Protokollsbilaga C
Direktionens protokoll 2018-12-13 §5

PM

DATUM: 2018-12-06
AVDELNING: STA RIE
HANDLÄGGARE: Johan Hultgren
HANTERINGSKLASS B E G R Ä N S A D

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR [Diarienummer]

Dataskyddsplan för 2019

Av Riksbankens instruktion framgår det att Riksbankens dataskyddombud (DSO) ska upprätta en årlig dataskyddsplan för beslut i direktionen.

Dataskyddsplanen för 2019 är den första som utarbetas i banken. Aktiviteterna i planen är adresserade till såväl dataskyddsombudet som till olika avdelningar i banken. Även om fler aktiviteter behöver genomföras under året har aktiviteterna i planen bedömts som de mest angelägna att genomföra under 2019.

Övergripande gäller att riskarbetet i Riksbanken följer modellen med tre försvarslinjer (även benämnda ansvarslinjer). Dataskyddsombudet hör till andra försvarslinjen enligt dataskyddsförordningens bestämmelser och instruktionen för Riksbanken. I Riksbanken är den första försvarslinjens ägarskap för frågor om dataskydd ännu inte tillräckligt medvetandegjord i organisationen. En konsekvens av detta kan vara att risker som relaterar till dataskydd eventuellt inte identifieras och lämpliga åtgärder för att hantera riskerna inte genomförs. Detta leder till otydlighet i Riksbanken vilket behöver avhjälpas genom ett medvetandegörande av ansvaret för dataskyddsfrågor i första försvarslinjen. Det krävs resurser för att utveckla verksamheten och frågan om resurstillgång behöver ingå i översynen.

1. Övergripande aktiviteter

1.1 Riskanalyser

Dataskyddsombudet ska delta i de självutvärderingar som verksamheten varje år genomför med stöd av riskenheten samt delta i arbetet med vidareutveckling av arbetet med riskanalyser avseende personuppgiftsbehandlingen i Riksbanken.

1.2 Planering och rapportering

En regelbunden tertialrapportering görs av dataskyddsombudet till direktionen vilken är inkluderad i riskenhetens tertialrapporter.

Dataskyddsombudet sammanställer årligen en separat årsrapport som presenteras i början av varje kalenderår för direktionen.

Dataskyddsombudet tar fram ett förslag till årsplan för arbetet för kommande år. Förslaget stäms av med relevanta delar av verksamheten och presenteras för ledningsgrupp, direktion och beslutas av direktionen före årsskiftet.

1.3 Hantering av registerförteckningen

Samtliga avdelningar behöver årligen uppmanas att se över sina uppgifter om personuppgiftsbehandlingar och vid behov revidera dessa. DSO ansvarar för att påminna om behov av översyn och revidering samt att kontrollera vilka eventuella ändringar som görs av verksamheten

1.4 Utbildning

Utbildning i dataskyddsförordningens bestämmelser har hållits för över 90 procent av personalen i Riksbanken. Samtidigt nyanställs personal och behovet av att fylla på kunskap finns ständigt. Det finns därför skäl att genomföra vissa kortare utbildningar för personal i banken. DSO ansvarar för att denna utbildning genomförs.

2. Särskilda aktiviteter för 2019

Nedan redovisas de iakttagelser inom området dataskydd som DSO bedömer behöver åtgärdas. Vissa av iakttagelserna har redovisats i riskrapporten för T2 2018. Det är första försvarslinjen som har det huvudsakliga ansvaret för att åtgärda iakttagelserna och dokumentera arbetet, men DSO ger råd och vägledning åt riskägarna i de särskilda aktiviteter som redogörs för nedan.

2.1 Ostrukturerat material

Iakttagelse: När dataskyddsförordningen började tillämpas försvann den så kallade missbruksregeln som innebar enklare regler för personuppgifter i ostrukturerat material. Det innebär att samma regler nu gäller för alla personuppgifter som behandlas, även vad avser personuppgifter i ostrukturerat material som t.ex. e-post, löpande texter eller på webbplatser. I samband med ikraftträdandet av dataskyddsförordningen vidtog Riksbanken ett antal åtgärder som inkluderade information om hantering av ostrukturerat material, bl.a. genom information på Banconätet om hantering av personuppgifter, utbildningar av medarbetare samt framtagande av en rutinbeskrivning för e-postanvändning. Riksbanken efterlever dock inte reglerna fullt ut. En inventering av personuppgifterna i allt ostrukturerat material behöver därför genomföras och det behöver tas ställning till om Riksbanken har rättslig grund för personuppgifts-behandlingen. Därtill behöver rutiner för hanteringen av personuppgifter i ostrukturerad data utarbetas. En del av detta arbete handlar om att undersöka möjligheterna att införskaffa ett verktyg för att göra sökningar i ostrukturerat material. Om någon begär ett registerutdrag från banken måste det vara möjligt att få fram personuppgifter i bankens ostrukturerade material.

Åtgärd: STA bör samordna arbetet med att bl.a. inventera personuppgiftsbehandling i ostrukturerat material och att analysera vilka ytterligare åtgärder som krävs av Riksbanken för att uppfylla kraven i dataskyddsförordningen avseende ostrukturerat material.

2.2 Integritet som standard

Iakttagelse: Samtliga bankens it-system och it-miljöer behöver genomlysas för att kontrollera om dessa uppfyller kraven på inbyggt dataskydd och integritet som standard, vilket betyder att systemen ska vara utformade på ett sådant sätt att de erbjuder ett arbetssätt som utgår från de grundläggande principerna i dataskyddsförordningen.

Åtgärd: AVS/IT behöver inventera it-systemen och it-miljön med syfte att ta ställning till vilka eventuella åtgärder som behöver vidtas för att trygga regelefterlevnaden. Om arbetet bedöms mycket omfattande behöver strategier tas fram för när förändringar kan genomföras.

