Personuppgiftsansvarig

Kommunstyrelsen, Gävle kommun

Granskningsrapport 2024/2025

Dataskyddsombud

Boel Burman

Datum

2025-11-19

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 visar att kommunstyrelsen har stora brister i sitt arbete med styrande dokument. Det saknas både kommunövergripande styrdokument i form av integritetspolicy och/eller riktlinje för dataskydd samt styrdokument för merparten av de ansvarsområden som det finns krav på i dataskyddsförordningen.

Dataskyddsombudet har också följt upp åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer som getts i samband med granskningarna 2022 och 2023. Såsom dataskyddsombudet förstår svaret på granskningen så har det inte förekommit ett systematiskt dataskyddsarbete utan mer ett reaktivt arbete utifrån dataskyddsombudets rekommendationer.

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)
- Personuppgiftsbiträdesavtal och uppföljning av leverantörer (2022)
- Motivering av rättsliga grunder (2022)

1.3 Avgränsning

Ingen avgränsning är gjord.

1.4 Metod

Ett antal frågor har skickats ut till den personuppgiftsansvariges dataskyddssamordnare som besvarats skriftligt. Svaret/yttrandet från dåvarande dataskyddssamordnaren är knapphändigt och det har därför varit svårt att fullt ut genomföra en granskning.

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[2].

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:

Svar på granskning av styrande dokument Kommunstyrelsen (594197)

2.1.2 Efterlevnad

Uppfyller till stora delar inte dataskyddsförordningens krav, stora brister finns

Dataskyddspolicy eller motsvarande
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, riktlinjer och

[1] artikel 5.2 Allmän dataskyddsförordning
[2] skäl 78 Allmän dataskyddsförordning

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.

Den personuppgiftsansvarige har en informationstext på sin publika webbplats om hur personuppgifter behandlas: Så här behandlar Kommunstyrelsen personuppgifter – Gävle kommun. Dataskyddsombudet anser att informationen är mer av karaktären ”information till de registrerade” än interna strategier för dataskydd.

Det finns en av kommunstyrelsen beslutad policy för informationssäkerhet och där ingår i begränsad utsträckning dataskydd: ”Informationssäkerhetspolicy – Gävle 2020”[3]. Den är enligt svaret på granskningen senast reviderad och fastställd 2022-11-22. 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”. Dataskyddsombudet rekommenderar att informationssäkerhetspolicyn revideras och fastställs regelbundet av KS och att den inkluderar dataskydd eller att en separat policy för dataskydd tas fram och att den/de därefter regelbundet fastställs för att visa på ansvarsskyldigheten i artikel 5.2 i dataskyddsförordningen.

Dataskyddsombudet har fått kännedom om att det finns utkast till kommunövergripande/kommunkoncernövergripande riktlinjer för dataskydd, informationssäkerhet och informationshantering men att dessa inte har upprättats fastställts eller implementerats. Varför så inte skett har dataskyddsombudet inte kännedom om. Kommunkoncernövergripande styrdokument som policy och riktlinjer är något som starkt efterfrågas av övriga personuppgiftsansvariga, vilket framkommit i samband med granskningarna av nämnderna och bolagen. Av ”Policy för styrdokument i Gävle kommun” framgår att ”fullmäktiges beslut är att fatta beslut i ärenden av principiell beskaffenhet eller annars av större vikt för kommunen” Det kan förstås som att det är KF som ska/bör anta en integritetspolicy eller riktlinje för kommunkoncernen. Alternativet är att varje nämnd/styrelse i egenskap av personuppgiftsansvarig antar en egen riktlinje/policy för att uppfylla kraven på ansvarsskyldighet enligt artikel 5.2 i dataskyddsförordningen. Dataskyddsombudet rekommenderar att utkastet till riktlinje för dataskydd (även de för informationssäkerhet och informationshantering då de indirekt visar på ansvarsskyldigheten) upprättas, fastställs och implementeras samt därefter regelbundet revideras och fastställs.

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.

