

| | | | |
|--------------------------------------|-------------------------------------|--------------------------------------|----------------------------------|
| Id: GSK dnr 1.1-034/2021 | Version: 0.1 | Dokumenttyp: Handlingsplan | Typ av styrning: |
| Framtagare: Carin Ahlinder | Godkännare: Birgitta Roos | Datum: 2021-09-06 | Uppdaterad: 2021-09-06 |

Handlingsplan för dataskyddsarbetet under 2021 avseende affärsstödet i GSK samt de helägda bolagen GSB och GST

Inledning

Under hösten 2019 genomförde dataskyddsombudet en granskning av arbetet med utbildning inom dataskyddslagstiftningen och kunskapsnivåerna hos de anställda inom hela GSK-koncernen.

Enkät till ca 140 personer skickades ut och syftet var att undersöka vilken nivå av kunskap bolagen har och identifiera eventuella behov av ytterligare utbildningsinsatser.

Resultatet av granskningen visade stora brister vad gällde kunskapsnivån om vad som är en personuppgift, vem som är personuppgiftsansvarig och hur en personuppgiftsincident ska hanteras inom bolagen.

Utifrån granskningsplanen och dataskyddsombudets rekommendationer gjordes en handlingsplan 2020 för affärsstödet i GSK och de helägda bolagen GSB och GST. Handlingsplanen innehöll fyra aktiviteter

Utbildning för chefer och medarbetare

På hösten 2020 genomfördes en halvdags grundläggande utbildning för personal som kommer i kontakt med personuppgifter i sitt dagliga arbete. Det var ca 40 personer från GSK, GSB och GST som deltog i utbildningen.

Förvaltningsorganisation för dataskyddsarbetet

GSK har beslutat om en förvaltningsorganisation där roller, ansvar och arbetsuppgifter är utpekade inom affärsstödet i GSK samt de helägda bolagen GSB och GST.

Information till externa, medarbetare och nyanställda

Under 2020 skapades egna sidor på goteborg.se där information om behandling av personuppgifter till externa finns beskrivna. Information lämnas vid nyanställning och ett informationsblad som dataskyddsenheten utformat har delats ut.

Rutin för personuppgiftsincidenter

Under 2020 har processen för personuppgiftsincidenter setts över och publicerats på verksamhetsledningssystemet GSK One. Processen avser affärsstöden i GSK samt de två helägda bolagen GSB och GST.

Dataskyddsenhetens arbete under 2021

Dataskyddsenheten på Intraservice tog fram en kontrollplan för affärsstöden i GSK samt de två helägda bolagen GSB och GST beträffande arbetet med dataskyddsförordningen som presenterades för styrelsen i GSK i februari 2021. Den innehåller en tidplan för kontroller och för delårsrapporter.

Den första delårsrapporten presenterades för styrelsen i juni och innehåller granskning av två kontrollområden; hantering av personuppgiftsincidenter och ökad kunskapsnivå beträffande dataskyddsförordningen för affärsstöd GSK samt bolagen GSB och GST.

De iakttagelser för affärsstöden i GSK samt för de helägda dotterbolagen GSB och GST från dataskyddombudet beträffande rutiner och hantering av personuppgiftsincidenter kan sammanfattas med att det finns förbättringsområden inom processen, kunskapen om vad som är en personuppgiftsincident samt rollerna.

Delårsrapporten som gäller ökad kunskapsnivå och utbildningsinsatser grundar sig på en enkät som gjordes av dataskyddsenheten under våren 2021. Enkäten hade hög svarsfrekvens och kunskapsnivån var hög.

Den första delårsrapporten för GSAB innehöll två kontrollområden; hantering av personuppgiftsincidenter samt hantering av de registrerades rättigheter med rubriken Hantering av de anställdas personuppgifter: Positioneringsteknik (GPS). GSAB har dock inte expedierat någon handlingsplan.

Dataskyddsombudets sammanfattande rekommendationer för affärsstöd GSK samt bolagen GSB och GST

Personuppgiftsincidenter

- Instruktionen bör tydliggöras och kompletteras med en beskrivning av hur bedömningen av risken för de registrerades fri- och rättigheter ska göras.
- Instruktionen bör kompletteras med beskrivning av när de registrerade ska informeras, vad informationen ska innehålla och hur den ska tillhandahållas.
- Bolaget bör ha en rutin/plan för att regelbundet informera sina anställda om den interna incidenthanteringen och göra det till en obligatorisk del av introduktionen för nyanställda.

