Granskning av kommunens styrdokument avseende personuppgiftsincidenter inom ramen för GDPR

Rapport

Perstorps kommun

KPMG AB

2022-05-18

Antal sidor 17

Perstorps kommun
Granskning av kommunens styrdokument avseende personuppgiftsincidenter inom ramen för

2022-05-18

Innehållsförteckning

1 Sammanfattning

KPMG har av Perstorps kommuns revisorer fått i uppdrag att granska kommunens rutiner med fokus på personuppgiftsincidenter inom ramen för dataskyddsförordningen.

Syftet med granskningen är att undersöka om kommunstyrelsen på ett ändamålsenligt sätt har säkerställt följsamhet till dataskyddsförordningen med inriktning på personuppgiftsincidenter.

Vår sammanfattande bedömning utifrån granskningens syfte är att hanteringen av personuppgiftsincidenter inte är på en tillfredställande nivå, där kommunstyrelsen behöver vidta åtgärder i syfte att säkerställa en korrekt dokumentation och hantering av personuppgiftsincidenter.

Vi bedömer att det finns behov av kunskapsökning bland medarbetarna i kommunens verksamheter gällande identifiering och hantering av personuppgiftsincidenter. Vidare erfordras utbildningsinsatser för utsedda dataskyddssamordnare i syfte att kunna hantera sitt uppdrag på ett tillfredställande sätt.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Fastställa ett kommunövergripande styrdokument avseende hantering, bedömning och dokumentation av personuppgiftsincidenter (se avsnitt 3.1.1). Det bör noteras att dokumentation och riskbedömning av samtliga personuppgiftsincidenter är obligatorisk.
- Säkerställa en korrekt dokumentation genom fastställande av en kommunövergripande mall innehållande centrala frågor i enlighet med avsnitt 3.4.5, där dagens dokumentation avseende personuppgiftsincidenter inte är tillfredställande. Vi rekommenderar att IMY:s mall används för dokumentation av personuppgiftsincidenter, där kommunstyrelsen inte behöver upprätta en egen mall. På så sätt säkerställs att samtliga nödvändiga delar kommer med samt att riskerna för bortfall av information och viktiga delar i processen minimeras (se sid 12–15).
- Säkerställa att de registrerade informeras i samband med de incidenter som medför en hög risk för fysiska personers rättigheter och friheter. Detta är juridiskt sett en central punkt där den registrerade ska informeras om incidenten **utan onödigt dröjsmål**, om incidenten sannolikt leder till en hög risk.
- Utöva en central styrning i syfte att säkerställa en enhetlig hantering av personuppgiftsincidenter inom samtliga nämnder.
- Årligen ta del av statistik avseende samtliga inträffade personuppgiftsincidenter inom ramen för styrelsens uppsiktsplikt.
- Genomföra utbildningsinsatser för medarbetarna, avseende upptäckt och hantering av personuppgiftsincidenter.
- Genomföra utbildningar för utsedda dataskyddssamordnare vad avser hantering, dokumentation samt risk- och konsekvensbedömning av inträffade personuppgiftsincidenter.

- Säkerställa att kommunstyrelsen får ta del av DSO:s årliga rapport. Detta är ytterst centralt för att kommunstyrelsen ska kunna hantera sin uppsiktsplikt.
- Ange i delegationsordningen vem som har befogenhet att ta beslut om huruvida en personuppgiftsincident ska anmälas till IMY och om den registrerade ska informeras.

2 Bakgrund

KPMG har av Perstorps kommuns revisorer fått i uppdrag att granska kommunens rutiner med fokus på personuppgiftsincidenter inom ramen för dataskyddsförordningen.

Dataskyddsförordningen (GDPR) trädde i kraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av GDPR upphävdes personuppgiftslagstiftningen (PuL 1998:204). Den nya lagstiftningen syftar bland annat till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter.

Bristande hantering samt överträdelser kan innebära betydande sanktionsavgifter, till skillnad från tidigare lagstiftning. Likaså riskerar en bristande hantering av personuppgifter leda till förtroendeskador för kommunen som helhet samt personuppgiftsansvariga nämnder och styrelser.

Vidare ska styrelsen och nämnderna utse ett dataskyddsombud, (DSO), som bland annat har till uppgift att agera rådgivande samt övervaka efterlevnaden av dataskyddsförordningen.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen syftar till att undersöka om kommunstyrelsen på ett ändamålsenligt sätt har säkerställt följsamhet till dataskyddsförordningen med inriktning på personuppgiftsincidenter.

- Finns det ett centralt utsett dataskyddsombud? Befinner sig dataskyddsombudet i en oberoendeposition?
- Har samtliga nämnder beslutat om att utse ett dataskyddsombud?
- Finns kommunövergripande styrdokument för hantering av personuppgiftsincidenter?
- Förmedlar rutinerna en korrekt hantering av personuppgiftsincidenter i enlighet med lagens intentioner?
- Har det genomförts någon riskbedömning av incidenterna och hur många har kategoriserats som allvarliga?
- Har incidenter som bedömts medföra allvarliga risker för den registrerades integritet anmälts till Integritetsskyddsmyndigheten?
- Hur många personuppgiftsincidenter har inträffat sedan lagens ikraftträdande?

