarar att de ofta kommer i kontakt med skyddade personuppgifter.

Enkätresultatet tydliggör att 36 procent av de medarbetare som svarat på enkäten inte vet hur de får information om förekomsten av skyddade personuppgifter, 26 procent får information om förekomsten av skyddade personuppgifter i IT-systemen och 24 procent anger att personen själv måste informera om sina skyddade personuppgifter. Graf 1 visar detta fördelat per kontor/bolag. Kommunstyrelsen och Telge AB har störst andel svarande som inte vet hur de får information om förekomsten av skyddade personuppgifter. Socialkontoret och Telge Energi AB är de verksamheter där störst andel medarbetare svarade att det tydligt framgår i deras IT-system om en person har skyddade personuppgifter.



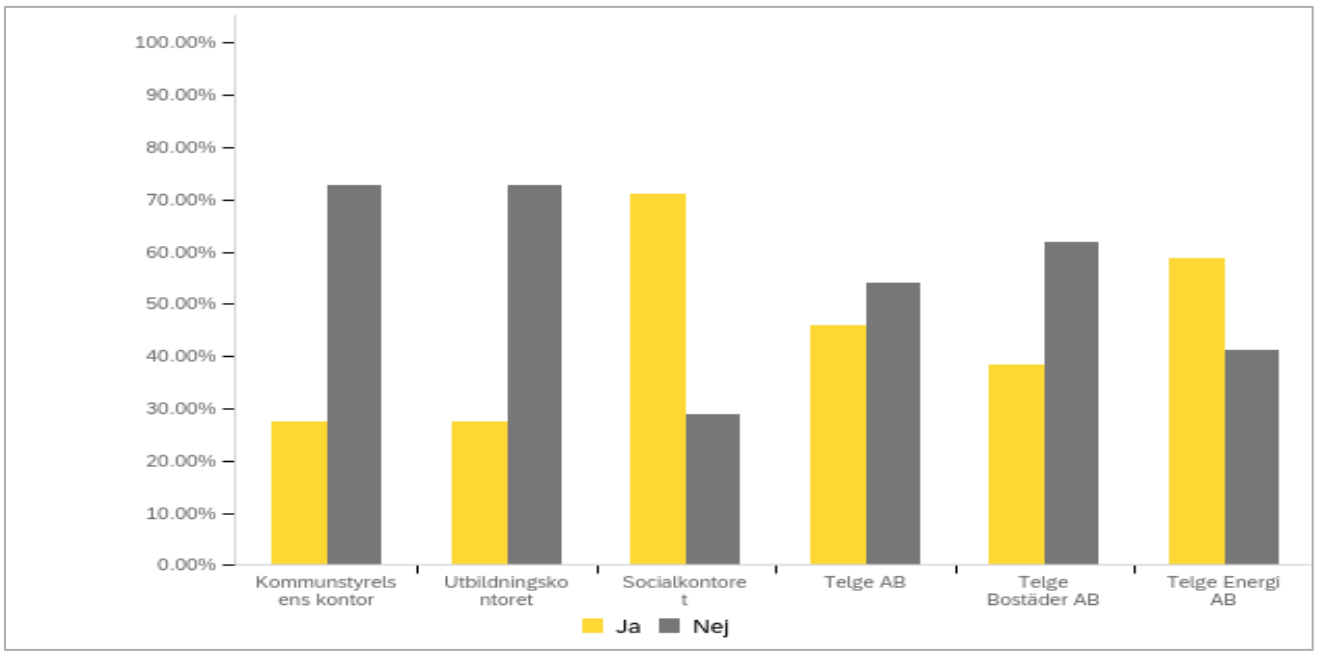

*Graf 1: Hur blir du informerad om att en person du kommer i kontakt med har skyddade personuppgifter? (Här kan du välja en eller flera svarsalternativ)*

Av respondenterna svarade 62,8 procent att de har tillräcklig kännedom om hur de skulle agera om de kom i kontakt med skyddade personuppgifter i sitt arbete. 18 procent svarade att de inte hade tillräcklig kännedom om hur man ska agera och 18 procent angav att de inte visste. Graf 2 redogör för kunskapen gällande hantering av skyddade personuppgifter fördelat per kontor och bolag. Det framgår att medarbetare inom socialkontoret har mest kunskap om hanteringen av skyddade personuppgifter.




*Graf 2: Har du tillräcklig kännedom om hur du ska agera när du kommer i kontakt med en person med skyddade personuppgifter i ditt arbete?*

En stor del av respondenterna är osäkra på om rutiner finns gällande hanteringen av skyddade personuppgifter samt om medarbetaren får tillräckligt stöd av dessa. Detta gäller även för medarbetare som innehar skyddade personuppgifter. Av alla respondenter svarade 58 procent att de inte visste var rutiner för hantering av skyddade personuppgifter kunde hittas. Graf 3 visar hur medarbetare inom respektive kontor/bolag svarade.

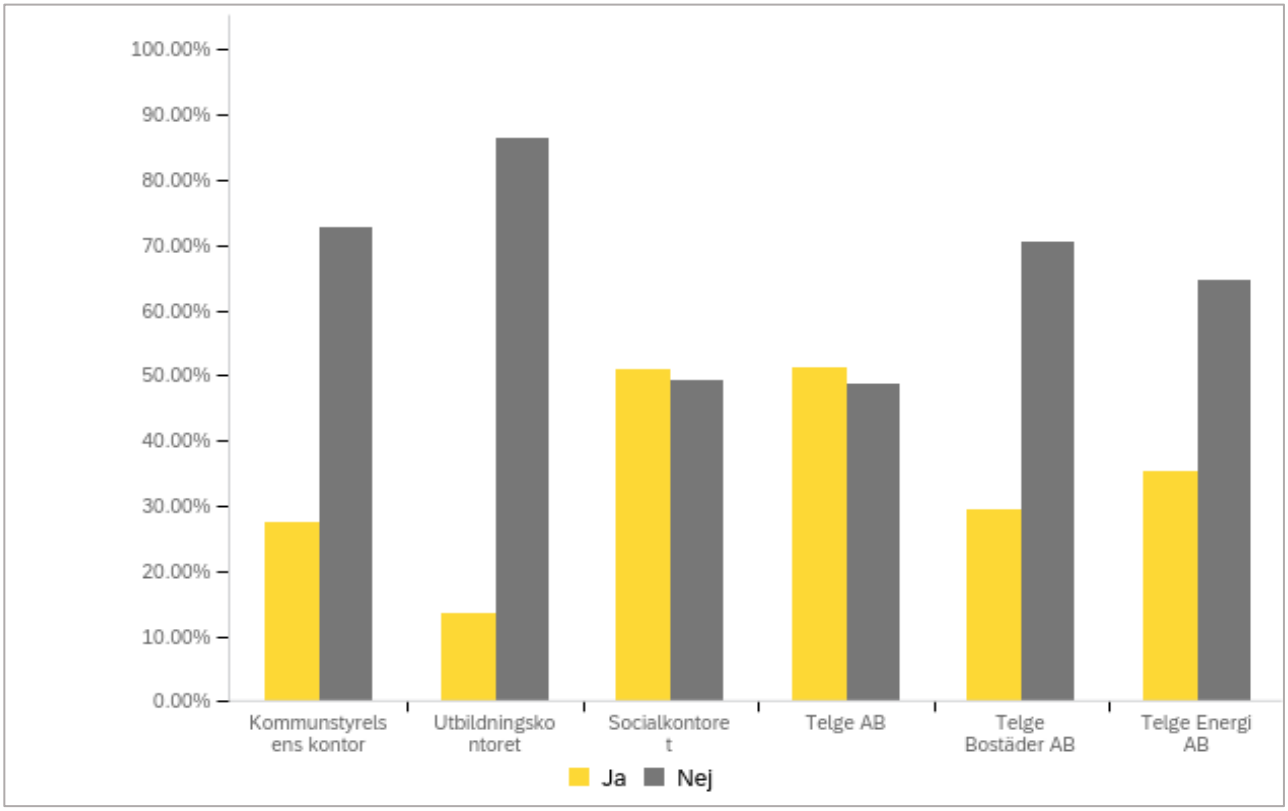



*Graf 3: Vet du var du hittar dessa skriftliga rutiner?*

Enkätundersökningen visar att 58 procent av respondenterna vet vem som ansvarar för hanteringen av skyddade personuppgifter samt vem medarbetaren vänder sig till vid frågor angående hanteringen. Den person som medarbetarna till största del vänder sig till vid frågor angående hantering av skyddade personuppgifter är sin närmaste chef (62,6 %). I enkäten gavs även möjligheten för respondenterna att skriva in ett alternativt svar på frågan. I svaren framkom det bland annat att HR, DSO (Dataskyddsombud) samt administratör är några funktioner som medarbetarna vänder sig till. Endast 4 procent uppger sig inte veta vem de skulle vända sig till vid frågor om hanteringen av skyddade personuppgifter.

Resultatet från enkäten påvisar att en stor del av respondenterna är osäkra på om skyddade personuppgifter framgår tydligt och/eller särmarkeras i IT-systemen. Gällande rapportering av röjning/avvikelse av skyddade personuppgifter svarar 71,3 procent att de inte vet var det ska registreras och 70,1 procent vet inte huruvida det finns rutiner för uppföljning av eventuella röjningar/avvikelser av hanteringen av skyddade personuppgifter.

***Graf 4: Vet du var du ska registrera eventuell röjning/avvikelse av hanteringen av skyddade personuppgifter?***




Enkätresultatet analyseras och återkopplas till i bedömningsavsnitten för att besvara revisionsfrågorna.

## 3.2. Sammanfattande analys

Enkätens svarsfrekvens var 14,5 procent vilket gör det svårt att dra generella slutsatser om kommunen som helhet. Enkäten skickades ut viss tid efter kommunens egen medarbetarenkät, vilket kan påverkat svarsfrekvensen. Dessutom genomförde de förtroendevalda revisorerna i oktober ett test avseende nätfiske där ett mejl som såg ut att komma från ekonomiavdelningen gick ut till över 900 anställda varav 263 klickade på en osäker länk. Erfarenheterna av detta kan också ha bidragit till lägre svarsfrekvens.

Fördelningen av svarsfrekvensen varierar mellan kontoren/bolagen där utbildningskontoret har lägst svarsfrekvens och Telge AB har högst. Detta medför att det kan dras säkrare slutsatser för kontor/bolag som Telge AB än för utbildningskontoret. Enkäten ger djupare inblick i verksamheterna och styrker de slutsatser som framkommit i granskningen.

Kunskapen gällande hanteringen av skyddade personuppgifter varierar mellan kontoren där enkätresultaten tyder på att medarbetare inom socialkontoret har mest kunskap. Denna kunskap kan bero på att socialkontoret redan arbetar med sekretessbelagda uppgifter och att medarbetarna har större erfarenhet gällande skyddade personuppgifter. Det kontrasteras med utbildningskontoret där det i enkätsvaren förekommer låg kännedom om hanteringen av skyddade personuppgifter, i synnerhet gällande rutiner och avvikelsehantering. Bland bolagen varierar kunskapsnivån där medarbetare inom Telge Energi AB anges ha mest kännedom avseende agerande vid kontakt med skyddade personuppgifter samt skriftliga rutiner. För avvikelsehanteringen verkar Telge AB vara det bolag med högst kunskap. Anledningen till att Telge AB har högst kunskap inom avvikelsehantering kan bero på att rutinen är centraliserad hos moderbolaget, läs mer i avsnitt 6.

Det finns övergripande indikationer på att kunskapen hos medarbetarna i kommunen och bolagen avseende hanteringen av skyddade personuppgifter är låg. Det svarsalternativ som förekom mest frekvent är "vet ej", i synnerhet gällande IT-system och avvikelsehanteringen. Det kan förklaras av att det finns brister inom medarbetarnas utbildning för hanteringen, att inte alla har tillgång till den typen av IT-system eller att skyddade personuppgifter inte förekommer så ofta. Trots att skyddade personuppgifter inte är en vanlig förekommande företeelse kan brist i hanteringen orsaka livsfarlig skada. Den befintliga okunskapen är bekymmersam och åtgärder för att stärka hanteringen bör genomföras.

