Protokollsbilaga C
Direktionens protokoll 2022-11-08, §4

Beslutsunderlag

DATUM: 2022-10-27
AVDELNING: Stabsavdelningen
HANDLÄGGARE: Sebastian Hall, Dataskyddsombud
HANTERINGSKLASS Ö P P E N

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 2022-01177

Beslutsunderlag – uppdaterad Policy för dataskydd

Förslag till direktionens beslut

Direktionen beslutar att Riksbankens Policy för dataskydd ska uppdateras och att den nya policyn träder i kraft samma dag. Genom detta beslut upphävs tidigare Policy för dataskydd (dnr 2020-01009) från den 7 oktober 2020.

Sammanfattning:

Föreslagna ändringar i Riksbankens Policy för dataskydd avser såväl ändringar i sak som dess utformning, det senare med anledning av anpassning till den nya mallen för styrande dokument. Vad gäller innehållet har huvudsakligen följande ändringar gjorts. Policyn har kortats ner och fokus har lagts på hur Riksbanken ska organisera sitt arbete med dataskydd. Det fastställs i policyn att Riksbanken ska bedriva ett aktivt dataskyddsarbete och att Riksbanken ska ha ett dataskyddsnätverk som har till uppgift att stötta verksamheten med frågor om behandling av personuppgifter i det dagliga arbetet. Dataskyddsnätverkets roller och ansvar har förtydligats.

Den tidigare policyn innehåller bland annat redogörelse för dataskyddsförordningens grundläggande principer och definitioner. Detta har tagits bort eftersom det redan följer direkt av dataskyddsförordningen och inte behöver återges i interna styrande dokument. För att vägleda verksamheten gällande vilka krav som måste efterlevas och säkerställa en enhetlig hantering kan dock kravens innebörd förklaras i andra styrande dokument, lämpligen i en regel eller rutinbeskrivning.

Ärendet

Riksbankens Policy för dataskydd behöver uppdateras både i sak och vad gäller sin utformning i enlighet med den nya mallen för styrande dokument. Till följd av det senare är det svårt att tillhandahålla en uppdaterad version med ändringsmarkeringar för beslut. Därför lämnas en särskild redogörelse, nedan under avsnitt Övervägande, för de ändringar som har gjorts i respektive avsnitt med hänvisning till eventuellt tidigare referenser i den tidigare policyn samt beskrivning av vad som lagts till.

Övervägande

Riksbankens Policy för dataskydd har ändrats på det sätt som framgår nedan i respektive avsnitt.

Innehåll och syfte

Referens i tidigare policy: Rubriken hette tidigare ”Syfte och mål”.

Vad har ändrats: Såväl som vad policyn innehåller och dess syfte har konkretiserats och förkortats. Information angående regelverk och hur Riksbanken ska arbeta med dataskydd har omformulerats och flyttats enligt disposition i ny mall. I den tidigare policyn står att *målsättningen* är att Riksbanken vid behandling av personuppgifter ska följa de grundläggande principerna för dataskydd – detta har strukits då Riksbanken är skyldig att bedriva sin verksamhet enligt gällande rätt.

Målgrupp

Referens i tidigare policy: ”Målgrupp och omfattning”

Vad har ändrats: Målgrupp har begränsats till medarbetare. Motiveringen är att Riksbanken saknar möjlighet att följa upp huruvida policyn efterlevs av *”alla personer som är associerade med Riksbankens, vilket innefattar både anställda och externa parter såsom uppdragstagare, leverantörer och samarbetspartner”.* Definitionen av medarbetare har hämtats från Riksbankens Etiska regler som beslutats den 29 juni 2022. Motsvarande målgrupp, dvs. medarbetare och inte externa parter, finns t.ex. i den nuvarande informationssäkerhetspolicyn.

Skrivningen om omfattning har tagits bort då det framgår av policyn i övrigt samt i enlighet med dispositionen i den nya mallen.

Inledning

Referens i tidigare policy: Motsvarande rubrik saknas men innehållet motsvarar i stora delar det som framgått av ”Syfte och mål” samt ”Målgrupp och omfattning”.

Vad har ändrats: Inledningen innehåller information om att Riksbankens behandlar personuppgifter och att det innebär att tillämplig dataskyddslagstiftning ska efterlevas för att den ska vara tillåten. Det framgår vidare att Riksbankens ska ha ett internt dataskyddsnätverk.

