

# Granskning av Polismyndighetens ledning och styrning av dataskyddsarbetet



Informationsklass Öppen

Internrevision, rapport, augusti 2024



Utgivare: Polismyndigheten, Internrevisionen, 106 75 Stockholm  
Diarienummer: A559.871/2023, Saknr: 977  
Omslagsfoto:  
Upplaga: Intrapolis  
Datum: 2024-08-26

## Innehåll

<b>1</b>	<b>Sammanfattning .....</b>	<b>4</b>
<b>2</b>	<b>Inledning .....</b>	<b>6</b>
2.1	Bakgrund .....	6
2.2	Syfte och revisionsfrågor .....	6
2.3	Omfattning och avgränsning .....	7
2.4	Informationsinsamling och metod .....	7
2.5	Bedömningsgrunder .....	8
<b>3</b>	<b>Ledning och styrning av dataskyddsarbetet .....</b>	<b>8</b>
3.1	Inledning .....	8
3.2	Iakttagelser .....	9
3.2.1	Externa regelverk .....	9
3.2.2	Styrdokument .....	10
3.2.3	Processägare och verksamhetsansvariga .....	12
3.2.4	Dataskyddsbud .....	13
3.2.5	Rättsavdelningen .....	14
3.2.5.1	Enheten för rättslig styrning och stöd (RSS) .....	14
3.2.5.2	Rättstillämpningsgrupper och dataskyddsamordnare .....	15
3.2.6	Nätverk för personuppgiftsbehandling .....	16
3.2.7	It-utveckling .....	16
3.2.8	It-stöd .....	17
3.3	Bedömning .....	17
3.4	Rekommendationer .....	19
<b>4</b>	<b>Kontroll och uppföljning av dataskyddsarbetet .....</b>	<b>20</b>
4.1	Inledning .....	20
4.2	Iakttagelser .....	20
4.2.1	Externa regelverk .....	20
4.2.2	Styrdokument .....	21
4.2.3	Dataskyddsbud .....	22
4.2.4	Processägare och verksamhetsansvariga .....	23
4.3	Bedömning .....	23
4.4	Rekommendationer .....	24

### Bilagor

Biträdande rikspolischefens beslut om åtgärder, 23 augusti 2024

Åtgärdsplaner

## 1 Sammanfattning

Internrevisionen gör den övergripande bedömningen att ledningen och styrningen av Polismyndighetens dataskyddsarbete i huvudsak är effektiv och ändamålsenlig. Det finns dock områden som behöver utvecklas. När det gäller kontrollen och uppföljningen av dataskyddsarbetet gör internrevisionen bedömningen att den inte är tillräckligt ändamålsenlig.




Processägarna har ett stort ansvar för ledningen och styrningen av dataskyddsarbetet, t.ex. genom personuppgiftsnätverk. Internrevisionen konstaterar att nätverken inte fungerar som det var tänkt vilket riskerar att styrning och information från processägarna inte når ut i organisationen. Processägarna behöver därför se över och vid behov säkerställa lämpliga forum för styrning och samordning av dataskyddsfrågor. Rättsavdelningen behöver även se över riktlinjerna om personuppgiftsnätverken då riktlinjerna upplevs som otydliga.

Polismyndighetens dataskyddsombud är en central funktion i dataskyddsarbetet. Ombuden ska självständigt kontrollera att personuppgifter behandlas lagenligt och även informera och ge råd till myndigheten i dataskyddsfrågor. På grund av krav i interna styrdokument och resursbrist på rättsavdelningen har dataskyddsombuden behövt lägga mycket tid på annat än ombudens granskande uppdrag. Rättsavdelningen behöver därför säkerställa att det ges förutsättningar för dataskyddsombuden att fullgöra sitt granskningsuppdrag på ett ändamålsenligt sätt, t.ex. genom att se över riktlinjer om dataskyddsombudens uppgifter.

Styrdokumenterna på dataskyddsområdet upplevs som alltför omfattande och komplicerade. Verksamheten efterfrågar också fler stöddokument på dataskyddsområdet. Det pågår redan ett arbete inom rättsavdelningen med att se över styrdokumenterna. I översynen bör rättsavdelningen överväga att ta fram fler myndighetsgemensamma stödjande dokument inom dataskyddsområdet som är av mer verksamhetsnära karaktär.

Kontrollen av dataskyddsarbetet varierar i myndigheten och följs inte alltid upp eller rapporteras till den som är ansvarig för personuppgiftsbehandlingen. Det leder till osäkerhet om regelverken efterlevs och en risk för att brister i personuppgiftsbehandlingar inte identifieras eller åtgärdas. Processägarna behöver därför säkerställa en ändamålsenlig kontroll och uppföljning av personuppgiftsbehandlingar inom sina respektive ansvarsområden.

Tabellen nedan visar att internrevisionens granskning har resulterat i totalt fyra rekommendationer, fördelade utifrån internrevisionens modell för bedömning av brister som presenteras i rapporten.

	<b>Antal</b>
 Mycket väsentlig brist	-
 Väsentlig brist	4
 Mindre väsentlig brist	-

## 2 Inledning

Granskningen har utförts i enlighet med revisionsplanen för 2023.

### 2.1 Bakgrund

Polismyndigheten behandlar stora mängder personuppgifter i sin verksamhet. Det rör sig t.ex. om uppgifter om personer som ingår i olika typer av ärenden hos polisen och uppgifter om polisens egna medarbetare. En stor andel av personuppgifterna är av känslig natur.

Skyddet av personuppgifter (dataskyddet) regleras för Polismyndighetens del av flera omfattande regelverk.<sup>1</sup> Lagarna syftar främst till att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter.

Regelverken innebär ett långtgående ansvar för Polismyndigheten vid behandling av personuppgifter. Om lagstiftningen inte efterlevs kan det få integritetsskadande konsekvenser för registrerade personer och ekonomiska konsekvenser för myndigheten i form av administrativa sanktionsavgifter och skadestånd. Myndighetens anseende riskerar också att skadas.

Detta ställer sammantaget höga krav på att Polismyndigheten organiserar sitt dataskyddsarbete på ett effektivt och ändamålsenligt sätt. Det krävs en balans mellan å ena sidan styrning och rådgivning som förklarar och omsätter lagkrav till konkreta lösningar i verksamheten och å andra sidan kontroll och uppföljning för att säkerställa att styrningen och råden implementeras och följs.

### 2.2 Syfte och revisionsfrågor

Syftet med granskningen är att bedöma effektiviteten och ändamålsenligheten i den interna styrningen och kontrollen av dataskyddsarbetet i Polismyndigheten.

---

<sup>1</sup> Se bland annat 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), lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område. Därutöver finns speciallagstiftning som avser t.ex. behandling av flygpassagerares personuppgifter och bildmaterial från allmän kamerabevakning.

Följande revisionsfrågor har ingått i granskningen.

- Har Polismyndigheten en effektiv och ändamålsenlig ledning och styrning av dataskyddsarbetet som skapar förutsättningar för myndigheten att leva upp till dataskyddsregelverkets krav?
- Finns en ändamålsenlig kontroll och uppföljning av dataskyddsarbetet?

## 2.3 Omfattning och avgränsning

Granskningen omfattar ett urval av processägare med avseende på deras roll och ansvar för personuppgiftsbehandling inom respektive ansvarsområde.<sup>2</sup> Granskningen omfattar även rättsavdelningen när det gäller avdelningens roll och ansvar för den rättsliga styrningen och stödet inom dataskyddsområdet, it-avdelningen i egenskap av it- och informationssäkerhetsexpertis samt ett urval av polisregioner utan processansvar.<sup>3</sup>

Granskningen omfattar inte processen för hantering av personuppgiftsincidenter eller granskning av specifika it-system och inte heller genomgång av specifika behandlingar av personuppgifter eller interna bedömningar av sådana behandlingar.

## 2.4 Informationsinsamling och metod

Informationsinsamling har skett genom dokumentstudier och intervjuer.

Granskningen har utförts under perioden september – november 2023 av internrevisorerna Carl Ygge och Elin Waara.

Rapporten sakgranskades i början av 2024 av rättsavdelningen inklusive dataskyddsbuden, it-avdelningen, nationella operativa avdelningen, HR-avdelningen, kommunikationsavdelningen, ekonomiavdelningen, säkerhetsavdelningen, nationellt forensiskt centrum, avdelningen för särskilda utredningar, polisregion Stockholm, Nord, Syd och Väst. Muntlig information om iakttagelser och bedömningar lämnades av internrevisionen till rikspolischefen den 11 mars. Arbetet med inhämtning av åtgärdsförslag slutfördes av internrevisionen under april. Rikspolischefen beslutade om åtgärder i augusti 2024, se beslutsbilaga till rapporten tillsammans med åtgärdsplaner.

