Gävle KOMMUN

Personuppgiftsansvarig

Arbetsmarknads- och funktionsrättsnämnden

Omvårdnadsnämnden

Socialnämnden

Granskningsrapport 2024

Dataskyddsombud

Boel Burman

Datum

2025-08-07

Innehåll

Sammanfattning

I aktuell granskning har dataskyddsombudet granskat styrande dokument. Det som har kontrolleras är hur den personuppgiftsansvarige uppfyller ansvarsskyldigheten i artikel 5.2. Granskningen visade att Arbetsmarknads- och funktionsrättsnämnden, Omvårdnadsnämnden och Socialnämnden i rätt stor utsträckning har relevanta styrdokument på plats för att kunna visa på ansvarsskyldigheten i artikel 5. Det som kan behöva kompletteras är styrdokument på ”högre nivå” som riktlinjer för att få en helhet (hierarkiskt) som visar på ansvarsskyldigheten.

De tre nämnderna har i denna granskning, granskats gemensamt eftersom styrdokumenten är framtagna gemensamt för Sektor Välfärd.

Dataskyddsombudet har också följt upp handlingsplaner och åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer som getts i samband med granskningarna 2022 och 2023. Uppföljningen indikerar att de tre nämnderna har ett kontinuerligt dataskyddsarbete.

1. Inledning

1.1 Allmänt om dataskyddsförordningen, GDPR

Dataskyddsförordningen, GDPR, trädde i kraft inom EU den 25 maj 2018 och är det generella regelverk som reglerar behandlingen av personuppgifter i såväl privat som offentlig sektor. Dataskyddsförordningen är bindande och direkt tillämplig i samtliga EU:s medlemsländer, men tillåter och förutsätter att medlemsstaterna kompletterar förordningen med nationell lagstiftning.

Dataskyddförordningen ska skydda enskildas grundläggande fri- och rättigheter, särskilt rätten till skydd av personuppgifter. Förordningens syfte är också att anpassa regelverket till det digitala samhället samt att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras.

Kraven i förordningen är ur ett internationellt perspektiv högt ställda och de organisationer som inte lever upp till dessa riskerar sanktioner från respektive lands tillsynsmyndighet. Den svenska tillsynsmyndigheten IMY, Integritetsskydds-myndigheten, har möjlighet att utdöma administrativa sanktionsavgifter för svenska myndigheter och företag.

1.2 Om årlig granskning

Enligt dataskyddsförordningen ska myndigheter samt företag som hanterar stora mängder personuppgifter ha ett utnämnt dataskyddsombud. Dataskyddsombudet, som har en fristående ställning i förhållande till myndigheten eller företaget, ska kontrollera att dataskyddsförordningen följs inom organisationen genom att bland annat genomföra kontroller och informationsinsatser.

Inom ramen för dataskyddsombudets kontrollerande arbete gör dataskyddsombudet en årlig granskning. Inriktningen på granskningen varierar år för år utifrån bland annat organisationens mognad och den risk som kan tänkas förekomma. I årets granskning har dataskyddsombudet under Q3-Q4 granskat styrande dokument. Det som har kontrolleras är hur den personuppgiftsansvarige uppfyller ansvarsskyldigheten i artikel 5.2..

Dataskyddsombudet har också följt upp handlingsplaner och åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer som getts i samband med granskningarna de senaste två åren:

- Registerförteckning (2023)
- Information till de registrerade (2023)
- Personuppgiftsbiträdesavtal (2023)
- Personuppgiftsbiträdesavtal och uppföljning av leverantörer (2022)
- Motivering av rättsliga grunder (2022)

1.3 Avgränsning

Ingen avgränsning.

1.4 Metod

Ett antal frågor har skickats ut till den personuppgiftsansvariges dataskyddssamordnare som besvarats skriftligt. I förekommande fall har dataskyddsombudet har begärt in relevanta dokument.

