

Kriminalvården  
Box 306  
Slottsgatan 78  
601 80 Norrköping

## Tillsyn enligt brottsdatalagen (2018:1177) - Kriminalvårdens rutiner för hantering av personuppgiftsincidenter

### Innehållsförteckning

Datainspektionens beslut.....	2
Redogörelse för tillsynsärendet.....	3
Tillämpliga bestämmelser.....	4
Motivering av beslutet.....	6
Datainspektionens granskning.....	6
Rutiner för att upptäcka personuppgiftsincidenter.....	7
Datainspektionens bedömning.....	8
Rutiner för hantering av personuppgiftsincidenter.....	9
Datainspektionens bedömning.....	9
Rutiner för dokumentation av personuppgiftsincidenter.....	10
Datainspektionens bedömning.....	10
Information och utbildning kring personuppgiftsincidenter.....	11
Datainspektionens bedömning.....	12
Hur man överklagar.....	13

## **Datainspektionens beslut**

Datainspektionen meddelar följande rekommendationer med stöd av 5 kap. 6 § brottsdatalagen (2018:1177):

1. Kriminalvården bör regelbundet utvärdera effektiviteten hos de vidtagna säkerhetsåtgärderna för att upptäcka personuppgiftsincidenter och vid behov revidera dessa för att upprätthålla tillräckligt skydd av personuppgifter.
2. Kriminalvården bör regelbundet kontrollera att rutinerna för hantering av personuppgiftsincidenter följs.
3. Kriminalvården bör i myndighetens rutiner för rapportering av personuppgiftsincidenter precisera vilka uppgifter av en inträffad incident som ska dokumenteras samt regelbundet kontrollera att rutinerna för dokumentation av personuppgiftsincidenter följs.
4. Kriminalvården bör ge sina anställda löpande information och återkommande utbildning i hanteringen av personuppgiftsincidenter och om rapporteringsskyldigheten.

Datainspektionen avslutar ärendet.

## Redogörelse för tillsynsärendet

Skyldigheten för den personuppgiftsansvarige – dvs. privata och offentliga aktörer – att anmäla vissa personuppgiftsincidenter till Datainspektionen infördes den 25 maj 2018 genom dataskyddsförordningen<sup>1</sup> (GDPR).

Motsvarande anmälningsskyldighet infördes den 1 augusti 2018 i brottsdatalagen (BDL) för s.k. behöriga myndigheter.<sup>2</sup> Skyldigheten att anmäla personuppgiftsincidenter (nedan kallad incident) syftar till att stärka integritetsskyddet genom att Datainspektionen får information om händelsen och kan välja att vidta åtgärder när inspektionen bedömer att det behövs för att den personuppgiftsansvarige ska hantera incidenten på ett tillfredställande sätt och vidta åtgärder för att förhindra att något liknande inträffar igen.

En personuppgiftsincident är enligt 1 kap. 6 § BDL en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring, eller obehörigt röjande av eller obehörig åtkomst till personuppgifter. I förarbetena till lagen anges att det som regel är fråga om en oplanerad händelse som påverkar säkerheten för personuppgifterna på ett negativt sätt och som medför allvarliga konsekvenser för skyddet av uppgifterna.<sup>3</sup> En personuppgiftsincident kan till exempel vara att personuppgifter har skickats till fel mottagare, att tillgången till personuppgifterna har förlorats, att datautrustning som lagrar personuppgifter har tappats bort eller stulits, att någon inom eller utanför organisationen tar del av information som den saknar behörighet till.

En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan medföra risker för den registrerades rättigheter eller friheter. En incident kan leda till fysisk, materiell eller immateriell skada genom exempelvis

---

<sup>1</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 (allmän dataskyddsförordning).

<sup>2</sup> En behörig myndighet är enligt i 1 kap. 6 § BDL en myndighet som behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

<sup>3</sup> Prop.2017/18:232 s. 438

diskriminering, identitetsstöld, identitetsbedrägeri, skadat anseende, finansiell förlust samt brott mot sekretess eller tystnadsplikt.

