Stockholms stad

GDPR Årsrapport

2023

Stockholm Business Region

GDPR årsrapport
December 2023

Dnr: SBR 2023/203
Utgivningsdatum: 2023-12-31
Kontaktperson: Mattias Rindberg

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

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.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. 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 nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 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.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för PUAs status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

2.1 Registerförteckning

2.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	61
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

2.1.2 Syfte

Det är ett krav enligt dataskyddsförordningen (artikel 30) att sammanställa information om alla slags behandlingar av person-uppgifter som en organisation utför och dokumentera dessa, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde. På så sätt skapa ett register över allting som man gör med personuppgifter.

Dessa register ska upprättas skriftligen, vara tillgängliga i elektronisk format och hållas uppdaterade. På begäran ska registret göras tillgängligt för Integritetsskyddsmyndigheten (IMY).

2.1.3 Resultat

Resultatet är baserat på den version av registerförteckning som DSO, granskade den 27 november 2023.

Total är 61 behandlingar registrerade i SBRs registerförteckning. Under året har SBR arbetat med att aktualisera register-förteckningen och genomfört nödvändiga uppdateringar.
I samband med detta har kompetensen stärkts hos respektive ansvarig genom individuella utbildningsinsatser. Vidare har en rutin för att hålla registerförteckningen enhetlig och aktuell är tagits fram.

Respektive ansvarig bedömer att registerförteckningen är uppdaterad och aktuell vilket är en bedömning som DSO delar. Även rutinen som tagits fram för att hålla registerförteckningen enhetlig och aktuell bedöms av DSO vara lämplig.

2.1.4 DSO anger hur allvarliga bristerna är på en skala

	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
X	Inga brister av nämnvärd betydelse identifierade

2.1.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att SBR fortsätter arbetet med att regelbundet och systematiskt arbeta med inventering av personuppgiftsbehandlingarna i verksamheten, uppdatera registerförteckningen varefter förändringar sker och säkerställa att registerförteckningen fortlöpande hålls enhetlig och aktuell.

2.2 Styrdokument

2.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja, delvis
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

2.2.2 Syfte

Dataskyddsförordningen ställer krav på att en organisation ska kunna visa att och hur dataskyddsförordningen efterlevs. Detta innebär att det ställs krav på en organisation att ha dokumentation om dataskyddsförordningen upprättad.

Dokumentationen är både ett verktyg för att organisationen ska få en bild av vilka rutiner som finns på plats, men också för att organisationen ska kunna uppvisa arbetet för tillsynsmyndigheten vid en eventuell tillsyn.

2.2.3 Resultat

Granskning av SBRs styrdokument inom detta område genomfördes av DSO i samarbete med verksamhetens informations-säkerhetssamordnare (ISAM) den 23 november 2023.

Av granskningen kan konstateras att SBR under året arbetat med att ta fram och implementera verksamhetsspecifika rutiner avseende:

- Rutin för att tillgodose registrerades rättigheter.
- Rutin för hur personuppgiftsincidenter ska utredas, analyseras, rapporteras och dokumenteras.
- Rutin för att hålla registerförteckningen enhetlig och aktuell.

- Rutin för att konsekvensbedömningar vid behov genomförs, och dokumenteras.

Dessa rutiner bedöms hålla lämplig kvalitet, ger ett tillräckligt stöd, är uppdaterade och har en utpekad ägare som kan säkerställa att uppdateringar kan bli gjorda vid behov.

Det kan vidare konstateras att verksamheten saknar en rutin för att säkerställa att informationsklassningar genomförs, eventuella skyddsåtgärder införs samt att vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller. Vidare kan konstateras att verksamheten saknar en rutin för att säkerställa arbetet med personuppgiftsbiträdesavtal.

2.2.4 DSO anger hur allvarliga bristerna är på en skala

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

2.2.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att SBR utvecklar och implementerar rutiner avseende:

- Rutin för att genomföra informationsklassningar, implementera eventuella skyddsåtgärder samt vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller.
- Rutin för att säkerställa arbetet med personuppgiftsbiträdesavtal.

2.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

2.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	10
Är klassade personuppgiftsbehandlingar aktuella?	Ja

2.3.2 Syfte

För att kunna vidta relevanta tekniska och organisatoriska åtgärder för att skydda information (däribland personuppgifter) behöver informationsägaren avgöra vilket skyddsvärde informationen har för verksamheten.

