

Polismyndigheten  
Skickas endast per e-post  
registrator.kansli@polisen.se

FÖRVALTNINGSRÄTTEN  
I STOCKHOLM  
Avdelning 34

INKOM: 2021-03-03  
MÅLNR: 4756-21  
AKTBIL: 3

**Diarienummer:**  
DI-2020-2719

**Ert diarienummer:**  
A126.614/2020

**Datum:**  
2021-02-10

# Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens användning av Clearview AI

## Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Polismyndigheten har behandlat personuppgifter i strid med 2 kap. 12 § samt 3 kap. 2 § och 7 § första stycket brottsdatalagen genom att använda applikationen Clearview AI under perioden hösten 2019 till och med 3 mars 2020.

Integritetsskyddsmyndigheten beslutar med stöd av 6 kap. 1 § brottsdatalagen att Polismyndigheten ska betala en sanktionsavgift på 2 500 000 (två miljoner femhundra tusen) kronor.

Integritetsskyddsmyndigheten förelägger Polismyndigheten enligt 5 kap. 7 § första stycket 2 brottsdatalagen att vidta utbildningsåtgärder och övriga organisatoriska åtgärder som krävs enligt 3 kap. 2 § brottsdatalagen för att säkerställa att de rutiner som finns når hela organisationen och att myndigheten därmed kan visa och säkerställa att all behandling av personuppgifter är författningsenlig. Åtgärderna ska ha vidtagits senast den 15 september 2021.

Integritetsskyddsmyndigheten förelägger med stöd av 5 kap. 7 § första stycket 2 brottsdatalagen Polismyndigheten att enligt 4 kap. 2 § brottsdatalagen informera de registrerade, vars personuppgifter Polismyndigheten matat in i Clearview AI, i den utsträckning skyldigheten att lämna information inte är begränsad enligt 4 kap. 5 § brottsdatalagen. Informationen ska ha lämnats senast den 15 september 2021.

Integritetsskyddsmyndigheten förelägger med stöd av 5 kap. 7 § första stycket 2 brottsdatalagen Polismyndigheten att vidta möjliga och relevanta åtgärder för att de personuppgifter som Polismyndigheten matat in i Clearview AI raderas från applikationen. Sådana åtgärder ska ha vidtagits den 15 september 2021.

**Postadress:**  
Box 8114  
104 20 Stockholm

**Webbplats:**  
www.imy.se

**E-post:**  
imy@imy.se

**Telefon:**  
08-657 61 00

## Redogörelse för tillsynsärendet

Integritetsskyddsmyndigheten (IMY), tidigare Datainspektionen, uppmärksammades i februari 2020 genom uppgifter i media på att brottsbekämpande myndigheter i Sverige kunde ha använt sig av applikationen Clearview AI. IMY inledde mot bakgrund av uppgifterna omgående en granskning där Polismyndigheten ombads besvara om myndigheten använt sig av applikationen samt med vilket rättsligt stöd behandling i så fall skett. Av yttranden från Polismyndigheten under våren 2020 framgick att applikationen använts av några anställda inom myndigheten vid ett antal tillfällen utan att myndigheten tillhandahållit applikationen till de anställda. IMY inledde därför en fördjupad granskning av Polismyndighetens användning av Clearview AI.

Clearview AI är en applikation tillhandahållen av ett amerikanskt företag som erbjuder en ansiktsgenkänningstjänst där användaren, efter att ha laddat ner applikationen på en digital enhet, laddar upp en bild som genom biometri matchas mot ett mycket stort antal bilder som skrapats från det öppna internet.<sup>1</sup> Användaren får sedan ett resultat i form av ett antal webbadresser där eventuella matchningar finns.<sup>2</sup>

### Polismyndighetens användning av applikationen Clearview AI

Polismyndigheten har uppgett att applikationen Clearview AI använts vid ett antal tillfällen under perioden hösten 2019 till och med 3 mars 2020.