Granskningen avser kommunens styrdokument för hantering av personuppgiftsincidenter inom ramen för dataskyddsförordningen.

2.2 Revisionskriterier

Granskningen utgår ifrån följande revisionskriterier:

- Europaparlamentets och rådets förordning (EU) 2016/679, daterad 2016-04-27, om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
- Riktlinjer från European Data Protection Board, (Europeiska dataskyddsstyrelsen)
- Interna riktlinjer/policys

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier av rutin för incidentrapportering.
- Intervjuer har genomförts med digitaliseringssamordnare, kommunsekreterare tillika dataskyddssamordnare, dataskyddsombud (DSO) och kommunstyrelsens ordförande.

Rapporten är faktakontrollerad av digitaliseringssamordnaren.

3 Resultat av granskningen

3.1 Styrdokument personuppgiftsincidenter

Vi har tagit del av ett Worddokument med benämningen ”Incidentrapportering”. Dokumentet anges av kommunkansliet vara ett kommunövergripande styrdokument i form av rutinbeskrivning avseende hantering av personuppgiftsincidenter. Av rutinbeskrivningen framgår inte kommunnamn, fastställesdatum eller beslutsinstans. Vidare har vi utifrån innehållet noterat att dokumentet riktar sig till skolans verksamheter, där följande framgår i rutinbeskrivningen avseende den information som ska ges till de registrerade i samband med incidenter som innebär en hög risk:

- Beskrivning vad **skolan** har gjort, eller tänker göra, för att hantera personuppgiftsincidenten.
- I förekommande fall: Beskriv vad **skolan** har gjort för att mildra eventuella negativa effekter.

I rutinen omnämns både Datainspektionen (DI) och Integritetsskyddsmyndigheten (IMY). Tillsynsmyndigheten namn ändrades från DI till IMY den 1 januari 2021.

Av dokumentet framgår inte vem som ansvarar för att genomföra risk- och konsekvensbedömning kopplat till inträffade incidenter och vem som ansvarar för upprättandet av den interna dokumentationen.

Enligt digitaliseringssamordnaren pågår vid tidpunkten för granskningen en omarbetning av rutiner och anvisningar avseende informationssäkerhet, där GDPR utgör en av de styrande lagstiftningarna.

3.1.1 Bedömning

I samband med faktakontrollen har det framkommit att den text som vi har delgivits är ett urklipp som enbart publicerats på kommunens intranät samt att texten är ett arbetsmaterial.

Vid tid för granskningen saknas ett formellt beslutat kommunövergripande styrdokument gällande hantering av personuppgiftsincidenter. Vi bedömer att ett kommunövergripande styrdokument behöver fastställas snarast.

Av styrdokumentet bör fastställesdatum, beslutsinstans samt kommunnamn framgå. Likaså är det av vikt att ha en korrekt benämning, där det tydligt bör framgå att styrdokumentet avser ”personuppgiftsincidenter” och inte endast ”incidenter”, då det finns flera kategorier av incidenter. Kommunövergripande styrdokument bör minst fastställas av kommunstyrelseförvaltningens ledning.

För att kunna efterleva lagstiftningen gällande bedömning av huruvida en personuppgiftsincident ska anmälas till tillsynsmyndigheten samt om den registrerade ska informeras, krävs genomförande av en risk- och konsekvensbedömning. På så vis behöver en framtida rutinbeskrivning tydliggöra ansvaret för denna centrala del. Likaså behöver ansvaret för dokumentation av inträffade incidenter framgå.

3.2 Organisation för hantering av personuppgifter

Organisationen för hanteringen av personuppgifter i Perstorps kommun utgår ifrån kommunens digitaliseringssamordnare, som arbetar med att samordna arbetet kring GDPR på en kommunövergripande nivå. Av intervjuerna framgår att eftersom respektive nämnd har det övergripande ansvaret för hanteringen av GDPR har varje nämnd utsett en egen samordnare för GDPR-arbetet. Vidare uttrycks att då GDPR-arbetet är nära knutet till exempelvis hanteringen av handlingar har respektive nämndsekreterare utsetts till dataskyddssamordnare.

Vid intervjuerna uttrycks att dataskyddssamordnarna ansvarar för att den grundläggande hanteringen av information är välfungerande, exempelvis genom registerförteckningar, att risk- och konsekvensbedömningar genomförs, att avtal hålls ordnade och att agera som internt stöd till verksamheten.

Vidare är digitaliseringssamordnaren huvudkontaktperson mot kommunens DSO.

