STOCKHOLMS STADSHUS AB
En del av Stockholms stad

Tjänsteutlåtande
Koncernstyrelsen
Ärende 9

Dnr SSAB 2017/169
Sid. 1 (3)
2018-02-1928

Handläggare
Sara Feinberg, 0850829097

Till
Koncernstyrelsen

GDPR - nya dataskyddsförordningen

Koncernledningens förslag till beslut

Koncernstyrelsen beslutar
att lägesrapporten om nya dataskyddsförordningen, GDPR, godkänns.

Ingela Lindh
VD

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 bolagen inom koncernen (motsvarande för nämnderna) innebär GDPR en del förändringar t.ex.:

- **Ökade krav på hantering av personuppgifter.** 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.

- **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.

- **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.

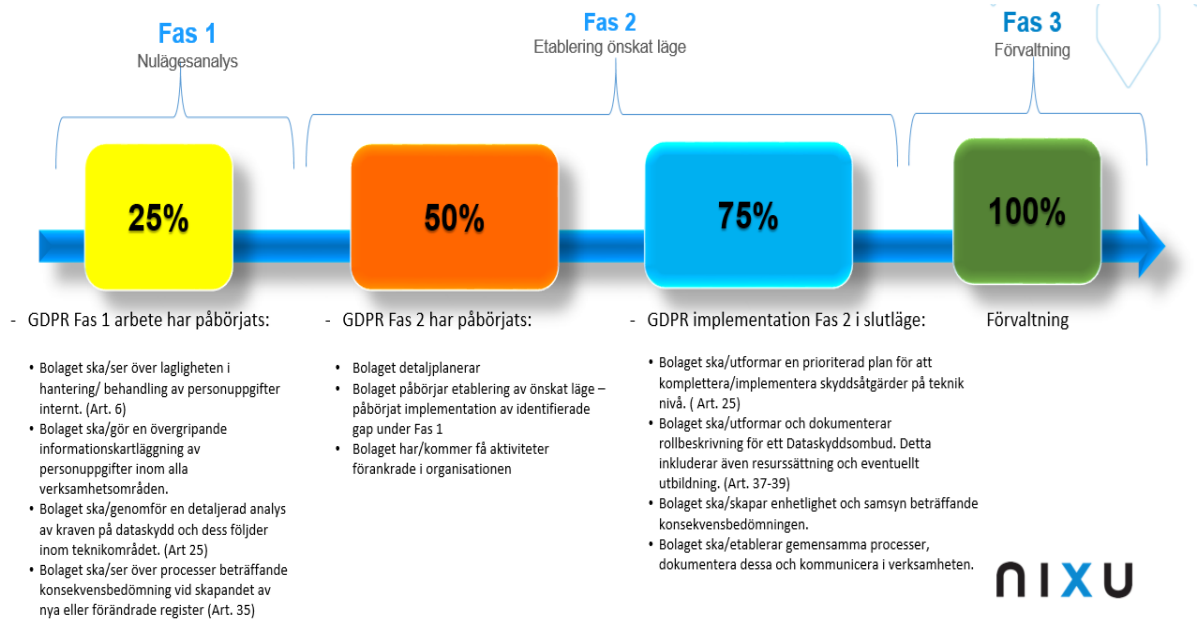
- **Sanktionsavgifter införs.** Om det skulle ske en allvarlig överträdelse kan sanktionsavgift utgå motsvarande 20 miljoner euro eller fyra procent av organisationens omsättning; 10 miljoner euro eller två procent av omsättningen i mindre allvarliga fall. Även enskilda personer kan begära skadestånd.

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

Bolagskoncernens arbete med GDPR
Flera av bolagen inom koncernen Stockholms Stadshus AB har under en längre tid arbetat med att implementera GDPR. Sedan hösten 2017 har Stockholms Stadshus AB arbetat med GDPR ur två perspektiv; *internt* för moderbolaget för att anpassa Stockholms Stadshus AB:s egen verksamhet och *övergripande* för bolagskoncernen för att bevaka och stödja bolagens GDPR-arbete ur ett koncernperspektiv. För att säkerställa struktur och rådgivning i arbete har extern expertis avropats, Nixu AB, vilka är informations- och IT-säkerhetskonsulter med specialistkompetens inom GDPR.

För att få en enkel översikt av alla aktiviteter som ska genomföras inför den 25 maj 2018 har arbetet delats upp i tre olika faser; nulägesanalys (fas 1), etablering önskat läge (fas 2) och förvaltning (fas 3). Inför den 25 maj 2018 behöver bolagen, inklusive Stockholms Stadshus AB, befinna sig inom ”Fas 2 slutläge”, där uppskattningsvis mer än 75 procent

av arbetet ska vara genomfört. Efter den 25 maj ska bolagen gå över till Fas 3, med förvaltning av det genomförda arbetet.



Stockholms Stadshus AB:s eget arbete med GDPR befinner sig i början av Fa
anpassa till den egna verksamheten genomförs ett antal aktiviteter, till exempel:
- GAP-analys för att identifiera vilka avvikelser vi har i hanteringen av personuppgifter som måste hanteras för att uppfylla de nya kraven.
- Övergripande kartläggning av personuppgifter inom alla verksamhetsdelar.
- Upprätta registerförteckning baserat på verksamhetens processer som innehåller personuppgifter.
- Informera och utbilda medarbetarna om GDPR:s grundläggande delar.
- Utse dataskyddsombud (DSO)
- Upprätta så kallade personuppgiftsbiträdesavtal (PuB-avtal) med de leverantörer som hanterar personuppgifter på uppdrag av oss.
- Upprätta samtycke i de fall vi ska hantera någons personuppgifter.

Stockholms Stadshus AB:s roll i bolagskoncernen innebär ett ansvar att *följa och stödja* bolagens arbete med införandet av GDPR. Varje enskilt bolag ansvarar för att *genomföra* verksamhetens arbete och vara klar till maj. Under hösten 2017 och våren 2018 genomför vi ett antal stickprov för att se till att alla bolagen arbetar med uppdraget. Dessutom ser vi till att bolagen samarbetar och delar med sig av sitt arbete eftersom många av bolagen är mycket kunniga inom området. I de fall bolagen behöver ett koncernövergripande stöd har vi avropat extern expertis inom GDPR.

Koncernledningens synpunkter och förslag
Bedömningen är att moderbolaget och dotterbolagens verksamheter i stort kommer att ha anpassats till GDPR till 25 maj 2018 och befinna sig i Fas 2, för att vara redo att övergå i Fas 3. I de fall det kommer finnas avvikelser kommer dessa att vara dokumenterade och kompletterade med åtgärdsplaner.

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Ingela Lindh (Huvudansvarig)	2018-02-28