Kumla kommun

Dataskyddsombudets granskning 2026

Efterlevnad av dataskyddslagstiftningen

Allmän granskningsrapport

Beslutande	Dataskyddsombud
Datum	2026-09-02
Gäller till	Tills vidare

Innehåll

Dataskyddsombudets granskning 2026 **1**

Efterlevnad av dataskyddslagstiftningen 1

Bakgrund **4**

Inledning och syfte 4

Dataskyddsombudets roll och ansvar 5

Avgränsning 5

Metod 5

Personuppgiftsincidenter **5**

Definition 5

Anmäla en personuppgiftsincident till tillsynsmyndigheten 6

Information till den registrerade om personuppgiftsincidenten 7

Säkerhetsåtgärder 8

Identifierande förbättringsområden **9**

Kommunikation av personuppgifter via extern meddelandetjänst 9

Felregistrering av personuppgifter 11

Kvarglömda personuppgifter 12

Bakgrund

Inledning och syfte

Dataskyddsförordningen (GDPR) trädde i kraft den 25 maj 2018 och syftar bland annat till att skydda fysiska personers grundläggande rättigheter och friheter, särskilt rätten till skydd av personuppgifter. Rätten till privatliv kommer till uttryck i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR), som är införlivad i svensk rätt. Den framgår även av EU:s stadga om de grundläggande rättigheterna, där rätten till respekt för privat- och familjeliv kommer till uttryck. Stadgan innehåller även en särskild bestämmelse om rätt till skydd för personuppgifter och är rättsligt bindande för EU:s medlemsstater. På svensk nivå finns en grundlagsstadgad rätt till skydd av den personliga integriteten vid behandling av personuppgifter i regeringsformen. Dessa bestämmelser utgör grunden för den mer detaljerade regleringen i dataskyddsförordningen.

Dataskyddsförordningen omfattar alla uppgifter som direkt eller indirekt kan kopplas till en fysisk person och reglerar all behandling av sådana personuppgifter, såsom insamling, lagring, användning och radering. Förordningen gäller både behandling som sker genom automatiserade processer och annan icke-automatiserad behandling av personuppgifter som ingår i, eller är avsedda att ingå i, ett register.

Förordningen ställer strikta krav på hur personuppgifter får behandlas. Behandlingen ska ske i enlighet med de grundläggande principerna i förordningen, vilket bland annat innebär att den ska ha ett tydligt och avgränsat ändamål, begränsas till nödvändiga uppgifter och vila på en rättslig grund. Förordningen ställer även krav på att den registrerades rättigheter respekteras, såsom rätten till tillgång till sina uppgifter och rätten till radering.

Personuppgifter ska dessutom behandlas på ett säkert sätt, vilket innebär att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna mot obehörig åtkomst, förlust och andra säkerhetsincidenter. Om personuppgifter behandlas av en extern leverantör ska ett personuppgiftsbiträdesavtal (PUB-avtal) upprättas. Vid personuppgiftsincidenter ska dessa, under vissa förutsättningar, anmälas till Integritetsskyddsmyndigheten (IMY). Organisationer som inte uppfyller kraven i förordningen riskerar att åläggas administrativa sanktionsavgifter.

Mot denna bakgrund har en granskning genomförts av kommunens dataskyddsombud (DSO/DPO) i syfte att granska och bedöma organisationens dataskyddsarbete i förhållande till dataskyddsförordningens krav, med fokus

på hanteringen av personuppgiftsincidenter enligt artiklarna 33 och 34 i GDPR.

Dataskyddsombudets roll och ansvar

Dataskyddsombudets uppdrag regleras i artiklarna 38 och 39 i GDPR och ska utföras självständigt och oberoende. En central del av uppdraget är att övervaka organisationens efterlevnad av förordningen, vilket bland annat innefattar att genomföra granskningar.

Avgränsning

Granskningen har avgränsats till organisationens hantering av personuppgiftsincidenter, med särskilt fokus på artiklarna 33 och 34 i GDPR.

