Protokollsbilaga A
Direktionens protokoll 2025-02-05, § 6

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 2025-00218

DATUM:	2025-02-05
AVDELNING:	Riskavdelningen
HANDLÄGGARE:	Dataskyddsombud, Anne Ronkainen
HANDLÄGGARE:	ÖPPEN

Dataskyddsombudets årsrapport 2024

Innehåll

1 Inledning

I denna årsrapport redogörs för dataskyddsarbetet inom Riksbanken under kalenderåret 2024. Rapporten redogör kortfattat för året som har gått, olika rapporteringsområden, genomförda granskningar samt identifierade risker inom dataskyddsområdet och slutligen ett avsnitt om övriga aktuella frågor.

2 Sammanfattning

Det finns fortfarande behov av att förstärka mognadsgraden för dataskydd och därför är det viktigt att kontinuerlig utbildning och riktade utbildningsinsatser sker samt att vägledning i form av mallar och styrdokument löpande ses över. För att säkerställa att fokus läggs på rätt åtgärder är det prioriterat att arbeta med åtgärdsplanen[1] men också att löpande utvärdera om åtgärderna omhändertar de risker som riskanalysen observerat. I början av året arbetade verksamheten fokuserat med åtgärdsplanen men under T2 och T3 har arbetet försenats. Arbete med åtgärdsplanen i början av året i kombination med framtagande av stöddokument och utbildningsinsatser resulterade även i att risken sänktes från medelhög till medel under T1. Arbetet med åtgärdsplanen bör prioriteras annars finns det risk för att dataskyddsrisken åter kommer att öka.

En förutsättning för medarbetarna att kunna arbeta med dataskyddsfrågor är att det finns aktuella och relevanta stöddokument. Dataskyddsombudet rekommenderar därför att en inventering sker under T1 2025 av vilka stöddokument som finns och en plan tas fram för när de ska ses över. För att tidigt adressera dataskyddsfrågor rekommenderar dataskyddsombudet även att det sker en översyn av stöddokument som i första hand avser it och säkerhet för att identifiera gemensamma processer**.**

Dataskyddsombudets ser även ett behov av riktade utbildningsinsatser om konsekvensbedömningar samt kontinuerlig utbildning avseende de registrerades rättigheter. Dataskyddsombudet rekommenderar att rutiner och processer avseende registrerades rättigheter utvärderas kontinuerlig på årsbasis. En översiktlig kontroll och sammanställning av registerförteckningen bör också ske på årsbasis och dataskyddsombudet rekommenderar att avdelningarna årligen avsätter tid för detta.

Dataskyddsombudets ser vidare ett behov av kontinuerlig utbildning om personuppgiftsincidenter samt att stabsavdelningen tar fram en särskild rutin eller regel för personuppgiftsincidenter**.**

En förutsättning för att kunna arbeta strukturerat med dataskydd på Riksbanken och minska risker förknippade med dataskydd är att frågor stäms av och bereds i ordnad form. I detta avseende finns det en tydlig förbättringspotential. Dataskyddsombudet rekommenderar därför att stabsavdelningen tillsammans med dataskyddsombudet ta fram processer som säkerställer att frågor om dataskydd, bereds och stäms av i god tid dels med dataskyddsombudet men även med andra stödfunktioner.

[1] En åtgärdsplan togs fram i slutet av 2023 för att hantera de risker som identifierats i samband med uppdaterad riskanalys avseende dataskydd.

3 Tillämplig dataskyddslagstiftning

3.1 Regler för behandling av personuppgifter

Det är främst EU:s dataskyddsförordning (EU 2016/679), nedan kallad dataskyddsförordningen eller GDPR, samt den kompletterande nationella dataskyddslagen (2018:218) och tillhörande förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning som reglerar den personuppgiftsbehandling som sker i Riksbankens verksamhet. Det finns också ytterligare reglering (EU-reglering, nationell lag och förordning samt bindande föreskrifter och beslut) om behandling av personuppgifter och dataskydd som tillsammans utgör tillämplig dataskyddslagstiftning för Riksbankens del.