Bakomliggande regelverk

Referens i tidigare policy: Motsvarande rubrik saknas men information om bakomliggande regelverk framgår av ”Syfte och mål”. En förklaring lämnas till samlingsbegreppet ”tillämplig dataskyddslagstiftning” som avser bakomliggande förordning, lag och föreskrifter som vid var tid är gällande och kan tillämpas på personuppgiftsbehandling i Riksbankens verksamhet.

Definitioner

Referens i tidigare policy: Bilaga: Definitions- och ordlista

Vad har ändrats: Samtliga begrepp och uttryck har strukits då dessa framgår direkt av dataskyddsförordningen, till vilken det lämnas en hänvisning.

Roller och ansvar

Referens i tidigare policy: Roller och ansvar

Vad har ändrats: Roller och ansvar har konkretiserats enligt följande;

- I egenskap av högsta förvaltningsorgan har direktionen det yttersta ansvaret för att personuppgifter behandlas i enlighet med tillämplig dataskyddslagstiftning.
- Riskchefens ansvar att se till att dataskyddsombudet har tillräckligt med tid och resurser har strukits. Det yttersta ansvaret för att se till att det finns resurser för dataskyddsombudets uppgifter framgår direkt av GDPR och det operativa ansvaret framgår av Riksbankens instruktion. Denna skrivning om riskchefens ansvar bör därför inte tas med i denna policy.
- Avdelningschefens ansvar har omformulerats. Det har förtydligats att avdelningscheferna ansvarar för att utse minst en dataskyddsambassadör och vid behov behandlingsansvariga på avdelningen. Vidare har det lagts till att avdelningscheferna ansvarar för att ge medarbetarna förutsättningar för att främja en god dataskyddskultur. Följden blir ett tydligare ansvar på avdelningschefen.
- Dataskyddsombudets roll har omformulerats, primärt då dess ställning och grundläggande uppgifter framgår direkt av dataskyddsförordningen. Det har förtydligats att dataskyddsombudet inte ansvarar för efterlevnaden av dataskyddsförordningen.
- En redogörelse för dataskyddssamordnarens roll och dataskyddsspecialistens uppgifter och ansvar har lagts till.
- Redogörelsen för dataskyddsambassadörernas och de behandlingsansvarigas ansvar har förkortats något. Skälet är att det i denna inte bedöms nödvändigt att uttömmande reglera i policyn vad som ingår i respektive rolls ansvar. Detta framgår av Riksbankens operativa modell för dataskydd som illustrerar Riksbankens dataskyddsnätverk.

Principer för personuppgiftsbehandling

Referens i tidigare policy: ”Grundläggande principer för behandling av personuppgifter”

Vad har ändrats: De grundläggande principerna har återges inte i policyn då detta framgår direkt av dataskyddsförordningen. Vidare har skrivningen om hantering av undantag från dataskyddsramverket som finns i den tidigare policyn tagits bort.

Riksbankens dataskyddsarbete

Avsnittet är nytt och innehåller två underrubriker:

Regelefterlevnad och en god dataskyddskultur: I detta stycke framgår att Riksbankens personuppgiftsbehandling ska följa de grundläggande principerna och specifika regler som följer av tillämplig dataskyddslagstiftning. Det framgår vidare att Riksbanken ska bedriva ett aktivt dataskyddsarbete som ska vara integrerat i den dagliga verksamheten. Detta ska leda till ökad medvetenhet om reglerna, främja regelefterlevnad samt en god dataskyddskultur. Till stöd för detta arbete ska Riksbanken ha ett dataskyddsnätverk.

Riksbankens dataskyddsnätverk: I detta stycke framgår vad syftet med dataskyddsnätverket är samt att nätverket illustreras i Riksbankens operativa modell för dataskydd, som finns att ta del av på Banconätet. Det beskrivs vilka roller som ingår i dataskyddsnätverket.

Efterlevnad

Ingen referens i tidigare policy utan ett nytt avsnitt i enlighet med den nya mallen. Avdelningschefernas ansvar att denna policy efterlevs har lyfts fram. Därtill framhålls att om policyn inte följs så kan det rapporteras till direktionen genom riskenhetens tertialrapportering samt att internrevision och dataskyddsombudet kan kontrollera efterlevnaden i samband med särskilda granskningar.