# 4. Styrning, organisation och uppföljning på koncernövergripande nivå

## 4.1. Det finns en kommunövergripande rutin för hanteringen av skyddade personuppgifter

Koncernens övergripande policys, riktlinjer och rutiner med indirekt och direkt koppling till hanteringen av skyddade personuppgifter sammanfattas i tabellen nedan:

| Riktlinje/rutin/anvisning | Kort beskrivning |
|---|---|
| *Digitaliseringsstrategi för Södertälje kommun*<br><br>*Kommunfullmäktige (19-06-2019)* | Strategi för hur kommunen ska digitaliseras. Information som kommunen producerar, tar emot samt hanterar behöver kartläggas, informationsklassas och hållas ordnad. Kommunens digitala tjänster ska ha höga krav på informationssäkerhet.<br><br>Inget specifikt om hanteringen av skyddade personuppgifter. |
| *e-Södertälje – vision och strategi för IT (revidering pågår)*<br><br>*(13-04-2004)* | Beskriver vad kommunen kan uppnå med IT samt hur kommunen ska nå visionen. I samma dokument redovisas IT-organisation samt IT-säkerhetspolicy.<br><br>Inget specifikt om hanteringen av skyddade personuppgifter. |

| | |
|---|---|
| *Informationssäkerhetspolicy*<br><br>*(Odaterad)* | Beskriver kommunens arbete med informationssäkerhet. All information ska värderas och klassificeras efter känslighet och vikt. Administrativa och tekniska skyddsåtgärder ska säkerställa att informationen är tillgänglig vid behov, att den är korrekt samt att obehöriga inte kan få tillgång till den.<br><br>Inget specifikt om hanteringen av skyddade personuppgifter. |
| *Riktlinje för hantering av personuppgifter (KS 22/71)*<br><br>*Kommunstyrelsen (15-02-2022)* | Beskriver Södertälje kommuns och dess bolags hantering av personuppgifter på övergripande nivå. Södertäljes kommuns mål är att all behandling sker med hänsyn till den enskildes frihet och rättigheter.<br><br>Inget specifikt om hanteringen av skyddade personuppgifter. |
| *Rutin för skyddade personuppgifter (KS 20/311)*<br><br>*Stadsdirektör (30-11-2021)* | Rutinen beskriver vad skyddade personuppgifter innebär och hur kommunen ska hantera dessa på ett säkert och enhetligt sätt. Rutinerna beskriver hur dokumentation och IT-stöd ska införlivas, hur kommunikation ska ske samt hur medarbetare med skyddade personuppgifter ska hanteras. |
| *Hantering av skyddade personuppgifter hos medarbetare*<br><br>*(Odaterad)* | En övergripande rutin som syftar till att säkerställa en enhetlig och säker hantering av skyddade personuppgifter hos medarbetare. Kopplat till rutinen finns även en checklista för hanteringen av skyddade personuppgifter hos medarbetare. |

Som tydliggörs av tabellen finns det en kommungemensam rutin för hanteringen av skyddade personuppgifter, utöver det regleras inte hanteringen av skyddade personuppgifter i styrdokumenten. Rutinen är fastställd av stadsdirektör och utformad av informationssäkerhetsansvarig, rutinen finns tillgänglig på intranätet. Vid intervjuer framgår att rutinen togs fram då det fanns en efterfråga inom förvaltningen av stöd vid hanteringen av skyddade personuppgifter. Det har inom granskningen inte noterats något arbete för att implementera eller uppmärksamma styrdokument specifikt för hanteringen av skyddade personuppgifter.

## 4.2. Personuppgiftsansvaret är delat mellan styrelse och nämnder

I *Riktlinje för hantering av personuppgifter* beskrivs organiseringen av arbetet med personuppgifter, policyn gäller för nämnder, kontor, verksamheter, medarbetare och i tillämpbara fall även för organisationer där Södertälje kommun har det rättsligt bestämmande inflytandet, exempelvis bolag. Kommunstyrelsen beslutar om den övergripande inriktningen för personuppgiftsarbetet och varje styrelse och nämnd är *personuppgiftsansvariga* för sina egna personuppgiftsbehandlingar[2].

Styrelser och nämnder är därav ytterst ansvariga för att bland annat:

- Följa gällande lagstiftning
- Säkerställa att det finns ett Dataskyddsombud
- Ansvara för att noggrann dokumentation av behandlingar finns
- Riskanalyser finns och är dokumenterade
- Säkerställa att det görs konsekvensbedömningar om behandlingar sannolikt medför en hög risk för den registrerades integritet
- Säkerställa att personuppgiftsincidenter rapporteras till tillsynsmyndigheten

[2] Med behandling av personuppgifter menas i princip allting som går att göra med personuppgifterna. Det kan till exempel vara att samla in, registrera, lagra, samköra eller skriva ut uppgifterna.

I *Riktlinje för hantering av personuppgifter* framgår även att samtliga personuppgiftsansvariga ska utse en kontaktperson som representerar dem som kallas för *dataskyddssamordnare (DSS)*. Kontorscheferna och bolagens VD:s utser sina respektive DSS. Det finns även en Dataskyddskoordinator (DSK) som ska stötta, samordna samt följa upp dataskyddsarbetet och DSS på övergripande nivå.

I *Rutin för skyddade personuppgifter* tydliggörs att respektive kontorschef och VD ansvarar för att fastställa lokala rutiner för hanteringen av skyddade personuppgifter utifrån den koncernövergripande rutinen, vid behov. Den koncernövergripande rutinen omfattar både den kommunala verksamheten samt bolagen.

*Dataskyddsombudet* (DSO) är en oberoende funktion som ska anmälas till Integritetsskyddsmyndigheten. I Södertälje kommun har dataskyddsombudet uppgiften att informera och stötta personuppgiftsansvarig, övervaka efterlevnad av personuppgiftbehandlingar samt ge råd och assistens vid riskanalyser/ konsekvensbedömningar. Dataskyddsombudet ska även vara kontakt för registrerade, den vars personuppgifter behandlas, samt tillsynsmyndigheten och vid behov samarbeta med myndigheten. Södertälje kommun har upphandlat en extern part som Dataskyddsombud som arbetar mot kommunen och koncernen. Vid intervju anges att dataskyddsarbetet är eftersatt och att resurserna som tilldelas rollen främst används för granskning och rådgivning, inte utveckling.

## 4.3. Största risken för röjning av personuppgifter är den mänskliga faktorn och vid kontakt med andra myndigheter

De största riskerna för röjning av skyddade personuppgifter anges vara den mänskliga faktorn och vid kontakt mellan myndigheter. Den generella kunskapsnivån gällande hanteringen av skyddade personuppgifter anges även variera mellan kontoren, vilket även enkätresultaten indikerar. Inom kommunen sägs det finnas ett större fokus på digitaliseringen än informationssäkerheten, dock anger intervjupersoner att glappet är hanterbart.

Skyddade personuppgifter hanteras inom den ordinarie verksamheten. På central nivå finns stöttande och rådgivande avdelningar för verksamheterna, som HR, säkerhetsavdelningen och IT. Exempelvis kan säkerhetsavdelningen bli kontaktad av utbildningskontoret om en elev vill införskaffa en privat mobiltelefon men på grund av hens skyddade personuppgifter krävs att hotbilden tas hänsyn till. Då fungerar säkerhetsavdelningen som rådgivande funktion gentemot eleven och eventuella vårdnadshavare. Säkerhetsavdelningen kan även fungera som en stöttande funktion vid upphandling av system.

I verksamhetssystemen framkommer det om en individ har skyddade personuppgifter. När medborgare vill få ut information från kommunen vänder de sig till Kontaktcenter. Medarbetarna i Kontaktcenter har tillgång till vissa av kommunens system och kan utifrån dessa lämna ut viss information. Intervjupersoner anger att personalen i Kontaktcenter kommer i kontakt med hanteringen av skyddade personuppgifter men kan inte besvara vilken utbildning eller kompetens det finns inom frågan. Det anges vara hög personalomsättning inom centret vilket försvårar förutsättningarna för en stabil kunskapsnivå. Kontaktcenter förmedlar inte uppgifter om/till medarbetare utan stämmer först av med medarbetaren huruvida det är hen som personen som ringer ska kontakta.

Vid intervjuer framkommer det att arbetet med informationssäkerhet inte är lika prioriterat som digitaliseringsarbetet då digitaliseringen ges större resurser.

IT-avdelningen ansvarar för de övergripande systemen men de lokala verksamhetssystemen upphandlas och förvaltas av respektive kontor. Det uppges att säkerhetskraven vid upphandling överlag varit lägre än önskvärt och att det är svårt för IT att fullt veta huruvida kommunens lokala system är ändamålsenliga utifrån ett säkerhetsperspektiv. Det pågår ett kartläggningsarbete där IT går igenom samtliga system, det är dock respektive kontor som ansvarar för IT-säkerheten i systemen.

## 4.4. HR-avdelningen stöttar vid rekrytering av medarbetare med skyddade personuppgifter

I *Rutin för skyddade personuppgifter* anges att en medarbetare som har skyddade personuppgifter i form av sekretessmarkering eller skyddad folkbokföring ska informera sin chef om detta. Chefen ska i sin tur informera lönechefen om att personen har skyddade personuppgifter. När en medarbetare har skyddade personuppgifter bör chef och medarbetare i nära dialog genomföra en gemensam riskbedömning. I riskbedömningen ska följande punkter beaktas:

- Vilka som ska informeras om att personen har skyddad identitet samt vilken information de ska få.
- Hur arbetsgivaren och annan personal ska förhålla sig till frågor från andra som rör medarbetaren.
- Beskrivning av hotbild och konsekvenser för arbetsplatsen.
- Hantering av fotografering på arbetsplatsen.

I rutinen *Hantering av skyddade personuppgifter hos medarbetare* framgår att arbetsgivaren samt medarbetaren med skyddade personuppgifter ska ha ett samtal för att reda ut praktiska frågor. Arbetsgivaren och arbetstagaren går igenom vilka system som är nödvändiga för att utföra arbetsuppgifterna. Om skyddsbehovet kräver det ska ett fingerat namn användas där det är möjligt. Utgångspunkt är den enskildes önskemål men arbetsgivaren behöver förklara vad de olika alternativen innebär. I vissa system måste arbetstagarens rätta namn framgå. Som stöd vid hanteringen av medarbetare med skyddade personuppgifter finns *Checklista skyddade personuppgifter*. Enkätresultaten visar att 65 procent av respondenterna inte känner till rutinerna som gäller för medarbetare med skyddade personuppgifter.

Vid intervjuer sägs att det finns förbättringspotential kring rekryteringsprocessen av individer med skyddade personuppgifter. Intervjupersoner anger att det inte finns tydliga rutiner vid rekrytering av personer med skyddade personuppgifter utan att HR kan kallas in som stöd. Dock upplever HR att de sällan kontaktas vid behov av stöd från kontoren vid hantering av skyddade personuppgifter. Att det inte är vanligt förekommande med skyddade personuppgifter bidrar även till osäkerhet i hanteringen.

Det finns ingen fastställd policy eller riktlinje kring vilka som bör känna till att en medarbetare har skyddade personuppgifter, det är upp till chefen och individen att diskutera. Vid rekrytering av en medarbetare med skyddade personuppgifter ska ansökan skickas in manuellt, inte via rekryteringssystemet då individen behöver ange personuppgifter. I HR-systemet finns individens verkliga namn registrerat, i systemet framgår också om individen har en sekretessmarkering.

Kommunen och koncernen har separata HR-avdelningar och det finns ingen samverkan mellan dessa gällande hanteringen av skyddade personuppgifter.

## 4.5. Det finns ingen kontinuerlig uppföljning av styrdokuments efterlevnad

Dataskyddskoordinator ansvarar för att följa upp dataskyddsarbetet på men har ingen rapporteringsrutin över sitt löpande arbete med lokala dataskyddssamordnare. Det anges dock vara en målsättning att framöver kunna sammanställa rapporter som redogör för hur kommunen arbetar med informationssäkerhet och dataskydd.

Kommunens dataskyddsombud granskar årligen verksamheten, under 2021 granskades kommunens förmåga att upptäcka, hantera, och följa upp personuppgiftsincidenter och informationssäkerhetshändelser. Resultatet visar att Södertälje kommun har etablerade rutiner och ansvarsfördelning. Förankring hos medarbetare och att göra rutiner kända återstår att arbeta vidare med då det fortsatt finns medarbetare och förtroendevalda som inte är medvetna om händelser och incidenter. Fokuset för dataskyddsombudets granskning fastställs utifrån omvärldsbevakning, incidenter föregående år och resultat av tidigare granskningar. I granskningen från 2021 kontrolleras inte hanteringen av skyddade personuppgifter specifikt.

I *Rutin för skyddade personuppgifter* anges att varje verksamhet ska utse en person med ansvar för att rutiner och regler för hantering av skyddade personuppgifter följs. I denna granskning har det inte gått att få del av sammanställningar eller annan dokumentation som säkerställer att en sådan uppföljning görs. Det går inte heller att få bekräftat att det finns en utsedd person inom varje verksamhet som ansvarar för att rutiner och regler för hantering av skyddade personuppgifter följs. Det finns i dagsläget ingen övergripande kontroll kring huruvida *Rutin för skyddade personuppgifter* efterlevs.

Ett sätt att följa upp informationssäkerheten är via kontroll av loggar. I verksamhetssystem skapas loggar över vilka användare som är inne i systemen och vad de gör i systemen. Intervjupersoner anger att det till stor del inte förekommer någon systematisk uppföljning och kontroll av loggarna för att säkerställa att endast behöriga medarbetare har tillgång till systemen. Intervjupersoner anger att det kan förekomma kontroller av loggar vid uppmärksammade incidenter men arbetet blir reaktivt. Socialkontoret har dock ett systematiskt arbete med loggkontroller för att säkerställa att endast behöriga medarbetare har tillgång till systemen. Kommunen genomförde under 2021 penetrationstester med hjälp av en extern aktör som testade kommunens säkerhetssystem och identifierade en del brister som kommunen arbetat vidare med.