---

<sup>2</sup> Vi har intervjuat Noa, HR, KA, säkerhetsavdelningen, polisregion Stockholm och Nord.

<sup>3</sup> Vi har intervjuat polisregion Öst och Syd.

## 2.5 Bedömningsgrunder

Internrevisionens iakttagelser, bedömningar och grunder för lämnade rekommendationer framgår av den löpande texten i rapporten. För respektive rekommendation har internrevisionen bedömt bristen vid tidpunkten för granskningen. Internrevisionens bedömning följer nedanstående mall.

Bedömning	Beskrivning
Röd - Mycket väsentlig brist	Brist som allvarligt påverkar Polismyndighetens måluppfyllelse enligt instruktion eller regleringsbrev och/eller medför stora negativa konsekvenser för Polismyndighetens verksamhet och/eller innebär att Polismyndigheten inte uppfyller myndighetsförordningens krav på effektivitet, lagenlighet, redovisning och hushållning.
Orange -Väsentlig brist	Brist som påverkar den granskade verksamheten så att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.
Gul - Mindre väsentlig brist	Brist som inte påverkar den granskade verksamhetens måluppfyllelse men som medför negativa konsekvenser för verksamheten.

## 3 Ledning och styrning av dataskyddsarbetet

### 3.1 Inledning

För att bedöma effektiviteten och ändamålsenligheten i den interna styrningen och kontrollen av dataskyddsarbetet i Polismyndigheten har internrevisionen granskat flera aspekter av arbetet. Internrevisionen har bland annat kartlagt hur dataskyddsarbetet är organiserat inom myndigheten och vilka externa och interna regler som påverkar, hur samarbetet mellan olika avdelningar fungerar och om det finns tillräckligt med resurser för att utföra dataskyddsarbetet.

Iakttagelserna från granskningen framgår nedan följt av en bedömning av effektiviteten och ändamålsenligheten i styrningen och kontrollen.



## 3.2 Iakttagelser

### 3.2.1 Externa regelverk

Av dataskyddsregelverken framgår att Polismyndigheten är personuppgiftsansvarig för behandlingen av personuppgifter i myndighetens verksamhet. Det innebär att myndigheten måste säkerställa och visa att den följer dataskyddsreglerna genom att vidta lämpliga tekniska och organisatoriska åtgärder.<sup>4</sup>

En sådan åtgärd är att föra en förteckning över personuppgiftsbehandlingar som utförs under myndighetens ansvar. Förteckningen ska bland annat innehålla ändamålen med behandlingen samt en beskrivning av kategorierna av registrerade, personuppgifter och mottagare av personuppgifterna.<sup>5</sup>

Polismyndigheten har även en skyldighet att göra en konsekvensbedömning innan myndigheten påbörjar särskilt riskfylld personuppgiftsbehandling samt i vissa fall genomföra samråd med tillsynsmyndigheten.<sup>6</sup> Polismyndigheten ska också upprätta interna riktlinjer och utbilda medarbetarna om dataskydd samt bygga in integritetsvänliga lösningar i sina it-system, så kallat inbyggt dataskydd.

Polismyndigheten ska vidare utnämna dataskyddsombud.<sup>7</sup> Dataskyddsombud definieras som den som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt.<sup>8</sup> Dataskyddsombudet ska även informera och ge råd till den personuppgiftsansvarige och de som behandlar personuppgifter under dennes ledning om deras skyldigheter vid behandling av personuppgifter, ge råd vid en konsekvensbedömning samt kontrollera att den genomförs på ett korrekt sätt.<sup>9</sup> Vid utförandet av sina uppgifter ska dataskyddsombudet ta hänsyn till

---

<sup>4</sup> Utgångspunkten att den personuppgiftsansvarige behöver visa att den uppfyller reglerna kallas principen om ansvarsskyldighet.

<sup>5</sup> Se artikel 30 i dataskyddsförordningen och 3 kap. 3 § brottsdataförordningen (2018:1202).

<sup>6</sup> Se 3 kap. 7 § brottsdatalagen och artikel 35-36 i dataskyddsförordningen.

<sup>7</sup> Se 3 kap. 13 § brottsdatalagen, artikel 37 i dataskyddsförordningen och 3 kap. 12 § PNR-lagen.

<sup>8</sup> Se 1 kap. 6 § brottsdatalagen.

<sup>9</sup> Se 14 § brottsdatalagen. Dataskyddsombudets arbetsuppgifter uttrycks på liknande sätt i dataskyddsförordningen, se artikel 39 i dataskyddsförordningen. PNR-lagen hänvisar till vad som gäller enligt brottsdatalagen.

de risker som är förknippade med en behandling med beaktande av behandlingens art, omfattning, sammanhang och syften.<sup>10</sup>

Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå.<sup>11</sup>

### 3.2.2 Styrdokument

Av de interna styrdokumenterna framgår att en processägare är ansvarig för Polismyndighetens personuppgiftsbehandling inom sitt ansvarsområde. Ansvaret kan fördelas inom processägarens egen organisation.<sup>12</sup> Sådan ansvarsfördelning sker bland annat i handläggningsordningar, anmälningar av personuppgiftsbehandling till myndighetens förteckning och särskilda instruktioner som den processansvarige har möjlighet att utfärda.<sup>13</sup>

Processägaren eller den som utsetts som ansvarig för personuppgiftsbehandlingen har ansvar för att initiera och se till att processen dataskydd vid verksamhetsutveckling tillämpas.<sup>14</sup> I det ligger bland annat en skyldighet att se till att personuppgiftsbehandlingen dokumenteras i särskilda formulär, att konsekvensbedömning och förhandssamråd genomförs om det bedöms nödvändigt och att behandlingen förs in i myndighetens förteckning över personuppgiftsbehandlingar. Om behandlingens karaktär medför risker för att integritetskänsliga uppgifter kommer att behandlas på ett felaktigt sätt kan processägaren också ta fram styrdokument med instruktioner om personuppgiftsbehandlingen.<sup>15</sup>

Chefen för rättsavdelningen är processägare för Polismyndighetens systematiska dataskyddsarbete.<sup>16</sup> Rättsavdelningen har vidare verksamhetsansvar för och chefen för avdelningen är processägare för

- rättslig styrning avseende rättsområden kopplade till dataskydd

---

<sup>10</sup> Se artikel 39.2 i dataskyddsförordningen.

<sup>11</sup> Se artikel 38 i dataskyddsförordningen.

<sup>12</sup> Se 3 kap. 13 § i arbetsordningen.

<sup>13</sup> Se riktlinjer för processägares instruktioner om personuppgiftsbehandling (PM 2020:10).

<sup>14</sup> Se riktlinjer för dataskydd vid verksamhetsutveckling (PM 2018:38).

<sup>15</sup> Se riktlinjer för processägares instruktioner om personuppgiftsbehandling (PM 2020:10).

<sup>16</sup> Se beslutsprotokoll i ärende A725.705/2021 (daterat 2023-11-24) avseende ändringar i bland annat 3 kap. 42 § första stycket i arbetsordningen. Ändringarna trädde ikraft den 1 december 2023.

- rättsligt stöd till avdelningarna och polisregionerna avseende dataskydd
- att föra en förteckning över de kategorier av behandlingar av personuppgifter som myndigheten ansvarar för.<sup>17</sup>

Vid Polismyndigheten ska det vidare finnas en dataskyddsombudsfunktion.<sup>18</sup> Dataskyddsombuden förordnas av rikspolischefen och är placerade på rättsavdelningen vid enheten för rättslig styrning och stöd (RSS). Dataskyddsombuden ska bland annat informera och ge råd om personuppgiftsbehandling till ansvariga inom myndigheten och de som behandlar personuppgifter under den ansvarigas ledning.<sup>19</sup> Ombuden har även getts särskilda uppgifter i flera av myndighetens riktlinjer på dataskyddsområdet. Bland annat ska dataskyddsombuden granska de formulär med dokumentation som ska fyllas i när en verksamhet vill påbörja en ny personuppgiftsbehandling eller genomföra förändringar i en pågående behandling.<sup>20</sup>

Dataskyddsombuden rapporterar direkt till rikspolischefen.<sup>21</sup>

För att uppnå enhetlighet och säkerställa att personuppgiftsfrågor omhändertas på ett rättssäkert sätt ska det inom Polismyndigheten finnas en sammanhållen struktur av personuppgiftsnätverk.<sup>22</sup>

- Processindelade personuppgiftsnätverk (PPN) ska användas av en processägare för att t.ex. lämna instruktioner till de verksamheter som behandlar personuppgifter inom processen eller införa nya personuppgiftsbehandlingar. Nätverken kan också användas för att samordna registervårdsinsatser, logguppföljningar eller gemensamma utbildningsinsatser. Nätverken kan även användas för att förmedla behov och förslag till förbättringar till processägaren.
- Samordnande personuppgiftsnätverk (SPN) kan användas inom en avdelning eller polisregion för att samordna personuppgiftsfrågor och för

<sup>17</sup> Se beslutsprotokoll i ärende A725.705/2021 (daterat 2023-11-24) avseende ändringar i bland annat 3 kap. 42 § andra stycket i arbetsordningen. Ändringarna trädde ikraft den 1 december 2023.