Vi har också delgivits en komplettering i form av en beskrivning från kommunens intranät: *Dataskyddssamordnare för respektive nämnd leder det kontinuerliga arbetet med dataskyddsförordningen. Dataskyddssamordnare ansvarar för att register och styrdokument hålls uppdaterade. Inkomna incidenter ska utvärderas i samråd med dataskyddsombudet och i enlighet med gällande lagstiftning samt eventuellt vidarerapportera till integritetsskyddsmyndigheten och personuppgiftslämnaren.*

3.2.1 Bedömning

Vi bedömer att det finns vissa oklarheter utifrån den information som vi har delgivits. I samband med faktakontrollen har det framkommit att det är upp till respektive nämnd att utse en dataskyddssamordnare. Detta innebär i praktiken att en nämnd kan välja att avstå från att utse en samordnare.

Vi har samtidigt delgivits att då rutinen för hantering av personuppgiftsincidenter presenterades för kommunledningen framhölls att dataskyddssamordnarnas uppdrag skulle upptas i delegationsordningen. Det finns dock inget dokumenterat beslut, vilket vi bedömer som en brist.

Därmed bedömer vi att vid tid för granskningen saknas en dokumenterad kommunövergripande struktur för huruvida dataskyddssamordnare ska utses inom verksamheterna. Vi bedömer att det erfordras en central styrning från kommunstyrelsens sida i syfte att uppnå en **enhetlig struktur och samsyn** inom nämnderna vad avser hantering och samordning av arbetet inom ramen för dataskyddsförordningen. Detta är avgörande för graden av efterlevnad av dataskyddsförordningen.

Vi anser att respektive nämnd bör formellt ta ett beslut om att utse en dataskyddssamordnare följt av en uppdragsbeskrivning. Att tydligt klargöra och fastställa vem som ska samordna dataskyddsarbetet inom respektive nämnd är en premiss för att uppnå en fungerande struktur.

En central uppgift är risk- och konsekvensbedömning av inträffade incidenter, som enligt intervjuerna ska hanteras av dataskyddssamordnarna. I samband med faktakontrollen framkommit att risk- och konsekvensbedömning ska hanteras av utsedda dataskyddssamordnare i dialog med dataskyddsombudet. Denna centrala uppgift bör framgå av uppdragsbeskrivningen samt i kommande kommunövergripande rutinbeskrivning.

3.3 Externt avtal gällande DSO

Inför att GDPR skulle träda i kraft i maj 2018 arbetade en mindre kärngrupp med att inventera vilka personuppgiftsbehandlingar som gjordes inom respektive nämnd och hur kommunens arbete skulle se ut framöver. Inför 2018 genomfördes även en gemensam upphandling av DSO med ett antal andra kommuner, som företaget JP Infonet vann. Enligt uppgift undersöktes även möjligheten att rekrytera en DSO på timanställning, men gå grund av stor efterfrågan avseende denna kompetensprofil, var detta inte varit möjligt.

Perstorps kommun inledde samarbetet med JP Infonet i maj 2018. Genomförd protokollgranskning visar på att samtliga nämnder i Perstorps kommun har beslutat om att utse JP Infonet till DSO under avtalsperioden. Avtalet med JP Infonet löper ut i maj 2022 och vid tidpunkten för granskningen pågår en ny upphandling av DSO tillsammans med Klippan och Åstorps kommuner. I samband med att avtalet med JP Infonet löper ut kommer en utvärdering av hur avtalet har löpt att genomföras.

Digitaliseringssamordnaren uppger att samarbetet med JP Infonet inte har varit helt felfritt och att det ibland har tagit lång tid att få svar på frågor. Vidare förekommer det enligt uppgift att svaret från JP Infonet varit svårtolkat för verksamheterna, på grund av juridiska formuleringar. Enligt digitaliseringssamordnaren har samarbetet med JP Infonet dock förbättrats över tid och JP Infonet har effektiviserat sitt arbete, vilket har medfört en ökad tillgänglighet från leverantörens sida. Vid tidpunkten för granskningen har kommunen en huvudkontaktperson på JP Infonet.

3.3.1 Bedömning

Vi gör bedömningen att kommunstyrelsen och samtliga nämnder har beslutat om att utse ett dataskyddsombud. Eftersom dataskyddsombudet är externt upphandlat befinner sig dataskyddsombudet i en oberoendeposition.

3.4 Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna innebär närmare att individer förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks genom exempelvis obehörigt röjande av eller obehörig åtkomst till personuppgifter.

Dataskyddsförordningen (artikel 33, punkt 1) fastställer att vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och inte senare än 72 timmar efter att ha fått vetskap om den anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig. I Sverige är det Integritetsskyddsmyndigheten som är behörig tillsynsmyndighet.

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (artikel 34, punkt 1) ska den registrerade informeras om personuppgiftsincidenten utan onödigt dröjsmål.