## 4.6. Bedömning

Bedömningen är att det finns ändamålsenliga styrande dokument och utformade rutiner för hanteringen av skyddade personuppgifter på kommunkoncernövergripande nivå. Rutinen för skyddade personuppgifter säkerställer en övergripande vägledning vid hanteringen av skyddade personuppgifter. Intervjupersoner anger att de saknar rutiner och riktlinjer för hanteringen av skyddade personuppgifter, även vid rekrytering av medarbetare med skyddade personuppgifter, vilket indikerar att rutinen inte är känd inom verksamheterna. I enkätresultatet framgår att 42,3 procent inte vet om det finns skriftliga rutiner för hanteringen av skyddade personuppgifter.

Under granskningen har det inte noterats något systematiskt arbete för att implementera rutinen inom kommunen.

För att säkerställa en högre kunskapsnivå och säkrare hantering av skyddade personuppgifter behöver styrande och stödjande dokument göras kända för medarbetarna.

Bedömningen är att ansvarsfördelningen tydliggörs i styrande dokument och det finns funktioner och avdelningar som fungerar stöttande och rådgivande vid hantering av skyddade personuppgifter. Dock noteras att kontor och bolag inte alltid känner till vilket stöd som finns att få vilket bekräftar observationen om att styrdokumenten inte är fullt kända inom verksamheterna.

Kommunkoncernen, den kommunala verksamheten inklusive bolagen, har inte tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad. Det sker ingen strukturerad eller dokumenterad uppföljning av hanteringen av skyddade personuppgifter.

# 5. Nämndernas rutiner och arbetssätt

- **Socialnämnden har ett flertal rutiner kopplat till hanteringen av skyddade personuppgifter**

Inom socialnämndens verksamhet är det vanligt att komma i kontakt med känsliga personuppgifter då samtliga ärenden föreläggs med sekretess. Det uppges finnas god kännedom kring hanteringen av sekretessbelagd information. I enkätresultatet framgår att respondenter från socialkontoret ofta kommer i kontakt med skyddade personuppgifter.

Vid implementeringen av kontorets verksamhetssystem, för två år sedan, beslutades att behörigheterna i systemet skulle ses över och stärkas. I systemet finns endast numera ett fåtal individer med behörigheter som möjliggör tillgång till skyddade personuppgifter. Systemförvaltare inom socialkontoret ansvarar bland annat för att administrera ansökningar för behörighet i systemet och vid intervju anges att ansökningar kritiskt granskas och ifrågasätts för att säkerställa att behovet för ytterligare behörighet är nödvändigt, det är berörd chef som sedan beviljar behörigheten. Inom socialkontoret har handläggarna i de olika verksamheterna tillgång till den egna organisationens brukaruppgifter med undantag för de brukare som har sekretessmarkering, antingen via Skatteverket eller via systemfunktionen "manuell sekretessmarkering". För att se sekretessmarkerade brukare krävs att man har en direktrelation, att man på något sätt står som ansvarig/medansvarig för just den brukaren. Det finns vissa funktioner i verksamheterna som kan se sekretessmarkerade personer utan att ha en direktrelation men då har beslutet tagits i Ledningsgrupp.

I och med socialnämndens ansvarsområden beaktas alltid hotbilden som följer med klienter inom socialtjänsten. Det finns fysiska hinder som låsta dörrar och separata personalingångar i socialkontorets lokaler, tjänstepersoner får även individuella personlarm vid behov, exempelvis vid hembesök eller andra besök där risk bedöms föreligga.

Intervjupersoner anser att det finns ändamålsenliga rutiner som stöttar personalen vid hanteringen av skyddade personuppgiftsärenden. Enkätresultatet visar att medarbetare inom socialkontoret har god kunskap om rutiner för hanteringen av skyddade personuppgifter samt var dessa rutiner går att finna.

I tabellen nedan framgår ett flertal rutiner som specifikt berör hanteringen av skyddade personuppgifter.

| Riktlinje/rutin/anvisning | Kort beskrivning |
|---|---|
| *Hantering av skyddade personuppgifter inom socialkontoret*<br><br>*(Odaterad)* | Rutin för hur individer med skyddade personuppgifter ska hanteras inom socialkontoret. Exempelvis tydliggörs vilka punkter som bör diskuteras vid första kontakten mellan klient och kontor samt hur journalföringen ska hanteras. |
| *Checklista för enskilda med skyddade personuppgifter som får insatser inom socialkontoret*<br><br>*(Odaterad)* | Checklistan är utformad som ett komplement till ovan nämnda rutin för att säkerställa att de viktigaste frågorna omhändertas. |
| *Rutin för hantering av ärenden som har skyddade personuppgifter*<br><br>*Ledningsgrupp (01-04-2021)* | Socialkontoret Barn och ungdom har rutin som syftar till att underlätta korrekt och säker handläggning av ärenden. Syftet är att klienter ska veta att deras skydd upprätthålls och att medarbetare vet hur man ska agera när ärenden omfattas av skyddade personuppgifter. |
| *Rutin för hantering av skyddade personuppgifter*<br><br>*Resultatområdeschef (01-02-2022)* | Socialkontorets Vuxenenhet har liknande rutin som Barn och ungdom ovan. |
| *Skyddade personuppgifter inom Arbete och Försörjning*<br><br>*Ledningsgrupp (01-02-2021)* | Socialkontorets resultatområde för Arbete och Försörjning har liknande rutin som Barn och ungdom ovan. |

Inom socialkontoret finns kvalitetsutvecklare inom respektive resultatområde som arbetar med avvikelsehantering för att säkerställa att rutiner finns och efterlevs. Det är dock respektive resultatenhetschef som ansvarar för att de rutiner som rör enheten är aktuella, fungerar och följs.

- **Det går inte att fastställa hur de styrande dokumenten används inom Utbildningsnämnden**

Vid intervju anges kunskapsnivån om hanteringen av skyddade personuppgifter variera inom ledningen men ökar längre ut i verksamheten där frågan hanteras mer regelbundet. I enkätundersökningen framgår att 60 procent känner att de har tillräcklig kunskap om hur man ska agera vid kontakt med personer som har skyddade personuppgifter. Vidare anger 20 procent att de inte har tillräcklig kunskap och 20 procent vet inte huruvida det har tillräcklig kunskap.

Utbildningskontorets elevregister importerar dagligen information från Skatteverket så systemet får direkt information om förekomsten av skyddade personuppgifter. När en elev har skyddade personuppgifter döljs dessa i systemet och endast ett fåtal behörigheter har tillgång till informationen. I nuläget arbetar kontoret för att bättre integrera systemen med varandra då en elev med skyddade personuppgifter inte kan använda vissa plattformar just på grund av sekretessbegräsningen. Det pågår ett utvecklingsarbete tillsammans med socialtjänsten gällande situationer där vårdnadshavaren är den som utgör ett hot mot barnet och hur nya bestämmelser på bästa sätt ska förmedlas till förskolorna eller skolorna.

Vid intervjuer lämnas olika uppgifter över hur välkända utbildningsnämndens rutiner och

riktlinjer kring hanteringen av skyddade personuppgifter är. I enkätresultatet framgår att det endast är 30 procent av medarbetarna inom utbildningskontoret som vet var dessa rutinbeskrivningar finns. Kontoret har rutiner för hanteringen av skyddade personuppgifter men dessa ska revideras. Vid utformning av rutiner utgår utbildningskontoret från Skolverkets råd. De reviderade rutinerna ska instruera användaren att dokumentera det skyddet som individen behöver.

| Riktlinje/rutin/anvisning | Kort beskrivning |
|---|---|
| *Barn och unga med skyddad identitet*<br><br>*(Odaterad)* | Rutinen är utformad som en handlingsplan där vissa uppgifter om eleven ska fyllas i samt hur verksamheten ska hantera skyddet, vilka som ska informeras och andra praktiska bestämmelser som fastställs tillsammans med eleven och vårdnadshavare. |
| *Hantering av skyddade personuppgifter inom utbildning*<br><br>*(Odaterad)* | Rutinen gäller för samtliga utbildningsformer och samtliga deltagare. I rutinen tydliggörs att eleven själv ska upplysa rektor om förekomsten av skyddade personuppgifter och att formerna för samarbetet fastställs vid samtal mellan skolan, eleven och vårdnadshavaren. Rutinen redogör även för hanteringen av skolans IT-system, betygsättning och beredskap vid akuta situationer. |

Den största risken för röjning av elever med skyddade personuppgifter inom utbildningsverksamheten anges vara vid kontakt med andra myndigheter samt den mänskliga faktorn. Barn och elever som inte förstår allvaret i situationen och vars agerande bidrar till ökad risk för röjning. Barn kan exempelvis vilja vara med på fotografier för olika marknadsföringskampanjer vilket till viss del kan vara svårt för medarbetarna att övervaka. Inom förskoleverksamheten används inte längre sociala medier som instagram då det inte går att ansvara för vad eller vem som publiceras på dessa. Överlag tillämpas samma sekretessbestämmelser för samtliga barn men vid skyddade personuppgifter genomförs särskilda samtal med vårdnadshavare och barn för att få en bättre bild av hotbilden.

Det finns en utpekad funktion inom kontoret som ansvarar för innehåll på utbildningswebbplatser vilket kan ge viss kontroll. Vid kontakt med myndigheter anges dessa ha färre regleringar om hanteringen av personuppgifter än utbildningskontoret. Om utbildningskontoret behöver skicka mejl med personuppgifter skickas det via ett säkert meddelande. Kontoret kan dock få mejl från vårdnadshavare med personuppgifter och annan känslig information.

## 5.1. Bedömning

Bedömningen är att kunskapen om hanteringen av skyddade personuppgifter varierar mellan kontor och ansvarsnivå. Tjänstepersoner som arbetar verksamhetsnära kommer i kontakt med den praktiska hanteringen av skyddade personuppgifter genom elever och klienter. Det finns specifika rutiner kring hanteringen av skyddade personuppgifter som medarbetare kan få stöd av. Det är dock inte tydligt hur välkända rutinerna är inom kontoret.

Det finns inga funktioner som har ett specifikt ansvar för arbetet med skyddade personuppgifter i likhet med Skatteverkets rekommendation att "Varje myndighet bör utse en person med ansvar för att rutiner och regler för hantering av skyddade personuppgifter efterföljs".

# 6. Bolagens rutiner och arbetssätt

- **Kännedom kring hanteringen av skyddade personuppgifter upplevs som god inom Telge AB**

Telge AB är kommunens moderbolag som äger åtta dotterbolag och fyra intressebolag.

Personuppgifter som hanteras inom Telge AB utgår främst från HR-systemet och bolagens medarbetare. I HR-systemet anger intervjupersoner att det tydligt framgår om en medarbetare har skyddade personuppgifter. Vidare framgår i enkätundersökningen att ca 19 procent av respondenterna anger att det tydligt framgår i verksamhetens IT-system vilka personuppgifter som är skyddade medan 68 procent anger att de inte vet huruvida det framgår. Intervjupersoner anger att det främst är medarbetare inom IT och HR som har tillgång till system där det framgår om individen har skyddade personuppgifter, därav förklaras varför kännedomen hos resterande medarbetare är lägre. Hanteringen av medarbetare som har skyddade personuppgifter skiljer sig beroende på individens skyddsbehov och egna önskemål.

Vid intervjuer anges den mänskliga faktorn vara den största risken för röjning av en skyddad personuppgift. För att minimera risken för röjning har bolaget vidtagit åtgärder kopplat till utskrivning av dokument. Vid utskrift skickas inte dokumenten direkt till skrivaren utan kopplas till medarbetarens konto. Medarbetaren måste använda sina personliga inloggningsuppgifter för att använda skrivaren vilket motverkar att obehöriga ska ta del av dokument.

Intervjupersoner inom Telge AB anges vara trygga med deras arbetssätt kopplat till hanteringen av skyddade personuppgifter. Av enkäten framgår dock att färre än hälften av respondenterna (45%) anser sig ha tillräckliga kunskaper för hantering av skyddade personuppgifter. Inom Telge AB finns en dataskyddssamordnare och vid arbete med informationssäkerhet, vilket inkluderar hanteringen av skyddade personuppgifter, finns kommunens säkerhetsavdelning och Telgekoncernens IT-avdelning som stödjande funktioner.

