



Datum

2021-03-05

Diarienummer

A126.614/2020

Saknr

128

Er referens

DI-2020-2719

Integritetsskyddsmyndigheten  
imy@imy.se

FÖRVALTNINGSRÄTTEN  
I STOCKHOLM  
Avdelning 34  
INKOM: 2021-03-15  
MÅLNR: 4756-21  
AKTBIL: 11

FÖRVALTNINGSRÄTTEN  
I STOCKHOLM

2021 -03- 15

Målnr:.....  
Aktbil:.....Avd:.....

## Komplettering av tidigare inskickat överklagande avseende Clearview AI

### Kompletterande överklagande och yrkanden

Polismyndigheten har den 1 mars 2021 överklagat Integritetsskyddsmyndighetens (IMY) beslut daterat den 10 februari 2021. I överklagandet angavs att Polismyndigheten skulle återkomma med yrkanden och grunder.

Polismyndigheten yrkar att myndigheten inte ska föreläggas att betala en sanktionsavgift, alternativt att sanktionsavgiften ska sättas ned.

### Grunder

Polismyndigheten är personuppgiftsansvarig för all personuppgiftsbehandling i myndighetens verksamhet. Polismyndigheten har i egenskap av personuppgiftsansvarig vidtagit de lämpliga tekniska och organisatoriska skyddsåtgärder som krävs enligt 3 kap. 2 § BDL.

Polismyndigheten bestrider att myndigheten har brutit mot bestämmelserna i 2 kap. 12 § och 3 kap. 7 § första stycket BDL i det aktuella fallet.

Om Polismyndigheten ska anses ha brutit mot någon eller några av dessa bestämmelser är överträdelsen inte så allvarlig att den motiverar en sanktionsavgift.

Även om Polismyndigheten bestrider att myndigheten har brutit mot aktuella bestämmelser har myndigheten ingen invändning mot de förelägganden som IMY har meddelat och har redan börjat arbeta med att tillgodose dem.

### Utveckling av talan

#### Tillsyn

Polismyndigheten står under regelbunden tillsyn av både IMY och Säkerhets- och integritetsskyddsnämnden (SIN). Under år 2020 hanterade Polismyndigheten ett tiotal tillsyner som rör dataskyddsregelverken och dessutom ett stort antal ärenden om kontroll på begäran av enskild (SIN) eller s.k. laglighetskontroll (IMY).

Polismyndigheten och tillsynsmyndigheterna har således ett välutvecklat samarbete som går ut på att tillsynsmyndigheten ställer de konkreta frågor som de vill ha svar på inom ramen för en tillsyn. Vissa tillsyner består av hundratals sådana frågor. För att möjliggöra en effektiv process har Polismyndigheten hittills fokuserat på att lämna tydligast möjliga svar på de frågor som tillsynsmyndigheten ställt i det aktuella ärendet. Polismyndigheten ger regelmässigt inte på eget initiativ in omfattande dokumentation till styrkande av de tekniska och organisatoriska åtgärder som myndigheten har vidtagit på dataskyddsområdet i stort, om det inte efterfrågas.

Även i det här ärendet har IMY ställt ett antal riktade och avgränsade frågor till Polismyndigheten. Enligt Polismyndighetens arbetsordning (PM 2020:46) ska rättsavdelningen ansvara för yttranden till tillsynsmyndigheterna. Rättsavdelningen, som vanligtvis inte har förhandskänedom om de omständigheter som tillsynsmyndigheten frågar om, vidtar olika interna utredningsåtgärder med anledning av tillsynerna. Så har även skett i det här fallet och myndigheten har svarat utförligt på de frågor som IMY ställt.

IMY har dock inte ställt några frågor om vilka skyddsåtgärder i form av riktlinjer, utbildningar, kommunikationskanaler etc. som myndigheten har tagit fram i enlighet med kraven i 3 kap. 2 § BDL. Enligt Polismyndigheten har IMY därför inte gjort sin bedömning utifrån ett korrekt underlag.