<sup>18</sup> Se beslutsprotokoll i ärende A725.705/2021 (daterat 2023-11-24) avseende ändringar i bland annat 4 kap. 10 § i arbetsordningen. Ändringarna trädde ikraft den 1 december 2023.

<sup>19</sup> Se beslutsprotokoll i ärende A725.705/2021 (daterat 2023-11-24) avseende ändringar i bland annat 4 kap. 10 § i arbetsordningen. Ändringarna trädde ikraft den 1 december 2023.

<sup>20</sup> Se riktlinjer för dataskydd vid verksamhetsutveckling (PM 2018:38).

<sup>21</sup> Se 4 kap. 9 § i arbetsordningen.

<sup>22</sup> Se Polismyndighetens riktlinjer för samordning av personuppgiftsfrågor (PM 2019:30). Nätverken är inga beslutsorgan.

att utreda ansvarsförhållanden rörande personuppgiftsbehandlings-  
internt.

- Myndighetsövergripande personuppgiftsnätverk (MPN) ska inrättas av RSS i syfte att samordna samtliga polisregioner och avdelningar i myndighetsövergripande personuppgiftsfrågor.

Enligt intervjuer anser flera, främst polisregionerna, att det finns för många styrdokument på dataskyddsområdet och att de är för komplexa för att verksamheten ska kunna ta till sig innehållet. De upplever svårigheter att utläsa vad som gäller och dokumenten upplevs som svåra att navigera i. Flera regioner har därför tagit fram lathundar och andra stöddokument för att förtydliga och underlätta dataskyddsarbetet ute i linjeverksamheten.

### 3.2.3 Processägare och verksamhetsansvariga

Processägarna och verksamhetsansvariga har organiserat dataskyddsarbetet på olika sätt. Personuppgiftsansvaret har i de flesta fall delegerats från processägaren till enhetschefer inom respektive avdelning eller polisregion. I något fall har processägaren behållit ansvaret för personuppgiftsbehandlingen. I ett annat fall har ansvaret delegerats till en processledare. Hos både processägare och de verksamhetsansvariga hålls arbetet ofta ihop av en dataskyddsamordnare eller en verksamhetscontroller. I flera fall är samordnaren även jurist.

Nivån på processägarnas och verksamhetsansvarigas arbete med dataskyddsfrågor varierar. Vissa processägare driver t.ex. nätverk enligt riktlinjerna medan andra, däribland vissa verksamhetsansvariga, inte känner till att nätverksstrukturen existerar. Det kan delvis förklaras av att personuppgiftsbehandlingen varierar i omfattning och är ett mer eller mindre centralt inslag i processerna eller verksamheterna. En annan faktor som framhålls i intervjuer är om processägaren har lyckats rekrytera och behålla engagerade och kunniga medarbetare.

Processägarnas kompetensnivå inom dataskydd varierar också. Flera intervjuade anser att processägarna behöver höja kompetensnivån inom sina organisationer. Vissa processägare håller utbildningar, t.ex. utredningsenheten inom Noa. De obligatoriska dataskyddsutbildningarna som rättsavdelningen har tagit fram är uppskattade men skulle kunna byggas på med fler riktade utbildningar. Processägare som blivit föremål för återkommande extern tillsyn har gjort stora insatser för att lyfta och prioritera dataskyddsarbetet.

Processägarna får som huvudregel juridiskt stöd i dataskyddsfrågor från RSS. I de fall processägaren är en polisregion kommer stödet i första hand från den regionala rättstillämpningsgruppen. Samma sak gäller regioner som saknar processansvar.

Baserat på intervjuer är den generella uppfattningen att processägarna och verksamhetsansvariga får bra stöd av rättsavdelningen. De flesta upplever dock rättsavdelningen som en trång resurs och att det ofta är långa handläggningstider, t.ex. när det gäller anmälningar till myndighetens förteckning över personuppgiftsbehandlingar. Ändringar i anmälningarna beskrivs som omständliga då anmälningarna görs i blanketter som måste uppdateras manuellt. Det upplevs också som oklart hur prioriteringarna mellan olika ärenden och frågor hos rättsavdelningen görs. De intervjuade anser även att kontinuiteten i det juridiska stödet har påverkats negativt av en relativt hög personalomsättning.

### 3.2.4 Dataskyddsombud

Polismyndighetens fem dataskyddsombud är förordnade av rikspolischefen och placerade på RSS. Dataskyddsombuden är placerade i en annan grupp än dataskyddsjuristerna och rapporterar direkt till rikspolischefen.

Dataskyddsombudens arbetsuppgifter motsvarar i huvudsak vad som framgår av dataskyddsregelverken och arbetsordningen. En generell uppfattning hos dataskyddsombuden är dock att de enligt styrdokumentet har getts vissa arbetsuppgifter som går längre än vad som krävs enligt lagstiftningen. Syftet med det har troligen varit att säkerställa att dataskyddsombuden involveras i dataskyddsarbetet och får goda möjligheter att arbeta proaktivt.

Ett exempel på en sådan arbetsuppgift är att dataskyddsombuden ska granska de formulär med dokumentation som ska fyllas i varje gång en verksamhet vill påbörja en ny personuppgiftsbehandling eller genomföra förändringar i en pågående behandling. Det medför att ombuden ägnar mycket tid till att sätta sig in i och ge råd om i stort sett varje ny eller förändrad personuppgiftsbehandling vid myndigheten, oavsett vilken risk den bedöms medföra. Ombuden får då svårt att hinna göra egna granskningar och arbeta riskbaserat på det sätt som förväntas enligt dataskyddsförordningen. Att dataskyddsombuden ska granska alla behandlingar innan de får påbörjas skulle också kunna uppfattas som att de har ett beslutande inflytande över behandlingarna. Det kan i sin tur innebära en risk för intressekonflikt om dataskyddsombuden senare genomför granskningar av samma behandlingar. Dataskyddsombuden

anser därför att styrdokumenterna inklusive beskrivningarna av ombudens uppgifter är i behov av uppdatering.

Dataskyddsombuden bistår även dataskyddsjuristerna med råd och stöd. Det kan leda till höjd kvalitet på rådgivningen men kan också medföra visst dubbelarbete.

Rättsavdelningen genomför för tillfället en allmän översyn av den rättsliga verksamheten som delvis påverkar dataskyddsombuden. Bland annat har en ny roll som rättslig expert införts inom ett antal rättsområden, däribland dataskydd, för att RSS ska kunna arbeta mer strategiskt med frågorna. Dataskyddsombuden arbetar också med att utveckla sina arbetssätt. Förhoppningen är att det sammantaget ska leda till klargöranden beträffande ansvarsfördelningen mellan dataskyddsombuden och dataskyddsjuristerna samt medföra att det blir tydligare i vilka fall ombuden behöver involveras och inte. Samtidigt framför dataskyddsombuden att det är viktigt för dem att vara fortsatt informerade om pågående verksamhetsutveckling och vad som är på gång i myndigheten.

### **3.2.5 Rättsavdelningen**

Enligt intervjuer anser flera att rättsavdelningen behöver ta ett mer övergripande perspektiv på myndighetens personuppgiftsbehandling. Idag hanteras ibland samma typ av frågor i olika spår och av olika handläggare istället för att koordineras och samordnas. Ökad samordning inom RSS skulle kunna underlätta och snabba på arbetet vilket skulle gynna såväl processägarna som rättsavdelningen, menar de intervjuade.

Den ovan nämnda översynen av rättsavdelningen innebär att dataskyddsjuristerna blir utspridda i fler grupper på RSS. Förhoppningen hos de intervjuade är att det kommer att korta ledtiderna på avdelningen. I översynen ingår även att uppdatera, förtydliga och förenkla de interna riktlinjerna om dataskydd, t.ex. de som avser personuppgiftsnätverken.