1.5 Efterlevnad

Uppfyller dataskyddsförordningens krav, mindre brister med låg risk kan förekomma

Uppfyller delvis dataskyddsförordningen krav, brister finns

Uppfyller till stora delar inte dataskyddsförordningens krav, stora brister finns

2. Granskning

2.1 Del 1: Styrande dokument

2.1.1 Utgångspunkt

Enligt dataskyddsförordningen ska den personuppgiftsansvarige ansvara för och kunna visa att förordningens sex principer efterlevs.[1] Detta kallas principen om *ansvarsskyldighet.*

Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Dessa åtgärder ska ses över och uppdateras vid behov. Om det står i proportion till behandlingen, ska åtgärderna omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

En del av ansvarsskyldigheten innebär således att organisationen ska ha styrande dokument som beskriver hur dataskyddsarbetet ska bedrivas i verksamheten. Styrande dokument är ett viktigt verktyg för ledning och styrning och anger vad verksamheten ska göra, vem som ska göra det och i vissa fall hur det ska göras.

Denna granskningsdel har som syfte att kontrollera hur den personuppgiftsansvarige uppfyller ansvarsskyldigheten i artikel 5.2.

Granskningsunderlag:
Välfärd svar på granskning på Granskningsprogram Q3-Q4 2024 – Q1-Q2 2025

VG-RUT-S -8089 v1.0 Rutin för videosamtal i Teams

VG-RUT-S 5707 v6.0 Rutin för hantering av personuppgiftsincidenter

VG-RUT-S 7770 v2.0 Rutin för upprättande och uppsägning av personuppgiftsbiträdesavtal

VG-RUT-S 5969 v5.0 Rutin för hantering av begäran av registerutdrag

VG-RUT-S 8376 v.2.0 Rutin för Konsekvensbedömning avseende dataskyddsförordningen

VG-RUT-S 4638 v6.0 Rutin för hantering och lagring av information

VG-RUT-S 8829 v2.0 Rutin vid användning av generativ AI

VG-RUT-S 8468 v2.0 Mellanlagring av information med högre skyddsbehov

VG-RUT-E 8541 v2.0 Rutin för administration av medarbetare med skyddad identitet

[1] artikel 5.2

VG-RUT-S 1241 v9.0 Rutin för kund med skyddade personuppgifter

VG-RUT-S 1407 v13.0 Rutin för loggkontroll

VG-RUT-S 7828 v2.0 Behörighetsbeställningar i Treserva VO och TES

VG-RUT-V 5888 v9.0 Rutin för hantering av elever med skyddad identitet

Instruktion för hantering av personuppgiftsincident Mindre allvarlig som inte anmäls till IMY

Instruktion för hantering av personuppgiftsincident Mindre allvarlig som anmäls till IMY

Instruktion för hantering av personuppgiftsincident Allvarlig som anmäls till IMY

2.1.2 Efterlevnad

Uppfyller dataskyddsförordningens krav, mindre brister med låg risk kan förekomma

Dataskyddspolicy
Skäl 78

För att den personuppgiftsansvarige ska kunna visa att och hur dataskyddsförordningen efterlevs bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder därav, exempelvis genom dataskyddspolicy / integritetspolicy, riktlinjer och andra rutiner. I sammanhanget ska nämnas att dataskydd ofta beskrivs som en juridisk mekanism som säkerställer integritet. I praktiken spelar det ingen större roll om dokumenten är namngivna med integritet eller dataskydd, det viktigaste är innehållet. Dataskyddsombudet har i fortsättningen av denna granskning valt att använda benämningen dataskyddspolicy, men det är innehållet som granskats, oaktat den personuppgiftsansvariges benämning av motsvarande dokument.

