

Verisure Sverige AB

Diarienummer:
IMY-2022-1558

Datum:
2024-11-27

Beslut efter tillsyn enligt dataskyddsförordningen – Verisure Sverige AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten (IMY) konstaterar att Verisure Sverige AB (556153-2176) under tiden den 20 april 2022 till augusti 2022 har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen¹ genom att inte ha vidtagit lämpliga åtgärder för att säkerställa en lämplig skyddsnivå för personuppgifter i form av bildmaterial från kameror i privatpersoners hem.

IMY ger Verisure Sverige AB en reprimand med stöd av artikel 58.2 b i dataskyddsförordningen för den konstaterade överträdelsen.

Redogörelse för tillsynsärendet

Bakgrund

Integritetsskyddsmyndigheten (IMY) har tagit del av uppgifter i media som bland annat gör gällande att anställda hos Verisure Sverige AB (härefter "Verisure" eller bolaget") i samband med inkomma larm har delat bildmaterial från kameror i privatpersoners hem mellan sig på olika sätt utan att det varit befogat. IMY har därför inlett tillsyn mot Verisure i syfte att utreda bolagets interna hantering av bildmaterial från kameror uppsatta i kunders hem.

IMY har efter tillsynens inledande mottagit tips gällande Verisures tekniska och organisatoriska säkerhetsåtgärder. Verisure har fått tillfälle att yttra sig med anledning därav.

Vad som framkommit i ärendet

Verisure har bland annat uppgett följande.

Om uppgifterna i media

Bolaget har tagit uppgifterna i medierapporteringen mycket allvarligt och har tillsatt stora resurser för att utreda påståendena i aktuell tidningsartikel. Verisure tar dock

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

¹ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

avstånd från uppgifterna i media i och med att ingenting i bolagets omfattande interna utredning tyder på att det skulle finnas utrymme för sådan behandling av bildmaterial som beskrivits eller att liknande behandling faktiskt sker. Den interna utredningen har bland annat bestått i intervjuer med anställda och tidigare anställda, en teknisk genomgång av logguppgifter för att kontrollera om bildmaterial har hanterats på ett avvikande sätt, genomgång av larmoperatörernas chattgrupper samt en genomgång av de tekniska begränsningarna i bolagets system för att identifiera eventuella brister som skulle kunna möjliggöra felaktig behandling av bildmaterialet. Bolagets internutredning har även inneburit en genomgång av listan för hanterade ärenden avseende begäran om registerutdrag i enlighet med dataskyddsförordningen, samt en granskning av efterlevnaden av det gällande dataskyddsregelverket och det interna regelverket. Vidare har internutredningen omfattat en granskning av de dataskyddsrelaterade utbildningsinsatser som bolaget genomför för nyanställda och i det löpande arbetet.

Resultatet av den interna utredningen visar att det inte finns något som tyder på att det har förekommit felaktig delning av personlig kundinformation på det sätt som beskrivits i media. I internutredningen kunde Verisure inte heller finna något bevis eller annars något som antyder pågående eller aktuella överträdelser av det interna regelverket. Bolaget har även en etablerad visselblåsarkanal som har använts av medarbetare i andra sammanhang men det finns inga rapporterade händelser som tyder på att felaktig behandling av bildmaterial har rapporterats via den kanalen.

Hade påståendena i media varit sanna hade det dock inte funnits någon laglig grund för en sådan uppenbart otillåten personuppgiftsbehandling.

Om Verisures hantering av personuppgifter från kunders kameror i övrigt

Verisure är en auktoriserad larmcentral vilket ställer omfattande regulatoriska krav på verksamheten. Verisure tar sitt ansvar som personuppgiftsansvarig på största allvar och arbetar strukturerat med integritets- och dataskyddsfrågor för att tillvarata de registrerades intressen. Kundernas integritet är en integrerad och avgörande del av Verisures verksamhet. Bolaget har bland annat ett omfattande internt regelverk i form av riktlinjer och rutiner.