Utbildning

- Bolaget bör ta fram en utbildningsplan för att säkerställa att anställda har tillräcklig kunskap om dataskydd. Av planen bör också framgå hur man säkerställer att kunskaperna upprätthålls.
- Bolaget bör säkerställa att det finns tydliga och uppdaterade rutiner/instruktioner som de anställda har tillgång till.

Handlingsplan för det fortsatta arbetet 2021 för affärsstöd GSK och bolagen GSB och GST

Nedan beskrivs de aktiviteter som GSK tillsammans med sina dotterbolag GSB och GST ska genomföra under 2021. Enligt dataskyddsombudets rekommendationer är utbildning och uppdatering av processen för personuppgiftsincidenter åtgärder som behöver genomföras. Om dataskyddsarbetet ska fungera måste medarbetare och chefer ha grundläggande kunskaper om personuppgiftsbehandlingar och processerna behöver förtydligas.

Aktiviteter

- **Fastställa utbildnings- och informationsplan**

Under hösten 2021 utarbeta ett förslag på utbildnings- och informationsplan. Dataskyddsenheten på Intraservice har tagit fram en kortfattad e-utbildning för samtliga medarbetare i Göteborgs Stad. Samtliga medarbetare ska ges möjlighet att få information om Dataskyddsförordningen/GDPR genom e-utbildningen. Anställningsavtalet ska uppdateras med lättförståelig information om hur bolaget hanterar personuppgifter. I checklistan för introduktion av nya medarbetare ska information om bolagets hantering av personuppgifter ingå.

- **Utbildning för chefer och administrativ personal**

Utbildning för chefer och medarbetare, som hanterar personuppgifter i större mängd ska genomföras under hösten 2021. Fokus ska ligga på personuppgiftsincidenter och processen kring dessa men även vara en repetition av 2020 års utbildning.

- **Översyn av personuppgiftsincidentprocessen**

Enligt dataskyddsombudets rekommendationer kommer personuppgiftsincidentprocessen ses över och förtydligas. Det gäller såväl roller, översyn av rutiner, och att säkerställa kunskapsnivån.

Dataskyddsombudets sammanfattande rekommendationer för GSAB. Styrelsen för GSAB har inte inkommit med någon handlingsplan utifrån dessa rekommendationer

Personuppgiftsincidenter

- Instruktionen bör kompletteras med en beskrivning av hur bedömningen av risken för de registrerades fri- och rättigheter ska göras
- Instruktionen bör kompletteras med instruktioner om när de registrerade ska informeras, vad informationen ska innehålla och hur den ska tillhandahållas
- Incidenthanteringen bör göras mindre personberoende genom att tydliggöra och konkretisera instruktionerna så att fler kan följa dem
- Bolaget bör ha en rutin för att regelbundet informera sina anställda om den interna incidenthanteringen och göra det till en obligatorisk del av introduktionen för nyanställda.

Hantering av de anställdas personuppgifter: Positioneringsteknik (GPS)

- GSAB rekommenderas att genomföra en kartläggning av personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer, och bedöma huruvida behandlingarna kan motiveras med hänvisning till ändamål, nödvändighet och rättslig grund.

- GSAB rekommenderas att genomföra konsekvensbedömningar för identifierade personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer.
- GSAB rekommenderas att skriftligen informera de anställda om personuppgiftsbehandlingarna.

Handlingsplan för det fortsatta arbetet 2021 för GSAB

GSAB har inte redovisat någon handlingsplan för det fortsatta arbetet 2021

Uppföljning av vidtagna åtgärder

Dataskyddsombudet kommer att följa upp vidtagna åtgärder enligt dataskyddsenhetens kontrollplan 2021.

Tidplan

Arbetet med aktiviteterna för affärsstöden i GSK samt för de helägda bolagen GSB, GST har påbörjats under sommaren 2021 och löper under hela året.

Ansvarig för aktiviteterna

Ledningen för GSK, GSB och GST ansvarar för att arbetet genomförs för respektive bolag.