Stockholms stad

Bilaga 10

# GDPR Årsrapport

År 2022

Serviceförvaltningen

**GDPR årsrapport**
Januari 2023

**Dnr:** SF 2023/91
**Utgivningsdatum:** 2022-12-13
**Kontaktperson:** Rosemarie Arnmark

# 1 Bakgrund

Denna rapport presenterar resultatet på årets granskning av efterlevnaden av Dataskyddsförordningen.

Rapporten är framtagen av dataskyddsombudet som nämnd eller bolagsstyrelse har utnämnt.

Målgrupp är beslutsfattare som ska fatta beslut om det kommande årets dataskyddsarbete. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever Dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnd/bolagsstyrelse uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

En annan målgrupp är medarbetare i den nämnd eller bolagsstyrelse som blivit granskad, som bistår dataskyddsombudet med information som ligger till grund för granskningen, och kvalitetssäkring att rätt information blivit granskad.

I Dataskyddsförordningen finns en stor mängd krav, tillämpliga krav har, i denna rapport, blivit indelad i granskningsområden. Granskningen innebär att dessa områden kontrolleras och bedöms i hur väl de möter lagens krav, och om det finns brister och vilka dessa brister i så fall är. Bristerna värderas utifrån de risker på dataskyddet som bristerna innebär. Även åtgärder föreslås för bristerna.
Granskningen är i sig krav från Dataskyddsförordningen, för att man ska mäta efterlevnad, kunna åtgärda brister och planera sitt förbättringsarbete.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med Dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå

**Förklaringar i rapporten**

I rapporten används så kallad trafikljus för att tydliggöra bedömd status för kontrollområdet. Här presenteras vad respektive färg motsvarar. Det innebär i realiteten att enbart status representerad av grön färg kan sägas vara godkänd status. För förbättringar bör fokus vara på att åtgärda brister som fått röd status omgående, brister som fått orange status bör planeras skyndsamt och brister som fått gul status kan planeras att genomföras i samband med andra närliggande insatser.

**Trafikljusförklaring**

| | |
|---|---|
| | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

# Innehåll

# 2 Sammanfattning av rapporten

I detta avsnitt kommenteras kort kring framsteg och översiktlig bedömd status.

Rapporten som helhet innehåller sammanfattningar och specificeringar. Den som i första hand vill läsa sammanfattning av granskning kan läsa Kapitel 2. I de följande kapitlen ges en fördjupad information av resultat av granskningar, bedömning och rekommendationer.

## 2.1 Framsteg under året

Under året har ett antal framsteg uppnåtts gentemot planering för förbättringsarbetet av efterlevnaden av Dataskyddsförordningen.

Under året har extern DSO tillsats som man delar med fem andra fackförvaltningar. Tanken är att det kan vara fördelaktigt med utomstående expertis, samt synergi effekter med en DSO som kan fånga styrkor hos enskilda förvaltningar som kan komma de övriga tillgodo.

En utbildningsinsats är planerad att genomföras under första kvartalet av 2023. Utbildningsinsatsen är avsedd att stärka de roller som har ansvarsområden på förvaltningen och stöttar den övriga organisationen i frågor som tangerar GDPR. Även här samordnat och gemensamt för förvaltningarna med tanke på synergi effekter. Även roller som objektansvariga och projektledare behöver få stärkt GDPR medvetenhet då de har ansvarspunkter för att upprätthålla och införa efterlevnadskraven i förvaltning och i projekt.

För att underlätta arbetet för konsekvensanalys, förbereds utbildningsinsats för att tydliggöra momentet tröskelanalysen för att formellt definiera då konsekvensbedömning inte anses behöva genomföras. Tröskelanalysen är beskriven i underlag för utbildningsinsatsen.

## 2.2 Översiktlig bedömd status för rapporteringsområden

| | | | | |
|---|---|---|---|---|
| Registerförteckning | | X | | |
| Styrdokument | | X | | |
| Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar | | | | X |
| Konsekvensbedömningar | | | | X |
| Individens rättigheter | X | | | |
| Personuppgiftsincidenter | | X | | |
| Personuppgiftsbiträdesavtal | | X | | |

(För specificering se respektive avsnitt)

## 2.3 Sammanfattning av föreslagna åtgärder

Under detta avsnitt sammanfattas de föreslagna åtgärderna från granskade efterlevnadsområden gällande dataskyddsarbete.