De personuppgiftsincidenter som inte bedöms medföra risker för individers rättigheter och friheter behöver inte anmälas till Integritetsskyddsmyndigheten. På så vis är det av vikt att ansvarig nämnd genomför en konsekvensanalys vid eventuella incidenter i syfte att bedöma allvarlighetsgraden.

EU-rätten fastställer vidare att i de fall där organisationen har anlitat ett personuppgiftsbiträde (PuB) ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige, nämnd och styrelse, utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident (artikel 33, punkt 2).

3.4.1 Hanteringen av personuppgiftsincidenter i Perstorps kommun

I samråd med DSO har en e-tjänst för inrapportering av personuppgiftsincident framarbetats för Perstorps kommun. Vi har delgivits att e-tjänsten infördes 2021. Innan 2021 saknades enligt digitaliseringssamordnaren tydliga rutiner för hantering av personuppgiftsincidenter.

När en medarbetare upptäcker en personuppgiftsincident rapporteras detta i e-tjänsten och rapporten skickas vidare både till ansvarig nämndsekreterare och till DSO för bedömning. Enligt digitaliseringssamordnaren användes inledningsvis en mall som

stöd i den interna dokumentationen av inträffade incidenter. När kommunen övergick till rapportering via e-tjänsten försvann enligt uppgift behovet av mallen. Detta eftersom rapporten som genereras i e-tjänsten automatiskt diarieförs (interndokumenteras) av berörd nämnd och skickas för bedömning till både dataskyddssamordnaren och DSO.

Inom ramen för incidentrapporteringen i e-tjänsten ska följande frågor besvaras:

1. Vad har inträffat?
2. Hur upptäcktes incidenten?
3. Varför inträffade incidenten?
4. Har incident inträffat hos personuppgiftsbiträde?
5. Hur många registrerade har drabbats?
6. Har integritetskänsliga eller känsliga personuppgifter omfattas av incidenten?

Enligt intervjuerna genomförs **riskbedömning** kopplat till en inträffad personuppgiftsincident av nämnsekreteraren och DSO parallellt, vilket medför att DSO kan utgöra ett stöd åt nämndsekreterarna i bedömningen.

Av intervjuerna framgår vidare att det formellt sett är nämnden via nämndsekreteraren som ansvarar för att en personuppgiftsincident som bedömts medföra hög risk anmäls till IMY. Enligt kommunstyrelsens ordförande (KSO), tar kommunstyrelsen dock inga beslut kring huruvida en personuppgiftsincident ska anmälas till IMY eller ej samt huruvida den registrerade ska informeras om inträffad personuppgiftsincident. Av kommunstyrelsens delegationsordning[1] framgår inte huruvida ovan nämnda beslut har delegerats till förvaltningsledningen.

Av intervjuerna framgår att det är för ärendet aktuell enhetschef eller verksamhetschef som i praktiken kontaktar den registrerade. En mall för vilken information som ska meddelas den drabbade registrerade har tagits fram.

3.4.1.1 Bedömning

Av granskningen framgår att respektive nämnd i egenskap av personuppgiftsansvarig är ansvarig för att upprätta anmälan till IMY. Vi gör bedömningen att det av kommunstyrelsens delegationsordning bör framgå vem som har befogenhet att ta beslut om huruvida en personuppgiftsincident ska anmälans till IMY eller ej och huruvida den registrerade ska informeras. Därmed bör varje personuppgiftsincident kompletteras med ett förvaltningsbeslut om huruvida personuppgiftsincidenten ska inrapporteras till nationell tillsynsmyndighet eller ej samt huruvida den registrerade ska informeras. Beslutet bör diarieföras.

3.5 Arbetsrutin DSO

DSO utgör en stödfunktion gentemot dataskyddssamordnarna i hanteringen av personuppgiftsincidenter och i bedömningen av allvarlighetsgrad gällande inträffade incidenter. DSO har hittills bistått kommunen i att göra en bedömning av

[1] 2009-09-23 § 109

allvarlighetsgrad i samtliga inträffade incidenter sedan maj 2018. Enligt överenskommelsen mellan DSO och kommunen ska DSO informeras även om incidenter där verksamheterna upplever att bedömning av allvarlighetsgrad är enkel att genomföra. Detta är av vikt eftersom DSO utgör kontaktperson gentemot IMY.

DSO får vetskap om inträffade incidenter antingen via en funktionsbrevlåda för Perstorps kommun, e-tjänsten eller över telefon. Det kan både vara dataskyddssamordnarna och andra tjänstepersoner som mejlar till funktionsbrevlådan.

DSO får notis om att incidentrapportering har genomförts via Perstorps kommuns e-tjänst. DSO har även möjlighet att logga in i e-tjänsten.

Det förekommer att DSO följer upp inkomna ärenden genom kompletterande telefonsamtal, framför allt i känsliga ärenden, men det beror på hur mycket stöd kommunen behöver. Enligt uppgift ringer berörd verksamhet ibland upp gällande stöd i hur anmälan till IMY ska fyllas i och bedömning av allvarlighetsgrad. Berörd verksamhet brukar enligt uppgift stämma av med digitaliseringssamordnaren innan kontakt med DSO inleds i ett ärende.