Det anges finnas ett flertal styrdokument för hanteringen av skyddade personuppgifter. Rutinerna som beskrivs nedan är koncernövergripande och inte specifika för Telge AB.

| Riktlinje/rutin/anvisning | Kort beskrivning |
|---|---|
| *Hantering av skyddade personuppgifter hos medarbetare*<br><br>*(Odaterad)* | Rutinen innehåller bland annat saker att tänka på vid rekrytering av medarbetare med skyddade personuppgifter, hanteringen i IT-system samt en checklista för samtal med medarbetare för att kartlägga behovet av skydd. |
| *Rutin för hantering av skyddade personuppgifter (KS 20/311)*<br><br>*(30-11-2021)* | Syftet med rutinen för hantering av skyddade personuppgifter är att skapa enhetlig och säker hantering av skyddade personuppgifter i samtliga av kommunkoncernens verksamheter för att uppfylla gällande lagkrav. Rutinen redogör för förhållningssätt vid hantering av skyddade personuppgifter samt vid hantering av skyddade personuppgifter för medarbetare. |
| *Rutin för bedömning och rapportering vid misstänkt personuppgiftsincident*<br><br>*(05-01-2021)* | Syftet med rutinen är att upptäcka, rapportera och utreda personuppgiftsincidenter i enlighet med lagstiftning. |

- **Telge Bostäder AB:s verksamhetssystem hanterar skyddade personuppgifter**

Telge Bostäder AB har ett verksamhetssystem för uthyrning av bostäder som möjliggör för bolaget att bland annat se hur många hyresgäster som har skyddade personuppgifter.

Vid registrering i Telge Bostäders kö krävs ett riktigt personnummer men när individen blivit erbjuden en lägenhet finns möjlighet att registrera ett fiktivt personnummer i systemet. Det finns riktlinjer som beskriver hur registrering till systemet ska ske.

I intervjuer nämns att hyresgäster framöver även kommer ha möjlighet att registrera sig med ett fiktivt namn. I dagsläget krävs ett riktigt namn vid registrering men det går att välja att skriva ett fiktivt namn på ytterdörren samt boendetavlan. Vidare anges att adresser eller personuppgifter inte behöver anges i kontakt med bolaget, det ska räcka att använda det personliga ID som varje lägenhetsinnehavare har.

Bolaget lämnar inte ut information om sina hyresgäster. Vanligt förekommande är emellertid att hyresgäster själva delar med sig av personuppgifter vid kontakt med bolaget, exempelvis via mejl, i stället för att uppge sitt personliga ID. Om bolaget behöver förmedla personuppgifter används s.k. "säkra meddelanden". Telgekoncernens IT-avdelning fungerar som stöd vid denna typ av hantering.

Arbetsplatsträffar och intranätet används för informationsspridning och uppdatering av regler. 40 procent av responderande medarbetare inom bolaget anser att de inte har tillräckliga kunskaper om hanteringen av skyddade personuppgifter och 60 procent anger att de inte vet var rutiner för hanteringen går att finna.

Nedan beskrivs rutiner med koppling till hanteringen av skyddade personuppgifter.

| Riktlinje/rutin/anvisning | Kort beskrivning |
|---|---|
| *Rutin skyddad ID*<br><br>*(22-09-2022)* | Rutinen redogör för vilka steg som ska vidtas när en kund med skyddat ID registrerar sig samt blir aktuell för en lägenhet. Det framgår vidare att kontrakt mellan bolaget och kunden ska skrivas under med individens riktiga namn och personnummer, vid e-signering skrivs avtalet ut och ska tas bort ur systemet. |
| *Riktlinjer för informationssäkerhet inom Telge Bostäder AB och Telge Hovsjö AB*<br><br>*(13-11-2020)* | I riktlinjerna framgår att avdelningar och enheter ska utforma anvisningar och rutiner för behandling av skyddade personuppgifter. Det ska även framgå tydligt om individen har skyddade personuppgifter i systemen. Kunder och medarbetare med skyddade personuppgifter ska uppvisa handling från Skatteverket som intyg. |

- **Telge Energi AB:s kundregister är utformat för att minimera riskerna för röjning av uppgifter genom den mänskliga faktorn**

Vid hantering av medarbetare med skyddade personuppgifter inom Telge Energi AB, både gällande eventuell avvikelse samt vid rekrytering, kontaktar chefer Telgekoncernens HR-avdelning. Intervjupersoner beskriver att det finns kunskap och erfarenhet inom verksamheten gällande hur skyddade personuppgifter ska hanteras vid kundärenden. I enkätresultatet framgår att 90 procent av bolagets respondenter anser att de har tillräcklig kunskap om hanteringen av skyddade personuppgifter.

Bolaget får information direkt från Skatteverket vilket gör att de inte vet var kunden bor eller heter. Den enda information som finns är kundens anläggningsadress. Det enda sättet att få tillgång till personuppgifter är genom inloggning med kundens personliga lösenord. Enligt intervjupersoner lämnas aldrig kundregistret ut.

Om det finns rimliga skäl för utlämning av registerutdrag kan jurister och VD för Telge AB tillfrågas. Om en myndighet vill ha uppgifter från bolagets kundregister måste det gå via e-post för att säkerställa trovärdigheten i förfrågan. Uppgifter lämnas aldrig ut över telefon.

I tidigare kundregister fanns information om kundens adress och namn, bolaget analyserade dock riskerna kring systemet och beslutade att den mänskliga faktorn kan resultera i röjning av uppgifter. Det nya kundregistret innehåller inga känsliga personuppgifter, dock nämner intervjupersoner att det finns vissa känsliga uppgifter i faktureringssystemet samt i systemet för inkasso. I enkätresultatet framgår att 40 procent av medarbetarna inom bolaget anser att de inte får tydlig information om att kunden har skyddade personuppgifter i verksamhetssystemet.

Telge Energi AB utgår bland annat från Telgekoncernens rutiner och riktlinjer, framför allt vid rekrytering och andra medarbetarfrågor. Granskningen har även tagit del av en processkarta för hur ett ärende där kunden har skyddat ID ska hanteras. Bolaget har även en utbildning/rutin gällande skyddad ID för utländska personnummer.

| Riktlinje/rutin/anvisning | Kort beskrivning |
|---|---|
| *Utbildning skyddad ID utländskt personnummer*<br><br>*(Odaterat)* | I rutinen tydliggörs bland annat vilka stödfunktioner som finns inom bolaget om medarbetaren stöter på hanteringen av skyddat ID, att kunden behöver ange sitt personliga lösenord innan bolaget ger ut någon specifik information om kunden samt att registret uppdateras i enlighet med folkbokföringen en till två gånger om året. |

## 6.1. Bedömning

Den övergripande bedömningen är att det finns kännedom kring frågorna gällande informationssäkerhet och hanteringen av skyddade personuppgifter, vilket även styrks av enkätundersökningen. Det finns framtagna rutiner kopplat till hanteringen av skyddade personuppgifter. Det vidtas åtgärder för att minska risken för röjning av uppgifter, exempelvis en restriktiv utlämning av uppgifter samt fysisk begränsning av papper med känsliga uppgifter. Samtliga granskade bolag behandlar skyddade personuppgifter och deras verksamhetssystem möjliggör sådan handläggning. Granskningen saknar emellertid, som även påpekas för granskade nämnder, specifika funktioner som ansvarar för hanteringen av skyddade personuppgifter. Det finns roller som arbetar löpande med informationssäkerhetsfrågor men inget riktat fokus görs på hanteringen av skyddade personuppgifter.

# 7. Kompetensutveckling kring skyddade personuppgifter

I *Rutin för skyddade personuppgifter* anges att säker hantering av skyddade personuppgifter kräver att personalen har goda kunskaper om de sekretessbestämmelser som gäller för verksamheten och om skyddsåtgärderna *sekretessmarkering* och *markering för skyddad folkbokföring*. Samma skrivning finns även i *Rutin för hantering av skyddade personuppgifter*, Telge AB:s koncernövergripande rutin. Vid intervjuer framgår att det inte genomförts någon koncernövergripande utbildning kopplat till hanteringen av skyddade personuppgifter.

Det har genomförts vissa utbildningsinsatser gällande GDPR och informationssäkerhet, exempelvis inom Telge Bostäder AB som erbjuder utbildningen vid nyanställning. Under granskningen har det dock inte noterats lokala utbildningsinsatser inom berörda kontor och bolag gällande hanteringen av skyddade personuppgifter.

Flera intervjupersoner anger att den mänskliga faktorn är den största risken för röjning av skyddade personuppgifter och för att minska den risken förespråkas kompetensutvecklingsinsatser. Intervjupersoner anger att det är viktigt att medarbetare inom kommunens och bolagens verksamheter förstår och har kunskap kring eventuella konsekvenser av röjning av skyddade personuppgifter för att säkerställa korrekt hantering. Om allvaret tydliggörs anges risken för incidenter orsakade av den mänskliga faktorn att minska.

I enkätundersökningen framgår att 63 procent av de tillfrågade anser att de har tillräcklig kännedom om hur du ska agera vid kontakt med en personmed skyddade personuppgifter. 19 procent anser att de inte har tillräcklig kännedom och 19 procent anser att de inte vet huruvida de har tillräcklig kännedom om hanteringen av skyddade personuppgifter. 40 procent anser att det finns skriftliga rutiner som stöd vid hanteringen av skyddade personuppgifter medan 42 procent inte vet huruvida det finns rutiner för hanteringen. Det noteras att det finns viss information på koncernensintranät gällande hanteringen av skyddade personuppgifter samt tillgång till flertalet rutiner och riktlinjer som redogörs i rapporten. Uppdaterad och tillgänglig information anges öka medvetenheten och kännedomen om skyddade personuppgifter.

## 7.1. Bedömning

Bedömningen är att det inte genomförs tillräcklig kompetensutveckling kring skyddade personuppgifter. Medvetandegrad och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning. Inom respektive kontor och bolag finns behov av ökad medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter. Det saknas en lärprocess uppbyggd av erfarenheter och riskbedömningar inom och mellan respektive kontor och bolag. Kompetenshöjande insatser bör planeras utifrån riskbedömningar om vilka verksamheter där risken för röjning är högst.

# 8. Riskanalys av skyddade personuppgifter

I *Rutin för skyddade personuppgifter* anges att kommunens olika verksamheter bör genom riskanalys kartlägga hur skyddade personuppgifter ska behandlas i den egna verksamheten och utifrån riskanalysen ta fram egna rutiner. Granskningen har inte tagit del av kontors/bolagsspecifika riskanalyser för att kartlägga hur skyddade personuppgifter ska hanteras. Granskningen har i stället gått igenom kontoren och bolagens riskanalyser som ligger till grund för internkontrollplanen.

I tabellen nedan tydliggörs huruvida skyddade personuppgifter lyfts som en risk i internkontrollplananalyserna under 2021 och 2022. Om nämnden eller styrelsen genomför någon annan form av riskanalys som faller utanför internkontrollarbetet redogörs det för i ”Övrig riskanalys”.

| Nämnd/ Styrelse | Riskanalys 2021 | Riskanalys 2022 | Övrig riskanalys |
|---|---|---|---|
| **Kommun-styrelsen** | Kommunstyrelsens internkontrollplan för 2021 har en identifierad risk avseende hantering av personuppgifter vid utlägg. Mallar har tagits fram för att underlätta hantering och en utredningsgrupp har tillsatts.<br><br>Inget specifikt om skyddade uppgifter.<br><br>Det saknas riskanalys som ligger till grund för internkontrollplanen. | Kommunstyrelsens internkontrollplan är inte beslutad och det finns ingen bakomliggande riskanalys. | Genomförs inga direkta riskbedömningar kring hanteringen av skyddade personuppgifter. |
| **Social-nämnden** | Socialnämnden har identifierat en risk i sin internkontrollplan om att obehöriga inte ska ha tillgång till SoL-journal. För att kontrollera detta görs stickprov.<br><br>Inget specifikt om skyddade uppgifter.<br><br>Det saknas riskanalys som ligger till grund för internkontrollplanen. | Socialnämnden har identifierat en risk i sin internkontrollplan om att obehöriga inte ska ha tillgång till SoL-journal. För att kontrollera detta görs stickprov.<br><br>Inget specifikt om skyddade uppgifter.<br><br>Det saknas riskanalys som ligger till grund för internkontrollplanen. | Genomförs inga direkta riskbedömningar kring hanteringen av skyddade personuppgifter. |
| **Utbildnings-nämnden** | I nämndens riskanalys och internkontrollplan finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter. | I nämndens riskanalys och internkontrollplan finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter. | Genomförs inga direkta riskbedömningar kring hanteringen av skyddade personuppgifter. |
| **Telge AB** | Telge AB har en rullande riskanalys som uppdateras regelbundet, det finns därav ingen specifik riskanalys från 2021.<br><br>I internkontrollplanen för 2021 är ett riskområde att GDPR inte efterföljs. Vidtagna åtgärder är att personuppgiftpolicy finns på plats samt att Dataskyddombudet samt dataskyddsamordnarna har | I den senaste versionen av Telge AB:s riskanalys identifieras ökad risk för intrång och läckage av data, vilket även inkluderar personuppgifter. Redan vidtagna åtgärder som tagits är att policy är framtagen samt att nanolearning i informationssäkerhet är inrättat. | Genomförs inga direkta riskbedömningar kring hanteringen av skyddade personuppgifter. |

| | | | |
|---|---|---|---|
| | påbörjat nanolearning (en kortare digital utbildning)<br><br>Inget specifikt om skyddade personuppgifter. | Denna risk inkluderas även i bolagets internkontrollplan. En annan risk som kvarstår är bristande efterlevnad av GDPR.<br><br>Inget specifikt om skyddade personuppgifter. | |
| **Telge Bostäder AB** | Telge Bostäder AB har en rullande riskanalys som uppdateras regelbundet, det finns därav ingen specifik riskanalys från 2021.<br><br>I bolagets internkontrollplan finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter. | I styrelsens riskanalys och internkontrollplan finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter. | Genomförs inga direkta riskbedömningar kring hanteringen av skyddade personuppgifter. |
| **Telge Energi AB** | Telge Energi AB har en rullande riskanalys som uppdateras regelbundet, det finns därav ingen specifik riskanalys från 2021.<br><br>I bolagets internkontrollplan för 2021 finns ingen risk identifierad som kan kopplas till hanteringen av skyddade personuppgifter. | I Telge Energi AB:s riskanalys identifieras personuppgifter som lämnas ut felaktigt som en risk samt personuppgifter som inte hanteras i enlighet med GDPR.<br><br>I internkontrollplanen inkluderas området dataskydd. En av riskerna i området handlar om dataintrång och läckage av personuppgifter.<br><br>Inget specifikt om skyddade uppgifter. | Genomförs inga direkta riskbedömningar kring hanteringen av skyddade personuppgifter. |

## 8.1. Bedömning

Det finns inte några kontors- eller bolagsspecifika riskanalyser kring hanteringen av skyddade personuppgifter. I flertalet riskanalyser och internkontrollplaner berörs hanteringen av personuppgifter, dock inte specifikt skyddade personuppgifter, inom ramen för informationssäkerhetsarbetet. Granskningen ser positivt på arbetet med informationssäkerhet men saknar en separat hantering av skyddade personuppgifter. En övergripande riskanalys över risken för röjning av skyddade personuppgifter skulle gynna den interna kontrollen och medvetenheten hos medarbetarna då allvarlighetsgraden vid röjning av skyddade personuppgifter är hög. Bedömningen är att varken kommunen eller bolagen analyserat risken för röjning av skyddade personuppgifter.