- Registerförteckningen kompletteras med föreslagen information.
- Rekommenderar att ansvar för dokument och mallar är fastställt och att aktualitet är tydlig.
- Stötta organisationen att jobba kontinuerligt och systematiskt med PuB avtal

## 2.4 Observationer

### Observation 1

Troligen bör ett utökat samarbete utformas för att skapa grund för effektivare och smidigare dataskyddsarbete.
Samarbetet är beroende av rollen informationssäkerhetssamordnaren som ansvarar för att hålla ihop arbetet med informationsklassning och riskanalys, samt informationsansvarig ör behandlingen som har information om själva behandlingen och vilka personuppgifter som ingår.

Risk: Om inte samsyn upprättas kring dessa moment inom dataskyddsarbetet kan det innebära att det blir svårt att höja kvalitén på dataskyddarbetet.

### Observation 2

Under hösten har administrativ chef beställt kompletterande utbildning för de roller som behöver förstå Dataskyddsdelarna i sitt eget ansvarsområde.
Utbildningen är planerad att genomföras under Q1 2023

### Observation 3

Säkerställ att den arbetsmodell som används för riskanalys på ett tydligt sätt får fram riskvärde för riskerna eftersom det i sin tur ligger till grund för bra konsekvensvärdering och åtgärdsframtagning.
Det skall vara tydligt vilka risker och behandlingar som har högst värde, dock bör även planeras för åtgärder även där riskvärdet är lägre.

Då DSO arbetar med ytterligare fem fackförvaltningar skulle ett likartat arbetssätt i detta även kunna underlätta för DSO’s arbete

## 2.5 Sammanfattning rekommendationer till PUA

- Säkerställa att goda förutsättningar finns för nära samarbete mellan DSO, informationssäkerhetssamordnare samt eventuellt sakkunniga för respektive behandling.
- Förbered utbildningsinsatsen med förberedande halvdags-workshop där DSO med informationssäkerhetssamordnare från respektive förvaltning av de sex

fackförvaltningarna som delar DSO, skapar samsyn inte minst för processen att sammanställa information för registerförteckning, informationsklassning, riskanalys och eventuell konsekvensbedömning.

# 3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som Dataskyddsförordningen avser.

Stadens obligatoriska rapporteringsområden är

- registerförteckning,
- styrdokument samt fastställda rutiner och processer
- tekniska och organisatoriska säkerhetsåtgärder för personuppgiftsbehandlingar,
- konsekvensbedömningar,
- individens rättigheter och
- personuppgiftsincidenter.
- Personuppgiftsbiträdesavtal med instruktioner

I rapporten redogörs för bedömning av bolagets status på efterlevnaden av kontrollerade rapporteringsområden, samt DSO:ns slutsatser samt rekommendationer för förbättringsinsatser.

Dataskyddsförordningen pekar genomgående på att arbetssätt och rutiner *ska* vara dokumenterade. Detta kan sättas i relevans till kravet på att den personuppgiftsansvarige måste kunna *visa* att Dataskyddsförordningen principer för behandling av personuppgifter efterlevs (artikel 5).

## 3.1 Registerförteckning

### 3.1.1 Bakgrund och syfte

Förteckning på behandlingar, generellt kallad registerförteckning, på Serviceförvaltningen benämnt behandlingsregister, är ett underlag som är viktigt på flera punkter. Det är lagkravkrav på att kartlägga de behandlingar som görs på personuppgifter samt att dokumentera kartläggningen med ett antal informationsuppgifter kravställda att de ska ingå som minimum i dokumentationen. Dessutom är förteckningens ingående information viktigt för att kunna arbeta med dataskydd, registerförteckningen kan sägas vara såväl grunden för och centralt för arbetet med att efterleva Dataskyddsförordningen.

Dataskyddsarbetet bör ha initierats av kartläggning och dokumentation på behandlingarna där minst villkorade informationspunkter kan ingå. Till det finns det informationspunkter som, i det fall de ingår, underlättar kontroll- och förbättringsarbetet.