Andra relevanta områden ur ett dataskyddsperspektiv, såsom personuppgiftsbiträdesavtal (PUB-avtal), hantering av registrerades rättigheter, konsekvensbedömningar (DPIA) samt interna styrdokument, omfattas inte av denna granskning men kan komma att granskas vid ett senare tillfälle.

Metod

Granskningen har utgått från de krav som följer av artiklarna 33 och 34 i GDPR. Som stöd för bedömningen har vägledning från Artikel 29-gruppens riktlinjer, relevant lagkommentar, förarbeten samt praxis beaktats.

Berörda nämnder har rapporterat in till dataskyddsombudet en sammanställning av hanterade personuppgiftsincidenter under perioden 2025-10-31 - 2026-04-24.

Granskningen har sedan genomförts genom stickprovskontroller av personuppgiftsincidenter. Dataskyddsombudets granskningsarbete har bedrivits under perioden 2026-04-17 -2026-05-30.

Personuppgiftsincidenter

Definition

En personuppgiftsincident definieras i artikel 4.12 i GDPR som ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”.

Personuppgiftsincidenter kan ta sig många olika uttryck, exempelvis genom att personuppgifter skickas till fel mottagare, att obehöriga får tillgång till system som innehåller personuppgifter, att information går förlorad till följd

av bristande säkerhetskopiering, att personuppgifter publiceras av misstag eller att tillgängligheten till personuppgifter påverkas, exempelvis genom driftstörningar eller ransomwareattacker.

Gemensamt för dessa händelser är att den personuppgiftsansvarige inte längre fullt ut kan säkerställa konfidentialitet, integritet eller tillgänglighet vid behandlingen av personuppgifter. Det bör även beaktas att en och samma personuppgiftsincident, beroende på omständigheterna i det enskilda fallet, kan påverka personuppgifters konfidentialitet, integritet och tillgänglighet samtidigt eller i olika kombinationer.[1] En personuppgiftsincident skiljer sig från andra säkerhetsincidenter genom att den påverkar personuppgifter och därigenom kan medföra risker för de registrerades rättigheter och friheter.

Anmäla en personuppgiftsincident till tillsynsmyndigheten

Enligt artikel 33 i GDPR ska den personuppgiftsansvarige anmäla en personuppgiftsincident till tillsynsmyndigheten utan onödigt dröjsmål och, om möjligt, senast 72 timmar efter att ha fått vetskap om incidenten, såvida det inte är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter. Om en personuppgiftsincident inträffar hos ett personuppgiftsbiträde ska biträdet utan onödigt dröjsmål underrätta den personuppgiftsansvarige efter att ha fått vetskap om incidenten.

Skyldigheten att anmäla en personuppgiftsincident gäller inte i alla situationer, utan förutsätter att incidenten sannolikt medför en risk för de registrerades rättigheter och friheter. Exempel på sådana risker är diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende samt förlust av konfidentialitet avseende personuppgifter som omfattas av tystnadsplikt.[2]

Beroende på det enskilda fallet och omständigheterna kan risken och allvarlighetsgraden variera. Exempelvis anses incidenter som rör uppgifter om hälsa typiskt sett medföra en sannolik risk för de registrerades rättigheter och friheter.[3] Därför ska en riskbedömning av personuppgiftsincidenten göras där flera omständigheter beaktas, exempelvis typen av incident, personuppgifternas natur, känslighet och omfattning samt konsekvensernas allvarlighetsgrad för de berörda individerna.[4]

En anmälan om en personuppgiftsincident till tillsynsmyndigheten ska innehålla följande uppgifter enligt artikel 33.3 i GDPR:

---

[1] Artikel 29-Arbetsgruppen för uppgiftsskydd, riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679 s. 7-8.
[2] Skäl 75 i GDPR.
[3] Artikel 29-Arbetsgruppen för uppgiftsskydd, riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679 s. 24.
[4] Artikel 29-Arbetsgruppen för uppgiftsskydd, riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679 s. 25-27.

a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om samtliga uppgifter inte kan tillhandahållas samtidigt får de lämnas i omgångar utan onödigt ytterligare dröjsmål.

