Verksamhetsutveckling
Johanna Munther

Styrelsen för Stockholm Vatten AB

Dataskyddsombudets Årsrapport 2022 – Stockholm Vatten och Avfall

FÖRSLAG TILL BESLUT

Styrelsen föreslås besluta

att anta årsrapporten från bolagets dataskyddsombud

Mårten Frumerie
Verkställande direktör

Johanna Munther
Avdelningschef
Verksamhetsutveckling

Sammanfattning

Ärendet avser den av dataskyddsombudets årligt framtagna DSO rapport för Stockholm Vatten och Avfall. Ärendet beskriver de rapporteringsområden som ska granskas av dataskyddsombudet, de särskilda granskningar som skett under 2022 samt de verksamhetsrisker som dataskyddsombudet redovisar.

Informationshanteringen är en prioriterad fråga inom bolaget och kommer att vara det fortsatt. Mycket arbete pågår och bolaget lyfter i detta ärende fram bolagets bedömning av de olika områden som dataskyddsombudet hanterar i rapporten.

Bakgrund

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. Dataskyddsombudet har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Den bilagda årsrapporten är således ett medel för styrelsen att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen.

ÄRENDET

Rapporteringsområden

Den oberoende DSO rapporten innefattar följande obligatoriska rapporteringsområden:

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter
- personuppgiftsincidenter

Nedan redogörs för bolagets bedömda status, dataskyddsombudets rekommendationer samt bolagets bedömning.

<u>Registerförteckning:</u>

- Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder

”Om registret över behandlingar hanteras som en naturlig del i det löpande dataskyddsarbetet, går det smidigare att se över registret och uppdatera när det sker förändringar eller tillkommer nya behandlingar, utan att det växer till ett onödigt stort arbete och upplevs som ett nödvändigt ont. I en förvaltningsmodell med tydliga roller och ansvarsområden kommer arbetet bli mer systematiserat än idag. Det behöver finnas en rutin som implementeras och kommuniceras i organisationen.”

Bolagets bedömning är att det pågår ett arbete med att tydliggöra informationsägarskap inom bolaget. Under våren genomförs bland annat en heldag med bolagets ledningsgrupp och specialister avseende informationshantering inom bolaget. Målet är att ta fram en långsiktig hanteringsplan.

Som alternativ lösning om arbetet drar ut på tiden ser bolaget över en temporär lösning avseende informationsägarskap kopplat till linjeorganisationen med delegeringsmöjligheter till den som praktiskt arbetar med en informationstillgång eller ett system.

Styrdokument:

- Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder.

”Dataskyddsombudets rekommendation är att anta de framtagna styrdokumenten och implementera dessa i organisationen.”

Bolagets bedömning är att det finns en framtagen anvisning för informationsklassificering som godkänts, den har dock inte implementerats i hela organisationen. Stadens tillämpningsanvisning finns i remissversion.

Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar:

- Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.

” Arbetet med att informationsklassa sker idag efter instruktioner och rutiner men med ett personberoende av systemförvaltare. Det betyder att systemen klassas men inte processer. Dataskyddsombudets råd är att implementera förvaltningsmodell och anta de dokument som tagits fram, bland annat anvisning för informationsklassificering.”

Bolagets bedömning är att de viktigaste processerna oftast har systemstöd vilket innebär att de klassas. På systemsidan genomfördes en stor utbildningsinsats förra året med syftet att höja kompetensen hos systemförvaltarna så att de själva kan handleda/genomföra klassningar.

Konsekvensbedömningar

- Inga brister av nämnvärd betydelse identifierade

”Dataskyddsombudets råd är att under året påminna om kraften i det verktyg som konsekvensbedömningen bidrar med. Ett systematiskt arbete med det underlättar upphandling, avtalsskrivning, förvaltning och kravställning.”

Bolaget har inga synpunkter på ovanstående bedömning.

Individens rättigheter

- Inga brister av nämnvärd betydelse identifierade.