Det kan finnas många orsaker till att en personuppgiftsincident uppstår. Av Datainspektionens rapportserie *Anmälda personuppgiftsincidenter* under perioden maj 2018 - december 2019 framgår att de vanligaste orsakerna bakom de anmälda incidenterna var bl.a. den mänskliga faktorn, tekniska fel, antagonistiska angrepp samt brister i organisatoriska rutiner eller processer.<sup>4</sup>

Datainspektionen har inlett detta tillsynsärende mot Kriminalvården i syfte att kontrollera om myndigheten har rutiner på plats för att upptäcka personuppgiftsincidenter och om myndigheten har och har haft rutiner för att hantera personuppgiftsincidenter enligt brottsdatalagen. I granskningen ingår även att kontrollera om Kriminalvården har rutiner för dokumentation av incidenter som svarar mot kraven i brottsdataförordningen (BDF) samt om myndigheten har genomfört informations- och utbildningsinsatser kring personuppgiftsincidenter.

Tillsynen inleddes med en skrivelse till Kriminalvården den 4 december 2019 och följdes upp med begäran om komplettering den 4 mars 2020. Myndighetens svar på tillsynsskrivelsen kom in den 4 februari 2020 och kompletteringen inkom den 9 april 2020.

## Tillämpliga bestämmelser

Den personuppgiftsansvarige ska enligt 3 kap. 2 § BDL, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningssenlig och att den registrerades rättigheter skyddas. Det innebär att behöriga myndigheter, med hjälp av dessa åtgärder, inte bara ska säkerställa att dataskyddsregelverket följs utan också ska kunna visa att så är fallet. Vilka tekniska och organisatoriska åtgärder som krävs för att skydda personuppgifterna regleras i 3 kap. 8 § BDL.

---

<sup>4</sup> Se Datainspektionens rapportserie om Anmälda personuppgiftsincidenter 2018 (Datainspektionens rapport 2019:1) s 7 f; Anmälda personuppgiftsincidenter januari-september 2019 (Datainspektionens rapport 2019:3) s.10 f. och Anmälda personuppgiftsincidenter 2019 (Datainspektionens rapport 2020:2) s. 12 f.

I förarbetena till lagen anges att organisatoriska åtgärder som avses i 2 § är bl.a. att ha interna strategier för dataskydd, att informera och utbilda personalen och att säkerställa en tydlig ansvarsfördelning. Åtgärder som vidtas för att visa att behandlingen är författningsenlig kan t.ex. vara dokumentation av IT-system, behandlingar och vidtagna åtgärder och teknisk spårbarhet genom loggning och logguppföljning. Vilka åtgärder som ska vidtas får avgöras efter en bedömning i varje enskilt fall.<sup>5</sup> Åtgärderna ska ses över och uppdateras vid behov. De åtgärder som den personuppgiftsansvarige ska vidta enligt denna bestämmelse ska enligt 3 kap. 1 § BDF vara rimliga med beaktande av behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen.

Av 3 kap. 8 § BDL framgår att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada. I förarbetena till brottsdatalogen anges att säkerheten ska omfatta åtkomstskydd för utrustning, kontroll av datamedier, lagringskontroll, användarkontroll, åtkomstkontroll, kommunikationskontroll, indatakontroll, transportkontroll, återställande, driftsäkerhet och dataintegritet. Denna uppräkningslista är dock inte uttömmande. Som exempel på organisatoriska säkerhetsåtgärder kan nämnas fastställandet av en säkerhetspolicy, kontroller och uppföljning av säkerheten, utbildning i datasäkerhet och information om vikten av att följa gällande säkerhetsrutiner. Rutiner för anmälan och uppföljning av personuppgiftsincidenter utgör också sådana åtgärder.<sup>6</sup>

Vilka omständigheter som bör beaktas för att uppnå en lämplig skyddsnivå är reglerat i 3 kap. 11 § BDF. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheterna, kostnaderna för åtgärderna, behandlingens art, omfattning, sammanhang och ändamål, samt de särskilda riskerna med behandlingen. Särskild hänsyn bör tas till i vilken utsträckning känsliga personuppgifter behandlas och hur integritetskänsliga övriga personuppgifter som behandlas är.<sup>7</sup> Överträdelse av bestämmelser i

---

<sup>5</sup> Prop. 2017/18:232 s. 453

<sup>6</sup> Prop. 2017/18:232 s. 457

<sup>7</sup> Prop. 2017/18:232 s. 189 f.