I bedömningen av allvarlighetsgrad av inträffad incident utgår DSO från EDPB:s (European Data Protection Board/Europeiska dataskyddsstyrelsen) och IMY:s riktlinjer, men även utifrån de sanktionsbelopp som har dömts ut i referensärenden.

DSO dokumenterar uppföljningen av efterlevnaden av GDPR i en årlig tillsynsrapport. Den senast färdigställda rapporten är daterad juni 2020. Enligt DSO är de åtgärder som identifierades i rapporten gällande personuppgiftsincidenter vidtagna vid tidpunkten för granskningen.

3.5.1 Bedömning

Av granskningen framkommer att kommunstyrelsen inte har den årliga tillsynsrapporten som har upprättats av DSO. Vi bedömer att det är ytterst centralt att kommunstyrelsens ledamöter i sin helhet tar del av den årliga statusrapporten. Detta i syfte att kunna hantera sitt uppdrag inom ramen för kommunstyrelsens uppsiktsplikt.

3.6 Förekomsten av personuppgiftsincidenter

Vi har begärt in statisk avseende totalt antal kända personuppgiftsincidenter sedan lagen trädde i kraft. Totalt finns 14 kända personuppgiftsincidenter, varav 5 anges ha anmälts till IMY. Digitaliseringssamordnaren uppskattar dock att mörkertalet gällande personuppgiftsincidenter inom kommunens verksamheter är stort.

DSO har rekommenderat att kommunen ska informera berörd registrerad i ett av fallen.

Enligt KSO har kommunstyrelsen inte fått någon återrapportering kring inträffade personuppgiftsincidenter. Enligt KSO samt digitaliseringssamordnaren ska statistiken gällande personuppgiftsincidenter framöver integreras i verksamhetssystemet Stratsys via en ny modul, vilket uttrycks kommer förenkla återrapporteringen till politiken vad avser dataskyddsarbete, statistik och genomförda utbildningar.

Det framgår dock att beslut har ännu inte tagits om modulen kommer att implementeras.

I tabell 1 framgår antalet kända personuppgiftsincidenter per nämnd.

Tabell 1.

Nämnd	Antal incidenter 2018	Varav anmälda till IMY	Antal incidenter 2019	Varav anmälda till IMY	Antal incidenter 2020	Varav anmälda till IMY	Antal incidenter 2021	Varav anmälda till IMY
Kommunstyrelsen	-	-	-	-	-	-	-	-
Barn- och utbildningsnämnden	-	-	1	-	2	-	1	-
Byggnadsnämnden	-	-	-	-	-	-	1	-
Kultur- och fritidsnämnden	-	-	-	-	-	-	1	-
Räddningsnämnden	-	-	-	-	-	-	-	-
Socialnämnden	-	-	-	-	2	-	6	5
Valnämnden	-	-	-	-	-	-	-	-
Överförmyndarnämnden	-	-	-	-	-	-	-	-
Totalt antal incidenter per år	**0**	**0**	**1**	**0**	**4**	**0**	**9**	**5**

3.7 Genomgång av personuppgiftsincidenter

Vi har begärt in underlag kopplade till samtliga kända incidenter under 2021. Vi har inte erhållit någon dokumentation avseende 2 av 9 incidenter som har inträffat inom bildningsnämnden och socialnämnden, där vi har delgivits att dokumentation saknas. Enligt uppgift har 5 av 9 incidenter inrapporterats till tillsynsmyndigheten, dock har vi endast delgivits 4 anmälningsunderlag.

Vidare saknas i 7 av 9 fall, ifylld mall från inrättad e-tjänst som infördes under 2021. Dock noterar vi att i två av fallen har en äldre mall ifyllts som var aktuell innan införandet av e-tjänsten. Den äldre mallen omfattar även en fråga avseende incidentens allvarlighetsgrad som saknas i dagens mall.

Vi noterar vidare att dokumentationen per incident är bristfällig.

3.7.1 Bedömning

I Perstorps kommun har totalt 14 personuppgiftsincidenter rapporterats in i kommunens e-tjänst sedan maj 2018. Vi bedömer att sannolikheten att flertalet nämnder inte har haft någon form av personuppgiftsincident sedan maj 2018, alternativt endast har ett eller två fall, som låg där vi bedömer att det finns ett mörkertal. Denna bild bekräftas vidare av digitaliseringssamordnaren.

Under 2021 fick IMY in ca 110 anmälningar per vecka. IMY framhåller att det finns ett stort mörkertal avseende anmälningspliktiga incidenter som inte anmäls.