### ***Personuppgiftsansvar och intern ansvarsfördelning***

Polismyndigheten är personuppgiftsansvarig för all personuppgiftsbehandling i myndighetens verksamhet. Enligt Polismyndighetens arbetsordning är en processägare som utgångspunkt ansvarig för myndighetens personuppgiftsbehandling inom sitt ansvarsområde. Processägaren ska inom ramen för processansvaret säkerställa att personuppgifter behandlas enhetligt och författningsenligt inom hela myndigheten för de definierade ändamålen med behandlingen.

Det är utredningsenheten, som är placerad under Nationella operativa avdelningen (NOA), som enligt arbetsordningen ansvarar för den personuppgiftsbehandling som sker av medarbetare inom it-brottscentrum och spaningssektionen. Även de anställda som använt applikationen Clearview AI (Clearview) inom polisregion Syd arbetar på spaningssektionen. Applikationen presenterades av Europol vid en utbildning i Haag.

### ***Tekniska och organisatoriska åtgärder***

Polismyndigheten anser att myndigheten har vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de personuppgiftsbehandlingar som vidtas inom myndigheten är författningsenliga och att de registrerades rättigheter skyddas. De viktigaste åtgärder som vidtagits framgår nedan.



## Nationella riktlinjer

### *Riktlinjer för processägares instruktioner om personuppgiftsbehandling*

Av Polismyndighetens riktlinjer för processägares instruktioner om personuppgiftsbehandling (PM 2020:10), Bilaga 1, framgår bland annat att en processägare enligt Polismyndighetens arbetsordning som utgångspunkt är ansvarig för myndighetens personuppgiftsbehandling inom sitt ansvarsområde. Processägaren eller den som är ansvarig för personuppgiftsbehandlingen ska inom ramen för processansvaret säkerställa att personuppgifter behandlas enhetligt och författningenligt inom hela myndigheten för de definierade ändamålen med behandlingen. För att säkerställa detta krävs att processägaren eller den som är ansvarig för personuppgiftsbehandlingen ger instruktioner om hur personuppgifter ska behandlas samt fördelar arbetsuppgifter till en eller flera medarbetare.

Riktlinjerna riktar sig till processägare och de som är ansvariga för personuppgiftsbehandling. Riktlinjerna reglerar:

1. i vilka situationer som processägaren behöver ge instruktioner om personuppgiftsbehandling genom styrdokument och när det är tillräckligt att det sker exempelvis genom dokumentation över personuppgiftsbehandling i myndighetens förteckning
2. hur styrdokument med instruktioner om personuppgiftsbehandling ska utformas, i de fall som det behövs.

Det framgår även att processägaren i styrdokument uttömmande ska reglera vilka it-system och/eller lagringsytor eller motsvarande som ska eller får användas för personuppgiftsbehandlingen samt vilka som regelmässigt ska eller får använda uppgifterna som omfattas av personuppgiftsbehandlingen.

### *Riktlinjer för dataskydd vid verksamhetsutveckling*

Polismyndigheten har även tagit fram de riktlinjer för dataskydd vid verksamhetsutveckling (PM 2018:38), Bilaga 2, som gavs in inom ramen för tillsynen. Av dem framgår bland annat vad en konsekvensbedömning är och att en konsekvensbedömning ska göras om en ny typ av behandling kan antas medföra särskild risk för intrång i registrerades personliga integritet. Det framgår även att en konsekvensbedömning ska göras om betydande förändringar av redan pågående behandlingar kan antas leda till sådan risk. Av riktlinjerna framgår dessutom vem som är ansvarig för att ta fram underlag till konsekvensbedömningen och vem som ska utföra konsekvensbedömningen.

Det framgår vidare att Polismyndigheten är skyldig att föra en förteckning över den personuppgiftsbehandling som den är personuppgiftsansvarig för. Ett syfte med förteckningen är att visa att behandlingen sker i överensstämmelse med författning. Ett annat syfte är att underlätta såväl tillsynsmyndighetens kontroll, som intern kontroll och granskning av den personuppgiftsbehandling som utförs.