Den personuppgiftsansvarige ska vidare dokumentera samtliga personuppgiftsincidenter, inklusive omständigheterna kring incidenten, dess sannolika effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska möjliggöra tillsynsmyndighetens kontroll av efterlevnaden av artikel 33 i GDPR.

Information till den registrerade om personuppgiftsincidenten

Enligt artikel 34 i GDPR ska den personuppgiftsansvarige utan onödigt dröjsmål informera de registrerade om en personuppgiftsincident, om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Syftet med informationen till enskilda är att ge dem specifik information om de åtgärder de bör vidta för att skydda sig själva.[5]

Tröskeln för att informera de berörda personerna är högre än för att anmäla incidenten till tillsynsmyndigheterna och inte alla personuppgiftsincidenter behöver därför meddelas enskilda personer. På så sätt slipper dessa tröttas ut av onödig information.

Artikel 29-gruppen har lämnat exempel på personuppgiftsincidenter som typiskt sett kan anses medföra en hög risk för de registrerades rättigheter och friheter. Bland annat anges följande situationer:

- En personuppgiftsansvarig driver en digital marknadsplats med kunder i flera medlemsstater. Marknadsplatsen utsätts för ett it-angrepp varvid angriparen publicerar användarnamn, lösenord och köphistorik på internet.

[5] Skäl 86 i GDPR.

- Patientjournaler vid ett sjukhus blir otillgängliga under en längre period, exempelvis 30 dagar, till följd av ett it-angrepp.[6]

Information som lämnas till den registrerade ska innehålla en klar och tydlig beskrivning av personuppgiftsincidentens art samt minst de uppgifter som anges i artikel 33.3 b-d i GDPR. Detta omfattar kontaktuppgifter till dataskyddsombudet eller annan kontaktpunkt, en beskrivning av incidentens sannolika konsekvenser samt en redogörelse för de åtgärder som har vidtagits eller föreslagits för att hantera incidenten och begränsa dess negativa effekter.

Information till de registrerade är dock inte nödvändigt om något av undantagen i artikel 34.3 i GDPR är tillämpligt. Detta gäller exempelvis om den personuppgiftsansvarige har vidtagit lämpliga tekniska och organisatoriska skyddsåtgärder som gör de berörda personuppgifterna oläsbara för obehöriga, såsom kryptering, eller om ytterligare åtgärder har vidtagits som säkerställer att den höga risken för de registrerades rättigheter och friheter sannolikt inte längre föreligger. Undantag kan även tillämpas om individuell information till de registrerade skulle innebära en oproportionerlig ansträngning. I sådana fall ska informationen i stället lämnas genom ett offentligt meddelande eller en likvärdig åtgärd som säkerställer att de registrerade informeras på ett lika effektivt sätt.[7]

Säkerhetsåtgärder

Artikel 33.2 GDPR anger att den personuppgiftsansvarige ska kunna redovisa vilka åtgärder som har vidtagits eller planeras för att hantera en personuppgiftsincident och begränsa dess negativa effekter. Kravet illustrerar att incidenthantering inte enbart handlar om dokumentation och anmälan, utan även om att identifiera och genomföra åtgärder som minskar riskerna för de registrerade.

Detta hänger nära samman med kraven i artikel 32 GDPR. Bestämmelsen innebär att organisationer ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att förebygga de risker som kan leda till personuppgiftsincidenter. När en incident inträffar bör verksamheten därför inte bara hantera den enskilda händelsen utan även bedöma om incidenten visar på brister i befintliga säkerhetsåtgärder och om ytterligare skyddsåtgärder behöver införas.