Granskningen noterar även att bolagen har rullande riskanalyser vilket gör att det inte går att spåra kopplingen mellan riskanalysen och internkontrollplanen för föregående år vilket försvårar bedömningen.

Vid de tillfällen som hanteringen av personuppgifter berörs i riskanalys och internkontrollplan beslutas även om åtgärder för att minska risken för röjning, vilket är positivt. Eftersom det saknas en övergripande riskanalys bedöms att det inte beslutats om tillräckliga åtgärder för att minska risken för röjning av skyddade personuppgifter.

Riskerna har inte analyserats och i avsaknad av en grundläggande analys finns inte tillräcklig kunskap om bristerna för att vidta ändamålsenliga åtgärder.

# 9. Avvikelsehanteringssystem

Telgekoncernen har en gemensam rutin för bedömning och rapportering vid misstänkt personuppgiftsincident. Granskningen har inte tagit del av något motsvarande för kommunen. Kommunen och koncernen har separata e-tjänster där avvikelser inrapporteras, bland annat personuppgiftsincidenter. Det finns ingen uppfattning inom kommunen om hur många personuppgiftsincidenter som berör skyddade personuppgifter då det inte framgår i systemet. Det går inte att följa upp hur många röjningar eller annan typ av incident kopplat till skyddade personuppgifter som kommunen har under ett verksamhetsår. Dock anger intervjupersoner att antalet personuppgiftsincidenter är lågt vilket kan tyda på att avvikelserna inte rapporteras i kommunens system. I Dataskyddsombudets granskning från 2021 framgår att antalet inkomna personuppgiftsincidenter under 1 september 2020 – 1 september 2021 var 24 inom kommunen och 7 inom Telgekoncernen. Av det totala antalet personuppgiftsincidenter var 22 följden av obehörigt röjande och 7 till följd av obehörig åtkomst. Under 2022 har det hittills (början av december 2022) rapporterats 32 incidenter inom kommunen och 6 inom Telgekoncernen.

Avvikelsehanteringen används inte för verksamhetsutveckling inom kommunen och incidentsstatistiken aggregeras inte för uppföljning. Det kan emellertid inom socialkontoret ske en informell kompetenshöjande process av bra och dåliga exempel. Enligt Telgekoncernens rutin för personuppgiftsincidenter framgår att uppföljning och utvärdering ska göras inom sex månader för att minska sannolikheten för liknande händelser framöver. Granskningen har inte tagit del av en sådan uppföljning och utvärdering kopplat till hanteringen av skyddade personuppgifter.

I enkätundersökningen framgår att endast 29 procent vet var en eventuell röjning eller annan avvikelse av hanteringen av skyddade personuppgifter ska registreras. Vidare anger 70 procent av respondenterna att de inte vet om det finns rutiner för uppföljning av eventuella röjningar eller andra avvikelser vid hanteringen av skyddade personuppgifter, endast 22 procent uppger sig känna till att sådana rutiner finns.

Vid intervjuer uppkommer olika bilder över hur rapporteringen av avvikelser är utformad, se tabellen nedan:

| Nämnd/Styrelse | Avvikelsehantering |
|---|---|
| **Utbildningsnämnden** | Utbildningskontoret har inget eget avvikelsehanteringssystem vid risk för eller röjning av skyddade personuppgifter. Vid en personuppgiftsincident rapporteras den i kommunens e-tjänst för avvikelser. Det sker ingen dokumenterad uppföljning av incidenten. |
| **Socialnämnden** | Det finns olika system för återrapportering av avvikelser. En personuppgiftsincident kan klassas som en Lex Sarah som återrapporteras och sammanställs enligt rutiner för Lex Sarah. I verksamhetssystemet kan avvikelser också anmälas.<br><br>Intervjupersoner anger att avvikelserna som omfattar skyddade personuppgifter faller under kategoriseringen *Kommunikation och sekretess*. Det finns inget sätt att särskilja ett ärende som gäller skyddade personuppgifter från övriga ärenden i systemen utan det kräver manuell hantering. |
| **Telgekoncernen** | Om incident skulle ske ska det rapporteras i ENIA, koncernens avvikelsehanteringssystem. Det ska även göras om det är nära att incident sker men enligt intervjuer råder det osäkerhet om detta genomförs. Anonyma anmälningar kan göras i ENIA. Vid en personuppgiftsincident kontaktas Dataskyddsombudet som genomför en första bedömning. Om kunds identitet skulle röjas kan även visselblåsarfunktionen användas. Kunder och anställda kan anmäla incidenten anonymt till denna funktion. |

## 9.1. Bedömning

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

# 10. Svar på revisionsfrågorna

| Fråga | Svar |
|---|---|
| Har kommunen/bolagen analyserat risken för att skyddade personuppgifter röjs? | Nej. Det finns inte några kontors- eller bolagsspecifika riskanalyser kring hanteringen av skyddade personuppgifter. I flertalet riskanalyser och internkontrollplaner berörs hanteringen av personuppgifter, dock inte specifikt skyddade personuppgifter. |
| Har kommunen/bolagen vidtagit åtgärder för att minska risken för röjning av skyddade personuppgifter? | Delvis. Det finns framtagna rutiner kopplat till hanteringen av skyddade personuppgifter. Det vidtas vidare vissa åtgärder för att minska risken för röjning av uppgifter, exempelvis en restriktiv utlämning av uppgifter samt fysisk begränsning av papper med känsliga uppgifter. Dock noteras att det inte finns några kontors- eller bolagsspecifika riskanalyser kring hanteringen av skyddade personuppgifter. Utifrån det bedöms att det inte beslutats om tillräckliga åtgärder för att minska risken för röjning av skyddade personuppgifter. Riskerna har inte analyserats och i avsaknad av en grundläggande analys finns inte tillräcklig kunskap om bristerna för att vidta ändamålsenliga åtgärder. |
| Finns styrande dokument och rutiner för hantering av skyddade personuppgifter? | Ja. Det finns ändamålsenliga styrande dokument och utformade rutiner för hanteringen av skyddade personuppgifter på koncernövergripande nivå. Rutinen för skyddade personuppgifter säkerställer en övergripande vägledning vid hanteringen av skyddade personuppgifter. Dock är det oklart hur välkända dessa styrande dokument är och huruvida de tillämpas vid hantering av skyddade personuppgifter. |
| Hur görs styrdokument och rutinbeskrivningar kända för medarbetare? | Under granskningen har det inte noterats något systematiskt arbete för att implementera styrande dokument kopplat till hanteringen av skyddade personuppgifter inom kommunen. |
| Finns ett tillräckligt stöd för medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter? | Delvis. Det finns en tydlig ansvarsfördelning i styrdokument samt stöd i framtagna rutiner och riktlinjer. Dock är dessa inte välkända vilket skapar en otydlighet i huruvida det finns tillräckligt stöd vid hanteringen av skyddade personuppgifter. |
| Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter? | Nej. Det genomförs inte tillräcklig kompetensutveckling kring skyddade personuppgifter. Inom respektive kontor och bolag finns behov av ökad medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter. |

| | |
|---|---|
| | Det saknas en lärprocess uppbyggd av erfarenheter och riskbedömningar inom och mellan respektive kontor och bolag. |
| Har kommunen/bolagen tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad? | Nej. Kommunkoncernen, den kommunala verksamheten inklusive bolagen, har inte tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad. Det sker ingen strukturerad eller dokumenterad uppföljning av hanteringen av skyddade personuppgifter. |
| Finns avvikelsehanteringssystem som omfattar skyddade personuppgifter? | Nej. Det finns inte ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns inget automatiskt sätt att samla personuppgiftsincidenter på koncernövergripande nivå utan manuell handläggning. Det bedöms som en brist att verksamheterna inte kan koda incidenten som ett skyddat personuppgiftsärende. |
| Hur tillvaratas erfarenhet från avvikelser? | Det sker ingen systematisk uppföljning och analys över verksamhetens egna personuppgiftsincidenter som ligger till grund för verksamhetsutveckling. |
| Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits? | Nej. Det finns inga dokumenterade analyser gällande hanteringen av individer med skyddade personuppgifter utifrån ett säkerhetsperspektiv. Dock kan säkerhetsavdelningen fungera som en stöttande och rådgivande funktion.<br><br>Exempelvis kan säkerhetsavdelningen bli kontaktad av utbildningskontoret om en elev vill införskaffa en privat mobiltelefon men på grund av hens skyddade personuppgifter krävs att hotbilden tas hänsyn till. Då fungerar säkerhetsavdelningen som rådgivande funktion gentemot eleven och eventuella vårdnadshavare. |
| Råder det samsyn inom Södertälje kommun och dess bolag kring hur skyddade personuppgifter ska hanteras? | Delvis. Det har inte uppmärksammats några väsentliga skillnader i hanteringen av skyddade personuppgifter inom kommunen kontra koncernen. Det förekommer dock kommun- respektive koncernspecifika styrdokument för hanteringen av skyddade personuppgifter. Kommunen och koncernen har även separata stödfunktioner i form av IT- och HR-avdelningar. Det finns inga övergripande riktlinjer som säkerställer en enhetlig hantering. |

Södertälje 2023-02-23

Jan Darrell
*Certifierad kommunal yrkesrevisor, EY*

Sara Jansson
*Verksamhetsrevisor, EY*

Lirigzon Karaqica
*EY*

# Bilaga 1: Källförteckning

## Intervjuade funktioner

- Socialdirektör
- Tjänstepersoner inom socialkontoret
- Utbildningsdirektör
- Tjänstepersoner inom utbildningskontoret
- Lönechef
- HR-Chef
- Kanslichef
- Dataskyddskoordinator
- Informationssäkerhetsansvarig
- TF kommunikations- och digitaliseringschef
- TF VD Telge AB
- HR koordinator Telge AB
- TF koncernekonomichef Telge AB
- VD Telge Bostäder AB
- Avdelningschef affärsutveckling Telge Bostäder AB
- Enhetschef Uthyrning Telge Bostäder AB
- Samordnare för ledningsgrupp, chefsgrupp och styrelse, Telge Bostäder AB
- Medarbetare inom avdelningen för affärsutveckling, Telge Bostäder AB
- TF VD Telge Energi AB
- Processledare, Telge Energi AB
- IT-chef, Telge Energi AB
- Kund- och Säljkoordinator, Telge Energi AB
- Dataskyddsombud
- Säkerhetsansvarig för Telge AB IT