De personuppgiftsansvariga nämnderna har varsin informationstext på Gävle kommuns publika webbplats om hur de behandlar personuppgifter inom respektive nämnd:

Så här behandlar Arbetsmarknads- och funktionsrättsnämnden dina personuppgifter – Gävle kommun

Så här behandlar Omvårdnadsnämnden dina personuppgifter – Gävle kommun

Så här behandlar Socialnämnden dina personuppgifter – Gävle kommun

Informationen är en komplettering med nämndspecifik information till kommunens gemensamma information om dataskydd. Dataskyddsombudet anser att texten är mer av karaktären ”information till de registrerade” än interna strategier för dataskydd.

Det finns en centralt framtagen policy för informationssäkerhet och där ingår i begränsad utsträckning dataskydd: ”Informationssäkerhetspolicy – Gävle 2020”[2]. Den

[2] Policy för informationssäkerhet Gävle kommun. Beslutad version 2020-09-28.pdf

har inte bifogats i svaret på granskningen, vilket skulle kunna indikera att de personuppgiftsansvariga inte känt till dokumentet och därmed inte heller fattat beslut om att det ska antas för de tre nämnderna med eventuella anpassningar. Dock hänvisas till ovan nämnda policy i andra styrdokument. Av policyn framgår att ” Respektive sektorchef eller bolags VD ska analysera behovet av och ta fram, egna rutiner/instruktioner för underliggande verksamheter till stöd för denna policy”. Ovannämnda policy verkar är inte uppdaterad på flera år vilket som dataskyddsombudet förstår det är kommunstyrelsens (Sektor Styrning och Stöd) ansvar att göra En personuppgiftsansvarig bör/ska ha en dataskydds-/integritetspolicy för att visa på ansvarsskyldigheten, inom en kommun är det rimligt att det finns en kommungemensam som antas av varje nämnd (med eventuella anpassningar). Utifrån detta resonemang rekommenderar dataskyddsombudet respektive nämnd att antingen anta den kommungemensamma policyn eller upprättar och fattar beslut om en egen för varje nämnd.

Rutiner för att hantera begäran om de registrerades rättigheter
Artikel 15–18, 20–22

Den registrerade, det vill säga den vars personuppgifter behandlas, har ett antal rättigheter enligt dataskyddsförordningen. Den personuppgiftsansvarige har ett ansvar att ha rutiner på plats för att hantera begäranden om att utöva dessa rättigheter när någon begär det. En sådan begäran ska hanteras så snabbt som möjligt, dock som huvudregel senast en månad efter att den inkom.

De tre personuppgiftsansvariga nämnderna har en gemensam rutin för hantering av registerutdrag ”VG-RUT 5969 v5 Rutin för hantering av begäran av registerutdrag, GDPR”. Det framgår tydligt vilken roll som upprättat den, vem som fattat beslut och när det gjordes (senast 2024-05-20). Det framgår också att den som upprättar dokumentet är ansvarig för revidering och att innehållet ska kontrolleras en gång per år av upprättare och granskare. Rutinen är mycket tydlig (och pedagogisk) med både bakgrund och tillvägagångssätt för att hantera en begäran om registerutdrag. För de andra rättigheterna som de registrerade har, rätten till radering, rättelse, begränsning av behandling, göra invändningar samt rätten till dataportabilitet verkar det saknas rutiner. Dataskyddsombudet rekommenderar att befintlig rutin kompletteras eller att separata rutiner tas fram för rätten till radering, rättelse, begränsning av behandling, göra invändningar samt rätten till dataportabilitet.

Tekniska och organisatoriska säkerhetsåtgärder
Artikel 24 och 27

Personuppgiftsansvariga måste vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till den risk som behandlingen av personuppgifter utgör för fysiska personers rättigheter och friheter, särskilt när det gäller rätten till skydd av personuppgifter. Tekniska åtgärder är sådana som ger data- eller systemsäkerhet, kommunikationssäkerhet eller fysisk säkerhet medan organisatoriska åtgärder omfattar sådant som styrdokument, processer, rutiner, metoder, analyser och utbildning. Utformningen av tekniska åtgärder förutsätter ofta organisatoriska åtgärder för att åtgärden ska ge det skydd som behövs. Många åtgärder innehåller därför både tekniska och organisatoriska delar. När det gäller till exempel säkerhetskopior behövs rutiner och ställningstaganden kring hur kopiorna ska sparas, hur ofta de ska tas och hur länge de ska sparas, med mera. Ett annat exempel, behörighetsstyrning, kräver både tekniska funktioner för att kunna begränsa åtkomst