3 kap. 2 och 8 §§ BDL kan leda till sanktionsavgifter enligt 6 kap. 1 § 2 BDL.

Den personuppgiftsansvarige ska enligt 3 kap. 14 § BDF dokumentera alla personuppgiftsincidenter. Dokumentationen ska redovisa omständigheterna kring incidenten, dess effekter och de åtgärder som vidtagits med anledning av den. Den personuppgiftsansvarige ska dokumentera alla inträffade incidenter oavsett om den måste anmälas till Datainspektionen eller inte.<sup>8</sup> Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av den aktuella bestämmelsen. Underlåtenhet att dokumentera personuppgiftsincidenter kan föranleda sanktionsavgifter enligt 6 kap. 1 § BDL.

En personuppgiftsincident ska också, enligt 3 kap. 9 § BDL, anmälas till Datainspektionen senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om incidenten. En anmälan behöver inte göras om det är osannolikt att incidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i den registrerades personliga integritet. Av 3 kap. 10 § BDL framgår att den personuppgiftsansvarige i vissa fall ska informera den registrerade som berörs av incidenten. Underlåtenhet att anmäla en personuppgiftsincident till Datainspektionen kan leda till administrativa sanktionsavgifter enligt 6 kap. 1 § BDL.<sup>9</sup>

## Motivering av beslutet

### Datainspektionens granskning

Datainspektionen har i detta tillsynsärende att ta ställning till om Kriminalvården har dokumenterade rutiner för att upptäcka personuppgiftsincidenter enligt brottsdatalagen och om myndigheten har och har haft rutiner för att hantera incidenter sedan BDL trädde ikraft. Granskningen omfattar även frågan om efterlevnaden av kravet på dokumentation av incidenter i 3 kap. 14 § BDF. Därutöver ska Datainspektionen ta ställning till om Kriminalvården har genomfört

---

<sup>8</sup> Prop. 2017/18:232 s. 198

<sup>9</sup> Ansvaret för överträdelser är strikt. Det krävs alltså varken uppsåt eller oaktsamhet för att sanktionsavgift ska kunna tas ut, se prop. 2017/18:232 s. 481.

informations- och utbildningsinsatser för sina anställda med fokus på hantering av personuppgiftsincidenter enligt BDL.

Granskningen omfattar inte innehållet i rutinerna eller utbildningsinsatserna utan är fokuserad på att kontrollera att den granskande myndigheten har rutiner på plats och att den har genomfört utbildningsinsatser för medarbetarna avseende personuppgiftsincidenter. Granskningen omfattar dock om myndighetens rutiner innehåller anvisningar att dokumentera de uppgifter som krävs enligt brottsdataförordningen.

### **Rutiner för att upptäcka personuppgiftsincidenter**

De personuppgifter som behöriga myndigheter hanterar inom ramen för sin brottsbekämpande och brottsutredande verksamhet är i stor utsträckning av känslig och integritetskänslig natur. Verksamhetens karaktär ställer höga krav på de brottsbekämpande myndigheternas förmåga att skydda de registrerades uppgifter genom nödvändiga skyddsåtgärder för att bl.a. förhindra att en incident uppstår.

Skyldigheten att rapportera personuppgiftsincidenter enligt 3 kap. 9 § BDL ska tolkas i ljuset av de generella kraven att vidta lämpliga tekniska och organisatoriska åtgärder, för att säkerställa lämplig säkerhet för personuppgifter, som föreskrivs i 3 kap. 2 och 8 §§. En förmåga att snabbt upptäcka och rapportera en incident är en nyckelfaktor. För att de brottsbekämpande myndigheterna ska kunna leva upp till rapporteringskravet måste de ha interna rutiner och tekniska möjligheter för att upptäcka en incident.

Utifrån verksamhetens behov och med stöd av risk- och sårbarhetsanalyser kan behöriga myndigheter identifiera de områden där det finns en större risk att en incident kan uppstå. Utifrån analyserna kan myndigheterna sedan använda olika instrument för att upptäcka ett säkerhetshot. Dessa kan vara både tekniska och organisatoriska åtgärder. Utgångspunkten är att de vidtagna säkerhetsåtgärderna ska ge tillräckligt skydd och att incidenter inte ska inträffa.