Dokumentationen är det som benämns som registerförteckningen, som ska hållas uppdaterad i vart fall på årsbasis eller då förändringar sker som förändringar i befintliga behandlingar, nya behandlingar eller behandlingar som upphört.

Syftet med kontroll av registerförteckningen är för att stämma av att den hålls uppdaterad, aktuell och komplett. Om brister noteras av DSO så rekommenderar denne lämpliga förbättringsinsatser.

### 3.1.2 Resultat

| Fråga/kontroll | Svar |
|---|---|
| Antal behandlingar som är registrerade? | 828 |
| Har nödvändiga uppdateringar gjorts? | En genomarbetning görs årligen |
| Bedöms registerförteckningen vara fullständig? | För de informationsposter som registerförteckningen innehåller är bristen marginell. Totalt 98 saknade poster av 828. Däremot bedömts registerförteckningen inte innehålla alla nödvändiga informationsposter |
| Har verksamheten lämpliga rutiner för registerföring? | En genomarbetning görs årligen, enstaka uppdateringar kan ske på initiativ av informationsägare |
| Övrigt | Tröskelanalys har diskuterats som komplement i arbetsprocessen och är planerad i extra GDPR utbildningsinsats. |

### 3.1.3 Status för brister gällande registerförteckningen

| | | | |
|---|---|---|---|
| | X | | |

För vissa behandlingar är det oklart om uppdatering är genomförd under året. Förslagsvis kan man införa rutin som stöttar kontinuerligt arbete med registerförteckningen, att kontrollera, komplettera samt uppdatera informationen i registerförteckningen. Att jobba med ett kontinuerligt arbete bör underlätta planeringen så att alla de uppdateringar man önskar åberopa för året är helt klara i god tid innan informationssammanställningar och granskningar för årsrapporten startar.

Komplettering av tröskelanalys information i registerförteckningen har diskuterats och beslutats av administrativ chef.

Med hänsyn taget till det stora antalet registreringar 828 så är saknade poster en mycket liten brist, totalt 98 saknade poster på de informationsposter i förteckningen som är viktiga i en registerförteckning.

Serviceförvaltningens behandlingsregister är matchad mot den miniminivå som IMY presenterar som nödvändig utifrån rent lagmässiga krav.

För att gynna ett framtida förenklat arbete med att överblicka status för efterlevnadsarbetet rekommenderas att utöka informationen enlig den interna bilagan som bifogats årsrapporten. Fördelarna med det gör att information om status för efterlevnad framgår i registerförteckningen för respektive behandling. Istället för att olika informationsdelar skall sökas fram på annat håll för varje behandling.

En noterad svaghet med Serviceförvaltningens registerförteckning, behandlingsregistret, är att alla kategorier personuppgifter står i ett och samma fält, man tydliggör alltså inte särskilda kategorier, eller eventuell förekomst av skyddade personuppgifter eller andra personuppgifter av känslig karaktär som exempelvis ekonomisk information. Exempelvis för behandling 3.3.1 förekommer hälsouppgifter, den enda notering på skyddsåtgärd för detta är ” Behörighetsstyrd åtkomst till funktionsbrevlåda”. Har i detta fall verkligen informationsklassning och riskanalys fastställt att det är tillräcklig säkerhetsåtgärd? Den informationen finns inte i Serviceförvaltningens registerförteckning.

Detta gör att arbetet med att sammanställa, överblicka och analysera informationen om graden av efterlevnad av Dataskyddsförordningen blir mödosam och tidskrävande i en redan komplex arbetsprocess.

Två alternativa förbättringar för framtida dataskyddsarbete presenteras:
Det ena är att i registerförteckning komplettera med den information som rekommenderas i den interna bilagan, där informationsdelarna för riskklassning, riskanalys och tröskelanalys alternativt konsekvensbedömning ingår. Det skulle i så fall också ha till fördel att man närmar sig övriga sex fackförvaltningars registerförteckningsdokumentation, vilket är fördelaktigt eftersom man delar samma externa DSO.

Det andra alternativet är att intern personal på förvaltningen i god tid innan arbetet med årsrapporten startar, i samråd med DSO sammanställer denna information, som innebär informationskomplettering för respektive listad behandling.