Det är medarbetare vid den Nationella Operativa Avdelningen (NOA) samt region Syd som har använt sig av Clearview AI. Vid NOA har applikationen använts av totalt sex medarbetare varav fem använt applikationen i operativ verksamhet, bl.a. för att identifiera målsäganden i misstänkta sexualbrott mot barn samt i spaningsverksamheten för att försöka identifiera okända personer vid spaning av grov organiserad brottslighet. Vid polisregion Syd har applikationen använts vid utredning av sexualbrott mot barn samt testats av medarbetare mot bilder i Polismyndighetens s.k. OBS-portal.<sup>3</sup> När Polismyndighetens användning av Clearview AI blev känd genom uppgifter i media gick myndighetens dataskyddsombud ut med en rekommendation om att Nationellt Forensiskt Centrum och NOA skulle klargöra och sprida att sådan användning inte var tillåten.

## Motivering av beslutet

### Polismyndighetens ansvar för anställdas behandling av personuppgifter inom den brottsbekämpande verksamheten

Polismyndigheten är en stor organisation med ett särskilt uppdrag att upprätthålla lag och ordning. Polismyndigheten styrs därtill av tydlig lagstiftning kring hur personuppgifter ska behandlas, särskilt inom den brottsbekämpande verksamheten. Den stora mängd personuppgifter, även känsliga sådana, som myndigheten behandlar samt de långtgående maktbefogenheter Polismyndigheten har gör att myndigheten har ett särskilt ansvar för att personuppgifter behandlas korrekt.

<sup>1</sup> Webbtjänsten uppger att de samlat tre miljarder ansiktsbilder från Facebook, YouTube och miljoner andra webbplatser. IMY rapport 2021:1; Integritetsskyddsrapport 2020 – redovisning av utvecklingen på it-området när det gäller integritet och ny teknik, sid. 70.

<sup>2</sup> <https://clearview.ai>, 2020-11-25.

<sup>3</sup> it-stöd inom Polismyndigheten där underrättelseuppgifter förmedlas till den brottsbekämpande verksamheten.

Polismyndigheten är, som personuppgiftsansvarig, ansvarig för all personuppgiftsbehandling som sker under myndighetens ledning eller på myndighetens vägnar enligt 3 kap. 1 § brottsdatalagen. Det innebär att all personuppgiftsbehandling som utförs vid myndigheten faller under Polismyndighetens personuppgiftsansvar, även den behandling personuppgiftsbiträden, anställda, personer som är att jämföras med anställda (t.ex. inhyrd personal) eller uppdragstagare utför.<sup>4</sup> Även av 2 kap. 1 § lagen (2018:1693) om polisens behandling inom brottsdatalagens område (PBDL) framgår att Polismyndigheten är ansvarig för den personuppgiftsbehandling som utförs vid myndigheten. Det innebär att det är Polismyndighetens skyldighet att tillse att all behandling som sker inom myndigheten har bl.a. en rättslig grund, ett berättigat ändamål och att tillräckliga skyddsåtgärder är på plats genom lämpliga tekniska och organisatoriska åtgärder. Polismyndigheten ska tillse att det finns tydliga riktlinjer och rutiner avseende de it-verktyg som de anställda får använda och att de anställda är tillräckligt utbildade och informerade om hur personuppgifter får behandlas.<sup>5</sup>

Enligt Polismyndigheten är det ett fåtal anställda som använt Clearview AI utan att myndigheten tillhandahållit applikationen till de anställda. Behandlingen har dock skett vid utförande av de anställdas arbetsuppgifter på myndigheten. Behandlingen har dessutom utförts med personuppgifter hämtade från aktuella utredningar och vid majoriteten av tillfällena under pågående brottsutredningar, dvs. under myndighetsutövning. Att det skett utan att myndigheten tillhandahållit Clearview AI eller godkänt användningen av it-verktyget frångår därmed inte Polismyndigheten det ansvar som myndigheten har som personuppgiftsansvarig.

IMY konstaterar mot denna bakgrund att Polismyndigheten är ansvarig för de anställdas behandling av personuppgifter vid användningen av Clearview AI.