#### **3.2.5.1 Enheten för rättslig styrning och stöd (RSS)**

På RSS finns dataskyddsjurister som ger rättsligt stöd till processägarna, t.ex. vid dokumentation av personuppgiftsbehandlingar, genomförande av konsekvensbedömningar, i samband med verksamhetsutveckling och i andra dataskyddsfrågor.

Enligt intervjuer upplever RSS att processägarna oftast tar sitt ansvar för personuppgiftsbehandlingen. I vissa situationer har dock gränsdragningsproblem uppstått mellan olika processägare och mellan processägare och rättsavdelningen. En utmaning som innebär att dataskyddsjuristerna ibland kommer sent in i utvecklingsarbeten är att det saknas en myndighetsgemensam process för verksamhetsutveckling. Det innebär att möjligheterna att påverka hur personuppgifter behandlas i nya eller förändrade it-stöd försämras.

Beträffande myndighetens samordning av personuppgiftsbehandling anser RSS att nätverken inte har fått det genomslag och blivit den naturliga ingång för dataskyddsfrågor till ansvariga respektive rättsavdelningen som det var tänkt. Det finns enligt RSS anledning att se över och förtydliga riktlinjerna om nätverken.

Angående Polismyndighetens förteckning över personuppgiftsbehandlingar är RSS av uppfattningen att den är i behov av översyn. Förteckningen är enligt RSS i förhållandevis gott skick vad gäller behandlingar inom det brottsbekämpande området medan den uppvisar större brister på det icke-brottsbekämpande området, t.ex. vad gäller avsaknad av eller icke uppdaterade anmälningar. En del av dessa ”brister” beror på förändrad lagstiftning och tolkning av densamma medan andra bedöms vara konsekvenser av tidigare organisationsstruktur och att vissa processägare inte prioriterar arbetet med att uppdatera förteckningen. Förteckningen bedöms även i vissa avseenden vara mer detaljerad än vad lagstiftningen idag kräver vilket innebär att onödiga resurser går åt till översyn. Det försvårar även vid sekretessprövningar. Det pågår sedan en tid tillbaka ett arbete på RSS med att uppdatera förteckningen.

### 3.2.5.2 Rättstillämpningsgrupper och dataskyddssamordnare

På rättsavdelningen finns även jurister i regionala rättstillämpningsgrupper som helt eller delvis arbetar med dataskyddsfrågor riktat mot polisregionerna. Juristerna har ett regionalt dataskyddsnätverk som träffas en gång per månad, en gemensam chatt och ett nationellt nätverk där även representanter från RSS deltar. Vissa regioner har även anställt dataskyddssamordnare som ofta arbetar tillsammans med regionens utpekade jurist.

De intervjuade beskriver att dataskyddsfrågorna hade en mycket hög prioritet hos processägarna och verksamhetsansvariga i samband med att dataskyddsförordningen började tillämpas 2018 men att intresset avtagit stegvis. Det märks bland annat genom att det inte längre kommer in lika många frågor till rättstillämpningsgrupperna. Det minskade intresset och engagemanget gör att

juristerna idag arbetar mer reaktivt och mindre proaktivt. De håller utbildningar på begäran men tar inte egna initiativ i så stor utsträckning.

Intervjupersonerna har inte tillgång till förteckningen över Polismyndighetens personuppgiftsbehandlings. Det skapar osäkerhet när de får frågor om personuppgiftsbehandlingar från verksamheten och merarbete eftersom de måste vända sig till RSS för att kontrollera om behandlingarna är registrerade och vad registreringarna omfattar.

Intervjupersonerna anser att processägarnas styrning i dataskyddsfrågor bör bli tydligare, t.ex. i form av instruktioner eller styrdokument. Den bristande styrningen leder ibland till en onödigt restriktiv hållning i dataskyddsfrågor trots att lagstiftningen är relativt generös. I kombination med dåligt fungerande nätverk för personuppgiftsbehandling och komplexa styrdokument skapar det en bitvis svår arbetssituation framförallt för juristerna i rättstillämpningsgrupperna och för dataskyddsamordnarna. Hög personalomsättning bland juristerna och svårigheter att rekrytera är också något som flera vittnar om.

### **3.2.6 Nätverk för personuppgiftsbehandling**

Enligt intervjuer anser merparten att de processindelade och samordnande personuppgiftsnätverken inte fungerar enligt vad som avses i styrdokumentet. Som tidigare nämnts är det flera intervjuade som inte ens känner till att nätverken existerar.

Det myndighetsövergripande nätverket som leds av rättsavdelningen (RSS) anses fungera relativt bra och har representation från polisregioner och nationella avdelningar. Intervjupersoner upplever dock att nätverket på senare tid har blivit en typ av envägskommunikation utan diskussion eller utbyte.

Det framförs också att riktlinjerna om nätverken behöver bli tydligare, mer styrande och faktiskt ålägga processägarna att skapa och aktivt driva personuppgiftsnätverk. Nätverken upplevs som centrala för att få bättre samordning och enhetlighet i myndighetens dataskyddsarbete. I samband med att rättsavdelningen ser över riktlinjerna på dataskyddsområdet kommer även riktlinjerna avseende nätverken ses över, enligt intervju med RSS.

### **3.2.7 It-utveckling**

Det framgår av riktlinjer att processägarna ansvarar för att involvera rättsavdelningen i it-utvecklingsarbete. Enligt intervjuer finns dataskyddsfrågorna



med och beaktas i samband med utveckling av nya it-system och vidareutveckling av befintliga system.

Uppfattningen är att samarbetet mellan processägare, it-avdelningen och rättsavdelningen har förbättrats och fungerar relativt bra. It-avdelningen och rättsavdelningen har bland annat initierat ett samarbete för att dela tidplaner och lägesbilder i syfte att planera och synkronisera arbetet bättre.

### **3.2.8 It-stöd**

Ur dataskyddsperspektiv finns det problem med flera av myndighetens äldre it-system. Problemen avser främst att flera system saknar funktioner för automatisk gallring och att det saknas funktioner för att bevaka längsta tid för personuppgiftsbehandlingen. Enligt de intervjuade pågår arbete med att åtgärda bristerna men man upplever problem med att behoven ofta prioriteras ner i förhållande till andra it-utvecklingsbehov. En utmaning enligt flera intervjuade är också den information som finns sparad i mappstrukturer eftersom det krävs manuella insatser för att hålla mapparna uppdaterade.

En problematik som flera intervjuade, inklusive rättsavdelningen, lyfter är att myndighetens förteckning över personuppgiftsbehandlingar saknar ändamålsenligt it-stöd. Förteckningen förs idag i Excel vilket innebär vissa risker.

Rättsavdelningen ser också behov av systemstöd för registerutdrag till enskilda enligt dataskyddsregelverken som förslagsvis skulle kunna vara tillgängligt via polisens hemsida. För det syftet krävs dock en lösning för elektronisk identifiering. Rättsavdelningen arbetar med att utveckla dessa behov och jobbar parallellt för att behoven ska komma upp på utvecklingsplaner för nya it-stöd.

## **3.3 Bedömning**

Internrevisionen gör den övergripande bedömningen att ledningen och styrningen av Polismyndighetens dataskyddsarbete i huvudsak är effektiv och ändamålsenlig. Det finns dock områden som behöver utvecklas.

Det finns en sammanhållen och heltäckande struktur för hur dataskyddsarbetet ska organiseras i Polismyndigheten. Strukturen framgår av styrdokument och inkluderar hur ansvaret för dataskyddsfrågor fördelas.

Ett stort ansvar vilar enligt styrdokumenterna på processägarna. Ett sätt för processägarna att driva ett aktivt dataskyddsarbete är genom strukturen för

personuppgiftsnätverk. Internrevisionen konstaterar att nätverken inte fungerar som det var tänkt. Det betyder att information från processägarna, t.ex. i form av instruktioner för personuppgiftsbehandlingen, riskerar att inte nå ut i organisationen. På motsvarande sätt riskerar relevant återkoppling från verksamheten i olika dataskyddsfrågor att inte nå processägarna. Processägarna behöver därför se över och vid behov säkerställa lämpliga forum för styrning, samordning och kanalisering av dataskyddsfrågor inom sina respektive ansvarsområden.

Internrevisionen konstaterar att på grund av krav i styrdokument och resursbrist på RSS har dataskyddsombuden behövt lägga mycket tid på granskning och rådgivning i samband med att verksamhet vill påbörja en ny, eller förändra en befintlig personuppgiftsbehandling. Det har gått ut över ombudens möjlighet att utföra sitt granskande uppdrag. Involveringen i samband med ny eller förändrad personuppgiftsbehandling innebär också att ombuden riskerar att hamna i intressekonflikt vid senare granskning.