Se även bilaga: ”analys av registerförteckning” alla rader som där är i grå text bedöms som av intresse för att göra risk och tröskelanalys, och därmed även konsekvensbedömning om det behövs.

Här sätts status för efterlevnaden till status gul, för att bedömningen av registerförteckningen i sin nuvarande utformning är komplett.

Dock är utformningen sådan att det finns en stor informationsbrist till stöd för ett effektivt kontrollarbete inför årsrapporten.

### 3.1.4 Rekommendationer till PUA

- Registerförteckningen kompletteras med föreslagen information, alternativt en arbetsmodell införs för att tillhandahålla den kompletta informationen för granskning på annat sätt.

## 3.2 Styrdokument

### 3.2.1 Bakgrund och syfte

I detta avsnitt avses dels de styrande dokument som uttrycker ledningens vilja i dataskyddsarbetet. Dokumentationen beskriver roller som har ett ansvar att upprätthålla efterlevnaden av Dataskyddsförordningen.

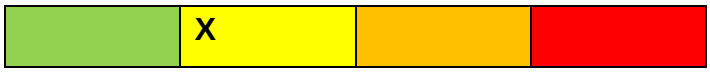
Dessutom kontrolleras i detta avsnitt *dokumentation* som beskriver hantering av personuppgiftsincidenter samt hantering av registrerades rättigheter. I detta avsnitt kontrolleras dokumentation, det vill säga dess existens, kvalitet och inbördes spårbarhet. Den operativa delen behandlas i egna avsnitt.

Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får information om regler, ramar och förutsättningar och stöd för att behålla kunskapen över tid och tillämpa den på ett konsekvent sätt.

### 3.2.2 Resultat

| Fråga/kontroll | Svar |
|---|---|
| Är dokumenten av lämpligt format, är pedagogiska och ger tillräckligt stöd? | Ja, de som finns tillgängliga |
| Är dokumenten uppdaterade? | Oklart |
| Finns ägare till dokumenten utpekade, så att ansvar för uppdateringar är tydliga? | Serviceförvaltningen står som ägare, utpekad informationsansvarig för dokumentet saknas |
| Ange dokumenten med namn och deras syfte, detta ger en kontroll på vilka dokument man hänvisar till. | 1)Roll och ansvarsbeskrivning: Nytt dokument som bl.a. innehåller detta är planerad<br>2)PU incident process beskrivning: finns på förvaltningens hemsida om dataskyddsarbete<br>3)Beskrivning av rutin för registrerades rättigheter: Blankett för begäran om registerutdrag |

### 3.2.3 Status för brister gällande styrdokument




- Vägledningar, mallar och annan stöddokumentation finns till största delen och är lättillgänglig.
- Det är oklart vilken roll i organisationen som ansvarar för dokumenten och deras status.

### 3.2.4 Rekommendationer till PUA

- Rekommenderar att ansvar för dokument och mallar är fastställt och att aktualitet är tydlig.

## 3.3 Tekniska och organisatoriska säkerhetsåtgärder

### 3.3.2 Sammanfattning och syfte

Tekniska och organisatoriska säkerhetsåtgärder handlar till stor del om att informationssäkerhet ska vara en del av organisationens arbete, och dataskyddsarbetet villkoras av ett antal krav på fungerande informationssäkerhet.

Informationssäkerhet innefattar *allt* säkerhetsarbete inom organisationen.

Tekniska säkerhetsåtgärder motsvaras som regel av fungerande och komplett IT-säkerhet (exempelvis brandvägg, viruskontroll, aktivitetsloggning mm) som är reglerad och fastställd åtkomst i form av roller med definierad access och rättigheter både fysiskt i lokaler och till system och andra digitala resurser.

Organisatoriska säkerhetsåtgärder representeras dels av det systematiska arbetet som innebär att registerförteckning/kartläggning ska följas av andra insatser, som också ska dokumenteras på ett konsekvent sätt, detta är

- Informationsklassning av personuppgifterna (enbart informationsklassning av personuppgifter krävs för efterlevnad av Dataskyddsförordningen)
- Riskanalys
- Tröskelanalys som fastställer om konsekvensanalys behöver göras
- Eventuell konsekvensanalys

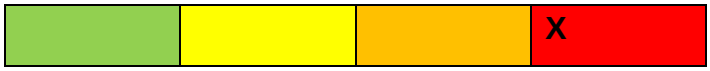
Syftet med att granskningen av detta område är att säkerställa säkerhetsresurser för respektive behandling.