### **Polismyndighetens skyldighet att genom tekniska och organisatoriska åtgärder säkerställa och visa att myndighetens personuppgiftsbehandling är författningsenlig**

Som personuppgiftsansvarig har Polismyndigheten enligt 3 kap. 2 § brottsdatalagen en skyldighet att, genom tekniska och organisatoriska åtgärder, säkerställa och kunna visa att myndighetens behandling av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Det ska i varje enskilt fall bedömas vilka sådana åtgärder som behövs med beaktande av bl.a. vilka personuppgifter som behandlas.<sup>6</sup> Organisatoriska åtgärder kan bl.a. vara att anta interna strategier för dataskydd, informera och utbilda anställda samt säkerställa en tydlig ansvarsfördelning.<sup>7</sup> Åtgärder som kan vidtas för att visa att behandlingen är författningsenlig kan t.ex. vara dokumentation av it-system, behandlingar och vidtagna åtgärder m.m.<sup>8</sup>

Polismyndigheten har i ärendet lämnat in en intern rutin för personuppgiftsbehandling inom myndigheten. Något ytterligare styrdokument för de anställdas behandling av personuppgifter har inte lämnats in. Inte heller något underlag kring hur utbildning av anställda eller hur den interna rutinen ska nå hela organisationen har lämnats in eller redogjorts för. Det saknas också uppgift om att någon utbildning eller motsvarande aktivitet faktiskt har genomförts inom myndigheten. Att anställda vid två olika

<sup>4</sup> Prop. 2017/18:232 s. 171 f., 319 och 452.

<sup>5</sup> Se vidare nedan under rubriken Polismyndighetens skyldighet att genom tekniska och organisatoriska åtgärder säkerställa och visa att myndighetens personuppgiftsbehandling är författningsenlig.

<sup>6</sup> Prop. 2017/18:232 s. 172 f.

<sup>7</sup> Sandén, H-O, 2019, SFS 2018:1177 Lagkommentar, Norstedts juridik.

<sup>8</sup> Prop 2017/18:232, s. 453.

organisatoriska enheter använt sig av Clearview AI i strid med gällande reglering visar att rutinen inte fått tillräckligt genomslag inom myndigheten. Polismyndigheten har mot denna bakgrund inte kunnat visa att det finns tillräckliga organisatoriska åtgärder, i form av t.ex. interna strategier eller utbildning, på plats för att säkerställa att behandlingen är författningsenlig.

IMY konstaterar att Polismyndigheten inte har vidtagit lämpliga organisatoriska åtgärder för att säkerställa och kunna visa att myndighetens behandling av personuppgifter varit författningsenlig. Polismyndigheten har därmed överträtt 3 kap. 2 § brottsdatalagen.

## **Polismyndighetens behandling av biometriska uppgifter i samband med användningen av Clearview AI**

Enligt Polismyndighetens uppgifter har bilder på personer, som sedan omvandlats till biometriska uppgifter, i pågående operativa ärenden lästs in i Clearview AI vid ett flertal tillfällen.

Polismyndigheten har inte redogjort för hur de biometriska uppgifterna som lästs in i Clearview AI behandlas i applikationen, t.ex. om och i så fall hur länge uppgifterna sparas, hur matchningen av biometriska uppgifter går till, om uppgifterna överförs till tredjeland eller om uppgifterna lämnas ut till andra i samband med användningen. Det beror enligt uppgifter från Polismyndigheten på att inga rättsliga bedömningar har gjorts före användningen av Clearview AI.

Biometriska personuppgifter är känsliga personuppgifter och får enligt 2 kap. 12 § brottsdatalagen endast behandlas om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen. Av 2 kap. 4 § PBDL framgår att Polismyndigheten får behandla biometriska uppgifter om användningen är absolut nödvändig för ändamålet med behandlingen.

Användningen av en tjänst som Clearview AI innebär att enskildas biometriska personuppgifter matchas mot stora mängder personuppgifter som ofiltrerat inhämtats från det öppna internet. Enligt IMY:s bedömning kan en brottsbekämpande myndighets behandling av personuppgifter vid användning av en sådan tjänst sannolikt inte uppfylla det strikta krav på nödvändighet som följer av brottsdatalagen och det bakomliggande brottsdatadirektivet.<sup>9</sup> Europeiska dataskyddsstyrelsen har gett uttryck för en liknande uppfattning.<sup>10</sup>

Den behandling av biometriska uppgifter som skett vid Polismyndighetens användning av Clearview AI har utförts utan någon kontroll eller kunskap från Polismyndigheten om hur uppgifterna hanteras av Clearview AI. Någon bedömning av om behandlingen varit absolut nödvändig enligt 2 kap. 12 § brottsdatalagen har inte skett. Genom den information som lämnats in i ärendet har Polismyndigheten inte visat att myndighetens behandling av biometriska uppgifter i tjänsten Clearview AI varit absolut nödvändig för ändamålet för behandlingen.

