Stockholms stad

Bilaga 10

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 *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 Dataskyddsombud (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.

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.

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 för dataskyddsarbetet

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

- Ett tydligt fokus för 2023 bör vara att komplettera informationen i registerförteckningen
- Införa års-mässig genomgång av registerförteckningen, tydliggjort ansvar på informationsägare.
- Information om informationsklassning och riskanalys är särskilt låg, Av 32 behandlingar finns information enbart om 5, 3 respektive 0 av behandlingarna. Inom dessa områden rekommenderas hög prioritet för att komplettera informationen, och vid behov genomföra alla moment i den process som risk analyserar och konsekvens bedömer behandlingarna. Alternativt kontrollera att informationen är aktuell om analys och klassningar är mer än ett år gamla.
- Införa stöd i form av process där registerförteckning, informationsklassning riskanalys, Tröskelanalys och vid behov konsekvensbedömning ingår
- Tillse att verksamheten har medel och resurser för att förändra arbetssätt och arbeta med dataskyddsarbetet kontinuerligt.
- Tillse att verksamheten har resurser för att 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:

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:

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.

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.

2.5 Sammanfattning rekommendationer till PUA om observationer

- 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.