Den nämnd/styrelse som ytterst ansvarar för att informationen är riktig samt för det sätt informationen används och sprids av både medarbetare och it-tjänster, är formellt sett informationsägare tillika PUA.

Informationsägaren ansvarar för att initiera informations-klassningar samt för att kraven från informationsklassningen kommuniceras och ställs till rätt part. Informationens skyddsvärde fastställs utifrån en skala (0-3). Ju större skadan bedöms kunna bli om informationen inte skyddas, desto högre skyddsvärde anges för informationen. Den grundläggande principen är att ju större skyddsvärde informationen har desto mer omfattande åtgärder krävs för att skydda informationen (tekniska och organisatoriska).

Därefter ska informationsägaren ta ställning till vilka skyddsåtgärder som redan finns på plats och vilka som behöver arbetas in i verksamheten. När skyddsåtgärderna är införda som informationen får det skydd som motsvarar dess betydelse för verksamheten.

Minst årligen, eller vid betydande förändringar i verksamheten eller omvärlden, ska informationsägaren ta ställning till om informationens skyddsvärde fortfarande gäller eller om nya risker och behov av skydd har uppstått.

2.3.3 Resultat

Granskning och resultatet är baserat på information från ISAM den 1 december 2023.

Tio informationsklassningar är genomförda och samtliga bedöms vara aktuella. ISAM bedömning är vidare att merparten och de huvudsakliga personuppgiftsbehandlingarna är informations-klassade.

2.3.4 DSO anger hur allvarliga bristerna är på en skala

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

2.3.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att SBR utvecklar och implementerar rutin avseende:

- Rutin för att genomföra informationsklassningar, implementera eventuella skyddsåtgärder samt vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller.

2.4 Konsekvensbedömningar

2.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja
Har alla potentiella högriskbehandlingar konsekvensbedömts?	N/a
Är de genomförda bedömningarna aktuella?	N/a

2.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen vidtas riskförebyggande åtgärder.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som viktiga verktyg för dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen. och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

2.4.3 Resultat

DSO:s granskning har tagit avstamp i SBRs registerförteckning då den ger en översiktsbild av vilka kategorier av personuppgifter som behandlas och vad som görs med uppgifterna.

DSO kan vid granskningen av registerförteckningen konstatera att samtliga behandlingar i SBRs registerförteckning har en risknivå angiven och att ingen behandling, av respektive ansvarig, bedöms kunna leda till hög risk för registrerade personers fri- och rättigheter.

Då ingen behandling bedöms kunna leda till en hög risk för den registrerades integritet, rättigheter och friheter finns inte grund för att genomföra någon konsekvensbedömning. Av den anledningen har ingen djupare granskning genomförts inom området.

2.4.4 DSO anger hur allvarliga bristerna är på en skala

	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
X	Inga brister av nämnvärd betydelse identifierade

2.4.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att SBR fortsätter arbetet med att stärka medarbetarnas kompetens inom området genom att uppmana medarbetarna att ta del av SBRs styrdokument och stadens fördjupande e-utbildning avseende konsekvensbedömningar.

2.5 Individens rättigheter

2.5.1 Sammanfattning

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

2.5.2 Syfte

De registrerade har ett antal rättigheter enligt dataskyddsförordningens artikel 15-22. Rättigheterna innefattar:

- Rätt till information.
- Rätt till tillgång.
- Rätt till rättelse.
- Rätt till radering.
- Rätt till begränsning av behandling.
- Rätt att göra invändningar.
- Rätt till dataportabilitet.
- Automatiserade beslut.

Personuppgiftsansvarig måste säkerställa att de registrerade har möjlighet att utöva dessa rättigheter. Om verksamheten inte har förmåga att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur ansvarig hanterar personuppgifter. Det kan även leda till tillsynsärenden från IMY.

2.5.3 Resultat

Granskningen har tagit utgångspunkt i om någon begäran att utöva rättigheter registrerats och om VD, eller administrativ chef fattat något beslut rörande registrerades rättigheter.