<sup>9</sup> Artikel 10 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters 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>10</sup> EDPB response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabienne Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI.

IMY konstaterar att Polismyndighetens behandling av biometriska uppgifter har skett i strid med 2 kap. 12 § brottsdatalagen.

## **Skyldighet att genomföra en konsekvensbedömning**

Enligt 3 kap. 7 § första stycket brottsdatalagen är en personuppgiftsansvarig skyldig att genomföra en konsekvensbedömning innan påbörjan av en ny behandling som kan antas medföra särskild risk för intrång i den registrerades personliga integritet.

Av förarbetena till brottsdatalagen och det bakomliggande brottsdatadirektivet framgår att vid bedömningen av om en konsekvensbedömning behövs ska behandlingens omfattning, art, sammanhang och art beaktas. Särskilt ska beaktas om behandlingen innefattar någon ny teknik.<sup>11</sup>

De personuppgifter som har behandlats i applikationen är biometriska uppgifter och dessa får, som redovisats ovan, endast behandlas om det är särskilt föreskrivet och absolut nödvändigt med hänsyn till ändamålet med behandlingen. Eftersom användningen av Clearview AI har inneburit behandling av biometriska uppgifter, som omfattar ansiktigenkänning, med ny teknik tillhandahållen av en extern aktör i tredjeland kan behandlingen antas ha inneburit en särskild risk för intrång i registrerades personliga integritet. En konsekvensbedömning skulle därför ha genomförts innan behandlingen påbörjades. Användningen av applikationen Clearview AI påbörjades dock utan att några rättsliga överväganden eller beaktande av risker för intrång i de registrerades personliga integritet ägde rum.

Polismyndigheten har inte använt applikationen systematiskt i sin verksamhet och applikationen har inte rekommenderats av myndigheten. Som IMY konstaterat ovan är dock Polismyndigheten ansvarig för den behandling anställda utfört vid användningen av Clearview AI. Bristen på organisatoriska åtgärder har medfört att anställda använt applikationen utan att dessförinnan genomföra en konsekvensbedömning, trots att det krävs enligt 3 kap. 7 § brottsdatalagen.

IMY konstaterar att Polismyndigheten i strid med 3 kap. 7 § första stycket brottsdatalagen underlåtit att genomföra en konsekvensbedömning före användningen av Clearview AI.

## **Val av ingripande**

Av 5 kap. 7 § brottsdatalagen följer de korrigerande befogenheter IMY har att tillgå vid överträdelser av nämnda lag. Dessa utgörs av bl.a. förelägganden, förbud mot behandling samt utfärdande av sanktionsavgift.

Av 6 kap. 1 och 2 §§ brottsdatalagen följer att IMY kan utfärda sanktionsavgift vid överträdelse av bl.a. bestämmelserna i 2 kap. 12 § samt 3 kap. 2 och 7 §§ brottsdatalagen. Sanktionsavgiften ska uppfylla de krav som ställs i brottsdatadirektivet på att sanktioner ska vara proportionella, avskräckande och effektiva.<sup>12</sup>

Vid bedömningen av om en sanktionsavgift ska tas ut och sanktionsavgiftens storlek ska särskild hänsyn tas till de omständigheter som anges i 6 kap. 4 § brottsdatalagen, dvs. om överträdelsen varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller

<sup>11</sup> Prop. 2017/18:232 s.181 f.

<sup>12</sup> Prop. 2017/18:232 s. 309 f.

kränkning som överträdelsen inneburit, överträdelsens karaktär, svårhetsgrad och varaktighet, vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa verkningarna av överträdelsen, och om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala en sanktionsavgift.

IMY konstaterar att Polismyndigheten brustit i flera avseenden i sitt personuppgiftsansvar vid användningen av Clearview AI. Polismyndigheten har inte vidtagit tillräckliga organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter i det aktuella fallet varit författningsenlig, behandlat biometrisk data i strid med brottsdatalagen samt underlåtit att genomföra en konsekvensbedömning.

