Gävle KOMMUN

**Personuppgiftsansvarig**

*Kultur- och fritidsnämnden, Gävle kommun*

# Granskningsrapport 2024/2025

**Dataskyddsombud**

Boel Burman (Fridah Gomér Pettersson)

**Datum**

2025-07-31

# 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 kultur- och fritidsnämnden vid det ursprungliga granskningstillfället hösten 2024 hade stora brister vad gäller interna strategier för dataskydd. Av det kompletterande svaret som lämnats i maj 2025 framkommer att ett omtag gjorts och att några styrdokument tagits fram och beslutats vilket visar på att det pågår ett arbete för att i större utsträckning visa på ansvarsskyldigheten. Det saknas alltjämt dokumentation och rutinbeskrivningar för intern hantering. Det är viktigt med dessa dokument för att säkerställa att dataskyddsförordningens regler följs och för att minska risken för personberoenden.

Dataskyddsombudet har också följt upp handlingsplaner och åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer som getts i samband med granskningarna 2022 och 2023. Enligt svar från den personuppgiftsansvarige finns ett pågående arbete för samtliga 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. Det första granskningssvaret inkom 1,5 månad efter ursprungsdatum. Dataskyddsombuden här därefter haft en dialog med såväl dåvarande som nuvarande dataskyddssamordnare och ett kompletterande svar inkom i maj 2025 från de nya dataskyddssamordnaren. Detta svar har i viss utsträckning tagits med i granskningen.

## 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:**

Frågesvar dokumentation DSO 2024- 11 - 11.xlsx

Kompletterande svar 2025-05-19 med bilagorna;

- Informationshanteringsplan Kultur- och fritidsnämnden
- LG-STÖ-9122-v1.0 Hantering av personuppgifter i e-post
- LG-STÖ-9121-v1.0 Hantering av begäran om registerutdrag
- Policy för informationssäkerhet Gävle kommun. Reviderad efter yttrande 2020-08-28
- Rutin hantering av personuppgiftsincident
- LG-STY-8367.v2.0 Delegationsordning Kultur- och fritidsnämnden

[1] artikel 5.2 Allmän dataskyddsförordning

[2] skäl 78 Allmän dataskyddsförordning

- KF beslut 3§ att anta informationssäkerhetspolicyn

Det kompletterande svaret har i viss utsträckning tagits med i granskningen efter en dialog med den personuppgiftsansvariges dataskyddssamordnare. Normalt tas inte kompletteringar med men eftersom granskningen av olika skäl dragit ut på tiden görs ett undantag så granskningen bättre speglar verkligheten.

### 2.1.2 Efterlevnad

Uppfyller delvis dataskyddsförordningen krav, brister finns[3]

**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 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 de behandlar personuppgifter inom nämnden Så här behandlar Kultur- och fritidsnämnden dina personuppgifter – Gävle kommun. Dataskyddsombudet anser att informationen 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”[4]. Den har inte bifogats i det ursprungliga svaret på granskningen, men har bifogats det kompletterande svaret som skickades in i maj. Att den inte nämns i det ursprungliga svaret skulle kunna indikera att de personuppgiftsansvariga inte då känt till dokumentet och att kunskapen om det är låg i organisationen. 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”. Kultur-

[3] Baserat på det ursprungliga granskningssvaret finns det stora brister i dataskyddsarbetet. Med kompletteringar landar resultatet något högre.

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

och fritidsnämnden har inte, som dataskyddsombudet förstår det fattat något beslut om att anta ovan nämnda policy som sin egen och av det kompletterande svaret framkommer att man bedömer att det inte behövs när KF fattat beslut som gäller för samtliga nämnder. Dataskyddsombudet rekommenderar att den personuppgiftsansvarige på något sätt gör det tydligt att policyn är en del av dennes ansvarsskyldighet enligt dataskyddförordningen och också tydliggör för verksamheten att så är fallet.

