Handläggare: Mattias Rindberg

Tel: 08-508 28 590

E-post: mattias.rindberg@stockholm.se

Dataskyddsförordningen (GDPR)

Stockholm Business Regions förslag till beslut

Styrelsen för Stockholm Business Region beslutar följande.

1. Godkänna SBRs rapport avseende implementeringen av dataskyddsförordningen (GDPR) i verksamheten.
2. Protokollet i denna paragraf förklaras omedelbart justerat.

Olle Zetterberg

Lena Häggdahl

Bakgrund

Dataskyddsförordningen (General Data Protection Regulation, GDPR) kommer den 25 maj 2018 att ersätta personuppgiftslagen (PuL). Förordningen gäller alla som behandlar personuppgifter i sin verksamhet, oavsett om det är en offentlig eller privat aktör och oaktat organisationens storlek. Mycket av det som GDPR reglerar gäller redan i dag, i och med PuL, men en del regler blir strängare.

Ärendet

För koncernen Stockholm Business Region (SBR) innebär GDPR en del förändringar t.ex.:

- Ökade krav på hantering av personuppgifter (PU). När GDPR ersätter PuL kommer den så kallade missbruksregeln inte längre finnas kvar. Missbruksregeln innebär att enklare regler gäller för personuppgifter i ostrukturerat material. Det handlar till exempel om information om personer i e-post, på internet eller i en enkel lista som finns i datorn. När missbruksregeln försvinner innebär det att samma regler som finns för alla personuppgifter även ska gälla för det som skrivs om personer i exempelvis e-post och på webbplatser. Det kommer att innebära krav på att bland annat ha en rättslig grund för att hantera personuppgifter, informera de registrerade och inhämta samtycke.

- Ökade krav på information till den registrerade. Den enskilda individen får en stärkt makt över sina personuppgifter genom rätten till insyn, till rättelser och ändringar. Om verksamheten registrerar personuppgifter måste verksamheten också informera de berörda om varför – på vilken rättslig grund – och hur länge informationen sparas. Det kommer inte att vara tillåtet att samla in och behandla fler uppgifter än nödvändigt för ändamålet.

- Krav på incidentrapportering inom 72 timmar. Om något händer, exempelvis att ett register kommer i orätta händer eller uppgifter skickas till fel mottagare, måste det finnas beredskap för att upptäcka, rapportera och utreda sådana incidenter. För känsliga uppgifter gäller att incidenterna måste rapporteras inom 72 timmar till Datainspektionen och till den/de registrerade.

- Sanktionsavgifter införs. Om det skulle ske en allvarlig överträdelse kan sanktionsavgift utgå motsvarande 20 miljoner euro eller fyra procent av organisationens omsättning; 10 miljoner euro eller två procent av omsättningen i mindre allvarliga fall. Även enskilda personer kan begära skadestånd.

- Ny roll som dataskyddsombud införs. Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att verksamheten följer GDPR. Det innebär bland annat att samla in information om hur verksamheten behandlar personuppgifter, kontrollera att organisationen följer bestämmelser och interna styrdokument samt informera och ge råd inom organisationen. Dataskyddsombudet har dock inget eget ansvar för att organisationen följer dataskyddsförordningen. Det ansvaret ligger alltid hos den personuppgiftsansvariga, det vill säga den juridiska personen.

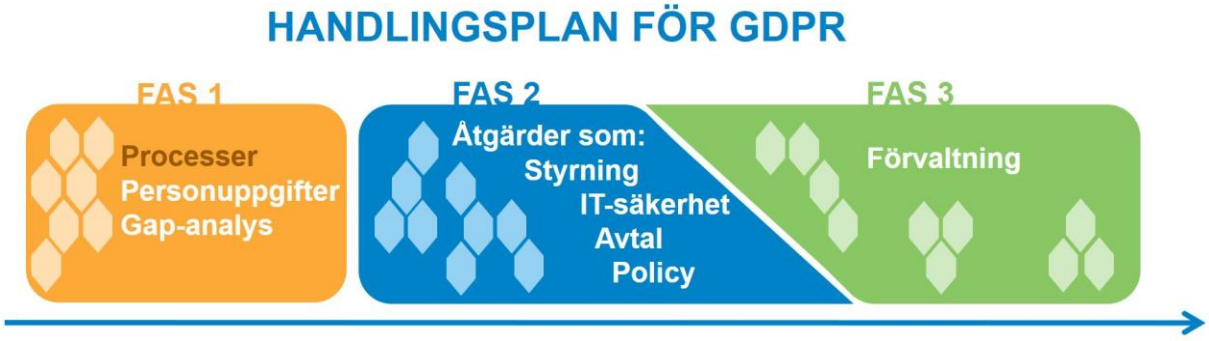
GDPR bedöms påverka hela koncernen, från interna verksamhetsprocesser och IT system, till kommunikationsaktiviteter och informationsinsamling. För att förbereda SBR till förordningen kommer åtgärder behövas inom respektive bolag. Varje bolag är personuppgiftsansvarigt för de uppgifter som bolaget behandlar i sin verksamhet, och ansvarar därmed för en korrekt personuppgiftshantering.