Som IMY konstaterat ovan innebär detta att Polismyndigheten behandlat personuppgifter i strid med 2 kap. 12 § samt 3 kap. 2 § och 7 § första stycket brottsdatalagen.

Det har inte kunnat utredas om de registrerade lidit någon faktiskt skada vid Polismyndighetens användning av Clearview AI. Detta är dock inte avgörande för om sanktionsavgift ska tas ut, utan det faktum att risk för skada förelegat är enligt förarbetena tillräckligt för detta.<sup>13</sup> Genom användningen av Clearview AI har anställda vid Polismyndigheten fått tillgång till integritetskänsliga uppgifter om ett stort antal registrerade. EU-domstolen har uttalat att tillgång till stora mängder av personuppgifter av en myndighet måste ses som ett särskilt intrång, oavsett om de enskilda lidit någon skada av behandlingen eller inte.<sup>14</sup> Även de uppgifter som Polismyndigheten matat in i applikationen har varit av integritetskänsligt slag och det har inte kunnat klarläggas vad som hänt med dessa personuppgifter efter inmatningen. Med anledning av vad som nu anförts bedömer IMY risken för skada för de registrerade som hög i det aktuella fallet.

Polismyndigheten har behandlat personuppgifter utan rättsliga överväganden och utan någon kontroll över eller bedömning av behandlingens intrång i enskildas personliga integritet. Vad avser användningen av Clearview AI har Polismyndigheten inte kunnat redogöra för vad som skett med de personuppgifter myndigheten matat in i applikationen samt med det resultat man erhållit. Det kan förutsättas att de uppgifter som matats in i applikationen ofta omfattats av någon form av sekretess, t.ex. 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), och Polismyndigheten har inte presenterat någon sekretessbrytande grund som kunnat motivera utlämnande av uppgifterna. Dessa omständigheter innebär att det finns skäl att se allvarligt på överträdelserna.

Också omfattningen och varaktigheten av behandlingen ska beaktas vid bestämmandet av sanktionsavgiftens storlek. En förmildrande omständighet är att det endast är ett fåtal registrerade vars personuppgifter delats med Clearview AI. Användningen av Clearview AI har dock sammanlagt skett under några månaders tid, och upphörde först sedan Integritetsskyddsmyndighetens granskning påbörjats. Dessutom har Polismyndigheten genom användningen av Clearview AI fått tillgång till ett stort antal personuppgifter och det är oklart hur länge de inmatade personuppgifterna och de uppgifter som erhållits genom matchningen behandlats.

Det får vidare anses försvårande att de registrerades uppgifter matchats mot en applikation med personuppgifter från hela det öppna internet samt att Polismyndigheten inte har någon kunskap om vad som hänt med de uppgifter som

<sup>13</sup> Prop. 2017/18:232 s. 483.

<sup>14</sup> Eu-domstolens domar i målen C-594/12 punkt 35 samt C-623/17 punkt 70.

matats in. Det faktum att det varit biometriska, dvs. känsliga personuppgifter, som behandlats och att uppgifterna använts för ansiktsgenkänning gör därutöver att det finns skäl att se allvarligt på överträdelsen.<sup>15</sup>

Sammanfattningsvis medför de redovisade omständigheterna att en sanktionsavgift ska tas ut och att en förhållandevis kännbar sanktionsavgift är motiverad.

## Sanktionsavgiftens storlek

Enligt 6 kap. 5 § brottsdatalagen får en sanktionsavgift sättas ned helt eller delvis om överträdelsen varit ursäktlig eller att det vore oskäligt att utfärda sanktionsavgift. Den omständigheten att den personuppgiftsansvariga inte känt till regler eller haft bristfälliga rutiner är inte en anledning att sätta ned sanktionsavgiften.<sup>16</sup> IMY konstaterar att det inte heller i övrigt framkommit skäl för att sätta ned sanktionsavgiften enligt 6 kap. 5 § brottsdatalagen.

Av 6 kap. 3 § första stycket brottsdatalagen följer att en sanktionsavgift för överträdelse av 3 kap. 7 § samma lag högst får uppgå till fem miljoner kronor. Av andra stycket följer att för en överträdelse av bl.a. 2 kap. 12 § och 3 kap. 2 § brottsdatalagen får en sanktionsavgift uppgå till högst tio miljoner kronor. Det högsta beloppet som kan fastställas är således tio miljoner kronor.