### 3.3.3 Resultat

| Fråga/kontroll | Svar |
|---|---|
| Ar alla behandlingar med personuppgifter informationsklassade? Om inte hur många är ej klassade? | Oklart |
| Är klassningarna aktuella? Om brister, hur många? | Oklart |
| Är behandlingarna riskanalyserade, om brist ange hur många? | Oklart |
| Finns tröskelanalys för alla behandlingar, alternativt konsekvensbedömning? Om inte, hur många saknas? | Oklart |
| Finns tekniska säkerhetsåtgärder som följer Stadens riktlinjer för alla behandlingar? | Oklart |
| Finns struktur och riktlinjer för access-tilldelning till roller med avgränsningar för tilldelade rättigheter? | Ja |

OBS! Det finns en informationspost i registerförteckning på ”säkerhetsåtgärder”.

### 3.3.4 Status för brister tekniska och organisatoriska säkerhetsåtgärder




- Om informationen finns förefaller den vara svårtillgänglig för kontroll. Det vore att föredra att informationen finns med i registerförteckningen

### 3.3.5 Rekommendationer till PUA

- Att registerförteckningen kompletteras så att de informationspunkter som utgör grund för Tröskelanalys finns med.

## 3.4 Konsekvensbedömningar

### 3.4.1 Sammanfattning och syfte

Behandlingar som kan innebära risker av en viss nivå ska enligt Dataskyddsförordningen bedömas utifrån vilka potentiella negativa konsekvenser behandlingen kan innebära för de behandlade.

Därför behöver varje behandling genomgå en tröskelanalys som värderar vad som framkommit vid kartläggning/registerförteckning av behandlingen, riskbedömning av ingående personuppgifter samt riskanalysen.

Om tröskelanalysen ger att konsekvensbedömning inte behöver göras ska denna bedömning dokumenteras och lagras i anslutning till behandlingen så att spårbarhet finns. Stöd för att göra detta arbete konstruktivt och med rätt kvalitet behöver finnas.

Syftet med kontroll av konsekvensbedömning består av två delar, dels om antingen tröskelanalys eller konsekvensbedömning har gjorts för varje behandling, dels att stöd för dessa rutiner finns, är kända och används.

| Fråga/kontroll | Svar |
|---|---|
| Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av? | Oklart |
| Har alla potentiella högriskbehandlingar konsekvensbedömts? | Oklart |
| Är de genomförda bedömningarna aktuella? | Oklart |
| Har tröskelanalys, med dokumentation, gjorts för alla behandlingar som inte är konsekvensbedömda? | Tröskelanalys planeras att införas i arbetsprocessen för dataskydd nästa år, beslutat av administrativ chef |
| Finns relevant stöd, som instruktioner, mallar och utbildning, för detta arbete? | Oklart |

### 3.4.2 Resultat

### 3.4.3 Status för brister gällande konsekvensbedömningar


- Om informationen finns förefaller den svårtillgänglig för kontroll. Det vore att föredra att den här informationen finns med i registerförteckningen

### 3.4.4 Rekommendationer till PUA

- Att registerförteckningen kompletteras med dessa informationspunkter, att dessa informationspunkter är kompletterade och aktuella.

## 3.5 Individens rättigheter

### 3.5.1 Sammanfattning och syfte

Individens rättigheter innefattar flera krav i Dataskyddsförordningen. Registrerade har rätt att begära och få registerutdrag. De har också rätt att exempelvis begära att bli raderade och få sina uppgifter rättade. I båda dessa fall kan det vara svårt att möta begäran, dels för att exempelvis radering kan gå i strid med det uppdrag som personuppgiftsansvarig är skyldig att utföra, för rättningsbegäran kan detta vara svårt att möta eftersom de personuppgifter som behandlas kommer från annan part.

Kontroll av individens rättigheter görs för att kontrollera att de interna rutinerna fyller sitt syfte och är effektiva.

