

# GDPR Årsrapport

År 2022

Kulturförvaltningen

**GDPR årsrapport**  
Januari 2023

**Dnr:** YYYY  
**Utgivningsdatum:** 2022-12-27  
**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 skall 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 *dokumenteringsskyldighet*. 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 skall 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

<b>1</b>	<b>Bakgrund .....</b>	<b>3</b>
<b>2</b>	<b>Sammanfattning av rapporten .....</b>	<b>6</b>
2.1	Framsteg under året .....	6
<b>3</b>	<b>Obligatoriska rapporteringsområden .....</b>	<b>7</b>
3.1	Registerförteckning .....	8
3.2	Styrdokument .....	9
•	Rapportering av personuppgiftsincident .....	10
•	Begäran om registerutdrag, rättelse och radering .....	10
3.	Tekniska och organisatoriska säkerhetsåtgärder .....	10
3.3	Konsekvensbedömningar .....	12
3.4	Individens rättigheter .....	14
3.5	Personuppgiftsincidenter .....	15
3.6	Personuppgiftsbiträdesavtal .....	16
<b>4</b>	<b>Strategi för granskningar .....</b>	<b>17</b>
4.1	Det gångna årets granskningar .....	17
4.2	Planerade granskningar kommande år .....	17
<b>5</b>	<b>Övrigt att rapportera .....</b>	<b>17</b>
5.1	Sammanfattning och syfte .....	17
5.2	Observationer utöver granskningsområden .....	17
5.3	DSO rekommendationer till PUA .....	18

## 2 Sammanfattning av rapporten

I detta kapitel kommenteras kort kring framsteg under året.

Rapporten som helhet innehåller sammanfattningar och specificeringar. Den som i första hand vill läsa sammanfattning av granskning kan istället läsa dokumentet ” 2022 GDPR Årsrapport till Kulturnämnden för Kulturförvaltningen”. 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 Dataskyddsombud (DSO) tillsatts 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.

Konsekvensbedömning har på förvaltningen upplevts som ett svårt moment i dataskyddsarbetet. Det har även upplevts svårt att veta när konsekvensbedömning måste göras. Den externa DSO:n ombads ta fram lösning som kan underlätta detta. DSO fann att inom staden finns delmomentet Tröskelanalys, även om detta inte varit spritt till alla förvaltningar. Tröskelanalys innebär en analys av behandlingen, personuppgifter som behandlas, informationsklassning samt riskanalys. För att på dessa informationspunkter kunna fastställa om konsekvensbedömning behövs eller inte. Under 2023 planeras att tydliggöra momentet Tröskelanalysen så att alla behandlingar har blivit värderade antingen i tröskelanalys eller 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 arbetsätt och rutiner *skall* 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, även kallad registerförteckning, 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 skall 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 skall 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?	32 st
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Det finns brister på vissa områden
Har verksamheten lämpliga rutiner för registerföring?	Det vore bra med kontinuerliga rutiner under året
Övrigt	Tröskelanalys är föreslagen som komplement

### 3.1.3 Status för brister gällande registerförteckningen

		X	
--	--	---	--



- Ett *kontinuerligt* arbete med DraftIT under året kan rekommenderas, Arbetet skulle
- Kunna planeras gemensamt med DSO tidigt på året, och aktiviteter utföras kontinuerligt under året så att ny status är uppnådd till mitten av Q4, då arbetet med att sammanställa information till årsrapporten startar.
- Hög svarsfrekvens är uppnådd på många av en registerförtecknings viktiga informationspunkter.
- En stor brist råder för informationsklassning, riskanalys och konsekvensbedömning där brist ligger mellan 84 % - 100 %

#### **3.1.4 Rekommendationer till PUA**

- Ett tydligt fokus för 2023 bör vara att arbeta med informationsklassning, riskanalys och konsekvensbedömning och komplettera informationen i DraftIT
- Införa planerad och strukturerad årlig genomgång i god tid under året av registerförteckningen.
- Införa stöd i form av process där registerförteckning, informationsklassning riskanalys samt konsekvensbedömning ingår

## **3.2 Styrdokument**

### **3.2.1 Bakgrund och syfte**

I detta avsnitt avses till att börja med de styrande dokument som uttrycker ledningens vilja i dataskyddsarbetet. Dokumentationen beskriver roller som har ett ansvar att upprätthålla efterlevnaden av Dataskyddsförordningen. Förslagsvis tjänsteägare och liknande roller, registrator, kundtjänst och projektledare.

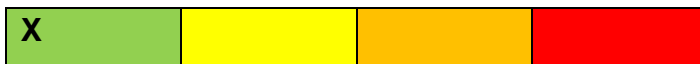
Dessutom kontrolleras i detta avsnitt dokumentation som beskriver hantering av personuppgiftsincidenter samt hantering av registrerades rättigheter med mera. I detta avsnitt kontrolleras dokumentation, det vill säga dess existens, kvalitet och inbördes spårbarhet.