I bolagets interna policy framgår tydligt hur larmoperatörerna får hantera bildmaterial och i vilka situationer de får titta på bilderna eller be en kollega att titta. Som en integritetshöjande åtgärd har Verisure även implementerat detaljerade instruktioner avseende hur kamerorna får installeras för att inte riskera att kränka den personliga integriteten. Verisure har även implementerat tekniska begränsningar som säkerställer att bildmaterial enbart behandlas om det är nödvändigt för att uppnå syftet med behandlingen.

Bildmaterialet är tillgängligt för behörig personal i bolagets system en viss tid, därefter raderas det automatiskt från systemet men arkiveras ytterligare en tid bland annat för behovet av att kunna dela bilder med brottsbekämpande myndigheter. Verisure har gjort bedömningen att den tid bildmaterialet sparas är en tillräckligt lång period för bolaget att lagra bildfilerna för att med beaktande av det tydliga integritetsintresset ändå kunna uppfylla bolagets ändamål med behandlingen. Till exempel kan det finnas behov av att kunna följa upp hur en viss incident har hanterats eller kunna besvara kunders frågor om en viss incident som kräver tillgång till bildmaterial.

Samtliga bildvisningar i bolagets system loggas. Det är tekniskt omöjligt att få tillgång till bildmaterialet utan att det loggas. Det innebär att om det inte finns en logg om

hantering av bilder i systemet kan Verisure med säkerhet konstatera att det inte förekommit någon åtkomst. Att all hantering av bildmaterialet loggas möjliggör utredning av otillåten åtkomst till materialet.

Som huvudregel ska bildmaterial inte exporteras från Verisures system. Det finns dock undantag där Veirsure är berättigad att dela bilder varför det finns en möjlighet att exportera bilder i särskilda fall. Denna funktion omfattas av accessbegränsningar och åtgärder loggas varför det alltid går att spåra hur en bild har delats.

Verisure har enbart möjlighet att eftersöka missförhållanden av det slag som påståtts i media under en viss period bakåt i tiden då bildmaterial raderas från systemet i enlighet med bolagets automatiska gallringsrutiner. Logguppgifter i form av bildernas filnamn har dock sparats en något längre tid, nämligen 100 dagar, innan även dessa uppgifter raderades. Med denna uppgift har Verisure kunnat kontrollera hur många gånger en viss operatör har öppnat en bild. Sedan augusti 2022 har en justering av lagringstiden för logguppgifter skett. Justeringen innebär att samtliga logguppgifter, förutom bilder, lagras i fem år. Justeringen avseende lagringstiden för logguppgifterna är delvis ett resultat av behovet av att kunna utreda bildhantering under en längre period bakåt i tiden.

Om tipsen

Gällande det första tipset som inkommit till IMY om inloggningsuppgifter stämmer uppgifterna i stora delar inte överens med Verisures uppfattning. Det har funnits goda skäl till det aktuella användandet av en viss typ av inloggningsuppgifter och förfarandet har utformats med beaktande av relevant dataskyddslagstiftning. Användningen har dessutom pågått under en begränsad tid och har nu avvecklats. Avseende de två andra tipsen är Verisure inte att anse som personuppgiftsansvarig för de beskriva behandlingarna. I det ena tipset har en av Verisures franchisetagare tillika personuppgiftsbiträde tydligt agerat utanför sin instruktion och det bolaget är därmed att anse som personuppgiftsansvarig för den aktuella händelsen. Trots att Verisure inte är personuppgiftsansvarig för den aktuella behandlingen har bolaget dock tagit tipset på stort allvar och agerat därefter. Verisure har bland annat bistått den aktuella franchisetagaren i utredningen av händelsen som beskrivs i tipset. Det andra tipset rör ett annat bolag.