### 3.5.2 Resultat

| Fråga/kontroll | Svar |
|---|---|
| Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer? | En begäran om delvis radering har inkommit, men personen fanns inte registrerad. |
| Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar? | Ej tillämpbart |

### 3.5.3 Status för brister gällande individens rättigheter

| | | | |
|---|---|---|---|
| X | | | |

Ingen brist noterad.

### 3.5.4 Rekommendationer till PUA

Ingen brist noterad.

## 3.6 Personuppgiftsincidenter

### 3.6.1 Sammanfattning och syfte

Identifiera och hantera personuppgiftsincidenter är viktiga av flera anledningar, dels är det ett direkt krav i Dataskyddsförordningen, men det ger även verksamheten möjlighet att

Kontrollområdet säkerställer både att det finns en medvetenhet som gör att personuppgifts-incidenter upptäcks och att det finns en fungerande process att hantera personuppgiftsincidenter. Samt kontrollerar att det planeras och utförs åtgärder för de brister som personuppgiftsincidenten identifierat.

### 3.6.2 Resultat

### 3.6.3 Status för brister gällande individens rättigheter

| Fråga/kontroll | Svar |
|---|---|
| Hur upptäcks personuppgiftsincidenter? | Främst av verksamheten, även hos biträde |
| Hur många personuppgiftsincidenter har dokumenterats? | Sju bekräftade personuppgiftsincidenter |
| Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte? | En |
| Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten? | En |


- Under året har frågor uppstått kring effektiv informationsdelning kring personuppgiftsincidenter i vissa personuppgiftsincidenter.

### 3.6.4 Rekommendationer till PUA

- Göra Gap-analys av de situationer då samma externa biträde används för samma behandling av flera förvaltningar. Med målsättning att identifiera eventuella brister, och lämpliga åtgärder.

## 3.7 Personuppgiftsbiträdesavtal

### 3.7.1 Sammanfattning och syfte

För varje personuppgiftsbehandling ska personuppgiftsbiträdesavtal PuB avtal) finnas i det fall ett biträde (leverantör) används. Behandlingarna ska beskrivas och regleras i enlighet med Stadens framtagna mall för PuB avtal. Personuppgiftsbiträdesavtalens riktighet bör kontrolleras med bestämd frekvens,

Post för att ange då för PuB-avtal behövs finns med i registerförteckningen. Även post för att kontrollera att PuB avtalens riktighet följs upp bör finnas med.

### 3.7.2 Resultat

| Fråga/kontroll | Svar |
|---|---|
| Finns personuppgiftsbiträdesavtal för alla behandlingar där personuppgiftsbiträde används | Enbart 5 poster saknas av 828 |
| Finns rutiner för att följa upp PuB avtal | Information saknas som standard i nuvarande registerförteckningen |

### 3.7.3 Status för brister gällande personuppgiftsbiträdes-avtal

| | X | | |
|---|---|---|---|

- Att ha fastslagna rutiner för att följa upp PuB avtal är en viktig del i det kontinuerliga och systematiska arbetet.

### 3.7.4 Rekommendationer till PUA

- Stötta organisationen att jobba kontinuerligt och systematiskt med PuB avtal

# 4 Strategi för granskningar

## 4.1 Det gångna årets granskningar

Det gångna året har granskningarna genomförts under en period i slutet av året.
Där har analys av informationen i registerförteckningen genomförts, kompletterat med informationsinsamling från några nyckelroller.

## 4.2 Planerade granskningar kommande år

Det finns intresse av att jobba med årshjulsplanering för att på så sätt möjliggöra initiering av uppdateringsarbete av objektansvariga och objektägare mer löpande under året. Vilket även kan vara till stöd för ett systematiskt och kontinuerligt dataskyddsarbete.

# 5 Övrigt att rapportera

## 5.1 Sammanfattning och syfte

Detta avsnitt används för att lyfta fram observationer som gjorts men som inte på ett naturligt sätt kunnat presenteras under övriga granskningsområden.

## 5.2 Observationer utöver granskningsområden

### Observation 1

Troligen bör ett bättre samarbete utformas för att skapa grund för ett dataskydd som är effektivare och bör innefatta struktur för informationsdelning och samsyn inom förvaltningen för de roller som arbetar med att stöta inom dataskydd, och de roller som har exempelvis informationsansvar och effektivare att arbeta med.