Baserad på vår erfarenhet är en grundläggande orsak, avsaknad av tillräckliga kunskaper om vad en personuppgiftsincident är och vad som ska klassas som en incident. Vi anser på så vis att det finns ett behov av kunskapsökning bland personalen i verksamheterna, där utbildning i form av återgivning av konkreta exempel är av betydelse för en ökad förståelse samt upptäckt av eventuella personuppgiftsincidenter.

Vi bedömer att det är bristfälligt att det förekommer personuppgiftsincidenter som inte har dokumenterats, vilket strider mot gällande lagstiftning. En korrekt hantering av inträffade incidenter är **avgörande för de registrerades integritetsskydd.**

Dokumentation av personuppgiftsincidenter är av central betydelse i syfte att kunna efterleva gällande lagstiftning. Vi vill betona att **dokumentationen är obligatorisk, där den personuppgiftsansvarige ska dokumentera samtliga personuppgiftsincidenter oavsett om incidenten ska anmälas till IMY eller ej**, inbegripet omständigheterna kring incidenten, effekter samt de korrigerande åtgärder som har vidtagits.

Dagens struktur

Idag sker dokumentation av personuppgiftsincidenter genom inrapportering i e-tjänsten. Av e-tjänstmallen samt dokumentationen saknas centrala frågor som är av vikt för den lagstadgade risk- och konsekvensbedömningen. Som tidigare nämnts ska en risk- och konsekvensbedömning genomföras för att i nästa steg möjliggöra en bedömning om **huruvida en incident ska till IMY eller ej** samt **huruvida den registrerade ska informeras.**

Dagens struktur saknar nedan centrala frågeställningar, där kommunstyrelsen behöver säkerställa att följande delar upptas:

- Ansvarig nämnd/styrelse ska anges.
- Datum för incidentens inträffande.
- Datum för incidentens upphörande.
- Av incidentbeskrivningen bör framgå huruvida det handlar om:
    - obehörigt röjande,
    - obehörig åtkomst,
    - förlust,
    - förstöring eller
    - ändring
- Orsak till incidentens inträffande.
- Antal berörda, dvs. hur många registrerade har påverkats.
- Antal Vilka kategorier av uppgifter som har drabbats.

- Kategori av drabbade (exempelvis anställda, brukare/boenden, kunder, barn mm.).
- Huruvida uppgifterna var krypterade (vilket är avgörande information för att kunna bedöma korrigerande åtgärder).
- Huruvida den registrerade genom incidenten har förlorat kontrollen över sina personuppgifter, begränsning av rättigheter, identitetsstöld, bedrägeri, ekonomisk förlust, förlust av konfidentialitet avseende uppgifter som omfattas av tystnadsplikt (här ingår t.ex. individer med skyddad identitet), skadat anseende mm.
- Datum för korrigerande åtgärder.
- Beskrivning av vilka korrigerande åtgärder som har vidtagits.
- Vilka konsekvenser som incidenten innebär för den registrerade.
- Riskbedömning. En incident ska bedömas utifrån följande allvarlighetsgrader:
    1. Obetydlig
    2. Begränsad
    3. Betydande
    4. Mycket allvarligt
- Huruvida den registrerade har informerats och när i tid. Vid beslut att inte informera den registrerade ska en motivering anges.

Hantering av personuppgiftsincidenter

Vi har genom vår granskning uppmärksammat att i majoriteten av fall saknas ovan väsentliga punkter i dokumentationen avseende personuppgiftsincidenter (**konsekvensbeskrivning, riskbedömning, korrigerande åtgärder, huruvida den registrerade har informerats m.fl**.)

Vi har vidare uppmärksammat att det förekommer att en incident anges omfattas av känsliga personuppgifter, men risk- och konsekvensbedömning saknas i dokumentationen.

Det förekommer vidare att den personal som har anmält incidenten till IMY har missuppfattat frågeställningen om ”**Hur har ni agerat efter incidenten**” och **Vilka åtgärder har vidtagits**”, där en beskrivning av korrigerande åtgärder för att *lösa*, *mildra* och *förebygga* konsekvenserna av inträffad incident ska anges. Dock har det förkommit att åtgärdsbeskrivningen anges till att en incidentrapport har upprättats.

Vid respektive frågeställning i tillsynsmyndighetens anmälningsblankett återfinns hjälprutor, där bl.a. följande framgår vad avser ovan nämnda frågeställningar: anmälningsblanketten framgår: *Beskriv vad ni har gjort. Har ni vidtagit åtgärder eller avser att vidta åtgärder för att lösa problem, förebygga eller mildra effekterna av incidenten?*

Vidare förekommer i anmälningsblanketten att frågan om ”**Varför den registrerade inte kommer att informeras**” tagits bort.

Det är centralt att personuppgiftsansvarig nämnd/styrelse framgår i samtliga underlag då det är berörd nämnd/styrelse som är juridiskt ansvarig. Vår granskning visar att information om personuppgiftsansvarig styrelse/nämnd framgår endast i ett fall i anmälningsunderlaget till IMY. I övriga fall saknas denna information, där kommunnamn har angivits i stället för personuppgiftsansvarig styrelse/nämnd.