Omfattningen av IMY:s prövning i ärendet

Dataskyddsförordningen innehåller ett stort antal regler som måste följas i samband med behandling av personuppgifter. Inom ramen för detta tillsynsärende granskar IMY inte samtliga regler och frågeställningar som kan aktualiseras i Verisures verksamhet.

IMY:s prövning i ärendet har avgränsats till att omfatta den i media beskriva personuppgiftsbehandlingen samt att avse i vad mån bolaget vidtagit lämpliga tekniska och organisatoriska åtgärder för att skydda bolagets kunders personuppgifter vid den interna hanteringen av bildmaterial i enlighet med artikel 32 i dataskyddsförordningen.

Motivering av beslutet

Tillämpliga bestämmelser

Personuppgiftsansvarig är enligt artikel 4.7 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller

tillsammans med andra bestämmelser ändamålen och medlen för behandlingen av personuppgifter.

Enligt principen om ansvarsskyldighet i artikel 5.2 i dataskyddsförordningen ska den personuppgiftsansvarige ansvara för efterlevnaden av principerna som beskrivs i första stycket i artikeln, däribland säkerhetsprincipen (artikel 5.1 f i dataskyddsförordningen). Ansvarsskyldighetsprincipen har vidareutvecklats i artikel 24 där det framgår att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen.

Av artikel 28.10 i dataskyddsförordningen följer att om ett personuppgiftsbiträde överträder denna förordning genom att fastställa ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen, utan att det påverkar tillämpningen av artiklarna 82, 83 och 84.

Av artikel 32.1 i dataskyddsförordningen följer att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Vid bedömningen av vilka tekniska och organisatoriska åtgärder som är lämpliga ska den personuppgiftsansvarige beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.

Enligt artikel 32.1 omfattar lämpliga skyddsåtgärder, när det är lämpligt,

- a) pseudonymisering och kryptering av personuppgifter,
- b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
- c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och
- d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Enligt artikel 32.2 i dataskyddsförordningen ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet för oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Personuppgiftsansvar

Personuppgiftsansvar i tipsen

Verisure har uppgett att bolaget är personuppgiftsansvarig för den personuppgiftsbehandling som det första tipset om inloggningsuppgifter har avsett, vilket stöds av utredningen i ärendet. IMY bedömer att Verisure är personuppgiftsansvarig för den behandlingen i den mening som avses i artikel 4.7 i dataskyddsförordningen.

Vad gäller de två andra tipsen har Verisure anfört att bolaget inte är personuppgiftsansvarig för de beskrivna behandlingarna. Avseende det ena tipset

bedömer IMY att det mot bakgrund av den i tipset aktuella personuppgiftsbehandlingen art inte finns skäl att ifrågasätta att behandlingen gått utanför de instruktioner som personuppgiftsbiträdet fått och att Verisure därför inte är att anse som personuppgiftsansvarig. Avseende det andra tipset konstaterar IMY att det inte finns skäl att ifrågasätta att ett annat bolag är personuppgiftsansvarig för den behandlingen. IMY bedömer därför att Verisure inte är personuppgiftsansvarig för behandlingarna som dessa två tips avser varför dessa behandlingar inte omfattas av den fortsatta prövningen i detta beslut.

Personuppgiftsansvar i övrigt

Verisure har anfört att bolaget är personuppgiftsansvarig för behandling av personuppgifter i form av bildmaterial inom ramen för bolagets incidenthantering. Verisure har även anfört att bolaget är gemensamt personuppgiftsansvarig med kunden för den övervakning som kunden själv företar genom att använda Verisures monitoreringsfunktion i sin bostad, tomt och andra privata byggnader. Enligt Verisure blir bolaget trots detta dock att anse som ensamt personuppgiftsansvarig även avseende den behandlingen om det så kallande privatundantaget i artikel 2.2 c i dataskyddsförordningen är tillämpligt för kunden. Detta då kundens behandling av personuppgifter i det fallet faller utanför dataskyddsförordningens tillämpningsområde.