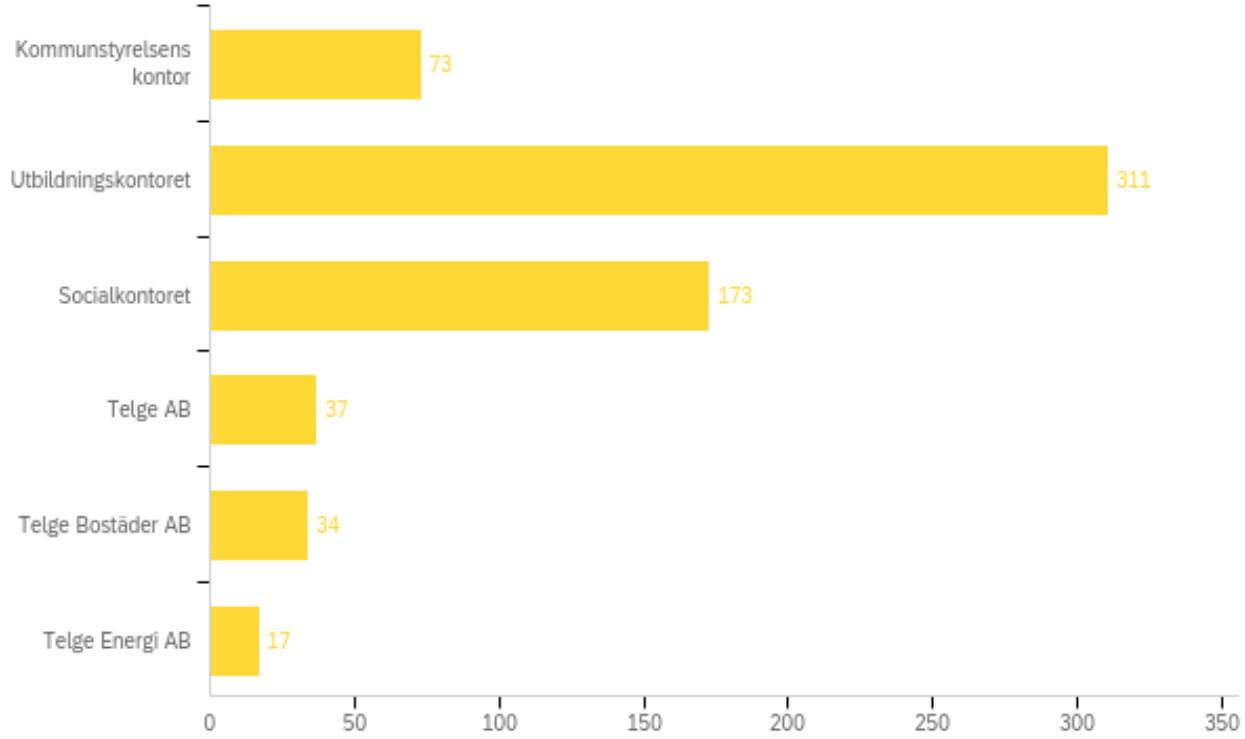
## Granskad dokumentation

- Mål och budget 2022–2024 2019-11-29)
- Digitaliseringsstrategi för Södertälje kommun (2019-06-19)
- e-Södertälje – vision och strategi för IT (revidering pågår) (2004-04-13)
- Informationssäkerhetspolicy (odaterad)
- Personuppgiftspolicy (KS 18/167) (2018-04-09)
- Riktlinje för hantering av personuppgifter (2022-02-15)
- Rutin för skyddade personuppgifter (KS 20/311) (2021-11-30)
- Hantering av skyddade personuppgifter hos medarbetare (Odaterad)
- Kommunstyrelsen internkontrollplan 2021 och obeslutad internkontrollplan 2022
- Socialnämndens internkontrollplan 2021 och 2022
- Utbildningsnämndens internkontrollplan 2021 och 2022 och riskbedömning
- Telge AB internkontrollplan 2021 och 2022
- Telge AB riskanalys
- Telge Energi AB internkontrollplan 2021 och 2022
- Telge Energi AB riskanalys
- Telge Bostäder AB internkontrollplan 2021 och 2022
- Telge Bostäder AB riskanalys
- Hanteringen av skyddade personuppgifter hos medarbetare, koncernövergripande
- Hanteringen av skyddade personuppgifter inom utbildning, utbildningskontoret
- Checklista skyddade personuppgifter, utbildningskontoret
- Barn och unga med skyddad identitet, utbildningskontoret
- Hantering av skyddade personuppgifter inom vård- och socialförvaltningen
- Checklista för enskilda med skyddade personuppgifter som får insatser inom vård- och socialförvaltningen
- Rutin för hantering av ärenden som har skyddade personuppgifter (2021-02-01)

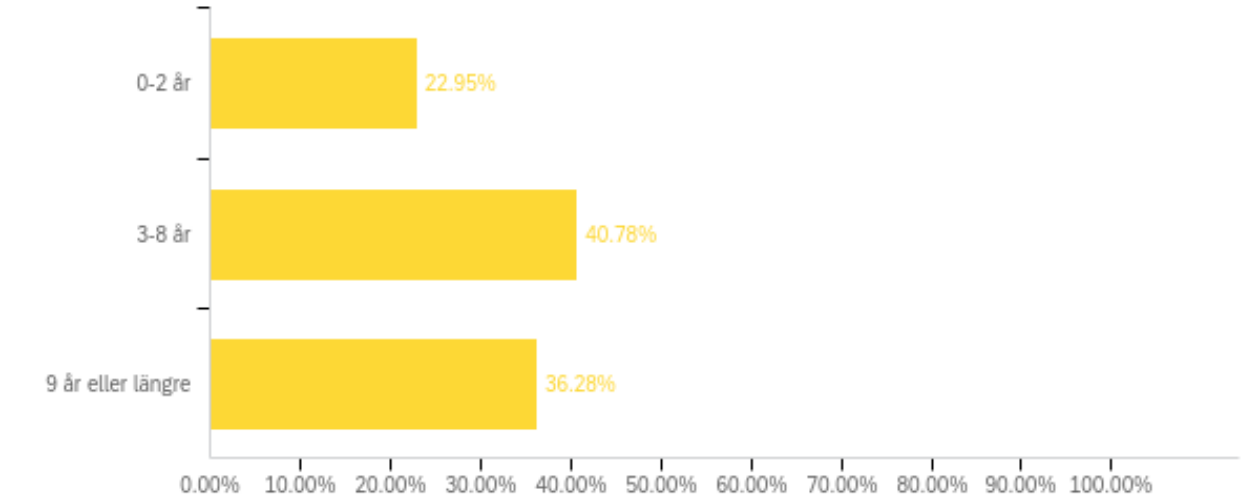
- Skyddade personuppgifter inom Arbete och försörjning (2021-02-01)
- Rutin för hantering av skyddade personuppgifter (2022-04-01)
- Rutin för hantering av skyddade personuppgifter, Telgekoncernen (2022-10-26)
- Rutin för bedömning och rapportering vid misstänkt personuppgiftsincident, Telgekoncernen (2021-01-05)
- Hantering av skyddade personuppgifter hos medarbetare, Telgekoncernen
- Rutin/utbildning skyddad ID utländskt personnummer – Telge Energi AB
- Riktlinjer för informationssäkerhet inom Telge Bostäder AB och Telge Hovsjö AB
- Rutin skyddat boende, Telge Bostäder
- Dataskyddsombud granskningsrapporter för 2021

# Bilaga 2: Enkätresultat

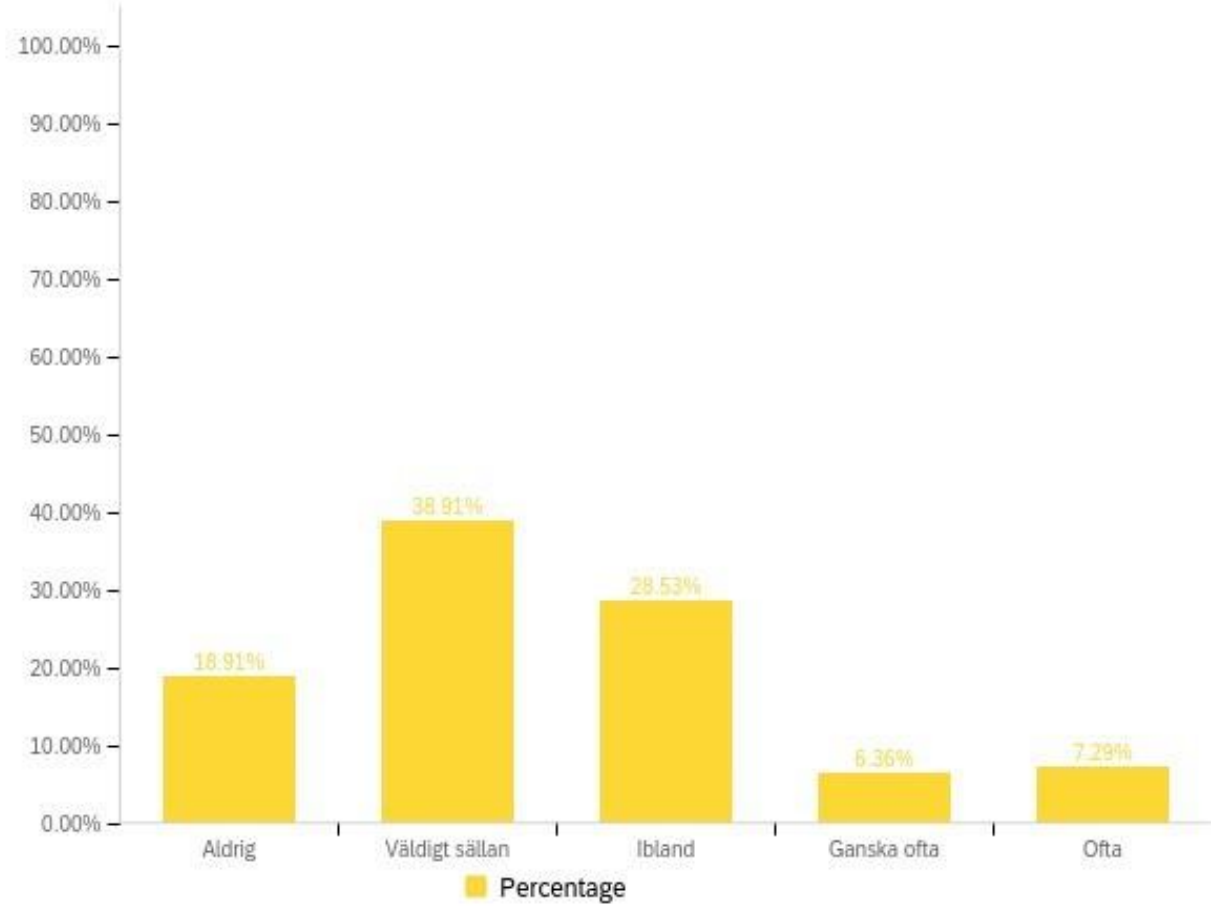
## Fråga 1 - Inom vilken verksamhet arbetar du?



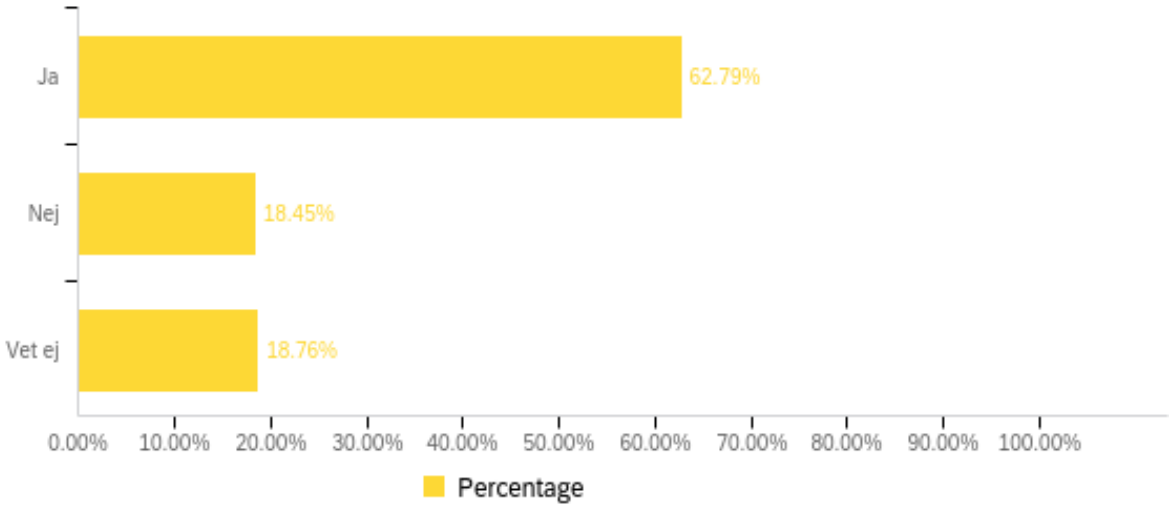

## Fråga 2 - Hur länge har du arbetat inom nuvarande verksamhet?



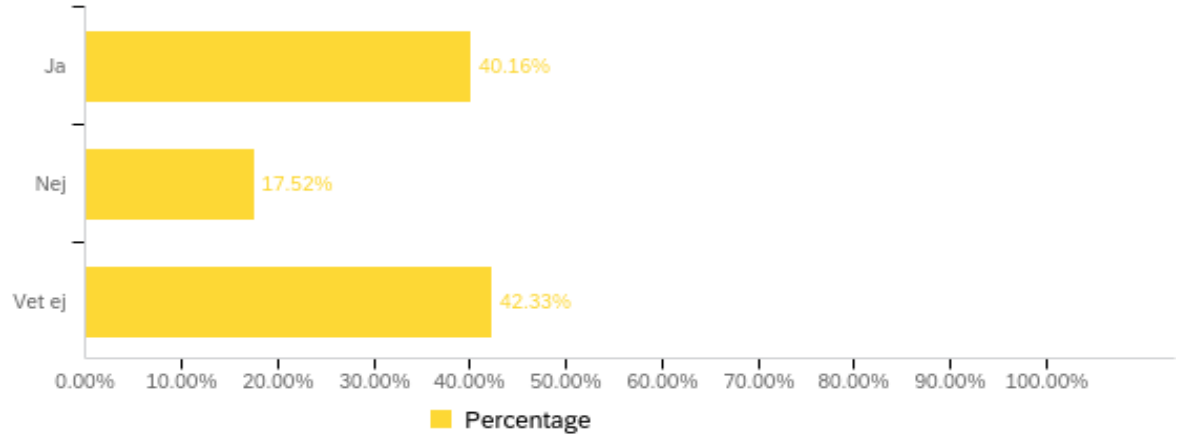
Fråga 3 - Hur ofta kommer du i kontakt med personer med skyddade personuppgifter i ditt arbete?