DSOs kontroll har tagit avstamp i systemstödet för ärende- och dokumenthantering, eDok, genomfördes den 27 november 2023 och omfattar tidsperioden fr.o.m. 2023-01 t.o.m. 2023-11.

Vid kontrollen kan konstateras att ingen begäran om att utöva rättigheter har registrerats i eDok och att inget beslut av vd eller administrativ chef, rörande registrerades rättigheter registrerats.

2.5.4 DSO anger hur allvarliga bristerna är på en skala

	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
X	Inga brister av nämnvärd betydelse identifierade

2.5.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att SBR fortsätter arbetet med att stärka medarbetarnas kompetens inom området genom att uppmana medarbetarna att ta del av SBRs styrdokument avseende registrerades rättigheter och stadens fördjupande e-utbildning avseende registerutdrag.

2.6 Personuppgiftsincidenter

2.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Inträffar något i verksamheten som kan vara en personuppgiftsincident ska det anmälas till respektive chef som har ansvar för rapportering, analys och åtgärder av inträffade incidenter. IA är Stockholms stads system för incidentrapportering vilket innebär att personuppgiftsincidenter rapporteras och följs upp i verktyget. VD fattar beslut om att anmäla incidenten till IMY och VD eller vid dennes frånvaro administrativ chef fattar beslut om att informera de registrerade.
Hur många personuppgiftsincidenter har dokumenterats?	N/a
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	N/a
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	N/a

2.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt

behandlats”. Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent och består av två huvudsakliga moment – dokumentering respektive rapportering.

Varje personuppgiftsincident ska dokumenteras och ett register ska föras över uppkomna incidenter. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, effekterna och åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden. Bristande dokumentering är sanktionsgrundande.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (artikel 33).

Detta innebär att de personuppgiftsincidenter som sannolikt leder till hög risk för fysiska personers rättigheter och friheter ska rapporteras till IMY, senast 72 timmar efter att PUA fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål.

2.6.3 Resultat

DSOs kontroll har dels skett i Stockholms stads incidentrapporteringssystem IA. Kontrollen genomfördes den 30 november 2023 och omfattar tidsperioden fr.o.m. 2023-01 t.o.m. 2023-11.

Av kontrollen framgår att ingen personuppgiftsincident dokumenterats i IA under den granskade perioden.

2.6.4 DSO anger hur allvarliga bristerna är på en skala

	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
X	Inga brister av nämnvärd betydelse identifierade

2.6.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att SBR fortsätter arbetet med att stärka medarbetarnas kompetens inom området genom att uppmana medarbetarna att ta del av SBRs styrdokument avseende personuppgiftsincident.

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskningar:

- Registerförteckningen.
- Verksamhetsspecifika rutiner.

3.2 Syfte

En av DSOs viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs.

Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året samt resultaten av granskningarna.

3.3 Genomförda granskningar och deras resultat

Granskning 1 – Registerförteckningen.

Resultatet är baserat på den version av registerförteckning som DSO granskade den 27 november 2023.

Total är 61 behandlingar registrerade i SBRs registerförteckning. Under året har SBR arbetat med att aktualisera register-förteckningen och genomfört nödvändiga uppdateringar.
I samband med detta har kompetensen stärkts hos respektive ansvarig genom individuella utbildningsinsatser. Vidare har en rutin för att hålla registerförteckningen enhetlig och aktuell är tagits fram.

Respektive ansvarig bedömer att registerförteckningen är uppdaterad och aktuell vilket är en bedömning som DSO delar. Även rutinen som tagits fram för att hålla registerförteckningen enhetlig och aktuell bedöms av DSO vara lämplig.

	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
X	Inga brister av nämnvärd betydelse identifierade

Granskning 2 - Verksamhetsspecifika rutiner.

Granskning av SBRs styrdokument inom detta område genomfördes av DSO i samarbete med verksamhetens informations-säkerhetssamordnare den 23 november 2023.

Av granskningen kan konstateras att SBRs styrdokument dels är stadsgemensamma och dels verksamhetsspecifika. De stadsgemensamma är framtagna av och granskade centralt inom Stockholms stad.

Under året har SBR arbetat med att ta fram och implementera verksamhetsspecifika rutiner avseende:

- Rutin för att tillgodose registrerades rättigheter.
- Rutin för hur personuppgiftsincidenter ska utredas, analyseras, rapporteras och dokumenteras.
- Rutin för att hålla registerförteckningen enhetlig och aktuell.
- Rutin för att konsekvensbedömningar vid behov genomförs, och dokumenteras.