IMY:s tillsyn av Sportadmin illustrerar detta samband. Även om tillsynen föranleddes av en personuppgiftsincident kom granskningen att omfatta bolagets efterlevnad av artikel 32 GDPR. IMY konstaterade att det hade funnits brister i säkerhetsarbetet redan före intrånget, vilket visar att en

[6] Artikel 29-Arbetsgruppen för uppgiftsskydd, riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, Bilaga B.
[7] Artikel 29-Arbetsgruppen för uppgiftsskydd, riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, s. 21-22.

personuppgiftsincident inte bara aktualiserar skyldigheter enligt artikel 33 utan även kan leda till en prövning av om verksamhetens säkerhetsnivå varit tillräcklig.

Identifierande förbättringsområden

Kommunikation av personuppgifter via extern meddelandetjänst

Medarbetare har kommunicerat personuppgifter med andra medarbetare via en extern meddelandetjänst. Personuppgifterna avsåg både vanliga och känsliga personuppgifter. I incidentutredningen beskrivs händelsen som ett obehörigt röjande av personuppgifter.

Dataskyddsombudet vill understryka att händelsen kan omfatta två personuppgiftsincidenter. Den första avser ett obehörigt röjande till tredje part genom att personuppgifter har kommunicerat via en extern meddelandetjänst. Den andra avser ett obehörigt röjande av personuppgifter till de medarbetare som var med i gruppen i den externa meddelandetjänst där personuppgifterna kommunicerades. Enligt incidentutredningen har endast händelsen med det obehöriga röjandet via den externa meddelandetjänsten hanterats. Detta medför en risk för att incidenten inte hanteras rätt och att den registrerades rättigheter samt den personuppgiftsansvariges skyldigheter enligt dataskyddslagstiftningen inte fullt ut beaktas. Det är därför viktigt att vid en incidenthantering som rör ett obehörigt röjande att identifiera samtliga mottagare av personuppgifterna. Dataskyddsombudet kommer att bedöma hanteringen utifrån röjande till tredje part, då röjande av personuppgifter till andra medarbetare inte har hanterats i incidentutredningen.

Vidare har dataskyddsombudet noterat att det inte tydligt framgår av incidentutredningen när den personuppgiftsansvarige fick vetskap om incidenten. Detta är viktigt eftersom det avgör när 72-timmarsfristen för anmälan till tillsynsmyndigheten börjar löpa. Artikel 29-arbetsgruppen anser att en personuppgiftsansvarig ska anses ha fått vetskap när den personuppgiftsansvarige är rimligt säker på att en säkerhetsincident har ägt rum som har medfört att personuppgifter äventyrats.[8]

I vissa fall kan den personuppgiftsansvarige anses ha fått vetskap redan vid första rapporteringen. I andra fall kan det krävas en kortare utredning för att fastställa om en personuppgiftsincident faktiskt har inträffat. Under denna undersökningsperiod kan den personuppgiftsansvarige inte anses ha fått vetskap om incidenten. Man kan dock förvänta sig att den inledande undersökningen ska inledas så snart som möjligt och med en rimlig grad av

[8]Artikel 29-arbetsgruppens riktlinjer om anmälan av personuppgiftsincidenter (s. 11).

säkerhet fastställa huruvida en incident har ägt rum. Detta kan sedan följas av en mer ingående undersökning.

Dataskyddsombudet vill understryka att i artikel 33.1 i GDPR klargörs att om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” behöver incidenterna inte anmälas till tillsynsmyndigheten. Ett exempel kan vara när personuppgifter redan är allmänt tillgängliga och utlämnandet av sådana uppgifter inte innebär en sannolik risk för den enskilde. Ett annat exempel är när personuppgifterna är krypterade och krypteringsnyckeln inte har äventyrats, vilket innebär att uppgifterna är oläsbara för obehöriga och därför är det osannolikt att incidenten medför skada för de registrerade.[9]

