Skrivelsen är riktad till samtliga personuppgiftsansvariga myndigheter som ingår i samverkansavtalet för dataskyddsombud i samverkan, Ale, Alingsås, Härryda, Lerum, Lilla Edet, Partille, Stenungssund, Öckerö samt Göteborgsregionens kommunalförbund. Samverkansavtalet gäller samtliga nämnder. Kommunala bolag har egna dataskyddsombud och omfattas inte av samverkansavtalet.

Årskontroll av dataskyddsarbetet 2022

Dataskyddsombuden kommer under hösten 2022 genomföra en efterlevnadskontroll på samtliga personuppgiftsansvariga som faller under samverkansavtalet för dataskyddsombud i samverkan. Totalt är det ca 70 unika personuppgiftsansvariga. Dataskyddsombuden förväntar sig således svar på nedanstående frågeställningar från varje personuppgiftsansvarig med en tydlig beskrivning och resonemang som så tydligt som möjligt beskriver verksamhets nuvarande förutsättningar att leva upp till GDPR och hur verksamheten har tagit sig an nämndens dataskyddsarbete.

Dataskyddsombuden önskar svar från respektive nämnds verksamhet senast 2022-11-18. Detta för att hinna sammanställa och färdigställa slutrapporterna innan årsskiftet.

Inledning

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 ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av

personuppgifter. Det innebär att nämnden behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd har i enlighet med dataskyddsförordningen utnämnt ett dataskyddsombud, DSO. Denna roll 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 nämnden att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen.
Årsrapporten syftar till att nämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnden ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten kan ses som en del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för nämndens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete

Kontrollpunkter

Årskontrollen bygger på fasta kontrollpunkter till vilka dataskyddsombuden önskar att nämndens förvaltning eller sektor beskriver arbetssätt och nuläge. Till varje kontrollpunkt önskar även dataskyddsombuden att verksamheten bifogar relevanta rutiner, riktlinjer eller andra styrdokument som kan styrka de påståenden som verksamheten lämnar i sina svar. Svaren från verksamheten önskar dataskyddsombuden i löptext i rapportform utifrån kontrollpunkterna då verksamhetens svar kommer vara en del i slutversionen ihop med dataskyddsombudens råd och rekommendationer.

1. Dataskyddsorganisation

Beskriv verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete. Dataskyddsombuden önskar att verksamheten beskriver och resonerar kring verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt de resurser som tillhandahålls för arbetet. Dataskyddsombuden vill att verksamheten i sina svar resonerar om de anser att organisationen fungerar, om de har

tillräckligt med resurser för att proaktivt arbeta med dataskydd, hur organisationen strategiskt arbetar med dataskydd, om det finns rätt kompetens, samt hur dataskyddsorganisationen bidrar till att dataskyddsarbetet är en naturlig del i verksamhetens processer.

Bifoga: Om möjligt en organisationsskiss som visar dataskyddsorganisationens struktur, och om det finn,s styrdokument i kommunen som beskriver hur en dataskyddsorganisation ska se ut. Bifoga gärna också om dataskyddsorganisationen har en strategi eller årsplanering för sitt dataskyddsarbete.

2. Behandlingsregister och informationsskyldigheten

Under denna punkt önskar dataskyddsombuden att verksamheten redovisar hur nämndens behandlingsregister ser ut både i egenskap av personuppgiftsansvarig men också i egenskap som personuppgiftsbiträde. Dessutom önskar dataskyddsombuden att verksamheten beskriver sitt bedömda nuläge och hur många av verksamhetens behandlingar som i dagsläget bedöms finns dokumenterade. Dataskyddsombuden önskar också en beskrivning hur verksamheten arbetar i val av rättslig grund samt en motivering kring när den rättsliga grunden samtycke används för personuppgiftsbehandling och de överväganden som gjorts kring användandet av den rättsliga grunden i verksamheten.

Bifoga kopia på registerförteckning som upprättats av nämnden som personuppgiftsansvarig och även det register som ska föras om nämnden som personuppgiftsbiträde.

Under denna punkt önskar dataskyddsombuden också få en beskrivning om hur verksamheten har arbetat med informationsskyldigheten i allmänhet. Av beskrivningen bör framgå om det huvudsakligen handlar om information när den enskilde själv har lämnat informationen (art. 13 GDPR) och i vilken omfattning som information sker utifrån att förvaltningen fått informationen från någon annan än den enskilde själv (art. 14 GDPR)

Bifoga: En eller flera informationstexter om behandling av personuppgifter som gått ut till de registrerade rörande någon/några av de behandlingar verksamheten har upprättade i sitt behandlingsregister.

3. Personuppgiftsincidenter

Beskriv verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier.
Beskriv också verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Beskriv också hur verksamheten lever upp till dokumentationsskyldigheten, att alla inträffade personuppgiftsincidenter dokumenteras.

Dataskyddsombuden önskar också en redogörelse kring hur verksamheten arbetar för att uppmärksamma sina anställda om deras viktiga roll att larma vid misstänkt personuppgiftsincident och om de känner till hur de ska agera vid misstanke.

Verksamheten bör ha dokumenterade rutiner som ger goda förutsättningar för att upptäcka och utreda personuppgiftsincidenter. (Fundera över om det finns rutiner, var de finns och om de är kända för all personal i verksamheten samt om de har en tydlig rollfördelning över vem som gör vad när en incident upptäcks eller misstänks ha skett. Fundera och argumentera också över om rutinen följer IMYs rekommendationer?

Bifoga: Rutiner kring arbetet med personuppgiftsincidenthanteringen. Bifoga också antal identifierade incidenter 2022 samt antal av dessa som anmälts till IMY.

4. Registrerades rättigheter

Beskriv verksamhetens förutsättningar för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering. Beskriv gärna hur verksamheten hanterar en begäran om ett registerutdrag eller radering av personuppgifter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan.

Bifoga: Rutin kopplat till hanteringen av de registrerades rättigheter. Bifoga också om det finns en rutin för att hantera ett tillbakadragande av

samtycke. Bifoga också antal ärenden som hanterats under 2022 rörande registrerades rättigheter.

5. Konsekvensbedömningar

Beskriv verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt arbetsprocessen vid genomförandet av en konsekvensbedömning. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet. Beskriv också verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Bifoga: Om sådan finns, en genomförd konsekvensbedömning och eventuell mall som ska användas i detta arbete.

Kontaktuppgifter till dataskyddsombuden

Vid eventuella frågor är förvaltningarna välkomna att höra av sig till någon av oss.

Johan Bergström
Dataskyddsombud
johan.bergstrom@gotebrogsregionen.se
031 – 335 52 53

Malin Ericsson
Dataskyddsombud
malin.ericsson@goteborgsregionen.se
031 – 335 52 54