Internrevisionen noterar att Polismyndighetens förteckning över personuppgiftsbehandlingar har brister avseende innehåll och it-stöd. RSS arbetar med att åtgärda bristerna och kommer inom kort att lämna in en behovsframställan om en mer robust it-lösning.

Beträffande styrdokumenterna på dataskyddsområdet upplevs de som alltför omfattande och komplicerade. Styrdokumenterna ses för tillfället över av RSS. Utöver riktlinjerna anser internrevisionen att RSS bör överväga att ta fram fler myndighetsgemensamma stödjande dokument inom dataskyddsområdet av mer verksamhetsnära karaktär.

Det är tydligt att flera av Polismyndighetens äldre it-system inte i tillräcklig utsträckning är anpassade till dataskyddsregelverken. Dataskyddsombuden och externa tillsynsmyndigheter har tidigare konstaterat samma sak. Internrevisionen noterar att det sker ett arbete med att åtgärda brister i äldre it-system. Det vore önskvärt att detta arbete skulle kunna få en högre prioritet än vad som gäller idag. Vad gäller utveckling av nya it-stöd fungerar samarbetet mellan processägare, rättsavdelningen och it-avdelningen i huvudsak bra och dataskyddsfrågorna omhändertas.

Internrevisionen noterar att rättsavdelningen för närvarande genomför förändringar baserade på en översyn av verksamheten. Förändringarna framstår som relevanta för att förstärka och effektivisera det juridiska stödet samt tydliggöra gränsdragningen mellan dataskyddsjurister och dataskyddsombud.

## 3.4 Rekommendationer

### Rekommendation 3.4.1

#### Orange – Väsentlig brist

Internrevisionen rekommenderar rättsavdelningen att

- översynen av riktlinjer för dataskyddsområdet även omfattar att se över regleringen av personuppgiftsnätverken och dataskyddsombudens arbetsuppgifter
- överväga att ta fram fler myndighetsgemensamma stödjande dokument inom dataskyddsområdet.

Konsekvenserna av om rekommendationen inte följs är en ökad risk för att ansvarsfördelningen och den rättsliga styrningen samt det rättsliga stödet inte är tillräckligt tydligt. Det riskerar att leda till ineffektivitet och kan försvåra för Polismyndigheten att efterleva externa regelverk.

### Rekommendation 3.4.2

#### Orange – Väsentlig brist

Internrevisionen rekommenderar processägarna att

- se över och vid behov säkerställa lämpliga forum för styrning, samordning och kanalisering av dataskyddsfrågor inom sina respektive ansvarsområden.

Konsekvenserna av om rekommendationen inte följs är en ökad risk för att processägarnas styrning inom dataskyddsområdet inte når ut i organisationen vilket kan leda till brister i personuppgiftsbehandlingar. Det kan i sin tur leda till integritetsskadande konsekvenser för registrerade personer och ekonomiska konsekvenser för Polismyndigheten. Det kan också skada förtroendet för myndigheten.

## 4 Kontroll och uppföljning av dataskyddsarbetet

### 4.1 Inledning

För att bedöma ändamålsenligheten i kontrollen och uppföljningen av dataskyddsarbetet har internrevisionen kartlagt myndighetens organisation och rutiner samt vilka externa och interna regler som påverkar. Iakttagelser från granskningen framgår nedan följt av en bedömning av ändamålsenligheten i kontrollen och uppföljningen av dataskyddsarbetet.

### 4.2 Iakttagelser

#### 4.2.1 Externa regelverk

Utifrån de integritetsrisker som finns med en viss personuppgiftsbehandling har den personuppgiftsansvarige ett generellt ansvar att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen utförs i enlighet med aktuellt dataskyddsregelverk. Det kan innebära att organisationen antar en policy med lämpliga strategier för dataskydd och ser till att genomföra den i organisationen. Uppförandekoder och certifieringar kan också vara ett sätt att visa att dataskyddsförordningens bestämmelser uppfylls.

En av dataskyddsombudets viktigaste uppgifter är att övervaka och kontrollera att organisationen följer dataskyddsregelverket. För att kunna utföra den och övriga uppgifter som ankommer på ombudet krävs den personuppgiftsansvariges medverkan och stöd. Den personuppgiftsansvarige ska bland annat säkerställa att dataskyddsombudet

- ges tillräcklig självständighet för att effektivt kunna utföra sina uppgifter. Dataskyddsombudet får inte ta emot instruktioner som gäller utförandet av sina arbetsuppgifter.
- har de resurser (medarbetare, infrastruktur, t.ex. utrustning, och ekonomiska medel) som krävs för att fullgöra sina uppgifter
- har tillräckligt med tid på sig för att fullgöra sina uppgifter
- informeras och rådfrågas i ett tidigt skede eftersom det underlättar efterlevnaden av regelverket och främjar en strategi för inbyggt dataskydd

- har högsta ledningens aktiva stöd i sitt arbete.<sup>23</sup>

Dataskyddsfunktionen måste vara effektiv och ha tillräckligt med resurser i förhållande till den personuppgiftsbehandling som utförs i organisationen som ombudet tillhör. Det är också av vikt att det finns andra kontrollfunktioner i organisationen som känner och tar ansvar för att dataskyddsregelverken efterlevs.

#### 4.2.2 Styrdokument

Processägaren eller den som är ansvarig för personuppgiftsbehandlingen inom ramen för processansvaret ska säkerställa att personuppgifter behandlas enhetligt och författningsenligt inom hela Polismyndigheten för de definierade ändamålen med behandlingen.<sup>24</sup> För att göra det krävs att processägaren eller den som är ansvarig för personuppgiftsbehandlingen ger instruktioner om hur personuppgifterna ska behandlas samt fördelar arbetsuppgifter till en eller flera medarbetare. Arbetsuppgifterna kan exempelvis vara att

- se till att uppgifter inte bevaras längre än nödvändigt och aldrig längre än vad regelverket medger
- utföra rättning av felaktiga uppgifter samt upprätta närmare rutiner för hur felaktigheter ska upptäckas och rättas
- utföra särskilda registervårdsinsatser i den utsträckning som har bestämts för personuppgiftsbehandlingen.

Processägaren kan också ställa upp ramar för och ge instruktioner om bland annat vilka obligatoriska kontroller eller åtgärder som ska vidtas vid särskild registervård.

Löpande registervård ska ske för alla personuppgiftsbehandlingar.<sup>25</sup> Med löpande registervård avses framförallt åtgärder som utförs som en integrerad del i verksamhetens hantering av informationen, t.ex. i samband med registrering och andra åtgärder som vidtas i enstaka fall när felaktigheter upptäcks.

---

<sup>23</sup> Se Riktlinjer om dataskyddsombud, Artikel 29-arbetsgruppen för skydd av personuppgifter, antagna den 13 december 2016.

<sup>24</sup> Se Polismyndighetens riktlinjer för processägares instruktioner om personuppgiftsbehandling, PM 2020:10.

<sup>25</sup> Se Polismyndighetens riktlinjer för särskild registervård av personuppgiftsbehandlingar, PM 2016:36

Utöver löpande registervård krävs det i vissa fall särskilda registervårdsåtgärder i syfte att kontrollera och utvärdera att registervården bedrivs i tillräcklig utsträckning och att den får avsedd effekt. I vilken utsträckning särskild registervård ska ske bör regleras i processansvarigas riktlinjer avseende ansvar för personuppgiftsbehandlingar inom dennes ansvarsområde. Hur särskild registervård ska bedrivas kan anges i en registervårdsplan eller direkt i anmälan till myndighetens förteckning över personuppgiftsbehandlingar. En registervårdsplan ska innehålla en uttömmande redogörelse för vilka kontroller som ska vidtas. Processansvarig eller den som denne pekar ut kan också besluta om en särskild registervårdsinsats.

Beträffande dataskyddsbuden och deras arbetsuppgifter görs en hänvisning i arbetsordningen till dataskyddsregelverken. I arbetsordningen framgår också att dataskyddsbuden självständigt ska granska personuppgiftsbehandlingar i myndigheten och påpeka eventuella brister för den personuppgiftsansvarige.

### 4.2.3 Dataskyddsbud

Enligt intervjuer med dataskyddsbuden genomför ombuden granskningar men inte i den utsträckning som de själva önskar. Det finns flera förklaringar till det varav huvudskälen är den tid som det tar att utföra de övriga arbetsuppgifter som ombuden har enligt styrdokumentet, hög personalomsättning, periodvis underbemanning samt att det har inträffat flera personuppgiftsincidenter som tagit mycket av ombudens tid i anspråk.