Dataskyddsförordningen är subsidiär, vilket innebär att eventuell speciallagstiftning gäller framför förordningens bestämmelser, däribland förvaltningsrättsliga krav på arkivering och utlämnande av allmänna handlingar som innehåller personuppgifter med stö,d av offentlighetsprincipen.

Dataskyddslagstiftningen tar dels sikte på att reglera den personuppgiftsansvariges, dvs. Riksbankens, ansvar och skyldigheter för den behandling som sker i verksamheten, dels syftar reglerna till att ge den registrerade kontroll över hur dennes personuppgifter behandlas. Denna kontroll kan bl.a. utövas genom ett antal lagstadgade rättigheter. Riksbanken är ansvarig för och måste se till att all behandling av personuppgifter sker i enlighet med tillämplig dataskyddslagstiftning och särskilt dataskyddsförordningens grundläggande principer. Enligt principen om ansvarsskyldighet måste Riksbanken kunna visa att de grundläggande principerna efterlevs (enligt artikel 5 GDPR).

3.2 Krav på dataskyddsombud och dess uppgifter

Enligt artikel 37.1 a) GDPR är Riksbanken, i egenskap av myndighet, skyldig att utnämna ett dataskyddsombud. Dataskyddsombudets ställning och uppgifter är särskilt reglerade i dataskyddsförordningen. De övergripande och viktigaste uppgifterna för dataskyddsombudet är att informera och ge råd samt stödja verksamheten i sitt dataskyddsarbete, oberoende övervaka att verksamheten efterlever tillämplig dataskyddslagstiftning samt att samarbeta med Integritetsskyddsmyndigheten (”IMY”). Dataskyddsombudet är även kontaktperson för såväl IMY som registrerade, det vill säga samtliga enskilda individer (interna och externa) vars personuppgifter behandlas av Riksbanken.

Dataskyddsombudet ska vid utförande av sina uppgifter, särskilt vad gäller granskning, arbeta riskbaserat. Vidare ska dataskyddsombudet rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå, vilket inom Riksbanken är direktionen. Detta görs för närvarande huvudsakligen genom Riskavdelningens tertialrapportering och därutöver vid behov. Denna årsrapport är avsedd att komplettera befintlig rapportering för att ge direktionen och Riksbankens ledningsgrupp en ökad medvetenhet och bredare insyn i det dataskyddsarbete som bedrivs inom Riksbanken.

4 Året som gått

Dataskyddsombudet har sedan 2021 rapporterat en risk för att Riksbanken inte uppfyller dataskyddsförordningen på grund av brister i skyddet för behandlade personuppgifter[2]. Under 2023 och i början av år 2024 skedde ett aktivt arbete med den åtgärdsplan som togs fram i samband med dataskyddsombudets riskanalys och som uppdaterades i slutet av 2023. Bland annat har stöddokument (mallar och styrande dokument) uppdaterats och riktade utbildningsinsatser genomförts för verksamheten. I det löpande arbetet med åtgärdsplanen ingår även att utvärdera om föreslagna åtgärderna faktiskt minskar de risker som identifierats eller om andra åtgärder bör tas fram. Arbetet med åtgärdsplanen saktade in under våren 2024 och har under hösten skett i mycket låg takt då det är få resurser i verksamheten som arbetar aktivt med åtgärdsplanen.

Det finns fortfarande behov av att förstärka mognadsgraden därför är det viktigt med återkommande och riktade utbildningar samt att vägledning i form av mallar och styrdokument löpande ses över för att säkerställa att medarbetare får relevant stöd. Det tar också tid att implementera rutiner och nya arbetssätt. **För att säkerställa att fokus läggs på rätt åtgärder är det viktigt att löpande arbeta med åtgärdsplanen men också att utvärdera om åtgärderna omhändertar de risker som riskanalysen observerat.**

5 Rapporteringsområden

5.1 Registerförteckning

Registerförteckningen är dataskyddsarbetets centrala utgångspunkt och den säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

Med en korrekt och uppdaterad registerförteckning skapas en god överblick av de behandlingar som sker. Med stöd av registerförteckningen kan verksamheten arbeta mer effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet.

