Stockholms stad

Bilaga 10

GDPR Årsrapport

År 2022

Stadsarkivet

GDPR årsrapport
Januari 2023

Dnr: YYYY
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 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 *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 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

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 förståelse för konsekvensanalys, pågår ett arbete för att tydliggöra momentet Tröskelanalysen för att formellt definiera då konsekvensbedömning anses ej behöva genomföras.

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

- Införa års-mässig genomgång av registerförteckningen, kontroll av status och kvalitet sammanställ brister.
- Införa tydlig process där registerförteckning, informationsklassning riskanalys samt konsekvensbedömning ingår. (Dessa informationsdelar är särskilt låg i registerförteckningen, ca 85 % saknas. Hög prioritet rekommenderas.)
- Tillse att verksamheten har medel och resurser för att arbeta med dokumentägarskap och dokumentkontroll kontinuerligt.
- Tillse att verksamheten har medel och resurser för att förändra arbetssätt och arbeta med dataskyddsarbetet kontinuerligt.
- Tillse att verksamheten har resurser och medel att komplettera fastställa om personuppgiftsbiträdesavtal skall finnas och uppdatera informationen om det i registerförteckningen.

2.4 Observationer

Följande observationer för integritet och dataskyddsarbetet har gjorts:

Observation 1:
Troligen bör ett bättre samarbete utformas för att skapa grund för ett dataskydd som är bättre och effektivare att arbeta med.
Samarbetet är beroende av rollen infosäk-samordnaren 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 är svårt att höja kvalitén på dataskyddarbetet.

Observation 2:
Under hösten har administrativ chef beställt kompletterande utbildning för de roller som behöver god förståelse för Dataskyddsdelarna i sitt eget ansvarsområde.
Utbildningen är planerad att genomföras under Q1 2023

Risk: Goda förutsättningar för insatsen rekommenderas, som tydlighet i vilka roller som bör delta och varför.

Observation 3:
Förslag att börja arbeta med KOS metoden i risk och konsekvensarbetet.

2.5 Sammanfattning rekommendationer till PUA

- Förutsättningar bör ges för att skapa ett bättre samarbete mellan DSO och infosäk-samordnare.

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 *skall* vara dokumenterade. Detta kan sättas i relevans till kravet på att den personuppgiftsansvarige måste kunna *visa* att Dataskyddsförordningens 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, det som benämns som Registerförteckningen, 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?	38
Har nödvändiga uppdateringar gjorts?	Uppdateringar har skett under 2022
Bedöms registerförteckningen vara fullständig?	Omfattande informationsbrister, se bilaga
Har verksamheten lämpliga rutiner för registerföring?	GDPR-samordnare och GDPR-redogörarens har ansvar att uppdatera. Inte alla upplever tydlighet kring detta ansvar och vilka rutiner som finns.
Övrigt	Tröskelanalys bör kompletteras i registerförteckningen och vara ett alternativ till konsekvensbedömning

3.1.3 Status för brister gällande registerförteckningen

På viktiga informationspunkter är bristen hög, omkring 50 %, upp till 90 % av alla registreringar saknas information, flera av dessa är viktig information för att kunna utföra dataskyddsarbete. Se bilaga med analys av registerförteckning

För vissa behandlingar är det oklart om uppdatering är genomförd under året. Förslagsvis kan man införa rutin för att påminna objektansvarig att planera sitt arbete med DraftIT, att kontrollera, komplettera, uppdatera.

På viktiga informationspunkter är bristen hög, omkring 50 %, upp till 90 % för alla registreringar saknas information, flera av dessa är viktig information för att kunna utföra dataskyddsarbete. Utan denna information om behandlingen är det mycket svårt att klarlägga behov av riskanalys, vilka risker som finns, samt om konsekvensbedömning behöver göras.

3.1.4 Rekommendationer till PUA

- Ett tydligt fokus för 2023 bör vara att komplettera informationen i registerförteckningen.
- Införa stöd i form av process där registerförteckning, informationsklassning riskanalys samt konsekvensbedömning ingår
- Information in informationsklassning riskanalys och konsekvensbedömning är särskilt låg, ca 90 % saknas. Hög prioritet för komplettering rekommenderas.