*Riktlinjer för samordning av personuppgiftsfrågor*

Av Polismyndighetens riktlinjer för samordning av personuppgiftsfrågor (PM 2019:30), Bilaga 3, framgår bland annat att ansvar för personuppgiftsbehandling utgår från det i arbetsordningen fördelade processansvaret. För att omhänderta personuppgiftsfrågor på ett enhetligt, ändamålsenligt och rättssäkert sätt inom myndigheten krävs samverkan mellan å ena sidan processägare med ansvar för personuppgiftsbehandling och å andra sidan den organisation som behandlar personuppgifterna. Riktlinjerna fastställer en arbetsmetod som innebär en sammanhållen struktur av personuppgiftsnätverk inom Polismyndigheten, samt redogör för vilka frågor nätverken hanterar, vilka som ingår samt formerna för hur arbetet bedrivs. På detta sätt anger riktlinjerna formen för hur processägare på personuppgiftsområdet ska säkerställa delaktighet, engagemang och förståelse genom förankring och kommunikation med berörda delar av verksamheten

Av riktlinjerna framgår bland annat att det är obligatoriskt för processägarna att ha processindelade personuppgiftsnätverk. Ett stort antal sådana nätverk har inrättats, bland annat inom Noa/utredningsenhetens ansvarsområde.

*Riktlinjer för särskild registervård av personuppgiftsbehandlingar*

Av Polismyndighetens riktlinjer för särskild registervård av personuppgiftsbehandlingar (PM 2016:36), Bilaga 4, framgår bland annat att löpande registervård ska ske för alla personuppgiftsbehandlingar. Med löpande registervård avses framförallt åtgärder som utförs som en integrerad del i verksamhetens hantering av informationen, t.ex. i samband med registrering. Det innefattar även åtgärder som vidtas i enstaka fall när felaktigheter upptäcks.

*Riktlinjer avseende informationsbehandling med stöd av it*

Vidare finns det framtagna riktlinjer avseende informationsbehandling med stöd av it (PM 2017:4), Bilaga 5, som riktar sig till samtliga medarbetare. Dessa riktlinjer reglerar bland annat hur Polismyndighetens it-miljö får användas samt hur anskaffning och utveckling av produkter ska gå till.

*Riktlinjer för mobil elektronisk utrustning*

Polismyndighetens riktlinjer för mobil elektronisk utrustning (PM 2016:43) Bilaga 6, gäller för tjänstemobiler. Av riktlinjerna framgår bland annat att endast mobiltelefoner, surfplattor och motsvarande som tillhandahålls av arbetsgivaren får användas i tjänsten. It-utrustningen är personlig och ska inte användas av andra. Mobil it-utrustning ska förvaras säkert. De mobila enheter som har tillgång till polisens it-system har en tjänstedel som endast får användas i tjänsten. Av riktlinjerna framgår även att användning av mobil it-utrustning i strid med riktlinjerna kan leda till att arbetsgivaren vidtar disciplinära åtgärder.



## Nationella utbildningar

### *Introduktionsutbildning i informationssäkerhet*

Samtliga anställda vid Polismyndigheten genomgår en obligatorisk introduktionsutbildning i informationssäkerhet som fokuserar på frågor kopplade till it-utrustning och hur den får användas. Utbildningen tar även upp vissa aspekter som rör skyddet för personuppgifter.

### *Dataskyddsutbildningar*

Polismyndigheten har tagit fram flera särskilda utbildningar på olika nivåer avseende dataskydd, bland annat:

- Grundläggande dataskyddsutbildning
- Dataskyddsutbildning för brottsbekämpande ändamål
- Dataskyddsutbildning för icke brottsbekämpande ändamål

Samtliga dessa utbildningar är tillgängliga för alla inom myndigheten och i vissa fall har processägare angett att genomgången utbildning är en förutsättning för att få behörighet till särskilda it-stöd. Utöver ovan angiva utbildningar finns det även specifika dataskyddsutbildningar riktade mot särskilda verksamhetsområden.

