Protokollsbilaga C
Direktionens protokoll 2026-01-09, § 5

DATUM: 2026-01-09
AVDELNING: Riskavdelningen
HANDLÄGGARE: Dataskyddsombud, Anne Ronkainen
HANDLÄGGARE: ÖPPEN

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 2026-00055

Dataskyddsombudets årsrapport 2025

Innehåll

1 Inledning

I denna årsrapport redogörs för dataskyddsarbetet inom Riksbanken under kalenderåret 2025. Rapporten redogör kortfattat för olika rapporteringsområden[1], genomförda uppföljningar och granskningar samt identifierade risker inom dataskyddsområdet och slutligen ett avsnitt om övriga aktuella frågor.

Årsrapporten är avsedd att ge direktionen och Riksbankens ledningsgrupp en ökad medvetenhet och bredare insyn i det dataskyddsarbete som bedrivs inom Riksbanken.

1.2 Personuppgiftsbehandlingar på Riksbanken

När Riksbanken behandlar personuppgifter i sin verksamhet ska det ske i enlighet med dataskyddsförordningens krav. Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften kan knytas till en levande person. Personuppgiftsbegreppet är alltså väldigt brett vilket innebär att det är väldigt många uppgifter som kan kopplas till och är personuppgifter. Beroende på vilken typ av personuppgifter det handlar om finns det olika faktorer att ta hänsyn till. Det ställs exempelvis högre krav på behandling av känsliga personuppgifter och integritetskänsliga personuppgifter.

Allting som någon gör med en personuppgift är en personuppgiftsbehandling och det innebär att sker väldigt mycket personuppgiftsbehandlingar på Riksbanken utan att vi tänker på det. För anställa behandlas exempelvis personuppgifter vid in/ut passering, när någon loggar in på datorn och under tiden vi jobbar med datorn. Även behandling av känsliga och integritetskänsliga personuppgifter förekommer vid exempelvis anmälan av finansiella instrument, sjukanmälan och säkerhetsprövningar. Personuppgifter behandlas även inom andra delar av Riksbanken exempelvis vid analysarbete och forskning samt vid avveckling m.m. Det sker alltså en mängd behandlingar av personuppgifter på Riksbanken inklusive behandling av känsliga och integritetskänsliga personuppgifter.

2 Sammanfattning av året som gått

Dataskyddsombudet har sedan 2021 rapporterat om risken för att Riksbanken inte uppfyller dataskyddsförordningen på grund av brister i skyddet för behandlade personuppgifter. Under 2023 och i början av år 2024 pågick ett aktivt arbete med den åtgärdsplan som togs fram i samband med dataskyddsombudets riskanalys. Arbetet har under 2025 skett i mycket låg takt då det är få resurser i verksamheten som arbetar aktivt med åtgärdsplanen. Utan framdrift med aktiviteterna i åtgärdsplanen så kvarstår identifierade brister i Riksbankens dataskyddsarbete och därmed även risken för att Riksbanken inte uppfyller dataskyddsförordningen.

Det finns fortfarande behov av att förstärka mognadsgraden inom Riksbankens dataskyddsarbete och därför är det viktigt med återkommande och riktade utbildningar samt att vägledning i form av mallar och styrdokument löpande ses över för att

[1] Områden som dataskyddsombudet bedömt lämpliga att rapportera om ur ett integritetsperspektiv är registerförteckningen, styrande och andra stöddokument, konsekvensbedömningar, hantering av registrerades rättigheter, personuppgiftsincidenter och utbildningar.

säkerställa att medarbetare får relevant stöd. En förutsättning för att kunna arbeta strukturerat med dataskydd samt minska riskerna är också att det finns en tydlig styrning för hur frågor stäms av och bereds. Det är även viktigt med ett nära samarbete mellan områdena dataskydd, informationssäkerhet och IT då det finns många gemensamma beröringspunkter. Exempelvis är det en förutsättning för en integritetsvänlig utveckling av AI att olika kompetenser deltar i arbetet, vilket kräver ett fungerande tvärfunktionellt samarbete.

3 Tillämplig dataskyddslagstiftning

3.1 Aktuell lagstiftning 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 stöd 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 och ska 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.

4 Rapporteringsområden

4.1 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. Dataskyddsombudet noterar att det finns flera behandlingar som finns upptagna flera gånger av olika avdelningar. Många behandlingar är gemensamma för samtliga avdelningar s.k. bankgemensamma behandlingar. **Dataskyddsombudet rekommenderar** att det sker en översyn av registerförteckningen och att bankgemensamma behandlingar registreras separat med en ansvarig avdelning per behandling.

4.2 Styrande och andra stöddokument

För att Riksbanken ska kunna visa att det bedrivs ett systematiskt dataskyddsarbete krävs det att det finns relevanta stöddokument på plats som styr och vägleder medarbetares hantering av personuppgifter, framför allt för att klargöra vad som förväntas av medarbetarna när de hanterar personuppgifter. Avsaknad av eller bristande stöddokument kan leda till bristfällig hantering och omedvetet risktagande. Under året har STA arbetat med att uppdatera mallar och stöddokument även om det har skett i låg takt.