Varje avdelning har en registerförteckning över aktuella personuppgiftsbehandlingar och ansvarar för att den hålls uppdaterad. Av den uppdaterade regeln om dataskydd framgår att en översiktlig kontroll och sammanställning av avdelningarnas registerförteckning ska ske på årsbasis**. För att säkerställa att det sker en översiktlig kontroll och sammanställning på årsbasis rekommenderar dataskyddsombudet att avdelningarna årligen avsätter tid för detta.** Som framgår av kapitel 6 har en granskning av registerförteckningen skett av laglig grund för personuppgiftsbehandling och granskningen avslutades utan synpunkter.

5.2 Stöddokument

För att Riksbanken ska kunna visa att den bedriver ett systematiskt dataskyddsarbete krävs det att det finns relevanta stöddokument på plats som styr och vägleder medarbetares hantering av personuppgifter, framförallt för att klargöra vad som

[2] Se Riskrapport T3 2023 samt kapitel 7 ”Risker inom dataskydd” i denna rapport.

förväntas av medarbetarna när de hanterar personuppgifter. Avsaknad av eller bristande stöddokument kan leda till bristfällig hantering och omedvetet risktagande.

Under året har vissa mallar och stöddokument uppdaterats. Det är mycket viktigt att medarbetare får aktuell och relevant stöd i sitt dataskyddsarbete. **Dataskyddsombudet rekommenderar därför att en inventering sker under T1 2025 av vilka stöddokument som finns och en plan tas fram för när dessa ska ses över.**

Såsom rapporterades i förra årsrapporten finns det många stöddokument i form av mallar och rutiner på Riksbanken och det kan vara svårt för medarbetare att hitta rätt. Flera av stöddokumenten har gemensamma beröringspunkter med dataskydd, framförallt informationssäkerhet och it. Det finns stora fördelar med ett ökat samarbete vid översyn av dessa stöddokument. Framförallt för att utvärdera om det är möjligt att använda befintliga processer[3] för att tidigt adressera dataskyddsfrågor. Om dataskyddsfrågor identifieras tidigt är det också enklare att hantera eventuella risker med personuppgiftsbehandlingarna. **Dataskyddsombudet rekommenderar därför att AC AID och Säkerhetschefen gör en översyn av sina respektive stöddokument för att identifiera gemensamma processer för att tidigt adressera dataskyddsfrågor.**

5.3 Konsekvensbedömningar

Konsekvensbedömningen är liksom registerförteckning ett viktigt verktyg för verksamhetens dataskyddsarbete. En konsekvensbedömning har till syfte att identifiera, bedöma, mitigera och dokumentera risker kopplade till en viss behandling. Arbetet hjälper en organisation att identifiera och minimera integritetsriskerna för de registrerade som berörs av behandlingen.

Enligt dataskyddsförordningen ska konsekvensbedömningar utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). IMY har också på sin webbplats publicerat en förtydligande förteckning över när personuppgiftsbehandlingar kräver en konsekvensbedömning.

Eftersom det i vissa fall är ett krav enligt dataskyddsförordningen att göra konsekvensbedömningar är det viktigt att verksamheten har kunskap om när och hur en konsekvensbedömning ska ske. Konsekvensbedömningar är också ett verktyg för verksamheten att identifiera och minimera riskerna med en personuppgiftsbehandling innan behandlingen påbörjas. Riksbanken har tagit fram stödmaterial för när och hur konsekvensbedömningar ska ske. Utbildningsinsatser om konsekvensbedömningar har ägt rum under året. Även mallen för konsekvensbedömningar har genomgått en översyn och är numera uppdelat i två[4] olika dokument. **Även om det finns stödmaterial bedömer dataskyddsombudet att kunskapen om när konsekvensbedömningar ska ske är låg**, bland annat mot bakgrunden av antalet konsekvensbedömningar som genomförts fortfarande är låg. **DSO kommer därför att genomföra riktade**