Dataskyddsombudet anser att incidentutredningen saknar en utredning av huruvida den externa meddelandetjänsten använder kryptering. Detta är en viktig omständighet vid riskbedömningen eftersom kryptering kan undanröja risken för obehörig åtkomst till personuppgifterna under överföring. Dataskyddsombudet anser dock att personuppgifterna har röjts för leverantören av den externa meddelandetjänsten oavsett om kryptering har använts. Eftersom det är sannolikt att leverantören har tillgång till de krypteringsnycklar som krävs för att dekryptera meddelandena och därmed kan få åtkomst till de personuppgifter som har kommunicerats. Personuppgifter som därmed har varit åtkomliga för obehöriga bör som utgångspunkt anses ha tagits del av, om det inte finns omständigheter som talar för motsatsen. Därför bedömer dataskyddsombudet att som huvudregel ska incidenten anmälas till tillsynsmyndigheten gällande röjandet via den externa meddelandetjänsten.

Utöver att bedöma om en personuppgiftsincident ska anmälas till tillsynsmyndigheten ska den personuppgiftsansvarige även ta ställning till om de registrerade ska informeras. För att sådan information ska krävas måste personuppgiftsincidenten sannolikt medföra en hög risk för de registrerades rättigheter och friheter, vilket är ett högre krav än för anmälan till tillsynsmyndigheten, där anmälningsskyldighet föreligger om personuppgiftsincidenten medför en sannolik risk för de registrerades rättigheter och friheter.

Vad som utgör en hög risk är en bedömningsfråga som behöver avgöras utifrån flera omständigheter,[10] exempelvis hur lätt det är att identifiera enskilda personer. Dataskyddsombudet anser att incidentutredningen saknar en bedömning av hög risk, vilket innebär en otydlighet i dokumentationen av incidenthanteringen och försvårar bedömningen av om skyldigheterna enligt artikel 34 i GDPR har uppfyllts.

---

[9] Artikel 29-arbetsgruppens riktlinjer om anmälan av personuppgiftsincidenter (s. 19)
[10] Artikel 29-arbetsgruppens riktlinjer om anmälan av personuppgiftsincidenter (s. 23-27).

Dataskyddsombudet bedömer att risken inte är hög eftersom leverantören är en etablerad aktör i världen med dokumenterade säkerhetsåtgärder, rutiner och policyer för behandling av personuppgifter. Det har inte heller framkommit några omständigheter som indikerar förhöjd risk för de registrerades rättigheter och friheter. Även om det även finns en teoretisk möjlighet att amerikanska myndigheter kan begära tillgång till uppgifterna, bedöms sannolikheten för detta som begränsad eftersom en sådan åtkomst normalt förutsätter en rättslig grund och ett formellt förfarande. Det finns heller inga omständigheter i det aktuella ärendet som tyder på att uppgifterna skulle vara föremål för ett sådant intresse.

Felregistrering av personuppgifter

En medarbetare har registrerat fel personuppgifter i ett verksamhetssystem med begränsad åtkomst. Personuppgifterna avsåg både vanliga, skyddsvärda och känsliga personuppgifter. I incidentutredningen beskrivs händelsen som ett obehörigt röjande av personuppgifter.

Dataskyddsombudet vill understryka att en personuppgiftsincident definieras enligt artikel 4.12 i GDPR som *"en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats*". Ett obehörigt röjande innebär att personuppgifter lämnas ut eller blir åtkomliga för personer som saknar behörighet att ta del av dem. Det kan exempelvis handla om att personuppgifter görs tillgängliga för medarbetare inom verksamheten som inte har rätt att få tillgång till uppgifterna.