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
Är dokumenten uppdaterade?	Oklart
Finns ägare till dokumenten utpekade, så att ansvar för uppdateringar är tydliga?	Ägarskap för dokument som rör dataskyddsarbetet verkar saknas
Ange dokumenten med namn och deras syfte, detta ger en kontroll på vilka dokument man hänvisar till.	1)Roll och ansvarsbeskrivning : Beslut Stadsarkivets dataskyddsorganisation 2)PU incident process beskrivning: Personuppgiftshantering på Stockholms Stadsarkiv 4)Beskrivning av rutin för registrerades rättigheter (mall finns) Blankett_Tillgång till personuppgifter

3.2.3 Status för brister gällande styrdokument

- Det framgår inte om dokumenten har kontrollerats av verksamheten att de är aktuella, och om de har uppdaterats.
- Ägarskap behöver tydliggöras. DSO rollen bör generellt inte ha ägarskap för dokument för dataskyddsarbetet eftersom det då går i strid mot kontrollfunktionen. Däremot kan DSO med fördel bistå i utformningen av dokumenten.

3.2.4 Rekommendationer till PUA

- Införa rutin för årlig granskning av dokumenten och vid behov uppdatering.
- Tydliggöra ägarskap för dokumenten, och fördela ansvaret i organisationen.

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 (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 skall följas av andra insatser, som också skall dokumenteras på ett konsekvent sätt, detta är

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

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

3.2.7 Resultat

Fråga/kontroll	Svar
Ar alla behandlingar med personuppgifter informationsklassade? Om inte hur många är ej klassade?	Nej, knappt hälften är det.
Är klassningarna aktuella? Om brister, hur många?	Oklart
Är behandlingarna riskanalyserade, om brist ange hur många?	Uppgift saknas för 32 behandlingar (av 38)
Finns tröskelanalys för alla behandlingar, alternativt konsekvensbedömning? Om inte, hur många saknas?	Uppgift saknas för 34 behandlingar (av 38)
Finns tekniska säkerhetsåtgärder som följer Stadens riktlinjer för alla behandlingar? *1	Av 38 behandlingar saknas information för 7

Finns struktur och riktlinjer för access-tilldelning till roller med avgränsningar för tilldelade rättigheter?	Oklart

För detta område saknas information helt för stora delar av behandlingarna (ca 50 - 90%), och man bör utvärdera vilka former av skyddsåtgärder som är relevanta.

För organisatoriska skyddsåtgärder kan avgränsning på vilka medarbetare som har åtkomst vara exempel. För tekniska skyddsåtgärder kan säkerhet inom ramen för IT-policyn vara möjliga förutsatt att behandlingen ligger inom IT-miljön.

3.2.8 Status för brister tekniska och organisatoriska säkerhetsåtgärder

- Dessa delar av dataskyddsarbetet verkar saknas för större delen av registrerade behandlingar.
- 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.

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
- Information in informationsklassning riskanalys och konsekvensbedömning är särskilt låg, upp till 90 % saknas. Hög prioritet rekommenderas.

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.

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

Stora brister för informationen om konsekvensbedömning har noterats. Detta kan sägas vara en större del av ett mer systematiskt arbetssätt som har föreslagits och som målsätter ett kontinuerligt dataskyddsarbete med lägre arbetsbelastning på verksamheten.

Förslag att dela upp innehållet i mallen på två delar, riskanalys separerat mot konsekvensbedömning. Då arbetar men enbart med riskanalys om det behövs, och har samlat information om man behöver fördjupa med en konsekvensbedömning.

3.3.2 Status för brister gällande konsekvensbedömningar

Den underliggande informationen för att kunna avgöra om konsekvensanalys behövs, och för att genomföra konsekvensanalysen saknas för merparten av behandlingarna.

Därför rekommenderas en justering av arbetsmodell.

Arbetsmodellen bör inkludera att systematiskt arbeta sig genom registerförteckning, informationsklassning samt riskanalys för att dessa faktorer skall utgöra underliggande information att bygga behov och eventuellt genomförande av konsekvensanalys.

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”.
Vid behov inför löpande påminnelser och uppföljningar

3.3.3 Rekommendationer till PUA

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

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
Finns stöd för att möta begäran om individens rättigheter?	Ja, det finns blankett för att besvara begäran. Oklart om rutin finns för att säkerställa vem personen är.
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	0

3.4.3 Status för brister gällande individens rättigheter

Oklart om rutin finns som säkerställer identitet för den som begär rättighet. Om sådan finns bör den nedtecknas och lagras lättillgängligt.