Exempel på tekniska åtgärder är bl.a. intrångsdetektorer som automatiskt analyserar och upptäcker dataintrång och användning av logganalysinstrument för att kunna detektera obehörig åtkomst (loggavvikelser). En ökad insikt om verksamhetens "normala" nätverks

trafikmönster hjälper till att identifiera sådant som avviker från den normala trafikbilden gentemot exempelvis servrar, applikationer eller datafiler. Organisatoriska åtgärder kan exempelvis vara antagande av interna strategier för dataskydd som avser interna regler, riktlinjer, rutiner och olika typer av styrdokument och policydokument.<sup>10</sup> Riktlinjer och regler för hantering av personuppgifter, rutiner för incidenthantering och logguppföljning<sup>11</sup> utgör exempel på sådana strategier. Periodisk uppföljning av tilldelade behörigheter är ett annat exempel på organisatoriska åtgärder. I en behörig myndighet ska det finnas rutiner för tilldelning, förändring, borttagning och regelbunden kontroll av behörigheter.<sup>12</sup> Information till och utbildning av personal om de regler och rutiner för incidenthantering som ska följas är också exempel på sådana åtgärder.

#### *Datainspektionens bedömning*

Kriminalvården har i huvudsak uppgett följande. Sedan 2005 arbetar myndigheten strukturerat med incidenthantering. Det finns även sedan flera år en riktlinje som reglerar rapporteringsskyldigheten av inträffade incidenter. Riktlinjen omfattar även incidenter som upptäcks och som berör personuppgifter. Avseende tekniska skydd är Kriminalvårdens it-infraktstruktur kopplad till IT-säkerhet. Exempel på skydd är bl.a. brandväggar, nätverkssegmentering, intrångsdetektering och logguppföljning. Kriminalvården uppger vidare att de tekniska och organisatoriska rutiner som myndigheten har för att upptäcka personuppgiftsincidenter kan delas in i förebyggande och i uppföljande rutiner. Förebyggande åtgärder beskrivs i Kriminalvårdens regelverk för IT-säkerhet och innefattar regelverk för att undvika informationssäkerhets- och IT-säkerhetsincidenter där personuppgiftsincidenter är en typ av incident. Därtill redogör Kriminalvården i sitt yttrande för vilka förebyggande åtgärder som myndigheten vidtagit och beskrivit t.ex. hur logguppföljning går till. Av utredningen framgår att Kriminalvården har genomfört utbildnings- och informationsinsatser för sina medarbetare om personuppgiftsbehandling vilket omfattar information om personuppgiftsincidenter och om rapporteringsskyldighet.

---

<sup>10</sup> Brottsdatalog – Delbetänkande av Utredningen om 2016 års dataskyddsdirektiv Stockholm 2017, SOU 2017:29 s. 302

<sup>11</sup> Behöriga myndigheter ska se till att det finns rutiner för logguppföljning, se prop. 2017/18:232 s. 455 f.

<sup>12</sup> 3 kap. 6 § BDL och kompletterande bestämmelser i 3 kap. 6 § BDF



Datainspektionen kan konstatera att Kriminalvården har rutiner för att upptäcka personuppgiftsincidenter på plats. Skyldigheten att vidta säkerhetsåtgärder för att upptäcka personuppgiftsincidenter är inte knuten till en viss tidpunkt utan åtgärderna ska kontinuerligt ses över och vid behov förändras. För att Kriminalvården ska kunna upprätthålla tillräcklig skyddsnivå av personuppgifter över tid rekommenderar Datainspektionen, med stöd av 5 kap. 6 § BDL, att myndigheten regelbundet utvärderar effektiviteten hos de vidtagna säkerhetsåtgärderna för att upptäcka personuppgiftsincidenter och att myndigheten vid behov uppdaterar dessa.

### **Rutiner för hantering av personuppgiftsincidenter**

För att kunna leva upp till kraven på organisatoriska åtgärder i 3 kap. 8 § BDL ska den personuppgiftsansvarige ha dokumenterade interna rutiner som beskriver vilken process som ska följas när en incident har upptäckts eller inträffat, inbegripet hur incidenten ska begränsas, hanteras och återställas, samt hur riskbedömningen ska gå till och hur incidenten ska anmälas internt och till Datainspektionen. Av rutinerna ska framgå bl.a. vad en personuppgiftsincident är/kan vara, när en incident behöver anmälas, och till vem, vad som ska dokumenteras, ansvarsfördelningen samt vilken information som bör tillhandahållas inom ramen för anmälan till Datainspektionen.