Ett annat samarbete kan rekommenderas att vara mellan de förvaltningar som delar DSO, så att man kan närma sig i väsentliga delar för dataskyddsarbetet. Här finns fördelar som att förvaltningarna kan dra nytta av varandras arbete, samt att det underlättar arbetet för den gemensamma DSO som då får en mer enhetlig arbetsplanering.

Risk: Om inte samsyn upprättas kring dessa moment inom dataskyddsarbetet kan det innebära att det är svårt att höja kvalitén på dataskyddarbetet, och risk för sämre tillvaratagande av den gemensamma resursen DSO.

### Observation 2

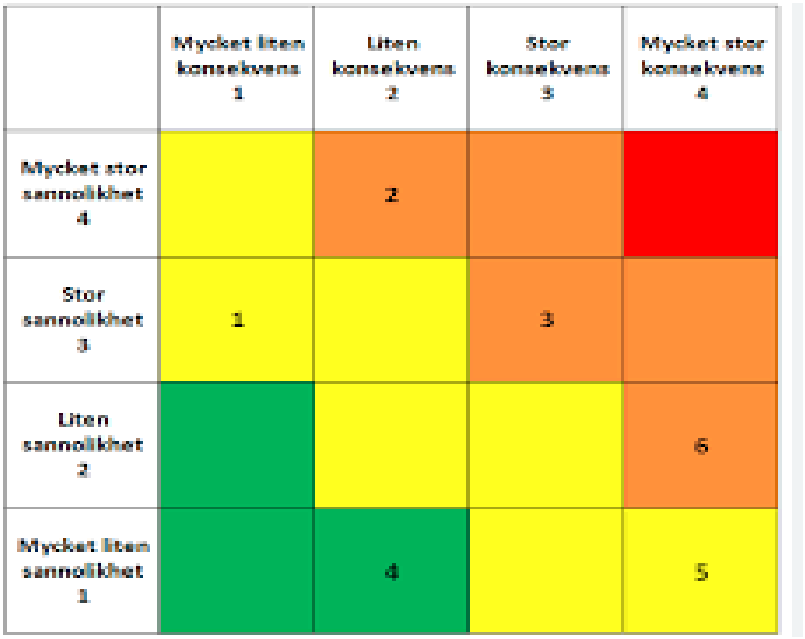
Under hösten har administrativ chef beställt kompletterande utbildning för de roller som behöver förstå Dataskyddsdelarna i sitt eget ansvarsområde.
Utbildningen är planerad att genomföras under Q1 2023

### Observation 3

En tydlig och lättarbetad modell för man för riskanalys och konsekvensbedömning är viktig för förståelse och arbete med risker och vilka konsekvenser dessa kan få. Vanligt förekommande är att arbeta med en tre eller ännu hellre fyrgradig skala. Man multiplicerar värdet för sannolikhet med värdet för konsekvens, därigenom får man en bättre tydlighet i olika nivåer för det totala riskvärde.

När detta är gjort går man vidare och definierar åtgärder som åtminstone reducerar riskerna nöjaktigt. I första hand fokuserar man på de risker med högst värde, man bör planera åtgärder även där riskvärdet är lägre.

Då DSO arbetar med ytterligare fem fackförvaltningar skulle ett likartat arbetssätt i detta även kunna underlätta för DSO's arbete.




Grafiskt exempel på riskanalys värdering.

| | | | | |
|---|---|---|---|---|
| Observation 1 | | | X | |
| Observation 2 | X | | | |
| Observation 3 | | | X | |

## 5.3 DSO rekommendationer till PUA

- Förutsättningar för nära samarbete mellan DSO, infosäk-samordnare samt eventuellt sakkunniga för respektive behandling.
- Förbered utbildningsinsatsen med förberedande halvdags-workshop där DSO med info-säk samordnare från respektive förvaltning av de sex fackförvaltningarna som delar DSO, skapar samsyn inte minst för processen att sammanställa information för registerförteckning, informationsklassning, riskanalys och eventuell konsekvensbedömning.