Dessa rutiner bedömer DSO håller lämplig kvalitet, ger ett tillräckligt stöd, är uppdaterade och har en utpekad ägare som kan säkerställa att uppdateringar kan bli gjorda vid behov.

Det kan konstateras att verksamheten saknar en rutin för att säkerställa att informationsklassningar genomförs, eventuella skyddsåtgärder införs samt att vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller. Vidare kan konstateras att verksamheten saknar en rutin för att säkerställa arbetet med personuppgiftsbiträdesavtal.

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

3.4 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendationer avseende granskning 1 – Registerförteckning.

- DSOs råd och rekommendation är att SBR fortsätter arbetet med att regelbundet och systematiskt arbeta med inventering av personuppgiftsbehandlingarna i verksamheten, uppdatera registerförteckningen varefter förändringar sker och säkerställa att registerförteckningen fortlöpande hålls enhetlig och aktuell.

DSOs råd och rekommendationer avseende granskning 2 - Verksamhetsspecifika rutiner.

DSOs råd och rekommendation är att SBR utvecklar och implementerar rutiner avseende:

- Rutin för att genomföra informationsklassningar, implementera eventuella skyddsåtgärder samt vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller.
- Rutin för att säkerställa arbetet med personuppgiftsbiträdesavtal.

4 Risker inom dataskydd

4.1 Sammanfattning

Relevanta risker inom verksamheten:

- Avsaknad av verksamhetsspecifika och implementerade rutiner.
- Informationstillgångar som inte klassificerats eller bristande införande av skyddsåtgärder (tekniska och organisatoriska) efter genomförda informationsklassningar.
- Bristande kunskap.

4.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Det kan därtill finnas mer övergripande, generella eller specifika risker ur ett dataskyddsperspektiv, ur såväl tekniskt som organisatoriskt perspektiv. För att säkerställa att dataskydds-förordningen efterföljs är det viktigt att identifiera och minimera eller eliminera alla typer av risker i verksamheten.

4.3 Resultatet av riskkartläggningen

Risk 1
Verksamhetsspecifika och implementerade rutiner krävs för att på ett enhetligt sätt och korrekt sätt kunna hantera personuppgifter. Vid avsaknad av verksamhetsspecifika och implementerade rutiner finns risken att inte hanterar ansvaret för personuppgifter på det sätt som Dataskyddsförordningen föreskriver.

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

Risk 2

Att informationstillgångar klassificeras är första steg mot att skydda information. Därefter behöver verksamheten ta ställning till vilka skyddsåtgärder (tekniska och organisatoriska), genererade med hjälp av klassningen, som redan finns på plats och vilka som behöver arbetas in i verksamheten. När skyddsåtgärderna är införda får informationen det skydd som motsvarar dess betydelse för verksamheten.

Informationstillgångar som inte klassificeras eller skyddsåtgärder som inte arbetas in i verksamheten medför risken att informationen inte får det skydd som motsvarar dess betydelse för verksamheten.

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

Risk 3

Kunskap krävs bland medarbetarna som på ett eller annat sätt hanterar personuppgifter för att verksamheten ska kunna leva upp till dataskyddsförordningen. Kunskap är en färskvara som bibehålls och kompetens- och utbildningsinsatser.

Vid bristande kunskapsnivå finns risken att PUAs förmåga inom området inte lever upp till kraven i lagstiftningen.

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

4.4 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendationer framgår av tidigare avsnitt i denna rapport.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Verksamhetsspecifika rutiner.
- Verksamhetens information till registrerade.

5.2 Syfte

En av DSOs viktigaste uppgifter är det granskande arbetet.

Granskningsområdena har DSO valt utifrån ett riskbaserat synsätt, dvs. de områden där DSO anser verksamhetens mest relevanta risker och brister identifierats.

På så sätt åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

5.3 Planerade granskningar

Granskning 1

- En granskning av verksamhetsspecifika rutiner (styrdokument).

Granskningen innefattar PUAs verksamhetsspecifika rutiner (styrdokument).

Granskning 2

- En granskning av verksamhetens information till registrerade.