Vi bedömer sammantaget att det i Perstorps kommun saknas en enhetlig dokumentationsstruktur gällande hantering av personuppgiftsincidenter. Existerande dokumentation är ostrukturerad i form av korrespondens, lösa worddokument, anteckningar och i vissa fall ifylld mall från e-tjänsten. Detta leder till en svårighet att få en helhetsbild av hanteringen av en incident. I de fyra fall där IMY:s anmälningsunderlag har ifyllts finns däremot en samlad bild av incidenten, (med undantag av en incident där det saknas information om huruvida den registrerade ska informeras, vilket vi bedömer som allvarligt, se sid 15)

Detta innebär att en nödvändig helhetsbild och bedömningar erhålls enbart i de fall där en incident har anmälts till tillsynsmyndigheten.

Vi bedömer att kommunstyrelsen behöver snarast säkerställa en korrekt dokumentation genom fastställande av en kommunövergripande mall, där dagens dokumentation avseende personuppgiftsincidenter inte är tillfredställande. Likaså krävs en central styrning från kommunstyrelsen sida i syfte att säkerställa en enhetlig hantering av personuppgiftsincidenter inom samtliga nämnder.

I syfte att underlätta arbetet för kommunstyrelsen, rekommenderar vi att IMY:s anmälningsblankett används internt, oavsett om incidenten ska vidare till tillsynsmyndigheten eller ej. På så sätt säkerställts att nödvändiga delar som syftar till att uppfylla lagstiftningens intentioner kommer med (förutsatt att blanketten ifylls på rätt sätt). Som tidigare nämnts är dokumentationen av personuppgiftsincidenter obligatorisk, där den personuppgiftsansvarige **ska dokumentera samtliga personuppgiftsincidenter oavsett om incidenten ska anmälas till IMY eller ej**,

Detta kan hanteras på två sätt:

1. Medarbetaren som upptäcker en incident fyller i blanketten efter bästa förmåga. Det finns tydliga svarsalternativ i form av kryssrutor i blanketten som underlättar ifyllandet. Därefter ska blanketten kompletteras av utsedd dataskyddssamordnare, utifrån vederbörandes ansvar för dokumentation. Blanketten ifylls och kompletteras allteftersom dataskyddssamordnaren får ny information rörande incidenten, vilket leder till ett samlat dokument för respektive incident.
2. Medarbetaren som upptäcker en incident svarar på de fåtal frågor (6st) som finns i e-tjänsten. Därefter ifylls IMY:s blankett av dataskyddssamordnaren för en nödvändig helhetsbild och bedömning.

Användning av IMY:s mall, bidrar per automatik till en samlad erforderlig bild och bedömning av inträffade incidenter, i form av ett centralt dokument per incident, där

dagens osammanhängande struktur som har lett till avsaknad av nödvändig information samt en bristfällig hantering, undviks.

Likaså bidrar mallen till minskad administration, där vid behov att anmäla en incident till IMY, behöver förvaltningen inte fylla i ett nytt underlag, utan redan ifylld blankett skickas in.

Vi noterar att kommunstyrelsen inte får regelbunden återrapportering kring inträffade personuppgiftsincidenter. Vi bedömer att kommunstyrelsen bör minst en gång årligen ta del av statistiken avseende inträffade personuppgiftsincidenter.

Incident socialnämnden

Av en inträffad incident inom socialnämnden framgår att flertalet obehöriga har tagit del av dokumentation innehållande känsliga uppgifter avseende en boende, där också informationen har spridits vidare till andra.

Vår bedömning är utifrån gällande föreskrifter, att incidenten är allvarlig, vilket per automatik innebär att den registrerade ska informeras (se sid 13 avseende skalan för riskbedömning och allvarlighetsgrader).

I anmälningsunderlaget till tillsynsmyndigheten bedöms allvarlighetsgraden till ”betydande”, vilket innebär att den registrerade ska informeras. Dock anges att ställning inte har tagits om huruvida den registrerade ska informeras om incidenten. En incident där risken bedöms som hög **ska utan dröjsmål informeras till den registrerade**.

Vi har efter genomförd granskning erhållit kompletterande information angående aktuell incident, där det framgår att nämnden vid tid för inlämning av anmälan inte har kunnat ta ställning till frågan p.g.a. den registrerades hälsotillstånd. Dock framgår inte denna information i anmälningsunderlaget, där anledningen till att inte ha informerat den registrerade ska framgå. Vi har fått information om att nämnden efter inlämning av anmälan har tagit beslut om att informera den registrerades gode man.

Därmed bedömer vi att kravet avseende information till den registrerande har uppfyllts.