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
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att ansvar för uppdateringar är tydliga?	Ja
Ange dokumenten med namn och deras syfte, detta ger en kontroll på vilka dokument man hänvisar till.	<a href="#">GDPR för kulturförvaltningen - Stockholms stads intranät</a> <ul style="list-style-type: none"> <li>• Roller och ansvar</li> <li>• Rapportering av personuppgiftsincident</li> <li>• Begäran om registerutdrag, rättelse och radering</li> </ul>

### 3.2.3 Status för brister gällande styrdokument



- Inga brister noterade

### 3.2.4 Rekommendationer till PUA

- Inga brister noterade

## 3. Tekniska och organisatoriska säkerhetsåtgärder

### 3.2.6 Sammanfattning och syfte

Tekniska och organisatoriska säkerhetsåtgärder handlar till stor del om att informationssäkerhet skall 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 och 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 här av det systematiska arbetet som innebär att registerförteckning/kartläggning skall följas dessa steg, som även skall dokumenteras på ett konsekvent sätt

- Informationsklassning av personuppgifterna
- Riskanalys
- Tröskelanalys som fastställer om konsekvensanalys behöver göras
- Eventuell konsekvensanalys

Syftet med att granskningen är att säkerställa säkerhetsresurser för respektive behandling.

### 3.2.7 Resultat

Fråga/kontroll	Svar
Ar alla behandlingar med personuppgifter informationsklassade? Om inte hur många är <i>ej klassade</i> ?	27 av 32, Många av dessa är besvarade med ”delvis” utan vidare förklaring
Är klassningarna aktuella? Om brister, hur många?	Genomgång behövs.
Är behandlingarna riskanalyserade, om brist ange hur många?	29 av 32
Finns tröskelanalys för alla behandlingar, alternativt konsekvensbedömning? Om inte, hur många saknas?	32 av 32
Finns tekniska säkerhetsåtgärder som följer Stadens riktlinjer för alla behandlingar?	Uppgifts saknas för 12 av 32 *
Finns struktur och riktlinjer för access-tilldelning till roller med avgränsningar för tilldelade rättigheter?	Uppgifts saknas för 13 av 32 **

### 3.2.8 Status för brister tekniska och organisatoriska säkerhetsåtgärder



- Dessa delar av dataskyddsarbetet verkar saknas för stora delar av registrerade behandlingar.

- Om den delvisa informationsklassningen är beslutad att vara tillräcklig behöver detta anges i registerförteckningen.
- Uppgifter som informationsklassning, riskanalys och Tröskelanalys är viktiga för att kunna bedöma om konsekvensbedömning behövs eller ej, och utgör tillsammans med övrig information i registerförteckningen den information som ligger till grund för Tröskelbedömning. behandlingar
- \* Kvalitén på säkerhetsåtgärd är inte bedömd vid genomgång, dock har vissa noteringar gjorts. Exempelvis är enbart "Informationsägare utsedd" (för 12 behandlingar) är inte tillräcklig som organisatorisk säkerhetsåtgärd.
- \*\*I ett fall är "Annat" angivet istället för beskrivning av skyddsmekanism, utan vidare förklaring.

### 3.2.9 Rekommendationer till PUA

Tillse att verksamheten har medel och resurser för att arbeta med nedanstående.

- Införa stöd i form av process där registerförteckning, informationsklassning riskanalys, Tröskelanalys och vid behov konsekvensbedömning ingår
- Hög prioritet rekommenderas för information om informationsklassning, riskanalys och konsekvensbedömning, eftersom mellan 84 % - 100 % saknas eller är ofullständig.

## 3.3 Konsekvensbedömningar

### 3.3.1 Sammanfattning och syfte

Behandlingar som kan innebära risker av en viss nivå skall 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 skall 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.

### 3.3.2 Resultat

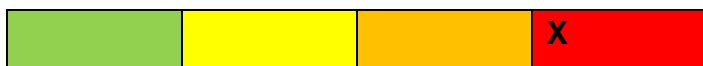
Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Oklart
Är de genomförda bedömningarna aktuella?	Oklart
Har tröskelanalys, med dokumentation, gjorts för alla behandlingar som inte är konsekvensbedömda?	Tröskelanalys föreslås att införas 2023
Finns relevant stöd, som instruktioner, mallar och utbildning, för detta arbete?	Enbart det stadsövergripande

Ett systematiskt arbetssätt föreslås som målsätter ett kontinuerligt dataskyddsarbete med att strukturera arbetet med informationsklassning, riskanalys och konsekvensbedömning av personuppgiftsbehandlingar. Ett bra system kan när det är infört innebära låg belastning på verksamheten

Förslag på systematiskt arbetssätt är presenterat för administrativa chefer.

Stadsövergripande stöd för informationsklassning, riskanalys och konsekvensbedömning: [Stadsövergripande informationssäkerhet - Stockholms stads intranät finns men](#), enligt uppgift används detta inte.