3.4.4 Rekommendationer till PUA

Komplettera med rutin som säkerställer identitet när information lämnas ut.

3.5 Personuppgiftsincidenter

3.5.1 Sammanfattning och syfte

Att 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.

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Personalen rapporterar
Hur många personuppgiftsincidenter har dokumenterats?	1
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	NA

3.5.2 Status för brister gällande individens rättigheter

Med så lång förekomst av personuppgiftsincidenter uppstår en stark misstanke om mörkertal. Vilket inte är bra. Enbart då personuppgiftsincidenter upptäcks kan man konkret arbeta med förbättringar.

Mest pragmatiskt för att jobba med förbättringar i detta segment är att kontinuerligt arbeta med utbildning, höja medvetenheten och återkommande information.

3.5.3 Rekommendationer till PUA

Kontinuerligt arbeta med utbildning, höja medvetenheten och återkommande information.

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. Spårbarhet mellan behandlingen och PuB avtalet som reglerar behandlingen är viktigt.

3.6.2 Resultat

Fråga/kontroll	Svar
Finns personuppgiftsbiträdesavtal för alla externa leverantörer	Saknas uppgift för 4 behandlingar
Finns rutiner för uppföljning av PuB avtal	Enbart 7, svar ”ja”, övriga svarar ”Nej” eller uppgift saknas

3.6.3 Status för brister gällande personuppgiftsbiträdes-avtal

Det viktiga är att det finns PuB avtal, även om kontinuerlig uppföljning också är viktigt. I det första fallet är svarsfrekvensen hög, i andra fallet låg.

3.6.4 Rekommendationer till PUA

Förordna komplett informationsinnehåll av de poster som har tydliga krav i GDPR för innehållet 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 nyckelroller.

4.2 Planerade granskningar kommande år

Det finns intresse att jobba med årshjulsplanering 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 infosäk-samordnaren är central för att hålla ihop arbetet med informationsklassning och riskanalys, medan objekt-ansvarig ansvarar för behandlingen som har information om själva behandlingen och vilka personuppgifter som ingår.
>
> 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

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

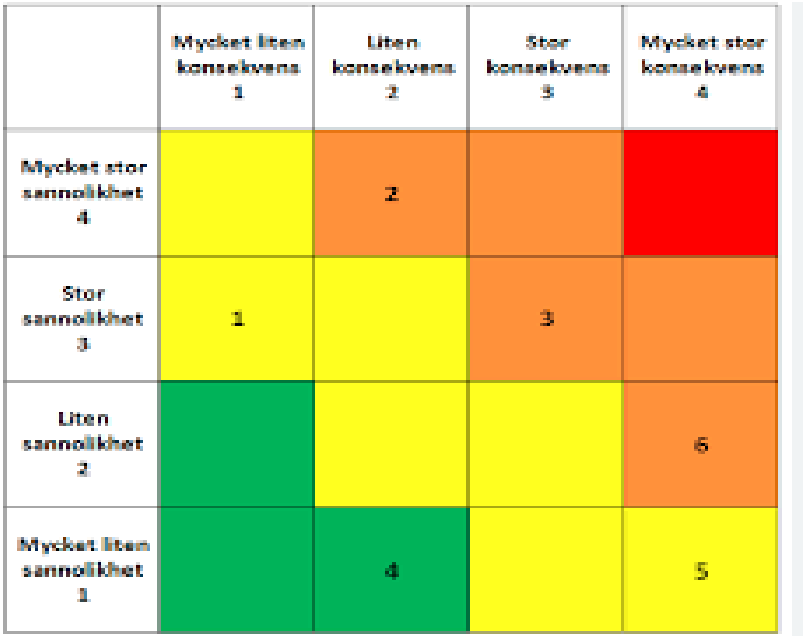
Observation 3

Om man för riskanalys och konsekvensbedömning väljer att gå över till KOS metoden för att identifiera och värdera risker och vilka konsekvenser dessa kan få. KOS metoden står för att man värderar sannolikhet för att en viss risk skal uppstå 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 riskvärdet.

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 KOS metoden.

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.