2.3 Data inom forsknings- och analysverksamhet

Iakttagelse: I Riksbanken förekommer forsknings- och analysverksamhet som innefattar personuppgiftsbehandling. Implementeringen av dataskyddsförordningen i banken och planerade nya insamlingar av personuppgifter för forskning (RUSH-projektet) är bägge anledningar till att utreda och dokumentera de rättsliga förutsättningarna för behandlingen av personuppgifter, detta för att banken ska kunna förvissa sig om de lagar och regler som finns inom detta område efterlevs.

Åtgärd: De berörda avdelningarna, AFS och APP, behöver utreda de rättsliga frågorna med syfte att ta ställning till vilka eventuella åtgärder som behöver vidtas för att trygga regelefterlevnaden.

2.4 Säkerhetsskydd och övervakning

Iakttagelse: Riksbankens säkerhetsskydd är utformat utifrån den risk- och hotbild som har bedömts finnas utifrån bankens uppgifter. Övervakning och säkerhetsskydd måste alltid vägas mot integritetsaspekter. Särskilt tydligt blir detta vid t.ex. kameraövervakning och användning av biometriska personuppgifter (fingeravtryck) vid in- och utpassering i bankens lokaler.

Åtgärd: Säkerhetsfunktionen behöver utreda om det befintliga säkerhetsskyddet och övervakningen är förenliga med dataskyddsförordningens bestämmelser. Vidare behöver säkerhetsfunktionen utreda de rättsliga förutsättningarna för att använda fingeravtryck vid all in- och utpassering eftersom dessa är känsliga personuppgifter.

2.5 Upphandling

Iakttagelse: Hos Riksbanken finns totalt nio personuppgiftsbiträdesavtal diarieförda. Ett sådant avtal används när en leverantör självständigt behandlar personuppgifter på den personuppgiftsansvariges vägnar. Sannolikt borde fler personuppgiftsbiträdesavtal finnas. Detta innebär att Riksbanken behöver se över personuppgiftsbehandlingen hos personuppgiftsbiträdena.

Åtgärd: Under 2019 behöver de olika avdelningarna i banken inventera vilka personuppgiftsbiträdesavtal som finns och om dessa behöver anpassas till dataskyddsförordningen. Ägarskapet för denna personuppgiftsbehandling behöver tydliggöras i banken och tills vidare bör upphandlingsfunktionen samordna arbetet. Det behöver också sättas rutiner för användningen av personuppgiftsbiträdesavtal samt vilka krav som ska ställas för att Riksbankens hantering ska följa dataskyddsförordningens

krav. Frågan om avtalsägares uppföljning och revision av personuppgiftsbiträdesavtalen behöver ingå i arbetet.

2.6 Informationshanteringsplan

Iakttagelse: Riksbanken saknar en informationshanteringsplan vilket innebär att det inte finns en samlad bild av bankens informationstillgångar. En följd av detta är att det inte går att veta om all personuppgiftsbehandling finns förtecknad.

En informationshanteringsplan syftar även till att ta ställning i frågor om behörighet och åtkomst till informationsmängder. Dessa krav har nära samband med kraven på Riksbanken som personuppgiftsansvarig att föra ett register över behandling av personuppgifter och att ta ställning till vilka som ska ta befattning med person-uppgifterna för att kunna utföra sina arbetsuppgifter.

Åtgärd: Bankens chief data officer bör leda arbetet med att ta fram en sådan plan.

2.7 Extern kommunikation

Iakttagelse: Till skillnad mot många andra myndigheter saknar Riksbanken ett rättsligt krav på att informera allmänheten övergripande om sin verksamhet på till exempel webbplatsen. Vanligen är detta oproblematiskt men när det gäller personuppgifts-behandling på t.ex. webbplatsen uppstår utmaningar i att rättsligt sett motivera behandling av personuppgifter.

Iakttagelse: STA/KOM bör utreda frågan för att se om det kan finnas begränsningar ifråga om vilken personuppgiftsbehandling som kan ske på Riksbankens webbplats. Frågan om en hemställan om lagändring av riksbankslagen bör ingå i denna utredning.

2.8 Styrdokument

Iakttagelse: En grundläggande princip i dataskyddsförordningen är den s.k. ansvarsskyldigheten. Syftet med ansvarsskyldigheten är inte enbart att bedöma fullgörandet av de lagstadgade kraven. Ett ytterligare syfte är att visa hur den personuppgiftsansvarige respekterar de registrerades dataskydd, det vill säga skyddet för de personer som är föremål för behandling av personuppgifter. Fullgörande av ansvarsskyldigheten ökar förtroendet för den personuppgiftsansvariges verksamhet. I samband med att dataskyddsförordningen implementerades i Riksbanken utarbetades en integritetspolicy och en regel för behandling av personuppgifter. Dessa styrande dokument behöver utvecklas så att det framgår hur Riksbanken integrerar frågor om dataskydd i sitt konkreta arbete och hur lagenlighet och korrekthet iakttas i verksamheten. Utöver att vara ett centralt stöd i arbetet behövs sådana riktlinjer för fullgörandet av principen om ansvarsskyldighet. Riskåtgärderna bör inkludera bl.a. policyer, regler och kontroller inom de operativa processerna. I riktlinjerna bör ställningstaganden göras till ledning för arbetet och ifråga om bankens risktolerans i avseende dataskydd. Andra styrdokument kan samtidigt behövas ses över för att säkra en enhetlighet.

Åtgärd: STA integrerat med Riksbankens ledningsgrupp bör utarbeta riktlinjer för personuppgiftsbehandlingen i Riksbanken.