Polismyndigheten har dessutom nyligen tagit fram en ny introduktionsutbildning i dataskydd som riktar sig till samtliga medarbetare och som berör många frågor av praktisk natur. Polismyndigheten har redan påbörjat en översyn av den nya utbildningen i syfte att uttryckligen förklara att externa applikationer inte får laddas ner och användas i tjänsten utan en föregående bedömning av relevanta instanser, vilket är viktigt både ut ett dataskyddsperspektiv och ett informationssäkerhetsperspektiv.

### *Information på intranätet*

På Polismyndighetens intranät finns omfattande och övergripande information om personuppgiftsbehandling tillgänglig för samtliga polisanställda. Bland annat finns information om framtagna riktlinjer och utbildningar på dataskyddsområdet. Informationspaketet är en följd av myndighetens mångåriga och löpande arbete med att höja den grundläggande kunskapen om dataskyddsregelverket och vikten av skyddet för personuppgifter.

### *Processägarens vidtagna åtgärder*

Som framgått ovan är det obligatoriskt för processägarna att ha processindelade personuppgiftsnätverk. I januari 2019 anställdes en samordnare av dataskydds- och informationssäkerhetsrättsliga frågor inom utredningsenhetens ansvarsområde. I dataskyddsamordnarens arbete ingår bland annat att lämna underlag till myndighetens förteckning gällande de personuppgiftsbehandlingar som sker eller kommer att påbörjas inom det aktuella ansvarsområdet. Inom ramen för det arbetet har dataskyddssamordnaren träffat både verksamhetsansvariga och grupper inom olika sektioner och informerat om hur en personuppgiftsanmälan går till. Dataskyddssamordnaren har även vid flera tillfällen

haft informations- och avstämningsmöten med processledare för de olika verksamheterna i dataskyddsrättsliga frågor och gått igenom viktiga aspekter i BDL och PBDL.

Chefen för nationella operativa avdelningen har även tagit fram riktlinjer avseende ansvar för personuppgiftsbehandling i utredningsverksamheten, (PM 2017:38), Bilaga 7.

#### Sammanfattning tekniska och organisatoriska åtgärder

Som framgått ovan delar Polismyndigheten bedömningen att myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar enligt 3 kap. 1 § BDL och 2 kap. 1 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalogens område (PBDL) och att Polismyndigheten därför ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av personuppgifter är författningsenlig enligt 3 kap. 2 § BDL. Polismyndigheten bedömer dock, till skillnad från IMY, att myndigheten har vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa författningsenlig behandling, varav de viktigaste har redogjorts för ovan.

Som framgår av handlingarna i tillsynsärendet har Polismyndigheten efter egna utredningsåtgärder inom ramen för tillsynen identifierat att ett fåtal av ca 33 000 anställda har behandlat personuppgifter i strid med framtagna riktlinjer och utbildningar vid användandet av applikationen Clearview. Att några få medarbetare behandlat personuppgifter på ett felaktigt sätt inom ramen för sin tjänst fråntar inte myndigheten sitt personuppgiftsansvar men bör inte innebära en presumtion för att myndigheten inte har vidtagit lämpliga organisatoriska och tekniska åtgärder enligt 3 kap. 2 § BDL.

Enligt 3 kap. 1 § brottsdataförordningen (2018:1202) ska de organisatoriska och tekniska åtgärder som den personuppgiftsansvarige ska vidta enligt 3 kap. 2 och 3 §§ BDL vara *rimliga* med hänsyn till behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen. Polismyndigheten anser inte att det är rimligt att det ska krävas att hundra procent av de anställda ska göra hundra procent rätt vid varje behandlingsåtgärd som sker inom myndighetens personuppgiftsansvar för att myndigheten ska anses ha uppfyllt kraven på lämpliga förebyggande åtgärder enligt dataskyddsregleringen.