liksom analyser av vem som behöver åtkomst till vilka uppgifter och när samt rutiner för hantering av behörigheterna. Särskilt viktiga områden att belysa är hantering av skyddad identitet, behörighetsstyrning och hantering av verksamhetskritiska system.

I svaret på granskningen har bifogats två rutiner, ”Rutin för hantering och lagring av information (VG-RUT-S-4638-6) och ”Mellanlagring av information med högre skyddsbehov” (VG-RUT-S-8468-2). Dataskyddsombudet bedömer att båda dessa rutiner är konkreta exempel på organisatoriska skyddsåtgärder som ger chefer och medarbetare god vägledning i var information ska lagras, tillfälligt i vissa fall och för lång tid. Båda hänvisar bland annat till Gävle kommuns informationssäkerhetspolicy. Det är oklart hur dessa rutiner kommuniceras men av svaret på granskningen framkommer att det inte finns beslutade sätt för att kommunicera rutiner till verksamheten.

Av svaret på granskningen framgår att de tre nämnderna gemensamt har rutiner fastställda för kund med skyddade personuppgifter (VG-RUT-S-1241-v.9.0); för elever med skyddad identitet (VG-RUT-V-5888-v.9.0) samt för medarbetare med skyddade personuppgifter i systemen Treserva, TES, MIM och HSA (VG-RUT-E-8541-v.1.0). Två av dem är senast beslutade i september 2024 och den tredje i november 2022 (kunder med skyddad identitet). Sammantaget bedömer dataskyddsombudet att dessa rutiner, utifrån dataskyddsförordningen, uppfyller kraven för säkerhetsåtgärder för skyddade identiteter för de grupper av individer som är aktuella i de olika nämndernas verksamhet.

Enligt svaret på granskningen finns det två rutiner för behörighetsstyrning, en för loggkontroll Treserva och NPÖ (VG-RUT-S 1407) senast beslutad 2024-03-20 och en för behörighetsbeställningar i Treservo VO och TES (VG-RUT-S 7828) beslutad 2024-09-10. Rutinerna är tydliga utifrån gällande regelverk och verkar stämma överens med de ändringar som gjordes i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, SoLPUL de första mars förra året. Dataskyddsombudet gör därför bedömningen att de uppfyller kraven i dataskyddsförordningen med tillhörande regelverk. Det är viktigt att rutinerna efterlevs och följs upp.

Det finns ett flertal rutiner för de personuppgiftsansvarigas verksamhetskritiska system, det rör framför allt systemen Treserva (IFO, VO och TES). Det finns tex. rutiner för att hantera driftsstopp (VG-RUT-S-5913-v.5.0 Rutin för att hantera driftstopp och VG-RUT-S-4265-v.6.0 Rutin för utförare att hantera driftstopp i Treserva och TES båda fastställda 2023). För Edlevo saknas skriftliga rutiner men enligt svaret finns etablerade arbetssätt. Dataskyddsombudet kan inte bedöma om det möjligen saknas någon rutin för de verksamhetskritiska systemen men uppmanar att verksamheten förvissar sig om att de är heltäckande utifrån ett dataskyddsperspektiv samt att ta fram skriftliga rutiner för Edlevo.

Inbyggt dataskydd och dataskydd som standard
Artikel 25

För att kunna visa att dataskyddsförordningen följs bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard.[3] Inbyggt dataskydd (privacy by design) innebär att den personuppgiftsansvariga tar hänsyn till integritetsskyddsreglerna redan när it-system och rutiner utformas, exempelvis användning av pseudonymisering det

[3] skäl 78 Allmän dataskyddsförordning

vill säga att ersätta personligt identifierbart material med artificiell identifiering eller hantering av fritextfält. Dataskydd som standard innebär att inställningarna för en produkt, ett system eller en tjänst ska vara dataskyddsvänliga, exempelvis ska inte opt-ins användas.