Ikraftträdande och övergångsbestämmelser

Ingen referens i tidigare policy utan ett helt nytt avsnitt i enlighet med den nya mallen. Tidigare policy upphävs genom beslut om denna policy. Några övergångsbestämmelser anses inte nödvändiga.

BESLUTSDATUM:	2022-11-08
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	Stabsavdelningen
FÖRVALTNINGSANSVARIG:	Dataskyddsombudet
DIARIENUMMER:	2022-01177
HANTERINGSKLASS:	ÖPPEN

Policy för dataskydd

Innehåll och syfte

I denna policy finns bestämmelser om hur Riksbanken ska arbeta med dataskydd.

Målgrupp

Denna policy riktar sig till Riksbankens samtliga medarbetare. Begreppet medarbetare avser alla arbetstagare och de uppdragstagare som har tillgång till en riksbanksdator och till Riksbankens system och som deltar i Riksbankens dagliga verksamhet.

Postadress: 103 37 Stockholm, **Besöksadress:** Brunkebergstorg 11
Telefon: 08-787 00 00, **Webb:** riksbank.se

Innehållsförteckning

1 Inledning

Riksbanken hanterar stora mängder information, däribland personuppgifter. För att personuppgifter ska få behandlas i Riksbankens verksamhet krävs att vi följer tillämplig dataskyddslagstiftning. För att göra det lättare att följa denna lagstiftning ska det finnas ett internt dataskyddsnätverk på Riksbanken.

1.1 Bakomliggande regelverk

EU:s allmänna dataskyddsförordning (2016/679)[1] (”**dataskyddsförordningen**” eller **GDPR**)

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (”**dataskyddslagen**”)

Dataskyddsförordningen gäller i alla EU:s och EES:s medlemsstater. I Sverige har dataskyddsförordningen kompletterats genom bland annat dataskyddslagen. Dataskyddsförordningen och dataskyddslagen samt andra vid var tid gällande svenska eller europeiska lagar, förordningar, föreskrifter eller direktiv för Riksbankens behandling av personuppgifter, benämns i den här policyn som ”tillämplig dataskyddslagstiftning”.

1.2 Definitioner

Begrepp som används i denna policy kommer från dataskyddsförordningen och ska ha samma betydelse som anges i den.

2 Roller och ansvar

Riksbanken: Direktionen är Riksbankens högsta ledande förvaltningsorgan och är ytterst ansvarig för att personuppgifter behandlas enligt tillämplig dataskyddslagstiftning.

Avdelningschefer: Avdelningscheferna ansvarar för att leda det dagliga dataskyddsarbetet på sina avdelningar samt för att säkerställa att den personuppgiftsbehandling som utförs i respektive avdelnings verksamhet följer tillämplig dataskyddslagstiftning. Det gäller även om Riksbanken har anlitat ett personuppgiftsbiträde som behandlar personuppgifter. Avdelningscheferna ansvarar för att hantera de risker som kan uppstå på respektive avdelning när personuppgifter behandlas. Avdelningscheferna ansvarar för att utse minst en dataskyddsambassadör och vid behov behandlingsansvariga på avdelningen. Dataskyddsambassadörerna ska ges tillräckligt med tid och resurser för att kunna samordna och leda

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

dataskyddsarbetet på respektive avdelning i samråd med sin avdelningschef. Avdelningscheferna ansvarar även för att medarbetarna ges förutsättningar att främja en god dataskyddskultur när de utför sina arbetsuppgifter.

Dataskyddsombudet: Riksbanken är skyldig att ha ett dataskyddsombud. Dataskyddsombudets ställning och grundläggande uppgifter framgår av dataskyddsförordningen. Dataskyddsombudet ska framför allt:

- vägleda, stötta och informera medarbetare i dataskyddsfrågor
- övervaka att verksamheten följer dataskyddsförordningen
- vara kontaktperson för den vars uppgifter behandlas av Riksbanken och som vill utöva sina rättigheter
- vara kontaktperson gentemot och samarbeta med Integritetsskyddsmyndigheten (”**IMY**”) som är tillsynsmyndighet för frågor om dataskydd.

Dataskyddsombudet ska rapportera till högsta förvaltningsnivå, det vill säga direktionen genom ledningsgruppen. Dataskyddsombudet ansvarar däremot inte för att dataskyddsförordningen efterlevs.