[3] Dataskyddsombudet har under året identifierat en sådan process – informationsklassningen - där dataskyddsfrågor kan identifieras tidigt och omhändertas.
[4]Numera finns ett dokument med titeln ”Riskbedömning personuppgiftsbehandling tröskelanalys avseende dataskydd del I” som är ett verktyg för ta reda på om man behöver göra en konsekvensbedömning samt ett dokument som är mall för när det konstateras att en konsekvensbedömning ska ske ”Riskbedömning personuppgiftsbehandling del II”.

utbildningsinsatser även kommande år med fokus på avdelningar som behandlar stora mängder personuppgifter eller känsliga/integritetskänsliga personuppgifter.

5.4 Hantering av registrerades rättigheter

Enligt dataskyddsförordningen (artikel 12–22) har de registrerade ett antal rättigheter som på olika sätt ska garantera bl.a. insyn i hur dennes personuppgifter hanteras. Rättigheterna innebär skyldigheter för den personuppgiftsansvarige att vidta vissa åtgärder, som exempelvis att ge en registrerad tillgång till sina personuppgifter samt information om behandlingen genom ett s.k. registerutdrag eller att rätta vissa uppgifter. Enligt dataskyddsförordningen artikel 12.3 har Riksbanken en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran, i vissa fall kan dock fristen kan förlängas till mer än en månad.

I Riksbankens verksamhet förekommer framförallt begäran om registerutdrag samt begäran om att bli raderad. Antalet begäranden är relativt låg på årsbasis. Det gäller även för 2024. Under året har det endast inkommit en begäran om registerutdrag till Riksbanken.

Under året har det inkommit flertalet frågor från allmänheten om radering av personuppgifter. Frågorna har primärt avsett radering av personuppgifter i rekryteringsärenden. Hantering av dessa har framförallt skett genom att besvara frågor och upplysa om krav på bevarande snarare än att hantera ett borttagande. Detta då frågorna primärt har förekommit i sammanhang där Riksbanken är förhindrad att ta bort personuppgifterna på grund av att de förekommer i allmänna handlingar som ska bevaras enligt särskilda regler. Radering, eller den så kallade ”rätten att bli glömd”, blir sällan möjlig att efterleva för personuppgiftsansvariga som är myndigheter och ska tillämpa offentlighetsprincipen.

Även om det är få registrerade som vänder sig till Riksbanken för att utöva sina rättigheter är det viktigt att verksamheten vet hur de ska gå tillväga om en registrerad kontaktar Riksbanken för att exempelvis begära ett registerutdrag. **Dataskyddsombudet rekommenderar därför även detta år att rutiner och processer avseende registrerades rättigheter utvärderas kontinuerlig på årsbasis av stabsavdelningen. Vidare rekommenderar dataskyddsombudet att verksamheten kontinuerligt utbildas i de registrerades rättigheter**, särskilt de delar av verksamheten som arbetar nära allmänheten samt i processer som tar sikte på behandling av anställdas personuppgifter. Riktade utbildningsinsatser är därför planerade av dataskyddsombudet under våren till de delar av verksamheten som får frågor om registrerades rättigheter.

5.5 Personuppgiftsincidenter

En personuppgiftsincident är enligt dataskyddsförordningen (artikel 4.12*) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”*

Enligt gällande rutin för incidentrapportering ingår den interna rapporteringen av personuppgiftsincidenter i den process för incidentrapportering som ägs av Riskavdelningen.

Riksbanken ska enligt artikel 33 GDPR utan onödigt dröjsmål, och inte senare än 72 timmar, anmäla en personuppgiftsincident till IMY om det inte är osannolikt att personuppgiftsincidenten inneburit en risk för fysiska personers rättigheter och friheter. Det är i praktiken en låg tröskel för vilka incidenter som behöver anmälas till IMY.