Den personuppgiftsansvarige har inga dokumenterade rutiner avseende inbyggt dataskydd och dataskydd som standard. Dataskyddsombudet rekommenderar den personuppgiftsansvarige att upprätta ett styrdokument eller komplettera annan befintlig med information om att principerna om inbyggt dataskydd och dataskydd som standard ska beaktas för tekniska system där personuppgifter behandlas (kan vara ett kommungemensamt styrdokument).

Ett sätt att arbeta med inbyggt dataskydd är att ha styrdokument avseende fritextfält. Enligt svaret på granskningen finns inget generellt styrdokument för fritextfält. Däremot pekar man i svaret på att det dokumenteras i de informationsklassningar, konsekvensbedömningar och riskanalyser som görs hos de personuppgiftsansvariga. Att använda fritextfält innebär en ökad risk för otillåten behandling och det är därför bra att där så är möjligt använda fördefinierade uppgifter i tex. kryssfält eller rullistor där så är möjligt. Tillsammans med ett styrdokument för fritextfält minimeras risken för otillåten behandling. Dataskyddsombudet rekommenderar de personuppgiftsansvariga att se över behovet av att ta fram ett styrdokument för användningen av fritextfält, troligen behövs det både ett generellt styrdokument och rutiner för vissa system såsom Treserva och Edlevo.

Personuppgiftsbiträden
Artikel 28

Det är vanligt att personuppgiftsansvariga anlitar personuppgiftsbiträden för att utföra en viss personuppgiftsbehandling. Även om den faktiska behandlingen överlåts kan aldrig själva personuppgiftsansvaret överlåtas. Den personuppgiftsansvarige måste således säkerställa att behandlingen sker i enlighet med dataskyddsförordningen, oavsett om denne utför behandlingen själv eller genom ett personuppgiftsbiträde. Ansvarsskyldighetsprincipen återspeglas bland annat i artikel 28 som fastställer den personuppgiftsansvariges skyldigheter när denne anlitar ett personuppgiftsbiträde.

Huvudregeln är att det är den personuppgiftsansvarige som är skadeståndsansvarig för skada som uppstår till följd av att personuppgifter har behandlats i strid med förordningen. Ett personuppgiftsbiträde kan dock bli ansvarigt för överträdelser av dataskyddsförordningen som är en följd av att biträdet inte har efterlevt den personuppgiftsansvariges instruktioner eller om biträdet har brutit mot de bestämmelser i förordningen som specifikt riktar sig till biträden. Eftersom den personuppgiftsansvarige måste säkerställa att personuppgiftsbehandlingarna som denne är ansvarig för sker i enlighet med dataskyddsförordningen, även om den faktiska behandlingen utförs av ett biträde, krävs det att denne har vetskap om hur biträdet behandlar och skyddar personuppgifterna. Ett första steg är att upprätta ett personuppgiftsbiträdesavtal eller annan rättsakt för att reglera förhållandet sinsemellan samt instruera personuppgiftsbiträdet. Nästa steg är att följa upp så att biträdet behandlar personuppgifterna i enlighet med de instruktioner som den personuppgiftsansvarige givit. Uppföljning av biträden bör göras löpande, men kan dock ske med olika intervall och olika omfattning beroende på hur riskfylld respektive behandling är. Rutiner för hantering av biträdessituationer bör finnas på plats hos verksamheten.

De personuppgiftsansvariga nämnderna har en gemensam rutin för upprättande och uppsägning av personuppgiftsbiträdesavtal (VG-RUT -S 7770-2). Precis som för tidigare rutiner så finns information om vem som upprättat dokumentet, vem som godkänt det samt när det reviderades. Det är tydligt i rutinen vad regelverket säger, vem som är ansvarig för vad. Det framgår också vad som gäller när någon av nämnderna är personuppgiftsbiträde. Dataskyddsombudet bedömer att rutinen mycket väl uppfyller kraven i dataskyddsförordningen.