För de granskningar som genomförs skrivs rapporter. Dataskyddsbuden sammanfattar även sitt arbete och ger sin syn på myndighetens dataskyddsarbete i en årsberättelse. Årsberättelsen innehåller förutom genomförda granskningar också bland annat resultat från extern tillsyn, personuppgiftsincidenter, skadeståndsärenden och centrala dataskyddsfrågor. I årsrapporten<sup>26</sup> för 2022 framgår att dataskyddsbuden genomfört tre granskningar 2022. Enligt intervjuer har det under 2023 genomförts två granskningar, varav båda avser personuppgiftsbehandling enligt PNR-lagen.

Enligt dataskyddsbuden pågår diskussioner kring hur de ska lägga upp sitt arbete framöver. Det finns idag ingen tydlig process för granskningsarbetet inklusive riskbedömningar. Dataskyddsbuden har hittills heller inte tagit fram någon granskningsplan för det kommande året utan vad som ska

---

<sup>26</sup> Årsberättelsen kallades tidigare för årsrapport och var något mer omfattande.

granskas bestäms löpande. Arbetet bedrivits huvudsakligen reaktivt och styrs främst av vilka ärenden som de får in. Dataskyddsombuden har för närvarande ingen pågående granskning.

#### **4.2.4 Processägare och verksamhetsansvariga**

Av de processägare och verksamhetsansvariga som intervjuats är det endast underrättelseverksamheten inom Noa som har upprättat registervårdsplaner för verksamheten enligt vilka regelbundna kontroller genomförs. Resultatet av registervårdskontrollerna rapporteras till en samordnare som sammanställer resultatet i en rapport till chefen för underrättelseenheten. Vid den senaste genomförda registervårdskontrollen 2022 upptäcktes inga allvarliga eller systematiska fel.

Vad gäller övriga processägare och verksamhetsansvariga som intervjuats finns inte på samma sätt en sammanhållen struktur för kontroll av personuppgiftsbehandlingar eller uppföljning av att kontrollerna verkligen genomförs. I många fall har det bedömts som tillräckligt att i personuppgiftsanmälningar ange hur löpande registervård ska göras. Det saknas i många av dessa fall en samordning, kontroll och återrapportering av att registervården verkligen genomförs. Enligt intervjuer med processägarna finns det i några fall planer på att ta fram en struktur och systematik avseende kontroll och uppföljning av personuppgiftsbehandlingarna och i ett fall har arbete kring detta inletts.

Flera intervjuade anser att processägarna i lärande syfte borde kommunicera ut systematiska brister som upptäcks i de kontroller som genomförs. Vad gäller de interna styrdokumenterna är de svåra att ta till sig även inom detta område, anser de intervjuade.

### **4.3 Bedömning**

Internrevisionen gör den övergripande bedömningen att kontrollen och uppföljningen av Polismyndighetens dataskyddsarbete inte är tillräckligt ändamålsenlig.

Internrevisionen konstaterar att rutinerna kring kontroll och uppföljning av dataskyddsarbetet varierar. I anmälningar till myndighetens förteckning över personuppgiftsbehandlingar anges vilken typ av registervård som ska genomföras. Att det verkligen sker följs sällan upp eller rapporteras till den som är ansvarig för personuppgiftsbehandlingen. Den bristande uppföljningen och rapporteringen leder till osäkerheter beträffande i vilken utsträckning

regelverken efterlevs och en ökad risk för att personuppgiftsbehandlingsmed brister inte identifieras och åtgärdas.

Endast i ett fall har internrevisionen noterat en processägare som på ett sammanhållet sätt upprättat registervårdsplaner och enligt vilka regelbundna kontroller genomförs, som också rapporteras till den ansvarige. Förbättringar behöver således ske avseende processägarnas rutiner för kontroll och uppföljning av dataskyddsarbetet. Enligt intervjuer finns i flera fall planer på att införa rutiner för det och enligt internrevisionen är det viktigt att detta verkligen realiserar.

Internrevisionen noterar att dataskyddsombuden under en längre tid, på grund av omständigheter beskrivna ovan, inte kunnat genomföra granskningar i den utsträckning som de önskat och att det för närvarande pågår diskussioner kring deras framtida arbetssätt. I dessa diskussioner vill internrevisionen betona vikten av att dataskyddsombuden ges förutsättningar att fullgöra sitt granskningsuppdrag. Enligt internrevisionen skulle en mer riskbaserad och planlagd ansats i det kommande arbetssättet underlätta arbetet. Ett exempel kan vara att ta fram en riskbaserad granskningsplan för kommande år. I en sådan plan kan t.ex. ingå att dataskyddsombuden granskar hur processägarna kontrollerar och följer upp sina personuppgiftsbehandlingsmed.

## 4.4 Rekommendationer

### Rekommendation 4.4.1

#### Orange – Väsentlig brist

Internrevisionen rekommenderar processägarna att

- säkerställa en ändamålsenlig kontroll och uppföljning av personuppgiftsbehandlingsmed inom sina respektive processansvar.

Konsekvenserna av om rekommendationen inte följs är en ökad risk för att brister i personuppgiftsbehandlingsmed inte upptäcks och åtgärdas, vilket kan leda till integritetsskadande konsekvenser för registrerade personer och ekonomiska konsekvenser för Polismyndigheten. Det kan också skada förtroendet för myndigheten.



## Rekommendation 4.4.2

### Orange – Väsentlig brist

Internrevisionen rekommenderar rättsavdelningen att

- säkerställa att det ges förutsättningar för dataskyddsombuden att fullgöra sitt granskningsuppdrag på ett ändamålsenligt sätt.

Konsekvenserna av om rekommendationen inte följs är en ökad risk för att brister i personuppgiftsbehandlingar inte upptäcks och åtgärdas, vilket kan leda till integritetsskadande konsekvenser för registrerade personer och ekonomiska konsekvenser för Polismyndigheten. Det kan också skada förtroendet för myndigheten.



Datum 2024-08-23

Informationsklass Öppen

Diariernr, ärende A559.871/2023

Saknr 977

Polismyndigheten

Beslutsprotokoll RPC 83/2024

Beslutande	Biträdande rikspolischefen Stefan Hector
Föredragande	Handläggaren Magnus Thomann
Övriga som deltagit i den slutliga handläggningen	Avdelningschefen Martin Valfridsson <i>MV</i> Rättschefen Gunilla Hedwall <i>GH</i>
Ärende	Beslut med anledning av internrevisionens granskning av dataskyddsarbetet.
Beslut	Internrevisionen har granskat Polismyndighetens ledning och styrning av dataskyddsarbetet.  Polismyndigheten beslutar att bilagda åtgärdsplaner ska genomföras.
Kostnad	-
Finansiering	-

Vid protokollet

Magnus Thomann

Justeras

Stefan Hector

Sändlista	Kopia till
Samtliga polisregioner och avdelningar	Arbetsstagarorganisationerna
Internrevisionen	Skyddsorganisationen



## FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	Att återaktivera EA:s interna personuppgiftsnätverk för att säkerställa att relevanta personer ingår samt stämna av läget per enhet.
Kommentarer	<p>EA gör bedömningen att styrning, samordning och kanalisering av dataskyddsfrågorna i grunden är ändamålsenlig varför större åtgärder inte är nödvändiga.</p> <p>Respektive enhet på EA har utsedda personerna vilka ingår i ett EA-internt nätverk för personuppgiftsfrågor med EA Kansli som sammankallande. Medarbetare från EA Kansli ingår därutöver i RA:s myndighetsnätverk. Det EA-interna nätverket har dock haft låg aktivitet det senaste året.</p>
Ansvarig	EA Kansli.
Tidplan	Klart 30 maj.

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	<p>Att via respektive utsedd person på enheterna med utgångspunkt från förtecknade personuppgiftsbehandlingar gå igenom läget vad gäller gallring/längsta tid för bevarande.</p> <p>EA Kansli hanterar uppgifter rörande personal på EA. Särskild aktivitet att säkerställa att denna hantering är korrekt.</p> <p>I ett tidigt skede utsågs ägare för mappar. De som utsågs på EA kontaktas för att ge lägesbild avseende hanteringen.</p>

Kommentarer	<p>Dataskydd vid ny- och vidareutveckling av it fungerar genomgående väl på EA. Produktägare/uppdragsledare på it bidrar också aktivt till detta.</p> <p>Systematik vad gäller kontroller av personuppgiftsbehandlingen inom befintliga it-stöd, information i mappar etc brister dock.</p>
Ansvarig	EA Kansli initierar och samordnar åtgärder enligt ovan.
Tidplan	30 juni.