Under 2024 har 25 (18 stycken 2023) personuppgiftsincidenter rapporterats till Riskavdelningen. Dataskyddsombudet har analyserat samtliga internt rapporterade personuppgiftsincidenter. En av dessa incidenter har anmälts vidare till IMY. Den avsåg en s.k. ransomware attack mot Primula, Riksbankens lönehanteringssystem. Ärendet som rapporterats till IMY har inte föranlett någon åtgärd från tillsynsmyndighetens sida.

Det samlade antalet internt rapporterade personuppgiftsincidenter är högre än föregående år. Trots detta bedöms ett visst mörkertal föreligga. Att ytterligare höja medvetenheten om risker som kan inträffa vid personuppgiftsbehandling är en viktig del i arbetet att minska mörkertalet och att förbättra styrning och kontroll.

Utbildning bör ske kontinuerligt till samtliga anställda för att säkerställa att personal har relevant kunskap om vad som ska rapporteras och när. Utbildningsinsatser är därför planerade under våren 2025 av dataskyddsombudet.

Det finns en rutin för incidenthanteringsprocesser på Riksbanken där olika typer av incidenter ska rapporteras. I samband med översynen av denna rutin konstaterades att särskild rutin för personuppgiftsincidenter bör tas fram för att säkerställa att personuppgiftsincidenter omhändertas i tid. **Dataskyddsombudet rekommenderar därför att stabsavdelningen tar fram en särskild rutin för personuppgiftsincidenter.**

5.6 Utbildningar

Grundutbildning för nyanställda har skett under våren 2024 i samarbete med bl.a. arkiv, registratur och informationssäkerhet. Under 2024 har särskilda utbildningsinsatser genomförts om bl.a. PUB-avtal och konsekvensbedömningar. Dessa utbildningar är riktade till framförallt avtalsägare, IT-personal, informationsägare och upphandling.

Riksbanken har under året och kommer även i början av 2025 att genomföra utbildningsinsatsen ”Riksbanken i staten” för samtliga anställda. Inom ramen för denna insats ingår även dataskydd.

6 Uppföljningar och granskningar under året

För att säkerställa att Riksbanken följer dataskyddsförordningen har dataskyddsombudet genomfört ett antal uppföljningar och granskningar.

Dataskyddsombudet har genomfört en granskning av den operativa modellen[5] för dataskydd. I granskningen har det framkommit att det framförallt är en nyckelroll, dataskyddsambassadören, som bör ses över för att modellen på ett mer ändamålsenligt sätt ska spegla det praktiska arbetet. **Dataskyddsombudet rekommenderade därför att**

[5] Riksbankens dataskyddsnätverk brukar benämna den operativa modellen och syftet med nätverket är att underlätta det operativa arbetet med dataskyddsfrågor i verksamheten, bland annat genom att skapa kontaktvägar mellan verksamheten och dataskyddsombudet, sprida kunskap samt samordna verksamhetsövergripande åtgärder och frågor som rör behandling av personuppgifter. För mer information, se Banconätet

respektive avdelning skulle utse en dataskyddsambassadör som arbetade mer operativt med behandlingar som sker i avdelningens kärnverksamhet eller hade kunskaper om vart i kärnverksamheten det förekom personuppgiftsbehandling och varför. Datasskyddsombudet rekommenderade även att stabsavdelningen som har två enheter (HR-enheten och kommunikationsenheten) som behandlar väldigt mycket personuppgifter utsåg en dataskyddsambassadör för respektive enhet och övervägde om ytterligare en dataskyddsambassadör skulle utses. HR har därefter utsett en dataskyddsambassadör. Datasskyddsombudet rekommenderade även att AIS, som har flera olika arbetsområden att utreda om fler dataskyddsambassadörer bör utses för att effektivera dataskyddsarbetet.