**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.

I det ursprungliga svaret på granskningen ingick inte några styrdokument avseende registrerades rättigheter. I det kompletterande svaret finns en rutin för hantering av registerutdrag. Som dataskyddsombudet bedömer det, är rutinen nyligen framtagen, dvs efter den egentliga granskningsperioden. Det framgår inte tydligt av dokumentet när det är upprättat och vem som fattat beslut om det. Rutinen innehåller i huvudsak det som krävs för att uppfylla kraven i ovan nämnda artiklar dock bedömer DSO att skrivningarna rörande gallring behöver anpassas till Livsmiljös verksamhet. Det saknas vidare styrdokument för de övriga rättigheter som de registrerade har såsom rätten till radering, rättelse, begränsning, invändning och dataportabilitet. Dataskyddsombudet rekommenderar att rutiner tas fram för samtliga av de registrerades rättigheter samt att det tydligt framgår när styrdokumenten upprättades och vem som fattat beslut.

**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.

Såvitt dataskyddsombudet känner till finns det inga styrande dokument antagna av den personuppgiftsansvarige som reglerar behörighetsstyrning och hantering av verksamhetskritiska system.

Den personuppgiftsansvarige har uppgivit att det finns rutin för hantering av skyddad identitet i processtödet CaneaOne. Dataskyddsombudet kan endast utläsa att rutinerna avser Budget- och skuldrådgivningen, Konsument Gästrikland. Dataskyddsombudet saknar således en rutin för övriga delar av den personuppgiftsansvariges verksamhet alternativt, och ännu hellre, en övergripande för samtliga verksamheter.

Den personuppgiftsansvarige rekommenderas att se över dessa delar och i förekommande fall upprätta rutin för desamma.

## 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.

Den personuppgiftsansvarige har inga dokumenterade rutiner avseende inbyggt dataskydd och dataskydd som standard. Den personuppgiftsansvarige har i det ursprungliga granskningssvaret hänvisat till ”handbok dataskyddsförordningen” vad gäller hantering av fritextfält, men vid dialog med den personuppgiftsansvarige framkommer att det inte verkar finnas någon handbok. Dataskyddsombudet rekommenderar den personuppgiftsansvarige att upprätta rutin med information om att principerna om inbyggt dataskydd och dataskydd som standard ska beaktas för tekniska system där personuppgifter behandlas.

## 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

[5] skäl 78 Allmän dataskyddsförordning

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.

Enligt den personuppgiftsansvarige används SKR:s mallar för personuppgiftsbiträdesavtal i de situationer där personuppgifter kan komma att behandlas av biträde. Vidare finns personuppgiftsbiträdesavtal dokumenterade i Platina. Dataskyddsombudet anser att det finns brister i dokumentationen av den praktiska hanteringen avseende biträdessituationer. Ovan upplysning är i sig tillfredsställande men det bör finnas en rutinbeskrivning med information om exempelvis hur biträdesförhållanden ska ingås, vilken roll som har rätt att besluta om att ingå biträdesavtal, hur ofta och av vem uppföljning ska ske. Dataskyddsombudet rekommenderar den personuppgiftsansvarige att upprätta rutin för hur biträdessituationer praktiskt ska hanteras internt.

## 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.

Dataskyddsombudet har inom ramen för granskningen inte fått ta del av någon rollbeskrivning för dataskyddssamordnarrollen men har kännedom om att det i en sådan beskrivs att denne är ansvarig för att uppdatera personuppgiftsbehandlingsregistret löpande. Såvitt dataskyddsombudet känner till finns det inga övriga styrande dokument som reglerar hantering av registerförteckningen. Såsom dataskyddsombudet förstått det har det efter den ursprungliga granskningsperioden gjorts ett omtag med arbetet med registerförteckningen dock saknas som det förstås alltjämt skriftliga rutiner för detta. Dataskyddsombudet rekommenderar den personuppgiftsansvarige att upprätta rutin för hur registerförteckningen praktiskt ska hanteras internt. Det kan handla om såväl vilken roll som är ansvarig administrera begäran om registerutdrag som tidsintervall för översyn etc.