## HR-avdelningens åtgärdsförslag utifrån Internrevisionens granskning av Polismyndighetens ledning och styrning av dataskyddsarbetet

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	HR-avdelningen ska säkerställa relevanta och ändamålsenliga forum för styrning, samordning och kanalisering av dataskyddsfrågor inom avdelningens ansvarsområden.
Kommentarer	Idag har samtliga organisatoriska enheter direkt underställda avdelningsnivån utsedda GDPR-samordnare. HR-avdelningens kansli har ansvar för att samordna och koordinera avdelningens dataskyddsarbete. I det arbetet ingår att säkerställa relevanta och ändamålsenliga forum på övergripande nivå, säkerställa administrativa strukturer på avdelningsnivå samt samverka med rättsavdelningen löpande.
Ansvarig	HR-avdelningen (kansli)
Tidplan	Klart senast 2024-06-31

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	HR-avdelningen ska, säkerställa en ändamålsenlig kontroll och uppföljning av personuppgiftsbehandlingar inom avdelningens ansvarsområden
Kommentarer	<p>HR avdelningen har genomfört ett arbete med att kartlägga vilka kontroller som genomförs utifrån avdelningens processansvar enligt riktlinjerna för intern styrning och kontroll. Ett nästa steg är att ta fram ändamålsenliga arbetssätt på övergripande nivå som stödjer avdelningens processansvar samt verksamhetsansvariga chefer.</p> <p>Kontroll och uppföljning av personuppgiftsbehandlingar utgör en del i det arbetet, i dag sker kontroller inom området men inte enhetligt och strukturerat.</p>
Ansvarig	HR-avdelningen (kansli)
Tidplan	Klart senast 2024-12-31



## FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	KA:s representant/samordnare är med i personuppgiftsnätverket (MPN). Arbetet med dataskyddsfrågor följs upp i KA:s riskportfölj vilket innebär att samtliga som behöver få information får det vid uppföljning (båda leden)
Kommentarer	I dagsläget löper arbetet med dataskyddsfrågor på inom avdelningen. VSA från KA kansli är samordnare för dataskyddsfrågor och har kontakt med funktions inom avdelningen som jobbar med dessa frågor. Uppföljning av dataskyddsarbete görs tertialvis då dessa finns med i vår riskportfölj vilket innebär att det kanaliseras ut i avdelningen för att kunna göra uppföljningen.
Ansvarig	KA kansli
Tidplan	Åtgärdad

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	KA kansli tar fram en struktur över hur uppföljning och egenkontroller ska ske och dokumenteras inom avdelningen.
Kommentarer	Uppföljning och egenkontroller genomförs inom avdelningen, däremot saknas avdelningsgemensam rutin för att göra det enhetligt. KA kansli tar fram en rutin som sedan kommer att kommuniceras ut inom avdelning. I arbetet får KA stöd av RA.
Ansvarig	KA kansli
Tidplan	Uppstart 2024 – Tertial 2. Slutfört 2025 – Tertial 3

Datum  
2024-04-03

Diariernr (åberopas)  
A559.871/2023

Saknr  
977

## FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	NFC ska se över personuppgiftsnätverk forensiks uppdrag och sammansättning i syfte att styra, samordna och kanalisera dataskyddsfrågor.
Kommentarer	NFC har ett nätverk för personuppgiftshantering. Dess uppdrag kopplat till dataskyddsfrågor kommer att ses över, och i sammanhanget också nätverkets sammansättning. De krav som följer av den nya biometrilagstiftningen kan också påverka hur åtgärden genomförs.
Ansvarig	NFC kanslichef.
Tidplan	Översynen ska vara genomförd senast 2024-09-30.

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	NFC ska kopplat till projektet Biometri 2025 se över styrningen av biometriska register inom den forensiska processen, i syfte att också säkerställa en ändamålsenlig kontroll och uppföljning av personuppgiftsbehandlingar.
Kommentarer	Projektet Biometri 2025 har påbörjat ett omfattande arbete under våren 2024 i syfte att kunna omhänderta den nya lagstiftningen. Arbetet inkluderar bland annat att upprätta styrdokument och registervårdsplan för de nya och samlade biometriregistret, vilket kommer att innefatta de nuvarande dna-registren, fingeravtrycks- och signalementsregistren men även de kommande biometrierna. Projektet drivs tillsammans med Noa.
Ansvarig	NFC kanslichef.
Tidplan	Arbetet ska vara klart tills den nya lagstiftningen träder i kraft, vilket beräknas ske under 2025.



## FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	<p>Det formella ansvaret för personuppgiftsbehandling inom Noa ska omfördelas. Syftet är att stärka styrningen och samordningen och förutsättningarna för samverkan inom avdelningen och myndigheten. Ärendet bereds sedan hösten 2023 inom Noa. Beslut förväntas innan sommaren.</p> <p>Noa kommer också att inventera vilka samverkansforum som finns och som fungerar idag. Vidare ska polisregioneras och enheternas vid Noas krav och behov identifieras.</p> <p>Noa avser också att intensifiera kommunikationen och samråd med de som behandlar personuppgifter genom att inrikta, prioritera och samordna ansvaret för den personuppgiftsbehandling som sker inom ramen för huvudprocesserna BF, UL och SE. I det ingår till exempel att ta fram en lämplig ordning för att sprida information till berörda.</p>
Kommentarer	-
Ansvarig	cNoa
Tidplan	Åtgärderna ska ha genomförts senast 2024-12-31

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	Noa ska inventera befintliga dokumentationer av personuppgiftshandlingar och registervårdsplaner vad avser innehåll, hantering, gallring och behörigheter och vid behov ta fram nya eller förändrade dokumenterade rutiner för att säkerställa en ändamålsenlig kontroll och uppföljning.



	<p>Noa ska inventera befintliga kompetenser och samordnare inom data-skyddsområdet för intern och extern tillsyn samt inrätta ett system för samordning för att omhänderta Noas identifierade av samordning och incidenthantering och kompetensförsörjning.</p> <p>Noa ska se till att det finns en samlad förteckning över de medarbetare som fullgör arbetsuppgifter inom ramen för ansvaret för personuppgiftsbehandling, bl.a. avseende dokumentation av personuppgiftsbehandlingar till myndighetens förteckning.</p> <p>Noa ska se till att kompetenshöjande insatser genomförs vid behov.</p>
Kommentarer	
Ansvarig	cNoa
Tidplan	Åtgärderna ska vara genomförda senast 2025-06-30



## FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.1	
Åtgärder	<ol style="list-style-type: none"><li>1) Rättsavdelningen kommer att se över Polismyndighetens riktlinjer för samordning av personuppgiftsfrågor (PM 2019:30).</li><li>2) Rättsavdelningen kommer att gå igenom dataskyddsbudens arbetsuppgifter i samband med pågående översyn och uppdatering av styrdokument på dataskyddsområdet.</li><li>3) Rättsavdelningen ska göra en inventering av vilket behov av myndighetsgemensamma stödjande dokument inom dataskyddsområdet som ansvariga för personuppgiftsbehandling har. Utifrån resultatet ska RA överväga vilka ytterligare myndighetsgemensamma stödjande dokument inom dataskyddsområdet som ska tas fram.</li></ol>
Kommentarer	
Ansvarig	Rättsavdelningen, RSS
Tidplan	<ol style="list-style-type: none"><li>1) 2025-08-31</li><li>2) 2025-12-31</li><li>3) 2025-04-30</li></ol>

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	Rättsavdelningen ska göra en översyn av de behandlingar av personuppgifter som ryms inom avdelningens ansvarsområde samt se över och vid behov säkerställa lämpliga forum för styrning, samordning och kanalisering av dataskyddsfrågor inom det egna ansvarsområdet. Avdelningen kommer i första hand vid behov att använda befintliga forum för styrning, samordning och kanalisering av dataskyddsfrågor inom respektive område.