Såsom har rapporterats i tidigare årsrapporter (2024 och 2025) har flera stöddokument 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 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 CISO gör en översyn av sina respektive stöddokument för att identifiera gemensamma processer för att tidigt adressera dataskyddsfrågor samt återkoppla resultatet till dataskyddsombudet. Det är viktigt att arbetet prioriteras.

4.3 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). Exempelvis på behandlingar som innebär höga risker för de registrerade är behandling av personuppgifter som sker inom säkerhetsprövningar, visselblåsningar, lönesystem, rekryteringssystem m.m.

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[2] för när och hur konsekvensbedömningar ska ske. Utbildningsinsatser om konsekvensbedömningar har ägt rum under året. Även mallen för konsekvensbedömningar har genomgått en översyn. 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. Det är viktigt att vara uppmärksam på att det exempelvis kan behövas en konsekvensbedömning för AI-funktioner som tillförs ett befintligt system.

4.4 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 2025.

De vanligaste frågorna från allmänheten 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

[2]Det 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”.

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.

4.5 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 efter att fått vetskap, 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. En incident har anmälts till IMY 2025[3] och det avser en felaktig registerkontroll. Riksbanken hade skickat en felaktig personuppgift vidare till Säkerhetspolisen. Incident inträffade då den person som skulle säkerhetsprövas hade uppgivit sitt personnummer fel i blanketten ”Ansökan om registerkontroll” vilket fick till följd att annan person felaktigt utretts och placerats säkerhetsklass av Säkerhetspolisen.

Även om det rapporteras in incidenter 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 sker kontinuerligt till samtliga anställda för att säkerställa att personal har relevant kunskap om vad som ska rapporteras och när.

Det finns en rutinbeskrivning för incidentrapportering på Riksbanken där olika typer av incidenter ska rapporteras. I samband med översynen av denna rutin konstaterades att en 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.

4.6 Utbildningar

Under 2025 har utbildningsinsatser genomförts inom bl.a. personuppgiftsincidenter, GDPR och AI samt konsekvensbedömningar. Även en fördjupad dataskyddsutbildning har genomförts enligt önskemål från RÄT. Riksbanken har under året också genomfört initiativet ”Riksbanken i staten” som bland annat innehöll dataskyddsutbildningar riktade till samtliga medarbetare och nyanställda.

[3] Se ärende dnr 2025-01554.

5 Uppföljningar och granskningar under året

För att utvärdera att Riksbanken följer dataskyddsförordningen har dataskyddsombudet genomfört ett antal uppföljningar och en granskning.

Dataskyddsombudet har följt upp i vilken utsträckning verksamheten genomför konsekvensbedömningar och tröskelanalyser. Uppföljningen fokuserade på s.k. högriskbehandlingar som sker relaterat till säkerhetsprövningar (AIS/SÄK), rekrytering (HR), visselblåsning (RIA) och delegering av brevlådor under semester (RÄT). DSO konstaterade att det saknades slutförda konsekvensbedömningar på samtliga områden. Konsekvensbedömningar avseende rekrytering och säkerhetsprövningar färdigställdes dock efter genomförd granskning. DSO har uppmanat ansvariga för behandlingarna att färdigställa tröskel/konsekvensbedömning för att analysera vilka risker detta kan innebär för de registrerade.

Vidare har en granskning av Regel för säkerhetsprövning ägt rum avseende raderingstiden. Regel för säkerhetsprövningar har uppdaterats och numera sparas färre personuppgifter och tiden för hur länge minnesanteckningar sparas har minskat till ett år. Eftersom radering är en mycket effektiv integritetsfrämjande åtgärd är det viktigt att regelbundet analysera när uppgifterna inte längre behövs.

6 Risker inom dataskydd

Dataskyddsombudet har sedan 2021 rapporterat om risken för att Riksbanken inte uppfyller dataskyddsförordningen på grund av brister i skyddet för behandlade personuppgifter[4].

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. Ett nära samarbete mellan avdelningarna och stödfunktioner är också väsentligt för att säkerställa att även andra aspekter som har kopplingar till dataskydd omhändertas, ex it-säkerhet, informationssäkerhet, förvaltningsrätt m.m. Dataskyddsombudet har redan i tidigare dataskyddsrapporter påpekat att det är 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. I den uppdaterade policyn för dataskydd har det bland annat tydliggjorts att dataskyddsombudet ska involveras i god tid vid frågor som rör dataskydd.

Dataskyddsombudet rekommenderar stabsavdelningen att under T2 2026 utvärdera effekten av vidtagna och pågående åtgärder, bland annat avseende arbetet med styrande dokument och de processförändringar som ämnar förtydliga när och hur dataskyddsombudet ska involveras i och/eller informeras om olika initiativ. Syftet är att bedöma om åtgärderna gett önskad effekt i praktiken och kunna identifiera behov av vidare arbete.

[4] Se Riskrapport T2 2025.

7 Övrigt att rapportera

Teknikutvecklingen går fort framåt och särskilt användningen av AI är mycket viktig att följa även ur ett dataskyddsperspektiv. Möjligheterna med AI är stora men det finns även risker, bland annat för den personliga integriteten. 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. En förutsättning för integritetsvänlig utveckling av AI är att olika kompetenser deltar i arbetet, vilket kräver ett fungerande tvärfunktionellt samarbete.