Registerförteckning
Artikel 30

Personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register över sina behandlingar av personuppgifter. Register över personuppgiftsbehandlingar ska upprättas skriftligen, vara tillgängliga i elektroniskt format och hållas uppdaterade. På begäran ska registret göras tillgängligt för IMY. Vad som ska finnas med i registret beskrivs i artikel 30. För att hålla behandlingarna uppdaterade och på så sätt säkerställa efterlevnad av dataskyddsförordningen bör den personuppgiftsansvariga ha rutiner för upprätthållandet av registerförteckning.

Det finns ingen upprättad rutin för upprätthållandet av de personuppgiftsansvariga nämndernas registerförteckning. Som dataskyddsombudet förstår det har det för samtliga nämnder gjort ett omtag med registerförteckningen där man byter förteckningsverktyg (från Draftit till Stratsys). När det grundarbetet är färdigt är det viktigt att det finns ett kontinuerligt arbete med registerförteckningarna så förteckningarna hålls uppdaterad. Dataskyddsombudet rekommenderar de personuppgiftsansvariga nämnderna att anta en rutin (eventuellt som en del av ett årshjul) och implementera denna i verksamheten.

Incidenthantering
Artikel 33–34

Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål anmäla personuppgiftsincidenten till IMY inom 72 timmar såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. Den personuppgiftsansvarige är skyldig att dokumentera alla personuppgiftsincidenter oavsett om de är av sådan grad att de ska anmälas till IMY eller inte. Dokumentationskravet inbegriper omständigheterna kring incidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationsskyldigheten hänger ihop med principen om ansvarsskyldighet vad gäller att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna i dataskyddsförordningen efterlevs. För att kunna uppfylla skyldigheterna enligt förordningen är det viktigt att ha tillräckliga rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.

Den personuppgiftsansvarige har en tydlig rutin för hantering av personuppgiftsincidenter. Den är upprättad i september 2024 och det är tydligt vem som är ägare av dokumentet (dataskyddssamordnare). Till rutinen finns tre tillhörande instruktioner, dessa ger tydliga steg för steg instruktioner som komplement till rutinen

och utgår ifrån olika scenarion, om incidenten är allvarlig eller mindre allvarlig och om den som mindre allvarlig ska anmälas till IMY eller ej. Dataskyddsombudets bedömning är att rutinen med tillhörande instruktioner mycket väl uppfyller kraven i artikel 33–34 i dataskyddsförordningen.

Högriskbehandlingar
Artikel 35–36

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Den personuppgiftsansvarige ska vidare samråda med IMY före behandling om en konsekvensbedömning visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken. För att säkerställa arbetsgången vid en sådan riskbedömning bör den personuppgiftsansvarige ha rutiner gällande konsekvensbedömning och eventuellt förhandssamråd.

De personuppgiftsansvariga nämnderna har en rutin för högriskbehandlingar VG-RUT-S 8376. Även för denna rutin är det tydligt vilken roll som ansvarar för att upprätta den, vem som godkänner och när den senast uppdaterades. Av rutinen framgår tydligt varför, när och hur en konsekvensbedömning ska göras. Samt vilka roller som behöver vara involverade inklusive dataskyddsombudets roll. Dataskyddsombudet bedömer att rutinen väl motsvarar kraven i artikel 35 i dataskyddsförordningen. Det vore önskvärt om det i en policy eller en riktlinje fanns en kortare skrivning avseende högriskbehandlingar för att följa den hierarki av styrdokument som är brukligt att en personuppgiftsansvarig har.