IMY bestämmer utifrån en samlad bedömning att Polismyndigheten ska betala en sanktionsavgift på 2 500 000 kronor.

## Förelägganden

Polismyndigheten ska föreläggas att vidta utbildningsåtgärder och övriga organisatoriska åtgärder som krävs enligt 3 kap. 2 § brottsdatalagen för att säkerställa att de rutiner som finns når hela organisationen och att myndigheten därmed kan visa och säkerställa att all behandling av personuppgifter är författningssenlig. Åtgärderna ska ha vidtagits senast den 15 september 2021.

Enligt 4 kap. 2 § brottsdatalagen ska den personuppgiftsansvarige i ett enskilt fall lämna viss information till den registrerade, om det behövs för att han eller hon ska kunna ta till vara sina rättigheter. Informationen ska bl.a. omfatta den rättsliga grunden för behandlingen, kategorier av mottagare av personuppgifterna och hur länge personuppgifterna får behandlas. Av förarbetena framgår att bestämmelsen är tillämplig t.ex. i fall där den registrerade riskerar att lida rättsförlust om han eller hon inte får del av informationen eller om det av annat skäl är viktigt för honom eller henne att känna till behandlingen för att kunna tillvarata sina rättigheter. Ett annat exempel som tas upp i förarbetena är att känsliga personuppgifter har behandlats i strid med 2 kap. 11 § om känsliga personuppgifter.<sup>17</sup>

Informationsskyldigheten enligt 4 kap. 2 § brottsdatalagen gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut bl.a. av hänsyn till intresset av att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, att andra rättsliga utredningar eller undersökningar inte

<sup>15</sup> Prop 2017/18:232 s. 485.

<sup>16</sup> Prop 2017/18:232 s.465

<sup>17</sup> Prop. 2017/18:232 s. 465

hindras, eller att någon annans rättigheter och friheter skyddas (4 kap. 5 § brottsdalagen).

Som IMY konstaterat har det inte kunnat klargöras vad som hänt med de personuppgifter som Polismyndigheten matat in i Clearview AI. Det är därför viktigt att de registrerade får kännedom om behandlingen för att kunna tillvarata sina rättigheter, särskilt som det är fråga om känsliga personuppgifter som behandlats i strid med 2 kap. 11 § BDL. IMY bedömer därför att Polismyndigheten har en skyldighet att lämna information enligt 4 kap. 2 § BDL. Under utredningen har Polismyndigheten inte framfört något om att de registrerade ska ha informerats om användningen.

Polismyndigheten ska mot denna bakgrund föreläggas att lämna information till de registrerade, vars personuppgifter Polismyndigheten matat in i Clearview AI, enligt 4 kap. 2 § brottsdatalogen med de begränsningar som följer av 4 kap. 5 § samma lag. Informationen ska ha lämnats senast den 15 september 2021.

Som IMY konstaterat har Polismyndigheten matat in känsliga personuppgifter i Clearview AI. Då det saknas information om vad som skett med de personuppgifter som delats med Clearview AI och om dessa ännu lagras hos applikationen ska Polismyndigheten slutligen föreläggas att vidta möjliga och relevanta åtgärder för att tillse att de personuppgifter som matats in i Clearview AI raderas från applikationen. Sådana åtgärder ska ha vidtagits senast den 15 september 2021.

---

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Elena Mazzotti Pallard. Vid handläggningen har även juristen Frida Orring och processägaren för tillsynsprocessen Katarina Tullstedt deltagit. Vid den slutliga handläggningen har rättschefen David Törngren och enhetschefen Charlotte Waller Dahlberg medverkat.

*Lena Lindgren Schelin, 2021-02-10 (Det här är en elektronisk signatur)*

**Bilaga:**

Hur man betalar sanktionsavgift.

**Kopia för kännedom till:**

Dataskyddsombudet: [dataskyddsombud@polisen.se](mailto:dataskyddsombud@polisen.se)

## Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Integritetsskyddsmyndigheten senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Integritetsskyddsmyndigheten det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Integritetsskyddsmyndigheten om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.