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

Det framgår inte av svaret på granskningen om den personuppgiftsansvarige har ett styrdokument för att hantera begäran av de registrerades rättigheter. På nuvarande intranätet Knutpunkten finns det, som dataskyddsombudet bedömer det, en informationstext om de registrerades rättigheter men den har inte karaktären av ett styrdokument. Informationen på intranätet har tillkommit efter granskningsperioden. Dataskyddsombudet rekommenderar att den personuppgiftsansvarige upprättar, fastställer (på lämplig nivå) och implementerar styrdokument för att hantera registrerades samtliga åtta rättigheter.

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.

Det finns inte, som dataskyddsombudet förstår svaret på granskningen något övergripande styrdokument avseende tekniska och organisatoriska skyddsåtgärder. Det är inte ett direkt krav i förordningen men för att visa på ansvarsskyldigheten bör det framgå av en policy eller riktlinje (följt av rutiner). På Knutpunkten, kommunens nya intranät finns information ”systematiskt dataskyddsarbete - en del av vardagen”[4] Det kan ses som en del av de organisatoriska säkerhetsåtgärder som en personuppgiftsansvarig behöver ha, för att ge anställda information. Texterna har tagits fram och publicerats efter granskningsperioden varför dessa inte granskats i detalj men dataskyddsombudet är positiv till att informationen finns. Det finns också på Knutpunkten ett metodstöd med mallar och vägledningar rörande dataskydd, dessa är troligen än så länge inte så kända i organisationen men kommer framöver kunna utgöra ett bra stöd. Dataskyddsombudet rekommenderar att det av integritetspolicyn och/eller riktlinje för dataskydd finns skrivningar rörande tekniska och organisatoriska skyddsåtgärder (som då är kommunövergripande) och att detta sedan kompletteras med specifika styrdokument.

Av svaret på granskningen framkommer att det pågår ett arbete tillsammans med HR för att fram rutiner kring hantering av de olika nivåerna av skyddad identitet när det gäller personer som söker anställning eller är anställda. Som dataskyddsombudet förstår det är detta arbete inte avslutat nästan ett år efter att granskningssvaret

[4] Systematiskt dataskyddsarbete | Knutpunkten

skickades in. Samtidigt kan man förstå svaret som att det finns vissa rutiner, det är lite oklart utifrån svaret hur det ska förstås och inga rutiner har bifogats svaret. Eftersom KS är anställande myndighet i kommunen är det viktigt att det finns styrdokument på plats som ger tydlighet kring hur anställda (och f.d. anställda) med skyddad identitet ska hanteras. Vidare framkommer det av svaret att det finns rutiner i ekonomisystemet för kunder med skyddad identitet, denna rutin har inte bifogats svaret. Dataskyddsombudet rekommenderar att arbetet kring skyddade identiteter färdigställs och att den personuppgiftsansvarige förvissar sig om att det finns rutiner för all verksamhet rörande skyddad identitet.

När det gäller behörighetsstyrning så framgår det av svaret att HR har tydliga rutiner för behörighetsstyrning men att det inte finns lika tydliga instruktioner för övrig verksamhet hos den personuppgiftsansvarige. Rutinerna har inte bifogats svaret på granskningen varför dataskyddsombudet inte granskat dem. Dataskyddsombudet rekommenderar att den personuppgiftsansvarige förvissar sig om att det finns styrdokument avseende behörighetsstyrning för all verksamhet.

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.[5] 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 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.

Det framkommer inte av svaret på granskningen om det finns något övergripande styrdokument för inbyggt dataskydd och dataskydd som standard. Det finns en informationstext på Knutpunkten om vad inbyggt dataskydd och dataskydd som standard är och varför det är viktigt. Dataskyddsombudet bedömer att texten inte har karaktären av ett styrdokument. Dataskyddsombudet rekommenderar att den personuppgiftsansvarige upprättar som minst ett styrdokument med information om att principerna om inbyggt dataskydd och dataskydd som standard ska beaktas för tekniska system där personuppgifter behandlas, styrdokumentet kan med fördel vara kommunövergripande.