IMY påtalar att applikationen använts av anställda inom olika verksamhetsområden, vilket enligt dem tyder på att myndigheten saknar upparbetade och väl fungerande informationskanaler för att kommunicera vidtagna organisatoriska och tekniska åtgärder till de anställda. Polismyndigheten menar att det inte stämmer. Spridningen av dataskyddsombudets rekommendation inom myndigheten i nu aktuell fråga är ett tydligt och verksamt exempel på att myndigheten har förmåga att sprida information rörande dataskyddsfrågor inom myndigheten eftersom behandlingen upphörde omedelbart därefter och sedan inte återupptagits. Denna information har spridits på Polismyndighetens intranät, där ovan riktlinjer och utbildningar finns att hitta.



Polismyndigheten har ovan redogjort för de viktigaste organisatoriska och tekniska åtgärder som myndigheten har vidtagit. Att några anställda trots detta ändå har gjort fel är naturligtvis beklagligt, vilket också har renderat i en anmälan om eventuella tjänstefel till avdelningen för särskilda utredningar. Det visar dock inte på att det föreligger systematiska brister inom myndigheten som IMY verkar mena.

Polismyndigheten anser att det hade varit skillnad om myndigheten inte hade några relevanta riktlinjer eller rutiner på området, inte genomförde utbildningar för personalen, saknade kompetens eller möjligheter att utföra konsekvensbedömningar, medvetet tagit en genväg eller medvetet underlåtit att följa gällande rätt eller liknande.

### **Konsekvensbedömning**

Polismyndigheten ska genomföra en konsekvensbedömning vid viss ny typ av behandling eller betydande förändringar av en redan pågående behandling enligt 3 kap. 7 § BDL. Som framgått ovan har Polismyndigheten tagit fram riktlinjer för att säkerställa att så sker.<sup>1</sup> Riktlinjerna har också resulterat i att myndigheten tagit fram ett stort antal konsekvensbedömningar i sin verksamhetsutveckling och vid flera tillfällen också genomfört strukturerade förhandssamråd med IMY. Riktlinjerna har också getts in till IMY inom ramen för tillsynen.

Som framgått ovan delar Polismyndigheten inte IMY:s bedömning om att det är bristen på organisatoriska åtgärder som har medfört att anställda använt applikationen utan att myndigheten dessförinnan har genomfört en konsekvensbedömning av personuppgiftsbehandlingen. Användandet av applikationen har inte varit sanktionerad av Polismyndigheten utan har bestått av att några få medarbetare under en begränsad tid testat en gratis applikation utan att dessförinnan ha informerat eller frågat sina chefer. Att några få medarbetare behandlat personuppgifter på ett felaktigt sätt inom ramen för sin tjänst fråntar inte myndigheten ett ansvar men det bör inte per automatik anses ge uttryck för bristande tekniska eller organisatoriska åtgärder. I det här fallet har inte myndigheten känt till att applikationen testats och följden har därför oundvikligen blivit att några rättsliga bedömningar inte har kunnat göras i enlighet med gällande rutiner och riktlinjer. Under sådana förhållanden anser Polismyndigheten inte att myndigheten kan klandras särskilt för att någon konsekvensbedömning inte har genomförts.

### **Behandling av biometriska uppgifter**

Med biometriska uppgifter avses personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen.<sup>2</sup> Biometri är således ett samlingsnamn för sådan automatiserad

<sup>1</sup> Ovan nämnda riktlinjer för dataskydd vid verksamhetsutveckling (PM 2018:38).