SBR har sedan hösten 2017 arbetat med att implementera GDPR i verksamheten och arbetet har på olika sätt har involverat alla medarbetare i koncernen. Planering och ledning av implementeringen har skett genom en koncernövergripande styrgrupp som bestått av;

- AdminC SBR
- Strategi & Utveckling SBR
- VD Visit Stockholm
- vVD Invest Stockholm

För att säkerställa struktur och rådgivning har SBR avropat stadens avtal avseende IT konsulter - informationssäkerhet. Deras uppdrag har bestått i att stötta SBR i arbete med att efterleva kraven i dataskyddsförordningen

För att få en översikt av alla aktiviteter som skulle genomföras inför den 25 maj 2018 delades arbetet upp i tre olika faser; nulägesanalys (fas 1), etablering önskat läge (fas 2) och förvaltning (fas 3).



Inom ramen för fas 1 har ett flertal workshoppar genomförts där inventering och kartläggning av personuppgifter i koncernens verksamhetsprocesser skett. Med utgångspunkt i detta har därefter bolagsspecifika registerförteckningar och en Gap-analys tagits fram. Vidare har SBRs medarbetare informerats och utbildats om dataskyddsförordningens grundläggande delar och krav.

I fas 2 har arbetet tagit utgångspunkt i genomförd Gap-analys. SBRs arbetet har under april – maj prioriterats utifrån särskilt viktiga åtgärder och en prioriterad åtgärdslista.

- Prioritet 1 – Förutsättningar för laglig behandling av PU.
- Prioritet 2 – Den registrerades rättigheter
- Prioritet 3 – Säkerhetsåtgärder vid behandling av PU.
- Prioritet 4 – Övergripande krav

Arbetet avseende prioritet 1, (Förutsättningar för laglig grund för behandling av PU) har bl.a. omfattat att komplettera upprättad registerförteckning med laglig grund för behandling av PU

för respektive verksamhetsprocess samt utreda huruvida särskilda PU behandlas och laglig grund för dessa m.m.

Inom ramen för den registrerades rättigheter (prioritet två) har arbetet bedrivits i syfte att tillgodose den registrerades rättigheter genom informationsplikt. Arbetet har bestått i att anpassa texter i exempelvis direktupphandlingsmallar och kontrakt, mallar för samtycke för behandling av PU m.m.

Beträffande säkerhetsåtgärder vid behandling av PU (prioritet 3) har arbetet bestått i att identifiera att adekvata säkerhetsåtgärder finns på plats. Det har innefattat att bl.a. ta fram mallar för s.k. personuppgiftsbiträdesavtal. Dessa säkerställer att tredje part, som behandlar PU på uppdrag av SBR, garanterar att kraven i GDPR följs. Personuppgiftsavtal därefter har tecknats med bl.a. Avonova som är leverantör av SBRs företagshälsovård samt Visma som är SBRs leverantör av lönesystem.

Inom prioritet 4 (övergripande krav) ingår bl.a. att säkerställa att de allmänna principerna för behandling av PU följs och att rutiner, dokumentation och information är implementerade och genomsyrar verksamhetsprocesserna. För detta ändamål är den personuppgiftsansvariga skyldig att föra ett register över de PU behandlingar som görs.

I enlighet med GDPR ska ett dataskyddsombud (DSO) utnämnas av personuppgiftsansvarig om verksamheten är en myndighet, ett offentligt organ eller om verksamheten kräver omfattande och systematisk övervakning av de registrerades personuppgifter. En koncern får utnämna ett dataskyddsombud om det är lätt att nå i hela organisationen eller om personuppgiftsansvarig är en myndighet/offentligt organ. Med anledning av detta har ett DSO utnämnts för koncernen SBR.

Den 25 maj 2018 övergår SBR till fas 3 (förvaltning) av GDPR och det genomförda arbetet. Den bolagsspecifika registerförteckning som är upprättad kommer då ingå i verksamhetens processer och löpande hållas aktuell för att säkerställa att principerna för behandling av PU i verksamheten följs och sker i enlighet med GDPR.

SBR bedömer att verksamheten till största del kommer att ha anpassats till GDPR till den 25 maj och de kvarvarande aktiviteterna och rutinerna kommer därefter löpande att åtgärdas och implementeras under våren.

Till stöd för det resterande arbetet finns juridisk kompetens tillgänglig för alla bolag i Stadshus AB koncernen inom ramen för stadens avtal avseende IT konsulter - informationssäkerhet.