Det finns inte heller enligt svaret på granskningen framtagna styrdokument för hanteringen av fritextfält utan det anges att det finns kännedom hos systemägare och systemförvaltare att fritextfält ska minimeras. Dataskyddsombudet rekommenderar att ett övergripande styrdokument avseende fritextfält, upprättas, fastställs och implementeras samt att den personuppgiftsansvarige ser över behovet av specifika rutiner för de system som KS ansvarar för.

[5] skäl 78 Allmän dataskyddsförordning

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.

Såsom dataskyddsombudet förstår svaret på granskningen saknas skriftliga styrdokument för att teckna personuppgiftsbiträdesavtal och för att följa upp ingångna avtal. I svaret hänvisas till en Teams-kanal där dataskyddssamordnarna informerar om gällande rutiner, någon rutin har dock inte bifogats svaret. På Knutpunkten finns en generell informationstext om personuppgiftsbiträde och PUB-avtal samt ett metodstöd i form av ”vägledning för hantering av instruktion i PUB-avtal” (information som tillkommit efter att svaret på granskningen skickats in) Dataskyddsombudet rekommenderar att den personuppgiftsansvarige upprättar, fastställer och implementerar ett styrdokument för tecknande och uppföljning av personuppgiftsbiträdesavtal där det bland annat tydliggörs när ett PUB-avtal ska tecknas, vilken roll som är ansvarig, vem som har mandat att underteckna PUB-avtalet samt när, hur och vilken roll som är ansvarig för uppföljningen.

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.

Enligt svaret på granskningen har den personuppgiftsansvarige gjort ett omtag med registerförteckningen efter granskningen 2023, den nya förteckningen kommer att finnas i Stratys. Enligt svaret så finns det ett årshjul (som inte bifogats svaret) där arbetet med registerförteckningen sker första kvartalet varje år. Dataskyddsombudet rekommenderar, utifrån att årshjulet inte bifogats svaret, att kommunstyrelsen tar fram ett styrdokument för regelbunden översyn av registerförteckningen och att man färdigställer registerförteckningen.

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.

Det har inte bifogats någon rutin för hantering av personuppgiftsincidenter i svaret på granskningen. Det framgår av svaret att ett utkast togs fram inför att dataskyddsförordningen trädde i kraft 2018 men att den rutinen (och andra som togs fram samtidigt) inte upprättats och fastställts. Även för personuppgiftsincidenter finns numera en information på Knutpunkten som i likhet med övrig text på intranätet inte har karaktären av styrdokument. Det finns också ett metodstöd i form av ”Vägledning för utredning av personuppgiftsincidenter” på intranätet. Dataskyddsombudet rekommenderar att den personuppgiftsansvarige upprättar, fastställer (på lämplig nivå) och implementerar ett styrdokument för hantering av personuppgiftsincidenter.

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.

Det framkommer inte av svaret om den personuppgiftsansvarige har något styrdokument avseende högriskbehandlingar. Den framkommer inte heller av svaret

om det görs konsekvensbedömningar. Dataskyddsombudet har kännedom om att konsekvensbedömningar görs men inte om det görs systematiskt och i den utsträckning som krävs enligt kraven i dataskyddsförordningen. Dataskyddsombudet rekommenderar den personuppgiftsansvarige att upprätta rutin som reglerar hantering av högriskbehandlingar. Dataskyddsombudet anser att det åtminstone bör finnas en generell skrivning kring när en konsekvensbedömning ska göras och att dataskyddsombudet ska involveras och rådfrågas vid behandlingar som kan medföra allvarliga risker för de registrerades rättigheter.

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.

Enligt svaret på granskningen togs ett utkast till dataskyddsorganisation fram 2018 (samt en organisation för dataskyddsombud för hela Gävle kommunkoncern med bolag och förbund samt Hofors och Ockelbo). Utkastet har dock som dataskyddsombudet förstått det inte fastställts skriftligt och implementerats. Det har dock i praktiken funnits en organisation med flera dataskyddssamordnare för Sektor Styrning och Stöd sedan införandet av dataskyddsförordningden. I januari 2025 förändrades dataskyddsorganisationen och består i dag av två (tre) dataskyddssamordnare i stället för en per enhet. Dataskyddsombudet har dock inte kännedom om organisationen är skriftligt beslutad och rekommenderar att så görs om det inte finns ett skriftligt beslut.

