



Beslutsunderlag

Utfärdat 2020-04-03

Diarienummer 0037/20

Handläggare

Katrin Gundersen

Telefon: 031-368 55 12

E-post: katrin.gundersen@gotalejon.goteborg.se

Årsplan för dataskyddsarbetet 2020

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anteckna årsplan för dataskyddsarbetet 2020

Sammanfattning

Årets dataskyddsplan innehåller fem fokusområden som är adresserade till såväl dataskyddsombudet som till dataskyddsansvariga inom organisationen. Även om fler aktiviteter kommer att genomföras under årets gång har dessa fem bedömts som mest angelägna att genomföra under år 2020.

- Integritetspolicy
- Kvalitetskontroll av befintliga personuppgifter
- Rutiner för notifiering av personuppgiftsincidenter
- Personuppgiftsbiträden och personuppgiftsbiträdesavtal
- Kunskapsnivå hos medarbetare

Bilagor

1. Årsplan för dataskyddsarbete 2020

Katrin Gundersen

Annika Forsgren

Bolagsjurist

VD

Årsplan för dataskyddsarbetet 2020

Försäkrings AB Göta Lejon

Årets dataskyddsplan innehåller fem fokusområden som är adresserade till såväl dataskyddsombudet som till dataskyddsansvariga inom organisationen. Även om fler aktiviteter kommer att genomföras under årets gång har dessa fem bedömts som mest angelägna att genomföra under år 2020.

1. Integritetspolicy

Information till den registrerade om hur deras personuppgifter behandlas.

En grundläggande princip i dataskyddsförordningen är den s.k. ansvarsskyldigheten, vars syfte inte enbart är att bedöma fullgörandet av de lagstadgade kraven utan också att visa hur den personuppgiftsansvarige respekterar de registrerades dataskydd, det vill säga skyddet för de personer som är föremål för behandlingen av personuppgifter. Fullgörandet av ansvarsskyldigheten ökar förtroendet för den personuppgiftsansvariges verksamhet.

Integritetspolicyn skall därför på ett tydligt och informativt sätt förklara för den registrerade vilka personuppgifter som verksamheten behandlar, varför de behandlas, huruvida känsliga personuppgifter behandlas, på vilket sätt de samlas in, på vilken laglig grund som verksamheten stödjer behandlingen, hur verksamheten skyddar den enskildes personuppgifter, vilka rättigheter den registrerade har avseende personuppgiftsbehandlingen ifråga, huruvida personuppgifterna transfereras till tredje land och i sådana fall varför, vilka som kan få tillgång till personuppgifterna, samt hur länge personuppgifterna sparas.

En komplett, välstrukturerad och överskådlig integritetspolicy visar på att organisationen är väl insatt i dataskyddsfrågor och att man tar den registrerades rättigheter på allvar. Den personuppgiftsansvarige kan också på så vis säkerställa att organisationen uppfyller ansvarskravet, öppenhetskravet och en stor del av informationsskyldigheten i Dataskyddsförordningen.

2. Kvalitetskontroll av befintliga personuppgifter

Analys av det rättsliga stödet för behandlingen av era personuppgifter, den här omgången med fokus på samtycke som rättslig grund.

Kvalitetskontroll i registerförteckningen kommer att genomföras i form av

stickprovskontroller för att säkerställa att verksamheten använder sig av en kvalificerad rättslig grund. Datainspektionen kommer i år att fokusera på tillsyn av den rättsliga grunden "samtycke", och det är således också ett lämpligt fokusområde för vår del.

3. Rutiner för notifiering av personuppgiftsincidenter

Vilka rutiner finns i verksamheten för hanteringen av en personuppgiftsincident?

Det är av stor vikt att verksamheten i god tid har skapat tydliga rutiner för att upptäcka personuppgiftsincidenter. En handlingsplan bör upprättas för de fall en personuppgiftsincident inträffar så att verksamheten snabbt kan skrida till handling.

Handlingsplanen ska innehålla:

- a) Rutiner för att kunna avgöra vad som är en personuppgiftsincident.
- b) Rutiner för hur arbetstagarna inom organisationen ska agera om en incident inträffar.
- c) En utsedd person eller en grupp som är ansvarig för att hantera personuppgiftsincidenter.
- d) Rutiner för anmälan av incident till Datainspektionen inom 72 timmar efter upptäckten.
- e) Rutiner för att informera registrerade personer.
- f) Rutiner för att hantera incidenter som har inträffat hos personuppgiftsbiträdet.
- g) Rutiner för att dokumentera alla personuppgiftsincidenter som inträffar, även de som inte behöver anmälas till Datainspektionen.

4. Personuppgiftsbiträden och personuppgiftsbiträdesavtalen

Vilka personuppgiftsbiträden finns och hur ser avtalen ut?

Det finns särskilda lagkrav i dataskyddsförordningen om vad ett biträdesavtal ska innehålla. Enligt dataskyddsförordningen ska biträdesavtalet reglera att biträdet enbart behandlar personuppgifter enligt dokumenterad instruktion. Biträdesavtalet och dess innehåll utgör därmed en viktig grund för förhållandet och ansvarsfördelningen mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Det är därför bra om en genomgång av avtalen görs för att kontrollera kvaliteten och innehållet i dessa för att säkerställa att de är lagenliga och håller god standard.

5. Kunskapsnivån hos medarbetarna

Det är viktigt att organisationen har en medveten och utbildad personalstyrka.

Senare i höst kommer en enkät att skickas ut till samtliga medarbetare för att se över kunskapsnivån vad gäller dataskyddsfrågor.

Dataskyddsbudet kan därefter komma till er för att hålla föreläsningar om ni önskar det. På så vis går det också att anpassa föreläsningsnivån utifrån medarbetarnas kunskap. Fram till dess är det bra om ni dokumenterar kompetenshöjande aktiviteter hos arbetstagarna. Om ni sänder era medarbetare på kurser inom GDPR, så dokumentera det.