3.8 Utbildningsinsatser

JP Infonet höll i oktober 2020 utbildning gällande GDPR för dataskyddssamordnarna. Enligt digitaliseringssamordnaren har samtliga dataskyddssamordnare fått genomgång om hur personuppgiftsincidenter rapporteras och var de hittar information om vad en incident är. Utöver detta har digitaliseringssamordnaren enligt uppgift vid ett antal tillfällen bjudits in till några verksamheter, i syfte att informera om bland annat personuppgiftsincidenter och rapporteringskravet. Digitaliseringssamordnaren uppskattar dock kunskapsnivån gällande personuppgiftsincidenter som generellt låg inom verksamheterna, men att kunskapsnivån sannolikt är något högre inom de verksamheter där man sedan tidigare arbetar med anmälningsplikt på ett systematiskt sätt.

Vid tidpunkten för granskningen har kommunen med hjälp av externa konsulter framarbetat utbildningsfilmer som behandlar GDPR och personuppgiftsincidenter. Målsättningen är att samtliga anställda ska gå utbildningen både vid nyanställning och fortsatt minst en gång per år.

På Perstorps kommuns hemsida framgår information kring GDPR, kommunens behandling av personuppgifter och personuppgiftsincidenter. På kommunens intranät framgår enligt uppgift hur medarbetarna kan arbeta förebyggande för att motverka personuppgiftsincidenter, exempelvis hur e-post, lösblad och skärmsläckare ska hanteras. Vidare framgår enligt uppgift länk till IMY:s system för anmälan av personuppgiftsincidenter.

3.8.1 Bedömning

Vi noterar att kommunens dataskyddsamordnare har tillhandahållits utbildning gällande hantering av personuppgiftsincidenter, dock anser vi att det krävs ytterligare utbildningsinsatser i syfte att höja kompetensnivån hos utsedda dataskyddssamordnare.

Som tidigare nämnts ser vi vidare ett behov av kunskapsökning bland personalen i verksamheterna, där utbildning i form av återgivning av konkreta exempel är av betydelse för en ökad förståelse samt upptäckt av eventuella personuppgiftsincidenter.

Vi ser positivt på att samtliga anställda framöver ska erbjudas utbildning både vid nyanställning och återkommande fortbildning.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att hanteringen av personuppgiftsincidenter inte är på en tillfredställande nivå, där kommunstyrelsen behöver vidta åtgärder i syfte att säkerställa en korrekt dokumentation och hantering av personuppgiftsincidenter.

Vi bedömer att det finns behov av kunskapsökning bland medarbetarna i kommunens verksamheter gällande identifiering och hantering av personuppgiftsincidenter. Vidare erfordras utbildningsinsatser för utsedda dataskyddssamordnare i syfte att kunna hantera sitt uppdrag på ett tillfredställande sätt.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Fastställa ett kommunövergripande styrdokument avseende hantering, bedömning och dokumentation av personuppgiftsincidenter (se avsnitt 3.1.1). Det bör noteras att dokumentation och riskbedömning av samtliga personuppgiftsincidenter är obligatorisk.
- Säkerställa en korrekt dokumentation genom fastställande av en kommunövergripande mall innehållande centrala frågor i enlighet med avsnitt 3.4.5, där dagens dokumentation avseende personuppgiftsincidenter inte är tillfredställande. Vi rekommenderar att IMY:s mall används för dokumentation av personuppgiftsincidenter, där kommunstyrelsen inte behöver upprätta en egen mall. På så sätt säkerställs att samtliga nödvändiga delar kommer med

samt att riskerna för bortfall av information och viktiga delar i processen minimeras (se sid 12–15)

- Säkerställa att de registrerade informeras i samband med de incidenter som medför en hög risk för fysiska personers rättigheter och friheter. Detta är juridiskt sett en central punkt där den registrerade ska informeras om incidenten utan onödigt dröjsmål, om incidenten sannolikt leder till en hög risk.
- Utöva en central styrning i syfte att säkerställa en enhetlig hantering av personuppgiftsincidenter inom samtliga nämnder.
- Årligen ta del av statistik avseende samtliga inträffade personuppgiftsincidenter inom ramen för styrelsens uppsiktsplikt.
- Genomföra utbildningsinsatser för medarbetarna, avseende upptäckt och hantering av personuppgiftsincidenter.
- Genomföra utbildningar för utsedda dataskyddssamordnare vad avser hantering, dokumentation samt risk- och konsekvensbedömning av inträffade personuppgiftsincidenter.
- Säkerställa att kommunstyrelsen får ta del av DSO:s årliga rapport. Detta är ytterst centralt för att kommunstyrelsen ska kunna hantera sin uppsiktsplikt.
- Ange i delegationsordningen vem som har befogenhet att ta beslut om huruvida en personuppgiftsincident ska anmälas till IMY och om den registrerade ska informeras.

Datum som ovan
KPMG AB

Frida Starbrant
Certifierad kommunal revisor

Viktoria Bernstam
Specialist/Certifierad kommunal revisor
Sakkunnig EU-rätt