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. Det framgår inte av svaret om de rekommendationer som gavs av dataskyddsombudet avseende kamerabevakning har åtgärdats.

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.

Då inga styrdokument bifogats svaret på granskningen och dataskyddsombudet inte heller funnit några egentliga styrdokument går det egentligen inte att granska hur

beslut, översyn och kommunikation ser ut. Dataskyddsombudet rekommenderar därför att skriftliga styrdokument tas fram och regelbundet uppdateras, där det tydligt framgår vem som är ansvarig.

Rekommendation
Dataskyddsombudet rekommenderar den personuppgiftsansvarige att:

- revidera och fastställa den kommunövergripande informationssäkerhetspolicyn där dataskydd ingår som en integrerad del och att den därefter regelbundet fastställs (även om inga ändringar skett) för att visa på ansvarsskyldigheten. Alternativt att upprätta en kommunövergripande integritetspolicy.
- fastställa och implementera det framtagna utkastet till riktlinje för dataskydd (samt informationssäkerhet och informationshantering) och att de därefter regelbundet fastställs (även om inga ändringar skett) för att visa på ansvarsskyldigheten
- ett eller flera styrdokument avseende registrerades rättigheter upprättas, fastställs och implementeras. Överväg om ett sådant styrdokument skulle kunna vara kommunövergripande
- det av en integritetspolicy och/eller riktlinje för dataskydd framgår på övergripande nivå skrivningar för tekniska och organisatoriska skyddsåtgärder samt att dessa kompletteras med specifika rutiner
- arbetet med styrdokument avseende skyddade identiteter färdigställs, fastställs och implementeras i verksamheten
- det upprättas som minst ett styrdokument med information om att principerna om inbyggt dataskydd och dataskydd som standard ska beaktas för tekniska system där personuppgifter behandlas, styrdokumentet kan med fördel vara kommunövergripande
- ett övergripande styrdokument avseende fritextfält, upprättas, fastställs och implementeras samt att den personuppgiftsansvarige ser över behovet av specifika rutiner för de system som KS ansvarar för
- det tas fram ett styrdokument för regelbunden översyn av registerförteckningen och att man färdigställer registerförteckningen
- det upprättas, fastställs (på lämplig nivå) och implementeras ett styrdokument för hantering av personuppgiftsincidenter
- upprätta rutin som reglerar hantering av högriskbehandlingar (som minst en generell skrivning om att konsekvensbedömningar ska göras och att DSO ska involveras)
- skriftligt fastställa den dataskyddsorganisation som finns i praktiken om så inte är gjort

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. Som nämnts ovan har den personuppgiftsansvarige gjort ett omtag med registerförteckning och lagt över det i ett nytt förteckningsverktyg, hur långt man kommit med det arbetet framgår inte. Det ska enligt svaret finnas ett årshjul (som DSO inte fått ta del av) där arbetet med

registerförteckningen sker första kvartalet varje år. Texten på kommunens hemsida har omarbetats enligt de rekommendationer som DSO gav vid granskningen. Dock är informationen på en övergripande nivå. När det gäller rekommendationerna för PUB-avtal (tecknande och uppföljning) kvarstår delvis arbetet som dataskyddsombudet förstår svaret (se även ovan).

3. Slutsats

Dataskyddsombudet har i sin granskning av styrande dokument funnit stora brister i den personuppgiftsansvariges dataskyddsarbete. 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. Rutinbeskrivningar är också betydelsefulla för att säkerställa att dataskyddsförordningens regler följs, inte minst för att reducera personberoenden.

Dataskyddsombudet rekommenderar därför den personuppgiftsansvarige att prioritera 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.