” Dataskyddsombudets rekommendation är att se över och ytterligare eventuellt vid behov optimera process och rutin för registerutdrag. Samma rekommendation gäller för övriga rättigheter som den registrerade kan vilja utöva. Rutiner och processer behöver sedan kommuniceras med verksamheten för att kunna implementeras.”

Bolaget har inga synpunkter på ovanstående bedömning.

Personuppgiftsincidenter

- Inga brister av nämnvärd betydelse identifierade.

”Dataskyddsombudets rekommendation under 2023 är att se över och förbättra efterarbetet med personuppgiftsincidenter. Det vill säga när incidenten är upptäckt och utredd, hur omhändertar man då kunskapen man lärt av den? Syftet med att anmäla en personuppgiftsincident är att förbättra verksamhetens arbete med dataskyddsfrågor och de eventuella risker som finns för den registrerade. Då de fördjupade utbildningarna har visat sig vara mycket bra för benägenheten att uppmärksamma och anmäla personuppgiftsincidenter, rekommenderas att flera får delta i dessa och repetitionsmöjlighet ges till de som behöver.”

Bolaget har inga synpunkter på ovanstående bedömning.

Genomförda granskningar
En av dataskyddsombudets 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. Två särskilda granskningar har genomförts under året, vilket avser *”Granska intern kommunikation och utbildning”* samt *”Fungerar processerna för att hantera de registrerades rättigheter”*

Intern kommunikation och utbildning:
”Granskningen som genomförts är hur utbildning och information om dataskydd skett i organisationen under 2022. Fokus har lagts på dels den fördjupade utbildning som togs fram och omnämndes i årsrapporten för dataskydd 2021, då kallad pilotutbildning, samt den digitala utbildning som är obligatorisk för alla anställda inom Stockholm stad och som finns på Utbildningsplattformen”

- Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.

Bolagets bedömning är att det finns krav på att genomföra den obligatoriska utbildningen samt att statistiken över vilka som genomfört utbildningarna är bristfällig. Under 2023 är målet att koppla både stadens utbildningskrav såväl som bolagets egna utbildningskrav till bolagets utbildningsportal vilket kommer att förbättra möjligheten att följa upp varje enskild medarbetare i samband med medarbetarsamtalen.

Fungerar processerna för att hantera de registrerades rättigheter:
”Verksamhetsutvecklingens enhet Informationshantering har arbetat med att uppdatera processen och förbättra rutiner för den registrerades rättigheter under år 2022. Detta var också ett av de områden som dataskyddsombudet granskade under samma år. Förbättringar gjordes genom att ta fram tydligare rutin och mall för registerutdrag. Processbeskrivningen i Kompassen uppdaterades och förtydligades.”

- Inga brister av nämnvärd betydelse identifierade.

Bolaget har inga synpunkter på ovanstående bedömning.

Verksamhetsrisker inom dataskydd
Dataskyddsombudet har även identifierat verksamhetsrisker inom dataskydd och lyfter fram följande:

- Problematik kring tredjelandsöverföringar likt tjänster som Azure m.fl.
- Osäker e-posthantering med personuppgifter
- Brist på styrmodell för information

Tredjelandsöverföringar:
- Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.

Bolagets bedömning är att vi följer stadens direktiv men kan konstatera att det i vissa fall försvårar samverkan med andra externa parter.

Osäker e-posthantering med personuppgifter:
- Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.

Bolagets bedömning är att det i enlighet med bolaget regler inte får skickas personuppgifter med extern e-post. De medarbetare som har uttalade behov använder tjänsterna KURIR eller MOVEit, vilket vid behov kan utökas att genom bolaget köper in fler licenser för KURIR. Ovanstående lyfts fram vid samtliga utbildningstillfällen inom bolaget rörande informationssäkerhet.

Brist på styrmodell för information:
- Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder.

Bolagets samlade bedömning är att bolagets informationshantering kommer att vara ett av bolagets mest prioriterade områden de kommande åren. På avdelning verksamhetsutveckling pågår ett arbete med att utvärdera lämplig form avseende styr- och samverkansmodell för bolaget.

SLUT

Bilaga: Dataskyddsombudets Årsrapport år 2022 Stockholm Vatten och Avfall