### 3.3.3 Status för brister gällande konsekvensbedömningar



- Information om informationsklassning, riskanalys saknas vilket är underliggande information om behandlingen som behövs för att avgöra om konsekvensbedömning behövs.
- Införande av Tröskelanalys som alternativ till konsekvensbedömning har föreslagits.
- Förslag på justering av arbetsmodell har presenterats.
- Ett tydliggörande till de roller som innehar informationsägarskapet är också en viktig del i ett framgångsrikt arbete. Mer om det under avsnitt "Övrigt att rapportera".

### 3.3.4 Rekommendationer till PUA

- Tillse att verksamheten har medel och resurser för att förändra arbetssätt och arbeta med dataskyddsarbetet kontinuerligt.

- Tillse att verksamheten arbetar med delarna informationsklassning, riskanalys, tröskelanalys samt konsekvensbedömning strukturerat. Inklusive att införa, förankra och använda konsekvent och sammanhängande stöddokumentation.

## 3.4 Individens rättigheter

### 3.4.1 Sammanfattning och syfte

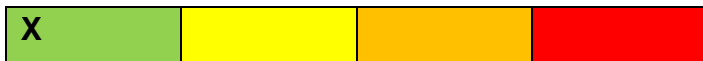
Individens rättigheter innefattar flera krav i Dataskyddsförordningen. Registrerade har rätt att begära och få registerutdrag. De har också rätt att exempelvis begära att bli raderade och få sina uppgifter rättade. I båda dessa fall kan det vara svårt att möta begäran, dels för att exempelvis radering 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.

### 3.4.2 Resultat

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	1

### 3.4.3 Status för brister gällande individens rättigheter



- Ingen brist noterad

### 3.4.4 Rekommendationer till PUA

- Ingen brist noterad

## 3.5 Personuppgiftsincidenter

### 3.5.1 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 personuppgiftsincidenter 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.

### 3.5.2 Resultat

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Via medarbetare
Hur många personuppgiftsincidenter har dokumenterats?	5
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	1

### 3.5.3 Status för brister gällande individens rättigheter



- Ingen brist identifierad

### 3.5.4 Rekommendationer till PUA

- Ingen brist identifierad

## 3.6 Personuppgiftsbiträdesavtal

### 3.6.1 Sammanfattning och syfte

För varje personuppgiftsbehandling skall personuppgiftsbiträdesavtal (PuB avtal) finnas i det fall ett biträde (leverantör) används. Behandlingarna skall 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 finns med.

### 3.6.2 Resultat

Fråga/kontroll	Svar
Finns personuppgiftsbiträdesavtal för alla behandlingar där personuppgiftsbiträde används	Saknas information för 7 av 32
Finns rutiner för att följa upp PuB avtal	Saknas information för 8 av 32

### 3.6.3 Status för brister gällande personuppgiftsbiträdes-avtal



- Viss brist på information.
- Dock inte säkert att det betyder att PuB avtal behövs i de fall information saknas.
- En förklaring kan vara oklarheter då PuB avtal ligger under Staden centralt, eftersom Kulturförvaltningen då inte har insyn.

### 3.6.4 Rekommendationer till PUA

- Tillse att verksamheten har resurser och medel att komplettera information om personuppgiftsbiträdesavtal skall finnas och uppdatera informationen om det i registerförteckningen.



## 4 Strategi för granskningar

### 4.1 Det gångna årets granskningar

Granskningarna genomförts under en period i slutet av året, genom analys av informationen i registerförteckningen, samt informationsinsamling från nyckelroll.

### 4.2 Planerade granskningar kommande år

Det finns intresse att jobba med årshjulsplanering (kan vara internkontrollplanering som skall lyftas här) för ett mer 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

Dataskyddsarbetet är beroende av flera roller där rollen informationssäkerhetssamordnaren är central för att hålla ihop arbetet med informationsklassning och riskanalys, medan informations-ansvarig ansvarar för behandlingen som har information om själva behandlingen och vilka personuppgifter som ingår. Förvaltningen har även en GDPR samordnare som har en viktig del i dataskyddsarbetet.

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

#### Observation 2

Det förefaller som ansvar inom dataskyddsarbetet på vissa roller, exempelvis informationsägare och projektledare, bör tydliggöras. Bland annat för att komplett information om behandlingarna skall uppnås och hålla god kvalitet. Utbildningsinsatsen kan med fördel användas för att sprida bättre förståelse kring ansvarsfördelning inom dataskyddsarbetet som även innefattar dessa roller.

Risk: Om inte utbildning av rollerna informationsägare och projektledare planeras och genomförs inom rimlig tid, så kan det innebära svårigheter att uppnå komplett information om behandlingarna som håller god kvalitet. Till det behöver ett kontinuerligt arbetssätt införas så att exempelvis informationsklassning kontrolleras årligen.

Observation 1			X	
Observation 2	X			

### 5.3 DSO rekommendationer till PUA

- Förutsättningar för nära samarbete mellan DSO, info-säk 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.