Dataskyddsorganisation
Artikel 37–39

Den personuppgiftsansvarige ska under alla omständigheter utnämna ett dataskyddsombud bland annat om behandlingen genomförs av en myndighet eller ett offentligt organ. Den personuppgiftsansvarige har en skyldighet att tillhandahålla de resurser som krävs för att dataskyddsombudet ska kunna fullgöra sina arbetsuppgifter enligt förordningen. Det innebär att den personuppgiftsansvarige måste ha en dataskyddsorganisation inom sin verksamhet för att organisatoriskt skapa ett effektivt dataskyddsarbete enligt förordningens krav. Den personuppgiftsansvarige bör således ha en rutin eller annan beskrivning för att tydliggöra dataskyddsorganisationens roller och ansvar.

Som svar på granskningen har inte de personuppgiftsansvariga nämnderna bifogat någon dataskyddsorganisation i egentlig mening. Sektor Välfärd har en utsedd dataskyddssamordnare. I svaret på frågan om det finns en dataskyddsorganisation har ett antal rutiner räknats upp som bland annat, var för sig, visar på hur olika krav i dataskyddsförordningen tas om hand organisatoriskt. Det rör tex. hanteringen av personuppgiftsincidenter och begäran om registerutdrag. Dataskyddsombudet rekommenderar, speciellt med beaktande av att det rör tre nämnder men många och känsliga personuppgifter, att ett styrdokument för en dataskyddsorganisation tas fram, fastställs på lämplig nivå och implementeras.

Övriga relevanta styrande dokument

För att den personuppgiftsansvarige ska kunna visa att och hur dataskyddsförordningen efterlevs kan andra styrande dokument än ovanstående vara nödvändiga. Ett sådant exempel kan vara i de fall det förekommer kamerabevakning. Av föregående års granskning avseende kamerabevakning rekommenderas de personuppgiftsansvariga nämnderna att ta fram styrdokument avseende kamerabevakning. Ett arbete som vid tidpunkten för denna granskning inte är färdigt.

I svaret på granskningen har bifogats en rutin för videosamtal i Teams (VG-RUT-S 8089-1). Rutinen redogör tydligt för bakgrunden (med bland annat utmaningen med tredjelandsöverföringar) och vad som gäller för att använda Teams och dess olika funktioner. Dataskyddsombudet är positiv till att det finns en rutin framtagen för samtal i Teams.

Beslut, översyn och kommunikation

För att effektivt arbeta med styrande dokument som ett verktyg för ledning och styrning rekommenderas att löpande göra översyn av dokumenten. Genom att kontinuerligt revidera och fastställa säkerställs regelefterlevnaden och dataskyddet inkluderas systematiskt. Det rekommenderas också att ha utpekad ägare som ansvarar för att dokumenten uppdateras. Det behöver inte vara samma roll som faktiskt uppdaterar dokumentet men en roll med ansvar att revidering görs med återkommande intervall. En tydlig kommunikationsplan för styrande dokument är också viktigt för att upprätthålla informationen hos berörda medarbetare.

Det framgår mycket tydligt av de rutiner som bifogats svaret vem som är ägare av dokumentet och när det senast revideras. Enligt svaret på granskningen ansvarar medarbetare och chefer själva för att ta del av nya och reviderade rutiner i ledningssystemet Canea. Önskemål finns från dataskydds- och informationssäkerhetssamordnare att nya och ändrade styrdokument ska kommuniceras dels på intranätet dels på olika chefsforum, något som inte sker i dag. Dataskyddsombudet rekommenderar att de personuppgiftsansvariga ser till att dataskyddsfrågor i allmänhet och nya styrdokument i synnerhet kommuniceras i organisationen så att medvetenheten om dessa frågor ökar.