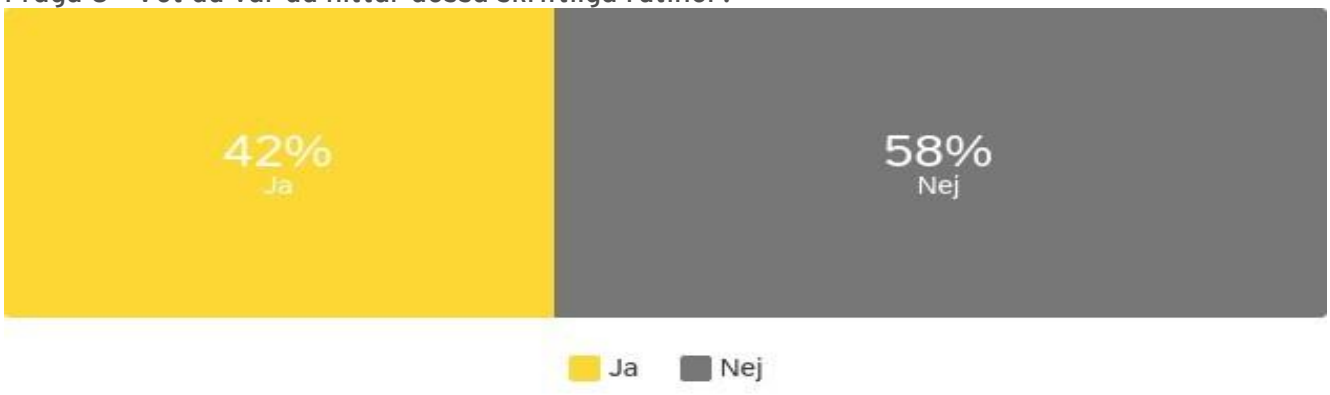

Fråga 4 - Har du tillräcklig kännedom om hur du ska agera när du kommer i kontakt med en person med skyddade personuppgifter i ditt arbete?



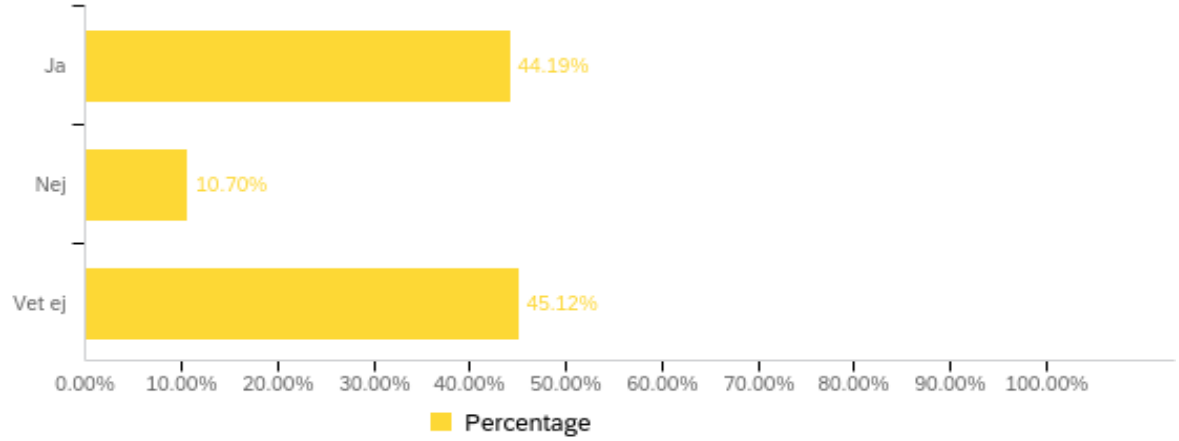
Fråga 5 - Har ni skriftliga rutiner för hur ni ska agera om ni kommer i kontakt med en person med skyddade personuppgifter?



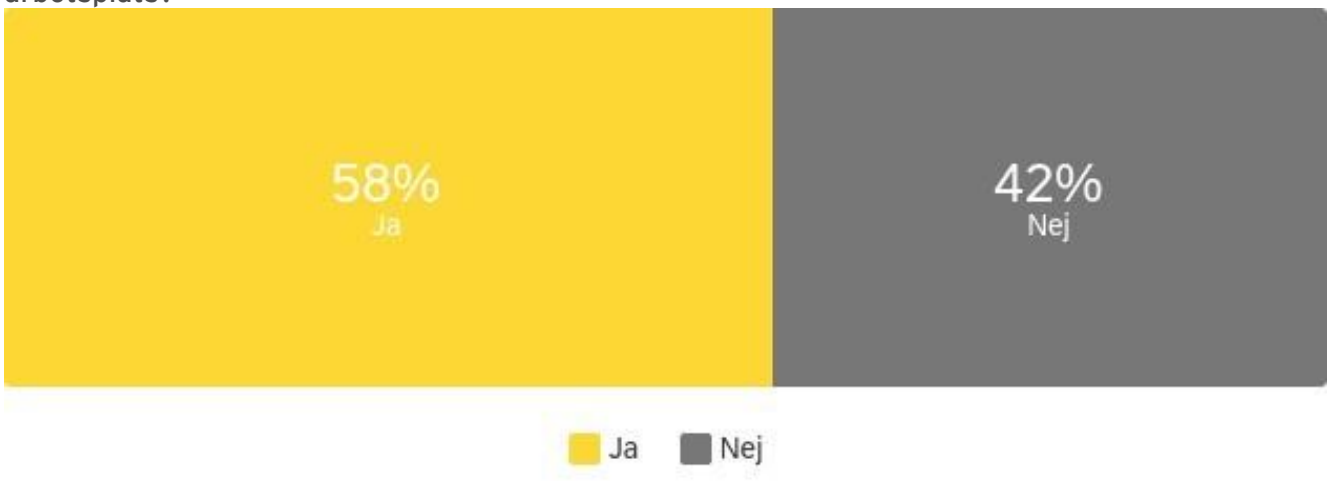

Fråga 6 - Vet du var du hittar dessa skriftliga rutiner?



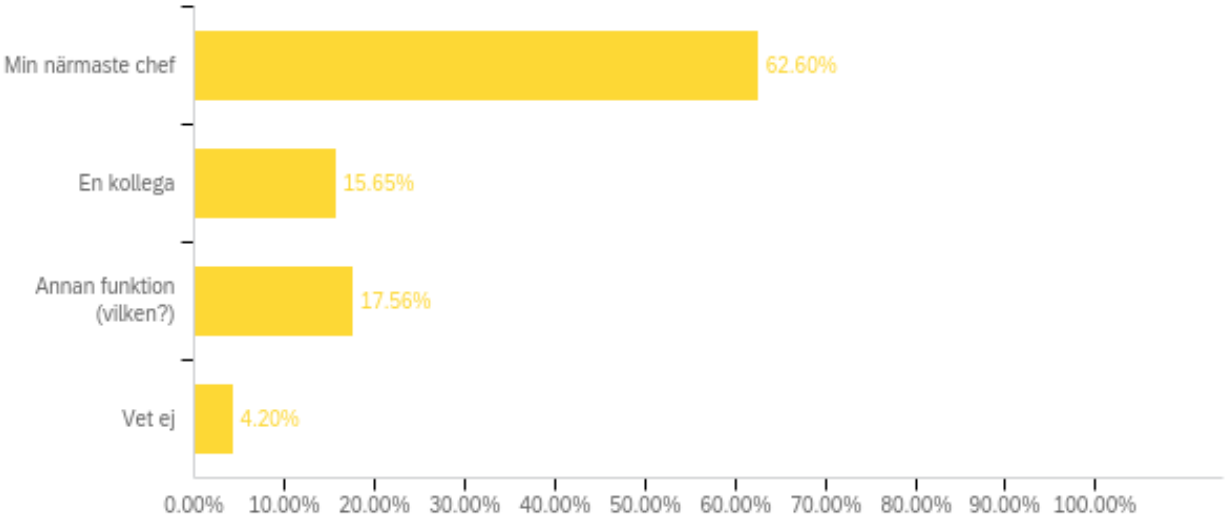

Fråga 7 - Får du det stöd du behöver av dessa rutiner?



Fråga 8 - Vet du vem som ansvarar för hantering av skyddade personuppgifter på din arbetsplats?




Fråga 9 - Vem vänder du dig till vid frågor om hantering av skyddade personuppgifter på din arbetsplats? (Här kan du välja en eller flera svarsalternativ)

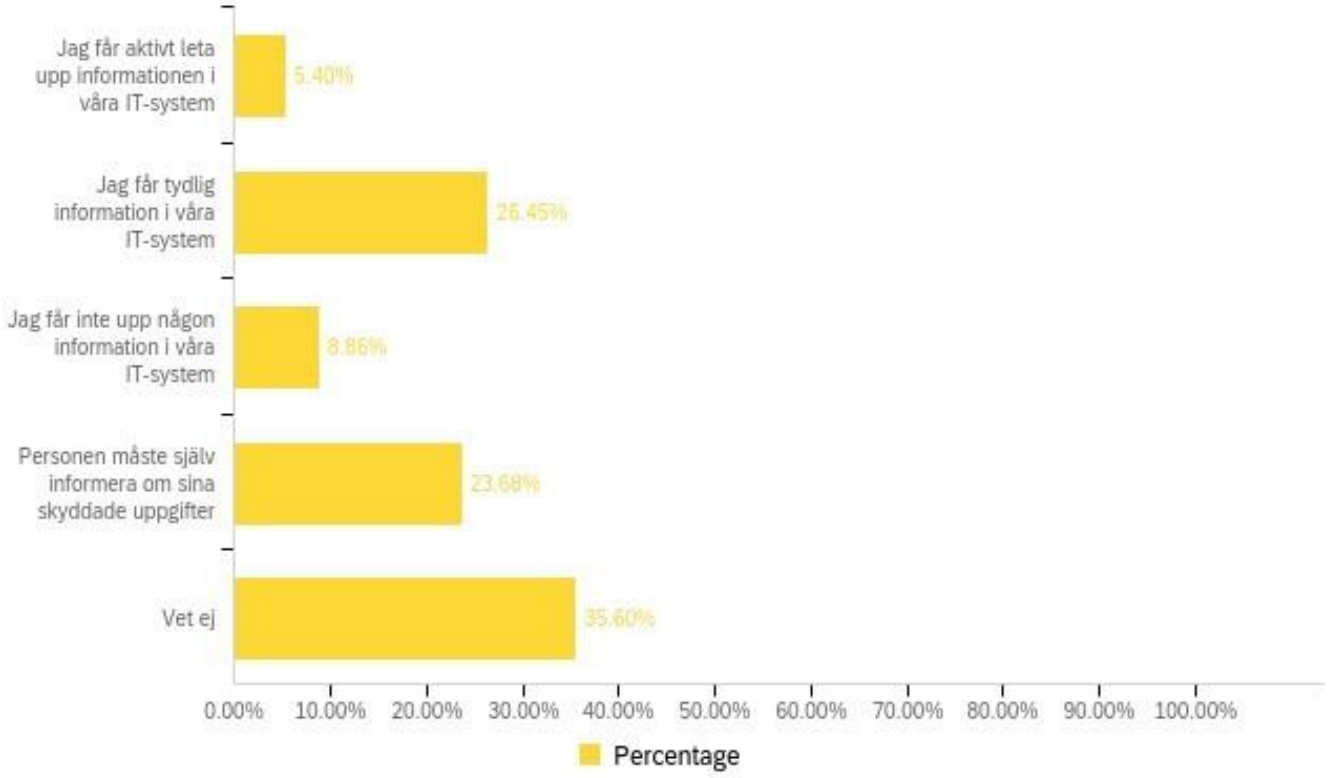



Fråga 9 - Annan funktion (vilken?)