## 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.

Av det första svaret på granskningen framkom såvitt dataskyddsombudet förstår det att det inte fanns några styrande dokument som reglerar hanteringen av personuppgiftsincidenter. På den personuppgiftsansvariges intranät finns en länk med information om personuppgiftsincidenter inom Gävle kommun samt en länk till en e-tjänst[6]. Dataskyddsombudet anser dock att informationen på intranätet inte är en upprättad, dokumenterad rutin hos den personuppgiftsansvarige för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter. I det kompletterande svaret från maj i år finns en ”Rutin för hantering av personuppgiftsincidenter” bifogat svaret. Den är som dataskyddsombudet förstår det nyligen upprättad och fastställd (även om det inte tydligt framgår av dokumentet i sig). Rutinen uppfyller i huvudsak de kraven som finns 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.

Såvitt dataskyddsombudet känner till finns det inga styrande dokument som reglerar hantering av högriskbehandlingar. Dataskyddsombudet rekommenderar därför den personuppgiftsansvarige att upprätta rutin som reglerar hantering av

[6] https://ankaret.gavle.se/Kommunen/Gemensamt/Datorskyddsforordningen-i-Gavle-kommun/Anmal-personuppgiftsincident1/

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.

Den personuppgiftsansvarige har i det ursprungliga svaret uppgivit att den personuppgiftsansvarige har en dataskyddsorganisation som sedan 2022 består av en dataskyddssamordnare samt ett dataskyddsombud. Organisationen beslutades i ledningsgruppen 2018 och uppdaterades 2022. I svaret från den personuppgiftsansvarige skrivs dock att det rör SBN (samhällsbyggnadsnämnden). Dataskyddsombudet misstänker att svaret är kopierat och inte justerat, på grund av den mänskliga faktorn. Dataskyddsombudet har inom ramen för granskningen inte fått ta del av någon ytterligare beskrivning av dataskyddsorganisationen men har kännedom om att det även finns dataskyddskoordinatorer (DSK) som stöttar dataskyddssamordnaren i det operativa dataskyddsarbetet. I granskningssvaret framkommer att det är många DSK:er som slutat, varför dataskyddsombudet gör kopplingen till den personuppgiftsansvariges dataskyddsorganisation.

Såsom dataskyddsombudet förstått det av dialogen med den nya dataskyddssamordnaren pågår under våren 2025 ett arbete med dataskyddsorganisationen om det även kommer att ingå att ta fram en ny skriftlig beslutad organisation är oklart.

Dataskyddsombudet anser att den personuppgiftsansvariges uppbyggnad av dataskyddsorganisation i teorin motsvarar de förväntningar som finns på en dataskyddsorganisation. Under våren har förändringar skett i dataskyddsorganisationen där en ny dataskyddssamordnare utsetts. Om så inte skett rekommenderar dataskyddsombudet att det dokumenteras vad som ingår i deras roller vad som ingår i dataskyddskoordinatorernas uppdrag samt vad som ingår i chefers uppdrag när det gäller dataskydd

**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.

Den personuppgiftsansvarige bedriver kamerabevakning sedan 2005 på Fjärran höjderbadet och sedan 2015 på Gavlevallen. Dataskyddsombudet har vid tidigare

granskning och även vid denna granskning fått information om att det ska finnas ett styrande dokument i form av checklista för kamerabevakningen. Detta har dock inte delgetts dataskyddsombudet och går inte att finna i CaneaOne. Dataskyddsombudet har därför inte kunnat göra någon bedömning av det. Dataskyddsombudet rekommenderar att säkerställa huruvida checklistan innehåller relevant information samt i förekommande fall uppdatera med rutinbeskrivning avseende arbetssätt, roller och ansvar för att regelbundet dokumentera och utvärdera kamerabevakningen[7].