Det är i huvudsak rutiner som bifogats svaret på granskningen inte någon policy eller några riktlinjer avseende dataskydd. Ett vanligt synsätt när det gäller struktur för styrdokument är att nämnden (eller kommunen centralt som sedan antas av respektive nämnd) antar en policy som beskriver inriktning och att något ska göras, i det här fallet en integritetspolicy. Därefter antar ledningsgrupp eller liknade en riktlinje som talar om vad som ska göras. Till dessa styrdokument finns det sedan ett antal rutiner som talar om hur det ska göras och som ansvarig tjänsteperson fattar beslut om. För de tre personuppgiftsansvariga nämnderna saknas åtminstone delvis de två första leden. Dataskyddsombudet rekommenderar att nämnderna ser över behovet att en integritetspolicy med tillhörande riktlinjer.

Rekommendation

Dataskyddsombudet rekommenderar de personuppgiftsansvariga att:

- anta en integritetspolicy med tillhörande riktlinje(r) avseende dataskydd

- komplettera befintlig rutin eller upprätta separata rutiner för registrerades rättigheter avseende, rätten till radering, rättelse, begränsning av behandling, göra invändningar samt rätten till dataportabilitet
- se över behovet av styrdokument avseende fritextfält såväl generellt som för enskilda personuppgiftsbehandlingar/system
- när grundarbetet med registerförteckningen är klar ta fram en rutin för kontinuerlig översyn av förteckningen
- upprätta, besluta och implementera om en dataskyddsorganisation
- upprätta, besluta och implementera styrdokument på lämplig nivå avseende kamerabevakning
- se över hur nya och förändrade styrdokument avseende dataskydd bäst kommuniceras till verksamheten och hur de följs upp

2.2 Del 2: Uppföljning av föregående års granskningar

Dataskyddsombudet har vid tidigare års granskningar funnit brister inom vissa områden i dataskyddsarbetet hos personuppgiftsansvarig. Dataskyddsombudet har i denna granskningsdel följt upp handlingsplaner och åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer.

De personuppgiftsansvariga nämnderna har sedan granskningen av registerförteckningen, som gjordes 2023, reviderat respektive registerförteckning i samband med att man flyttat över förteckningen från Draftit till Stratsys. Av svaret framgår på generell nivå vilka åtgärder som vidtagits. Dataskyddsombudet har inte inom ramen för denna granskning, granskat innehållet i registerförteckningarna. 2023 granskades även information till de registrerade och för samtliga tre nämnder har ett arbete gjorts för att uppfylla kraven i artikel 13–14 i dataskyddsförordningen. I dag framgår det på hemsidan tex. tydligare vilka olika personuppgiftsbehandlingar respektive nämnd har. Sedan granskningen 2023 har en rutin för tecknande och uppsägning av PUB-avtal tagits fram, denna rekommendation ses därför som åtgärdad. Det återstår ett arbete med att få till uppföljning av ingångna PUB-avtal.

Dataskyddsombudet rekommenderar den personuppgiftsansvarige att prioritera samtliga rekommendationer i utförda granskningar. Hanteringen bör göras med ett riskbaserat angreppssätt. Det är viktigt att tillräckligt med resurser avsätts för att kunna genomföra ett systematiskt dataskyddsarbete över tid.

3. Slutsats

Dataskyddsombudet har i sin granskning av styrande dokument funnit mindre brister med låg risk. Det framstår som att de tre nämnderna i rätt stor utsträckning jobbar proaktivt med styrdokument rörande dataskydd framför allt rutiner. Arbetet med dataskydd, är precis som övrigt kvalitetsarbete en löpande process som ständigt pågår och som aldrig är något som blir färdig. Samhällsutvecklingen går allt snabbare och de förändringar som sker i omvärlden ställer nya krav när det kommer till dataskyddsarbetet i stort. Styrande dokument är ett viktigt verktyg för ledning och styrning och anger vad verksamheten ska göra, vem som ska göra det och i vissa fall hur det ska göras. Dataskyddsombudet rekommenderar därför den personuppgiftsansvarige att prioritera, resurssätta och aktivt arbeta med frågor kopplade till dataskydd för att hantera de brister som konstaterats och för att fortsätta arbeta med att skapa en god dataskyddskultur.