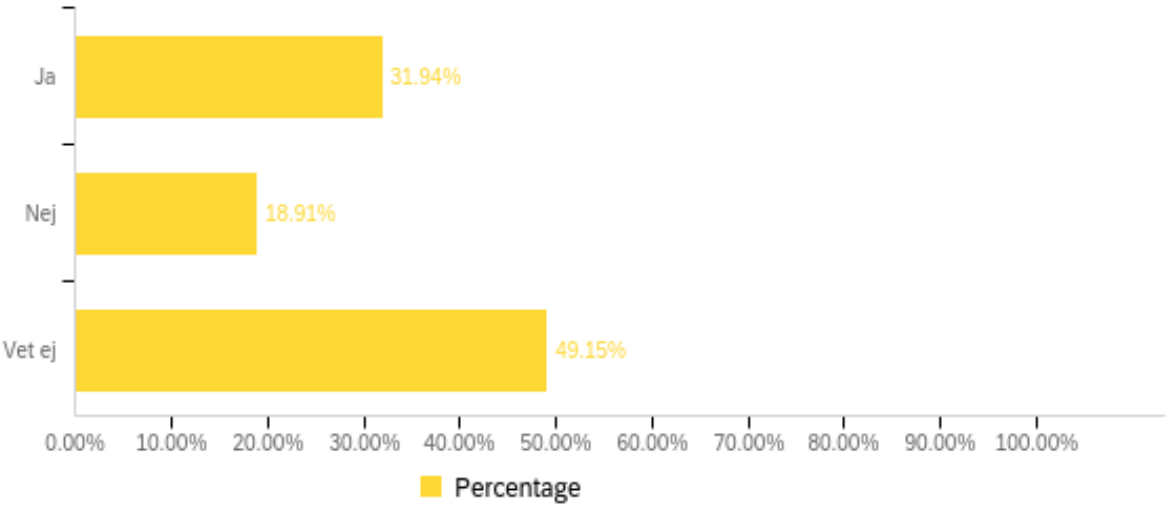
I alternativet gällande annan funktion fick enkätrespondenterna svara fritt. Följande är de mest förekommande svaren:

- HR
- Administration
- Dataskyddsomdud/koordinator/samordnare
- Jurist

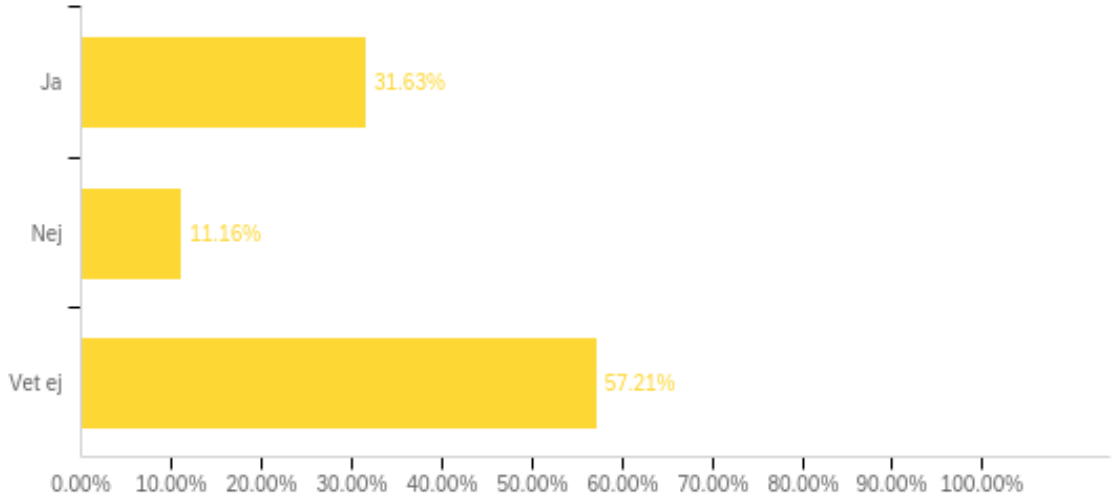
Fråga 10 - Hur blir du informerad om att en person du kommer i kontakt med har skyddade personuppgifter? (Här kan du välja en eller flera svarsalternativ)



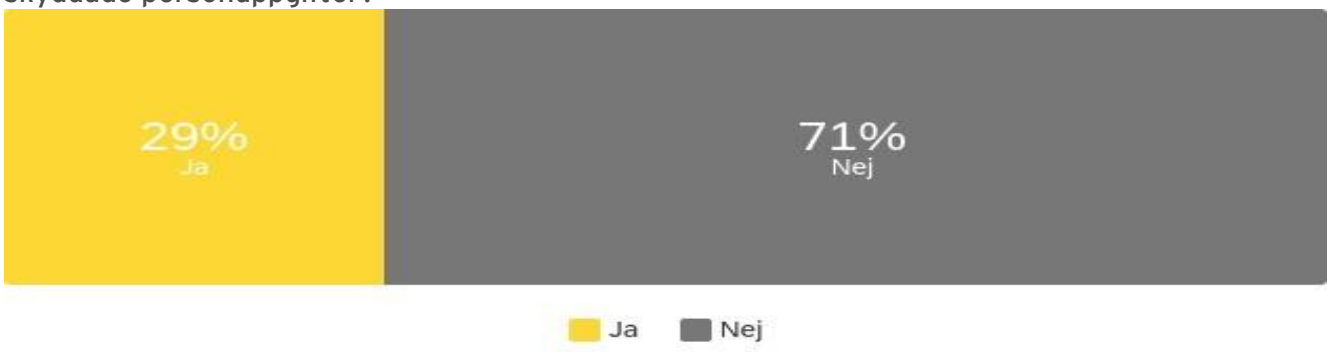

Fråga 11 - Framgår det tydligt i era IT-system vilka personuppgifter som är skyddade?



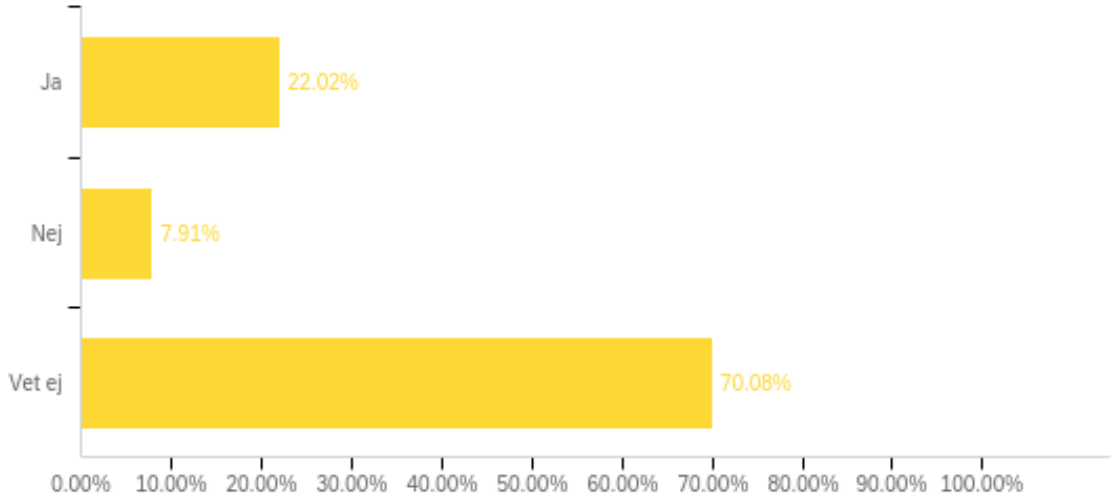
Fråga 12 - Särmarkeras personuppgifter i era IT-system? Exempelvis "skyddad folkbokföring" eller "sekretessmarkering"



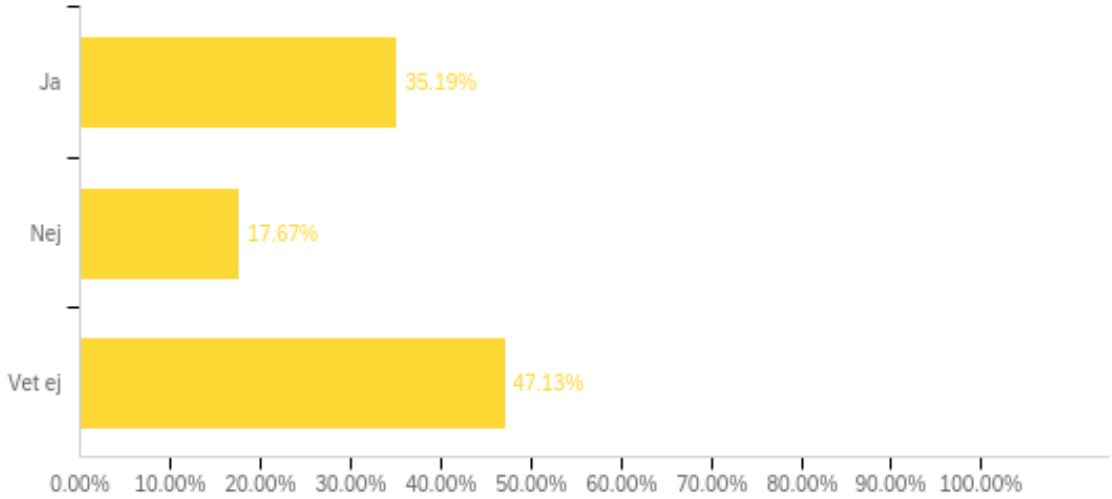

Fråga 13 - Vet du var du ska registrera eventuell röjning/avvikelse av hanteringen av skyddade personuppgifter?




Fråga 14 - Finns det rutiner för uppföljning av eventuella röjningar/avvikelser av hanteringen av skyddade personuppgifter?



**Fråga 15 - Även medarbetare kan ha skyddade personuppgifter, känner du dig trygg med rutinerna för hur medarbetares skyddade personuppgifter hanteras?**




**Fråga 16 - Övriga kommentarer gällande hanteringen av skyddade personuppgifter**
Här redovisas ett antal övriga kommentarer som respondenterna valde att skriva:
*"Vi behöver tydliga rutiner och utbildning"*
*"Det är väldigt lite information man får som medarbetare kring detta ämne. Som medarbetare får man ta reda på själv mycket själv för att veta hur man ska hantera och agera. jag tycker att det är viktigt att informationen kommer till alla som är eller blir berörda kring informationen som finns, för att veta hur man ska agera"*
*"Vi har aldrig pratat om personer med skyddade personuppgifter"*

*" Mer kunskap behövs"*

*"Alla rutiner behöver ses över och informeras till personalen"*

*"Jag arbetar i barngrupp och rör mig inte i så många it system men har fått info av barnplacerare/ lagledare vid behov och då tagit reda på vad som gäller samt haft en ständig dialog med förälder i förekommande fall"*

*"Det nya verksamhetssystemet och kommunens skrivare/scanner som infördes för drygt ett år sedan medför risker för att skyddade personuppgifter kan komma att röjas"*

*"I mitt arbete hanterar jag nästan aldrig andra personuppgifter än namn och kontaktuppgifter som e-postadress och telefonnummer. Personnummer och hemadress förekommer ytterst sällan. Därmed får jag heller inte info om ev. skyddade personuppgifter om inte någon själv skulle uppge det (vilket hittills inte har hänt). Däremot har jag själv skyddade personuppgifter. Mina kollegor känner till det, men jag tror både min och deras kunskap om hur det ska hanteras är låg"*

*"...det går att komma åt uppgifter om låntagare i systemen från bibliotek i kommunen och bibliotek i andra kommuner inom södertörnssamarbetet. Jag informeras muntligt om elever med skyddad identitet och tömmer då systemet på uppgifter. Alias och lånekort kvarstår. Samma lika vid skapande av nya låntagarkonton"*
*"Elever med skyddad identitet saknas helt i alla system vi använder inom skolan"*

*"Våra huvudsakliga problem ligger i konflikten mellan lagar som rör skyddade*

*personuppgifter och skollagen. Skollagen kräver att vi tillhandahåller materiel för eleverna som behövs för undervisning. Elever med skyddade personuppgifter får inte det materialet eftersom att informationen går via oskyddade system. Vi bryter alltså mot lagen oavsett hur vi gör"*

*"Vi vet ingenting om detta ämne"*
*"Jag har aldrig under 8 års tid varit i kontakt med någon med skyddade personuppgifter men vi har rutiner för hur det ska hanteras ifall att vi får in någon med skyddade personuppgifter"*

*"När jag kommit i kontakt med personer med skyddad identitet "syns" inga uppgifter varken digitalt eller via anteckningar för oss medarbetare"*

*"Kommunen har inget fungerande sätt för elever med skyddad identitet att få tillgång till samma plattformar som alla andra elever har, till exempel v- klass eller Teams. Det är under all kritik och går ut över dessa elevers rättigheter att få samma möjligheter som alla andra"*

*"Det är ytterst få i arbetsgruppen som kan se sekretessmarkerade personers uppgifter. Övriga kan inte ens söka info i systemet. Om du inte får upp någon info när du slår på ett personnummer så lämnas handlingarna direkt till ansvarig gruppledare vare sig det rör sig om sekretess eller att personen inte är aktuell hos oss. Handlingarna lämnas vidare till berörd handläggare av gruppledare. Allt för att säkerställa att personen inte röjs av misstag"*