Datainspektionens kontroll av rutiner för att hantera personuppgiftsincidenter avser tiden från brottsdatalogens ikraftträdande dvs. den 1 augusti 2018.

### *Datainspektionens bedömning*

Kriminalvården har bl.a. uppgett följande. Myndigheten har sedan flera år en riktlinje som reglerar rapporteringsskyldighet av inträffade incidenter. Enligt riktlinjen ska alla typer av incidenter rapporteras inom 24 timmar i myndighetens gemensamma incidentrapporteringssystem Isap. Det framgår vidare att alla medarbetare har behörighet och en skyldighet att rapportera incidenter. Personuppgiftsincidenter, liksom andra incidenter, rapporteras också i Isap. Kriminalvården har lämnat in myndighetens *riktlinjer för rapportering och utredning av incidenter (2018:8)* daterad 2018-09-11 samt en *intern rutin för rapportering av personuppgifter till Datainspektionen* daterad 2018-04-09. Kriminalvården har angett att den förstnämnda riktlinjen är en generell rutin för myndighetens rapportering och utredning av incidenter.

Detta omfattar alla olika typer av incidenter som kan inträffa inom myndigheten och gäller också för personuppgiftsincidenter. Beträffande den interna rutinen anges att den gäller specifikt för den funktion inom myndigheten som analyserar, bedömer och även rapporterar personuppgiftsincidenter till Datainspektionen.

Med beaktande av de inlämnade handlingarna och vad som framkommit i ärendet konstaterar Datainspektionen att Kriminalvården från tidpunkten då brottsdatalagen trädde ikraft har haft och har rutiner för att hantera personuppgiftsincidenter på plats.

Att kunna hantera upptäckta personuppgiftsincidenter på ett korrekt sätt och motverka dess effekter och risker för de registrerades personliga integritet är viktigt. Datainspektionen rekommenderar därför, med stöd av 5 kap. 6 § BDL, att Kriminalvården regelbundet kontrollerar att rutinerna för hantering av personuppgiftsincidenter följs.

#### **Rutiner för dokumentation av personuppgiftsincidenter**

En förutsättning för att Datainspektionen ska kunna kontrollera efterlevnaden av dokumentationskravet av incidenter i 3 kap. 14 § BDF är att dokumentationen omfattar vissa uppgifter som alltid bör ingå.

Dokumentationen ska omfatta alla detaljer kring incidenten, inbegripet dess orsaker, vad som skedde och de personuppgifter som berördes. Den ska även innehålla incidentens konsekvenser och de korrigerande åtgärder som den personuppgiftsansvarige vidtagit.

#### *Datainspektionens bedömning*

Kriminalvården har huvudsakligen uppgett följande. Alla incidenter dokumenteras initialt i incidentrapporteringssystemet Isap, vilket även omfattar personuppgiftsincidenter. Gällande de incidenter som bedöms utgöra personuppgiftsincidenter används Datainspektionens blanketter för att analysera, bedöma och i förekommande fall rapportera. Detta gäller även de personuppgiftsincidenter som efter bedömning inte har rapporterats till Datainspektionen. Av Kriminalvårdens interna rutin för rapportering av personuppgiftsincidenter till Datainspektionen framgår att för de fall en personuppgiftsincident inte är rapporteringspliktig dokumenteras den också genom Datainspektionens rapportmall och lagras internt.

Datainspektionen konstaterar att Kriminalvården har ett internt IT-system för att bl.a. rapportera incidenter som rör personuppgifter. Därutöver framgår av myndighetens interna rutin att alla personuppgiftsincidenter ska dokumenteras och att myndigheten använder sig av Datainspektionens blanketter för anmälan av personuppgiftsincidenter för att dokumentera inträffade personuppgiftsincidenter även om de inte är rapporteringspliktiga. Datainspektionen konstaterar dock att de interna rutinerna saknar en beskrivning av vad vilka uppgifter som dokumentationen ska omfatta.