<sup>2</sup> 1 kap. 6 § brottsdatalagen.

teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig.<sup>3</sup> I dataskyddsförordningen<sup>4</sup> och brottsdatadirektivets<sup>5</sup> definition av biometriska uppgifter anges ansiktsbilder och fingeravtrycksuppgifter som exempel på sådana uppgifter.<sup>6</sup> Som framgår av förarbetena till brottsdatalagen kan det leda tanken till att vanliga fotografier och filmer skulle omfattas av definitionen. Om de inte bearbetas tekniskt genom en särskild metod som syftar till identifiering faller de dock utanför definitionen. Om de däremot bearbetas i exempelvis ett ansiktsigenkänningsprogram så att det går att identifiera personer på bilden eller filmen omfattas de av definitionen.<sup>7</sup> Biometriska uppgifter får endast behandlas om det är absolut nödvändigt för ändamålet med behandlingen enligt 2 kap. 12 § BDL och 2 kap. 4 § PBDL.

Som framgått ovan vidgår Polismyndigheten att dessa frågor inte har utretts av myndigheten inför den behandling som enstaka medarbetare har utfört genom att testa det aktuella verktyget i ett fåtal fall. Polismyndigheten vill ändå framhålla att det vid utredning av specifika fall av sexuella övergrepp mot barn eller för att identifiera individer kopplade till grov organiserad brottslighet kan vara en absolut nödvändig utredningsåtgärd att göra en biometrisk jämförelse mellan utredningsmaterial och ett tillgängligt jämförelsematerial. Exempelvis för att kunna identifiera en gärningsperson eller ett offer. Polismyndigheten anser därför sammantaget inte att myndigheten har behandlat personuppgifter i strid med 2 kap. 12 § BDL.

### **Sanktionsavgift**

IMY har angett att det är överträdelserna av 2 kap. 12 § samt 3 kap. 2 § och 7 § första stycket BDL som föranleder sanktionsavgiften. Som framgått ovan anser Polismyndigheten inte att myndigheten har överträtt nämnda bestämmelser. För det fall det bedöms att Polismyndigheten har överträtt bestämmelserna är det inte motiverat med en sanktionsavgift, i vart fall inte en sanktionsavgift av den här storleken.

Det framgår av BDL att ansvaret för överträdelser är strikt. Strikt ansvar innebär dock inte att sanktionsavgift måste tas ut vid varje överträdelse. Som exempel på situationer när sanktionsavgift bör kunna övervägas nämns i förarbetena till BDL att det satts i system att göra felaktiga behandlingar eller om påpekanden om att det krävs utbildning för att undvika sådant felbeteende inte följs. Det framgår uttryckligen att det inte är rimligt att ålägga en myndighet sanktionsavgift om någon i ett enstaka fall behandlat en personuppgift felakt-

<sup>3</sup> Prop. 2017/18:232, s. 86.

<sup>4</sup> 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.

<sup>5</sup> Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behörig myndighets behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

<sup>6</sup> Art. 3 punkten 13 brottsdatadirektivet.

<sup>7</sup> Prop. 2017/18:232 s. 86.



Chefen för enheten för rättslig styrning och stöd, Eva Lindeblad, har efter fördragning av juristen Karin Höglund beslutat detta överklagande. I den slutliga beredningen har även t.f. gruppchef Linnea Tegernäs deltagit.

#### **POLISMYNDIGHETEN**

  
Eva Lindeblad

  
Karin Höglund

#### **Bilagor:**

1. Polismyndighets riktlinjer för processägares instruktioner om personuppgiftsbehandling (PM 2020:10)
2. Polismyndighetens riktlinjer för dataskydd vid verksamhetsutveckling (PM 2018:38)
3. Polismyndighetens riktlinjer för samordning av personuppgiftsfrågor (PM 2019:30)
4. Polismyndighetens riktlinjer för särskild registervård av personuppgiftsbehandlingar (PM 2016:36)
5. Polismyndighetens riktlinjer avseende informationsbehandling med stöd av it (PM 2017:4)
6. Polismyndighetens riktlinjer för mobil elektronisk utrustning (PM 2016:43)
7. Polismyndighetens riktlinjer avseende ansvar för personuppgiftsbehandling i utredningsverksamheten, (PM 2017:38)