I det första, ursprungliga svaret på granskningen fanns få styrande dokument bifogade, tex. så saknades informationshanteringsplan och delegationsordning. Dessa bifogades det kompletterande svaret som skickades in i maj. Eftersom dessa dokument inte bifogats det ursprungliga svaret har dataskyddsombudet inte gjort någon detaljerad granskning av dem. Men konstaterar att det av delegationsordningen framgår vilka ärenden som det ska fattas beslut på delegation och av vem och att det av. Av informationshanteringsplanen framgår för de flesta handlingsslag om gallring ska ske och i så fall när (om informationshanteringsplanen omfattar samtliga handlingsslag har inte granskats).

Dataskyddsombudet rekommenderar att den personuppgiftsansvarige fortsätter arbetet med att ta fram styrande dokument avseende dataskydd och att man tar fram en åtgärdsplan för de styrdokument som saknas (för att visa på ansvarsskyldigheten)

**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.

Den personuppgiftsansvarige har uppgett att dokumenten finns i ledningssystemet CaneaOne och dokumentupprättaren får en påminnelse om att dokumentet ska uppdateras en gång per år. Vid uppdatering i CaneaOne finns en godkännare utsedd. Dokumenten kommuniceras via verksamhetens processstödjare. Att inkludera styrande dokument i verksamhetens årshjul för att löpande uppdatera och fastställa dokumenten anser dataskyddsombudet är ett bra och effektivt arbetssätt.

*Rekommendation*

Dataskyddsombudet rekommenderar den personuppgiftsansvarige att:

1. anta kommunövergripande policy för informationssäkerhet alternativt på annat sätt tydligt visa att policyn tillämpas inom nämnden

2. Upprätta eller komplettera rutin för att hantera begäran om de registrerades rättigheter för rättelse, radering, begränsning, invändning samt dataportabilitet.

[7] Se resonemang i granskningsrapport avseende kamerabevakning.

3. se över befintliga rutiner för skyddad identitet och i förekommande fall upprätta övergripande rutin för samtliga verksamheter.

4. upprätta rutin med information om att principerna om inbyggt dataskydd och dataskydd som standard ska beaktas för tekniska system där personuppgifter behandlas.

5. upprätta rutin för hur biträdessituationer praktiskt ska hanteras internt.

6. upprätta rutin för hur registerförteckningen praktiskt ska hanteras internt.

7. upprätta rutin som reglerar hantering av högriskbehandlingar.

8. upprätta styrande dokument som beskriver dataskyddsorganisationens roller och ansvar.

9. säkerställa checklista och i förekommande fall uppdatera rutin avseende kamerabevakning.

10. genomföra en kartläggning och sammanställning över de styrande dokument som i dagsläget finns och berör dataskydd samt ta fram en åtgärdsplan för de som inte finns men som bör finnas enligt dataskyddsförordningen.

## 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. Enligt svar från den personuppgiftsansvarige finns ett pågående arbete för samtliga rekommendationer från 2022 och 2023. Flera av åtgärderna som vidtas hanteras genom upprättande av rutiner, vilket dataskyddsombudet är positiv till. Den personuppgiftsansvarige har ett pågående arbete med att genomföra anpassningar i samband med implementation av systemstödet Stratsys för registerförteckningen.

Dataskyddsombudet rekommenderar den personuppgiftsansvarige att prioritera hantering av tidigare lämnade rekommendationer, särskilt få till en korrekt registerförteckning eftersom det är en av grundpelarna i dataskyddsförordningen.

# 3. Slutsats

Dataskyddsombudet har i sin granskning av styrande dokument funnit flertalet brister i delar av den personuppgiftsansvariges dataskyddsarbete. Under våren 2025 har ett arbete påbörjats som dataskyddsombudet bedömer kommer att höja nivån på den personuppgiftsansvariges dataskyddsarbete, vilket är positivt. 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.