Även en granskning avseende ägare till informationstexter har skett och i granskningen framkom det att ägarskapet till vissa informationstexter har varit otydligt samt att det varit oklart med vad det innebär att vara ägare till en informationstext. **Dataskyddsombudet rekommenderade därför respektive avdelning att årligen inventerar vilka informationstexter de ansvarar för och se över dessa informationstexter.**

Även en granskning av Regel för säkerhetsprövning har ägt rum. I granskningen har det bl. a. framkommit att det finns **vissa skrivningar i regeln för säkerhetsprövningar som bör ses över för att tydliggöra vad säkerhetsenheten ansvarar för och vad personalansvarig chef ansvarar för**.

Dataskyddsombudet har vidare genomfört en granskning av rensning av personuppgifter. I granskningen har det framkommit att det saknas styrdokument för när och hur personuppgifter ska rensas. **För att underlätta arbetet med rensning och för att säkerställa att Riksbanken inte sparar uppgifter länge än vad som är nödvändigt rekommenderades att sådana styrdokument tas fram av stabsavdelningen**.

Slutligen har en granskning av registerförteckningen skett av laglig grund för personuppgiftsbehandling och granskningen avslutades utan synpunkter.

En granskningsplan har tagits fram för 2025 som kommer att presenteras för ledningsgruppen. Arbetet med granskningarna sker löpande under året och finns också inplanerade i dataskyddsombudets årshjul.

7 Risker inom dataskydd

Dataskyddsombudet och dataskyddsspecialisten hade under slutet av 2023 genomfört en riskanalys för att få en uppdaterad riskbild av dataskyddsriskerna samt för att säkerställa att rätt åtgärder prioriterades. Baserat på riskanalysen som skedde under 2023 har verksamheten tagit fram en åtgärdsplan för att följa upp och hantera identifierade risker. Arbete med åtgärdsplanen i kombination med framtagande av stöddokument och utbildningsinsatser resulterade även till att risken sänktes från medelhög till medel under T1. Under T2 och T3 har arbetet med åtgärdsplanen dock försenats. Om arbetet med åtgärdsplanen inte prioriteras finns det risk för att dataskyddsrisken återigen kommer att öka. I arbetet med åtgärdsplanen ingår även att utvärdera om åtgärderna omhändertar de risker som identifierats eller om andra åtgärder bör tas fram.

En förutsättning för att kunna arbeta strukturerat med dataskydd samt minska riskerna är att det finns en tydlig styrning för hur frågor stäms av och bereds. Även processer som tidigt identifierar dataskyddsfrågor bör finnas på plats och det är viktigt att samarbete sker mellan olika avdelningar. I Riksbankens portföljsverktyg finns det delvis en funktion som initiativ kan använda för flagga för att personuppgifter kan förekomma. Men det är oklart på vilket sätt detta innebär att dataskyddsfrågor kommer att omhändertas. Ett nära samarbete mellan avdelningarna och stödfunktioner är också viktigt för att säkerställa att även andra aspekter som har kopplingar till dataskydd omhändertas, ex it-säkerhet, informationssäkerhet, förvaltningsrätt m.m. Dataskyddsombudet har redan i föregående års dataskyddsrapport konstaterat att det pågår flera större projekt inom Riksbanken som aktualiserar dataskyddsfrågor. Och det är därför viktigt att verksamheten tidigt i processen stämmer av och informerar dataskyddsombudet om frågor av dataskyddsrättslig karaktär, för att säkerställa att frågorna blir omhändertagna i tid. **Dataskyddsombudet rekommenderar därför stabsavdelningen att se över och tillsammans med dataskyddsombudet ta fram processer som säkerställer att frågor om dataskydd, bereds och stäms av i god tid dels med dataskyddsombudet men även med andra stödfunktioner.**

8 Övrigt att rapportera

Teknikutvecklingen går fort framåt och särskilt användningen av AI är mycket viktig att följa. Frågor av dataskyddsrättslig karaktär uppstår ofta vid AI relaterade frågor. Mot bakgrund av den snabba utvecklingen av AI blir det därför **särskilt viktigt att i god tid bereda och informera dataskyddsombudet i frågor som har dataskyddsrättslig koppling**. Det är också viktigt med ett nära samarbete med dataskydd, informationssäkerhet och IT då det finns många gemensamma beröringspunkter.