Enligt incidentutredningen har ingen obehörig tagit del av personuppgifterna. Det anges dock att det finns en risk för detta genom en begäran om utlämnande av allmän handling, men någon sådan begäran har inte inkommit och något utlämnande har inte heller skett. Dataskyddsombudet anser att bedömningen av incidentens typ ska utgå från de faktiska omständigheter som har inträffat. Samtidigt ska potentiella risker för de registrerade beaktas i den fortsatta riskbedömningen. I detta fall finns det inget som tyder på att obehöriga har tagit del av personuppgifterna. Däremot har uppgifternas riktighet påverkats, varför händelsen bör bedömas utgöra en ändring av personuppgifter snarare än ett röjande av personuppgifter.
Dataskyddsombudet anser att eftersom typ av incident har beskrivits felaktigt har det påverkat incidenthanteringen i sin helhet, vilket kan medföra bristande efterlevnad av dataskyddslagstiftningen. Dataskyddsombudet kan inte ta ställning till riskbedömningen eftersom incidenten har beskrivits felaktigt och det därmed saknas tillräckligt underlag för att bedöma risken för de registrerade.

Vidare noterar dataskyddsombudet att anmälan till tillsynsmyndigheten gjordes innan incidentutredningen var färdig. Anledningarna till detta kan

vara olika, exempelvis tidspress eller i förbyggande syfte. Enligt artikel 33.3 i GDPR ska vissa uppgifter lämnas till tillsynsmyndigheten vid anmälan av en personuppgiftsincident. Om samtliga uppgifter inte finns tillgängliga vid anmälningstillfället får de lämnas i flera omgångar och kompletteras så snart de blivit tillgängliga.

Det är den personuppgiftsansvarigas ansvar att se till att kompletterande uppgifter lämnas in till tillsynsmyndigheten. Om sådana uppgifter inte kommer in inom cirka fyra veckor kan tillsynsmyndigheten komma att handlägga ärendet och fatta beslut utifrån den information som redan har lämnats. Detta kan innebära att nya uppgifter som framkommer under den fortsatta incidentutredningen och som kan vara av betydelse för bedömningen av incidenten och de vidtagna åtgärderna, inte nödvändigtvis beaktas i tillsynsmyndighetens handläggning.[11]

I detta fall framgår det inte i incidentutredningen om den initiala anmälan har kompletterats. Detta innebär en otydlighet i dokumentationen av incidenthanteringen och försvårar bedömningen av om skyldigheterna enligt artikel 33 i GDPR har uppfyllts.

Kvarglömda personuppgifter

En arbetsanteckning har lämnats kvar av en medarbetare i verksamhetens lokaler med begränsat tillträde och därefter hittats av en annan medarbetare. Anteckningen innehöll vanliga och känsliga personuppgifter. I incidentutredningen beskrivs händelsen som ett obehörigt röjande av personuppgifter.

Enligt incidentutredningen bedöms personuppgiftsincidenten medföra en risk för att den registrerade förlorar kontrollen över sina personuppgifter, att ett konfidentialitetsbrott uppstår, att den registrerades anseende skadas samt att personuppgifterna kan användas för bedrägerier. Motiveringen till bedömningen är att obehöriga har fått åtkomst till personuppgifter som är känsliga och rör sårbara registrerade. Enligt incidentutredningen ska personuppgiftsincidenten anmälas till tillsynsmyndigheten. Incidentutredningen bedömer däremot att de registrerade inte behöver informeras om incidenten, eftersom personuppgifterna har röjts enbart inom den egna verksamheten och mottagarna omfattas av sekretess- och tystnadsplikt.

Dataskyddsombudet vill understryka att en personuppgiftsincident ska anmälas till IMY om det inte är osannolikt att incidenten medför en risk för de registrerades rättigheter och friheter. Enligt Artikel 29-arbetsgruppens riktlinjer ska personuppgiftsincidenter som rör känsliga personuppgifter enligt artikel 9 i GDPR som utgångspunkt anses medföra en sannolik risk för

[11] Hantering av personuppgiftsincidenter | IMY

de registrerades rättigheter och friheter.[12] Som huvudregel ska därför en personuppgiftsincident som rör känsliga personuppgifter anmälas till tillsynsmyndigheten.