Att kunna dokumentera inträffade personuppgiftsincidenter på ett korrekt sätt och därmed motverka risken av att dokumentationen blir bristfällig eller ofullständig är viktigt. Bristfällig dokumentation kan leda till att incidenterna inte hanteras och åtgärdas på ett korrekt sätt, vilket kan få påverkan på integritetsskyddet. Datainspektionen rekommenderar därför, med stöd av 5 kap. 6 § BDL, att Kriminalvårdens interna rutiner för rapportering av personuppgiftsincidenter kompletteras med en beskrivning av vilka uppgifter av en inträffad incident som ska dokumenteras. Därutöver bör Kriminalvården genomföra regelbundna kontroller av den interna dokumentationen av personuppgiftsincidenter.

### **Information och utbildning kring personuppgiftsincidenter**

Personalen är en viktig resurs i säkerhetsarbetet. Det räcker inte bara med interna rutiner, regler eller styrdokument om användarna inte följer dem. Alla användare måste förstå att hantering av personuppgifter ska ske på ett rättssäkert sätt samt att det är allvarigare att inte rapportera en incident än att rapportera t.ex. ett misstag eller ett fel. Det krävs därför att alla användare får en adekvat utbildning och tydlig information om dataskydd.

Den personuppgiftsansvarige ska informera och utbilda sin personal i frågor om dataskydd inbegripet hantering av personuppgiftsincidenter. Av Datainspektionens rapportserie *Anmälda Personuppgiftsincidenter* under perioden 2018-2019 framgår att den mänskliga faktorn utgör den vanligaste orsaken till anmälda personuppgiftsincidenter.<sup>13</sup> Dessa består i huvudsak av individer som, medvetet eller omedvetet, inte följer interna rutiner vid

---

<sup>13</sup> Rapport 2019:1, rapport 2019:3 och rapport 2020:2. Liknande slutsatser har MSB dragit i sin årsrapport för allvarliga IT-incidenter, dvs. att de flesta av incidenterna beror på mänskliga misstag, se <https://www.msb.se/sv/aktuellt/nyheter/2020/april/arsrapporten-for-allvarliga-it-incidenter-2019-ar-slappt/>

behandling av personuppgifter eller begått ett misstag vid hantering av personuppgifter. Omkring hälften av de incidenter som beror på den mänskliga faktorn handlar om felskickade brev och e-postmeddelanden. Detta understryker enligt Datainspektionens mening betydelsen av att interna rutiner och tekniska säkerhetsåtgärder behöver kompletteras med löpande utbildning, information och andra åtgärder för att öka kunskap och medvetenhet hos medarbetarna.

#### *Datainspektionens bedömning*

På frågan om på vilket sätt information och utbildning om incidenter ges till anställda har Kriminalvården uppgett bl.a. följande. Myndigheten har informerat personalen om rapportering av personuppgiftsincidenter bl.a. via intranätet, en obligatorisk e-kurs för samtliga anställda, informationsfilm, utbildning för chefer och för viss administrativ personal, e-postutskick samt genom regionala Isap-samordnare.

Mot bakgrund av vad som framgår av utredningen anser Datainspektionen att Kriminalvården har visat att myndigheten har gett information och utbildning om hantering av personuppgiftsincidenter till sina medarbetare.

För att upprätthålla kompetensen och säkerställa att ny personal får utbildning är det viktigt med återkommande information och utbildning till de anställda och inhyrd personal. Datainspektionen rekommenderar, med stöd av 5 kap. 6 § BDL, att Kriminalvården ger de anställda löpande information och återkommande utbildningar i hanteringen av personuppgiftsincidenter och skyldigheten att rapportera dessa.

---

Detta beslut har fattats av enhetschefen Charlotte Waller Dahlberg efter föredragning av juristen Maria Angelica Westerberg. Vid den slutliga handläggningen av ärendet har även IT-säkerhetsspecialisten Ulrika Sundling och juristen Jonas Agnvall medverkat.

Charlotte Waller Dahlberg, 2020-12-17 (Det här är en elektronisk signatur)

#### **Kopia för kännedom till:**

Kriminalvårdens dataskyddsombud

## Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär.

Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Datainspektionen det vidare till Förvaltningsrätten i Stockholm för prövning.

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