Kommentarer	
Ansvarig	Respektive personuppgiftsansvarig enligt processägarens delegation
Tidplan	2025-06-30

#### Åtgärder med anledning av internrevisionens rekommendation 4.4.1

Åtgärder	Rättsavdelningen ska göra en intern översyn över befintliga kontroll- och uppföljningsmekanismer och vid behov vidta åtgärder för att säkerställa en ändamålsenlig av personuppgiftsbehandling inom det egna ansvarsområdet. Det kan t.ex. innebära att i anmälningar till personuppgiftsförteckningen ange vilken löpande eller särskild registervård som ska anmälas samt vilka regelbundna kontroller som ska göras och när/hur de ska rapporteras till processledaren.
Kommentarer	
Ansvarig	Respektive personuppgiftsansvarig enligt processägarens delegation
Tidplan	2025-06-30

#### Åtgärder med anledning av internrevisionens rekommendation 4.4.2

Åtgärder	Rättsavdelningen ska göra en genomgång av styrdokument och rutiner på dataskyddsområdet och se över dataskyddsombudens uppgifter för att säkerställa att ianspråktagande av dataskyddsombudens tid sker med beaktande av dataskyddsombudens granskningsuppdrag.
Kommentarer	
Ansvarig	Rättsavdelningen, RSS
Tidplan	2025-12-31

## FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	Processägarskapet inför en återkommande punkt i årsplaneringen i det nationella räddningsrådet.
Kommentarer	Åtgärden syftar till att verksamhetsansvariga påminns om sitt ansvar att genomföra översyn och/eller gallring av sina upprättade personuppgiftssamlingar inom ämnesområdet.
Ansvarig	Polisregion Nord, Processledare Marcus Grahn
Tidplan	Årligen fr.o.m. 2024. GENOMFÖRT

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	<p>Processägarskapet inkluderar/hänvisar/utvecklar metodstöd till verksamheten för att underlätta för verksamheten att kontinuerligt granska sina personuppgiftshandlingar i kommande omarbetning av metodstöd kopplat till ämnet.</p> <p>Utbildning/Information om ämnet och vilka krav detta innebär kommer att utföras i det nationella räddningsrådet under oktober månad.</p> <p>Därefter kommer frågan att stämmas av årligen vid det nationella räddningsrådet.</p>
Kommentarer	<p>I kommande uppdatering skrivs det in vilka personuppgiftshandlingar som är upprättade för verksamhetsområdet samt beskrivning av ansvarsförhållanden och exempel på tillvägagångssätt för gallring.</p> <p>Till detta kopplas ansvaret med att granska, gallra eller korrigera uppgifter samt med vilket intervall det ska utföras.</p>

	Rekommendationer till verksamhetsansvariga att söka stöd för arbetet vid uppkomna frågetecken via rättsavdelningens dataskyddsjurister kommer införas i metodstödet.
Ansvarig	Polisregion Nord, Processledare Marcus Grahn.
Tidplan	I början av oktober 2024 genomförs ett informationspaket till den ansvariga och därefter som en del i det nya metodstödet. Arbetet är påbörjat och beräknas vara klart under 2025.

Datum  
2024-03-1304

Diariennr (åberopas)  
A559.871/2023

Saknr  
977

## FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	Polisregion Stockholm avser att skapa och aktivt driva ett processindelad personuppgiftsnätverk (PPN) avseende den personuppgiftsbehandling inom polisrytteriet och sjöpolisverksamheten som faller inom ramen för chefen för polisregion Stockholms ansvar enligt arbetsordningen.
Kommentarer	Åtgärdsförslaget har stämts av med tf chef regionkansliet Anette Öberg efter föredragning av juristerna Mattias Aspegren och Tomas Alvarsson
Ansvarig	Regionpolischef Mattias Andersson
Tidplan	Åtgärden ska vara genomförd senast 2024-06-01

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	Polisregion Stockholm avser att se över behov och tillämpning av registervårdsplaner eller annan, mer ändamålsenlig, kontroll och uppföljning av personuppgiftsbehandling avseende den personuppgiftsbehandling inom polisrytteriet och sjöpolisverksamheten som faller inom ramen för chefen för polisregion Stockholms ansvar enligt arbetsordningen.
Kommentarer	Åtgärdsförslaget har stämts av med tf chef regionkansliet Anette Öberg efter föredragning av juristerna Mattias Aspegren och Tomas Alvarsson
Ansvarig	Regionpolischef Mattias Andersson
Tidplan	Åtgärden ska vara genomförd senast 2024-12-31

Datum  
2024-04-03Diariernr (åberopas)  
A559.871/2023Saknr  
977

Internrevisionen

**Polisregion Västs åtgärdsförslag med anledning av internrevisionens rekommendationer**

<b>Åtgärder med anledning av internrevisionens rekommendation 3.4.2</b>	
Åtgärder	<p>Polisregionen avser färdigställa det påbörjade arbetet avseende ett "dataskyddsprogram" i syfte att tydliggöra processägaransvar och lämpliga kommunikationsvägar. Detta innefattar i huvudsak:</p> <ul style="list-style-type: none"><li>- Kartläggning (pågående) av personuppgiftsbehandlingar hänförliga till processägarskapet för NPHT</li><li>- Revidera/ta fram nödvändig dokumentation för personuppgiftsbehandling</li><li>- Uppföljning och utvärdering av nuvarande forum/nätverk</li><li>- Involvering av dataskyddssamordnaren på ett tidigt stadie vid framtagande av nya it-stöd</li></ul>
Kommentarer	<p>Nuvarande forum består av dataskyddssamordnaren och representanter från NPHT. Kommunikationen sker såväl fysiskt som digitalt. Programmet och dess innehåll (utkastnivå) har diskuterats med representant från RSS. Kontakt har även initierats med IT.</p>
Ansvarig	<p>Polisregion Väst, regionkansli Väst, dataskyddssamordnare, Emilia Heiman</p>
Tidplan	<p>Åtgärden ska vara genomförd 2024-06-30</p>

<b>Åtgärder med anledning av internrevisionens rekommendation 4.4.1</b>	
Åtgärder	<p>Polisregion Väst ska ha en rutin för genomförande av kontinuerliga registervårdskontroller av ostrukturerat material som hanteras på gemensamma kataloger.</p>
Kommentarer	<p>En mer utökad registervårdskontroll inleddes i januari 2024. Denna är ännu inte avslutad. Tidigare har dialog förts med ansvariga på NPHT angående hantering av gemensamma kataloger.</p>

Ansvarig	Polisregion Väst, regionkansli Väst, dataskyddssamordnare, Emilia Heiman
Tidplan	Åtgärden ska vara genomförd 2024-06-30

<b>Åtgärder med anledning av internrevisionens rekommendation 4.4.1</b>	
Åtgärder	Polisregion Väst avser vidareutveckla och implementera dataskyddsprocess i redan befintligt ISK-arbete.
Kommentarer	Dialog förs regelbundet med regional ISK-samordnare. Under hösten 2023 har underlag inhämtats från den fördjupade riskanalysen för att utröna lämpliga sätt att följa upp. Ambitionen är att implementering ska ske befintlig ISK-process med beaktande av bl.a. riskportföljer, åtgärdsplaner, uppföljning och avstämning.
Ansvarig	Polisregion Väst, regionkansli Väst, dataskyddssamordnare, Emilia Heiman
Tidplan	Åtgärden ska vara genomförd 2024-12-31





Datum  
2024-04-22

Diariennr (åberopas)  
A559.871/2023

Saknr  
977

### FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	RPCK avser att tillse att frågan lyfts internt i relevanta gruppsammanhang vid jämna mellanrum som en påminnelse och i övriga relevanta forum, t.ex. nationella kanslichefsforumet. Syftet är att öka produktionen och medvetenheten.
Kommentarer	
Ansvarig	Chef RPCK eller av denne utsedd
Tidplan	30 juni 2024

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	RPCK kommer under 2024 införa en tydligare rutin/tydligare omhändertagande för kontroll av personuppgiftsbehandling samt att det löpande säkerställs om rutinens målsättning.
Kommentarer	
Ansvarig	Chef RPCK eller av denne utsedd
Tidplan	30 juni 2024



Datum  
2024-03-13

Diariernr (åberopas)  
A559.871/2023

Saknr  
977

## FORMULÄR FÖR IFYLLANDE AV ÅTGÄRDSFÖRSLAG MED ANLEDNING AV INTERNREVISIONENS REKOMMENDATIONER

Åtgärder med anledning av internrevisionens rekommendation 3.4.2	
Åtgärder	Säka kommer att samla avdelningens processledare för att informera och samordna dataskyddsarbetet samt inventerandet av lämpliga forum för processledarna.
Kommentarer	
Ansvarig	Säka kansli
Tidplan	2024-06-03

Åtgärder med anledning av internrevisionens rekommendation 4.4.1	
Åtgärder	Säka ska förankra rekommendationerna med processledarna för att säkerställa ett implementerande av personuppgiftsbehandlingen i processledarnas arbete med att ta fram styrdokument samt utbildningar.
Kommentarer	
Ansvarig	Säka kansli
Tidplan	2024-06-03