Det kan dock finnas omständigheter som kan minska risknivån,[13] exempelvis vilka mottagarna är. I detta fall har personuppgifter varit åtkomliga för anställda inom den egna verksamheten. Därför bör det bedömas om dessa mottagare kan anses vara betrodda mottagare. Att mottagaren är betrodd kan innebära att incidentens allvarlighetsgrad minskar, men det innebär inte att någon personuppgiftsincident inte har inträffat. Om mottagaren kan anses vara betrodd kan det dock undanröja sannolikheten för en risk för enskilda, och det är därför inte längre nödvändigt att anmäla incidenten till tillsynsmyndigheten, eller informera de personer som påverkas. [14]

Med betrodda mottagare avses när personuppgiftsansvarige har ett pågående förhållande med mottagarna och känner till deras rutiner, historik och andra relevanta detaljer. Den personuppgiftsansvarige kan då begära att mottagaren antingen skickar tillbaka de uppgifter som mottagits eller på ett säkert sätt förstör dem. Den personuppgiftsansvarige kan med andra ord i viss grad vara säker på att mottagaren inte kommer att läsa eller försöka få åtkomst till de uppgifter som felaktigt skickats till dem, utan följa instruktionerna och skicka tillbaka uppgifterna.

Dataskyddsombudet bedömer att personuppgifterna, enligt incidentutredningen, har röjts enbart inom den egna verksamheten. Mottagarna omfattas av samma sekretesskydd avseende uppgifter om enskilda samt av samma krav på dataskydd och informationssäkerhet. Det finns dessutom inga indikationer på att uppgifterna har behandlats på annat otillåtet sätt efter röjandet. Mot denna bakgrund bedöms mottagarna vara betrodda mottagare. Dataskyddsombudets bedömning är därför att personuppgiftsincidenten inte medför någon sannolik risk för de registrerades rättigheter och friheter och att incidenten därmed inte behöver anmälas till tillsynsmyndigheten. Av samma skäl bedöms det inte heller vara nödvändigt att informera de registrerade om incidenten.

Dataskyddsombudet vill betona vikten av säkerhetsåtgärder. En enskild incident kan vara resultatet av ett misstag eller en tillfällig brist, men när liknande incidenter inträffar upprepade gånger kan det tyda på brister i verksamhetens arbetssätt, rutiner eller organisation. När incidenter av samma eller liknande slag återkommer bör fokus därför inte enbart riktas mot individrelaterade åtgärder, såsom information eller påminnelser till enskilda

[12] Artikel 29-arbetsgruppens riktlinjer om anmälan av personuppgiftsincidenter (s. 24).
[13] Artikel 29-arbetsgruppens riktlinjer om anmälan av personuppgiftsincidenter (s. 23-27).
[14] Artikel 29-Arbetsgruppen för uppgiftsskydd, riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, s 26.

medarbetare. Verksamheten bör även göra en bredare översyn av arbetssätt, rutiner och tekniska eller organisatoriska skyddsåtgärder.

Exempel på åtgärder som kan övervägas är att:

- se över och tydliggöra rutiner för hantering, förvaring och kommunikation av personuppgifter,
- införa gemensamma och praktiska kontrollmoment, exempelvis dagliga kontroller för att säkerställa att känsliga handlingar inte har lämnats framme eller kommit bort,
- tillhandahålla ändamålsenliga hjälpmedel för säker förvaring, såsom pärmar, låsbara skåp eller andra skyddande lösningar,
- samt, där det är möjligt och lämpligt, digitalisera arbetsprocesser som idag är beroende av omfattande pappershantering.

För verksamheter som behandlar känsliga personuppgifter är det särskilt viktigt att inte bara vidta åtgärder för att minska risken för incidenter, utan även att regelbundet följa upp och utvärdera åtgärdernas effektivitet. Utan sådan uppföljning finns en risk att brister kvarstår och att verksamheten inte kan bedriva personuppgiftsbehandlingen på ett tillräckligt säkert och effektivt sätt.