Dataskyddssamordnare: Dataskyddssamordnarens främsta uppgift är att leda och samordna dataskyddsarbetet i dataskyddsnätverket i samråd med stabschefen.

Dataskyddsspecialist: Dataskyddsspecialistens främsta uppgift är att stötta och bistå verksamheten i frågor som rör behandling av personuppgifter.

Dataskyddsambassadörer: Dataskyddsambassadörerna representerar Riksbankens avdelningar i dataskyddsnätverket och har till främsta uppgift att vägleda i frågor om dataskydd inom respektive avdelning, exempelvis genom att vid behov involvera dataskyddsombudet. Dataskyddsambassadören ska även dokumentera avdelningens personuppgiftsbehandlingar tillsammans med behandlingsansvariga.

Behandlingsansvariga: Behandlingsansvariga är kontaktpersoner och ansvarar för att dokumentera specifika personuppgiftsbehandlingar inom respektive avdelning tillsammans med dataskyddsambassadören.

3 Riksbankens dataskyddsarbete

3.1 Regelefterlevnad och en god dataskyddskultur

Riksbanken ska följa tillämplig dataskyddslagstiftning när personuppgifter behandlas inom Riksbankens verksamhet. I dataskyddsförordningen finns grundläggande principer och specifika regler som alltid gäller när personuppgifter behandlas. Riksbanken ska bedriva ett aktivt dataskyddsarbete för att säkerställa efterlevnad av tillämplig dataskyddslagstiftning. Det arbetet ska vara integrerat i den dagliga verksamheten och öka medarbetarnas medvetenhet om dataskydd i syfte att främja

regelefterlevnad och en god dataskyddskultur. Till stöd för detta arbete ska Riksbanken ha ett dataskyddsnätverk.

3.2 Riksbankens dataskyddsnätverk

Dataskyddsnätverket ska 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. Dataskyddsnätverket illustreras i Riksbankens operativa modell för dataskydd, som finns att ta del av via Banconätet. Utöver dataskyddsombudet består nätverket av dataskyddsambassadörer, behandlingsansvariga, en dataskyddsspecialist och en dataskyddssamordnare.

4 Efterlevnad

Avdelningscheferna ansvarar för att denna policy efterlevs.

Om det finns risk för att reglerna i denna policy inte följs kan riskenheten rapportera detta till direktionen i sin tertialrapport. Internrevision och dataskyddsombudet kan även kontrollera hur väl reglerna i policyn följs i samband med särskilda granskningar av Riksbankens verksamhet.

5 Ikraftträdande och övergångsbestämmelser

Denna policy träder i kraft samma dag som direktionen beslutar om den. Genom denna policy upphävs tidigare Policy för dataskydd (dnr 2020-01009) som beslutades den 7 oktober 2020.

5.1 Versionshistorik

Senast granskad	Version	Kommentar till ändringar
2022-10-27	1.1	Anpassningar till Riksbankens nya mall för styrande dokument samt till Regel för styrande dokument.

Checklista

Syftet med denna checklista är att dokumentera kvalitetsgranskning av en policy eller regel. Checklistan ska fyllas i av förvaltningsansvarig.

Checklistan ska bifogas beslutsunderlaget till beslutsfattare.

Namn på styrande dokument: Policy för dataskydd

Datum för kvalitetsgranskning: september 2022

Namn på förvaltningsansvarig: Dataskyddsombud

Aktivitet	Genomfört	Ej tillämpligt
Dokumentet är skrivet enligt befintlig mall	JA	
Dokumentet är avstämt mot andra styrande dokument	JA	
Dokumentet har blivit språkgranskat (av Kommunikationsenhetens klarspråksansvarige om dokumentet beslutas av direktionen)	JA	
Dokumentet har genomgått en juridisk granskning	JA	
En införandeplan är framtagen		X
En kommunikationsplan är framtagen		X - en artikel om dataskyddsnätverket och en uppdatering av den operativa modellen för dataskydd publicerades augusti 2022 på Banconätet.
En utbildningsplan är framtagen		X
Det finns ett beslut om översättning till engelska, när så behövs		X – det ska utvärderas om det finns behov av översättning till engelska.
Dokumentet är granskat av Regelefterlevnadsfunktionen	JA	
Checklistan har stämts av med regelefterlevnadsfunktionen	JA	