Vad Verisure anfört vinner stöd av övrig utredning i ärendet. IMY bedömer därför att Verisure är personuppgiftsansvarig för den aktuella personuppgiftsbehandlingen i den mening som avses i artikel 4.7 i dataskyddsförordningen.

Tipset om inloggningsuppgifter

I tipset har gjorts gällande att Verisure använt en viss typ av inloggningsuppgifter på ett sätt som skulle kunna strida mot dataskyddsförordningen. Mot bakgrund av vad Verisure uppgett om användandet av de aktuella inloggningsuppgifterna och vad som i övrigt framkommit i utredningen kan IMY dock inte konstatera någon brist i förhållande till dataskyddsförordningen.

Den i media påstådda hanteringen av bilder

I medierapporteringen som IMY tog del av innan tillsynen mot Verisure inleddes gjordes det gällande att anställda på Verisure delat uppgifter om bilder på lättklädda personer mellan sig och att flera av de anställda tagit del av bilderna genom bolagets larmhanteringssystem i syfte att roa sig. Den aktuella nyhetsartikeln gjorde också gällande att bilder kunde skickas mellan de anställda, bland annat i ett chattprogram.

IMY konstaterar att den behandling av bildmaterial som har beskrivits i media är mycket allvarlig och skulle kunna innebära ett stort intrång i enskildas personliga integritet. En sådan behandling skulle, som även Verisure har anfört, sakna rättslig grund i artikel 6 i dataskyddsförordningen och därmed vara otillåten. För att kunna konstatera en brist enligt dataskyddsförordningen måste det dock stå klart att den behandling av bildmaterial som beskrivits i media har skett.

Verisure har redogjort för den interna utredning som bolaget vidtagit för att utreda uppgifterna i media och har uppgett att det inte framkommit något i utredningen som tyder på att hantering av bildmaterial har skett på det sätt som har beskrivits i media.

IMY konstaterar att Verisure har vidtagit en omfattande intern utredning för att utreda den påstådda hanteringen av bildmaterial. Bolagets internutredning har inte visat att

det som påståtts i media har inträffat. Det har inte heller genom IMY:s utredning i ärendet i övrigt kunnat visas att det som beskrivits i media har skett. IMY bedömer därför att utredningen i ärendet inte ger stöd för att Verisure har brustit i efterlevnaden av dataskyddsförordningen på det sätt som har beskrivits i media.

Verisure har inte vidtagit lämpliga säkerhetsåtgärder

Mot bakgrund av vad som framkommit av utredningen i ärendet finner IMY dock skäl att pröva om Verisure vidtagit lämpliga åtgärder för att säkerställa en skyddsnivå som är lämplig utifrån riskerna med behandlingen.

Behandlingen har inneburit stora integritetsrisker och krävt en hög skyddsnivå

Den personuppgiftsansvariga ska säkerhetsställa en säkerhet som är lämplig utifrån riskerna med behandlingen. Bedömningen av lämplig skyddsnivå ska göras med beaktande av bland annat behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. Vid bedömningen ska särskild hänsyn tas till de risker som behandlingen medför, bland annat obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

IMY konstaterar att Verisure i sin verksamhet hanterar personuppgifter från ett stort antal registrerade.² IMY konstaterar vidare att det är fråga om en larmhanteringstjänst där kameror uppsatta i privatpersoners hem är en del av den tjänsten. Den behandling av personuppgifter som sker i och med detta är således bland annat insamling och hantering av bildmaterial bestående av personer som befinner sig i sin hemmiljö. Detta är en mycket integritetskänslig behandling. Vidare kan konstateras att personer som är kunder hos Verisure har anlitat bolaget i trygghets- och säkerhetssyfte och förlitar sig på att de kameror som finns uppsatta i hemmet endast används av Verisure för att säkerställa detta syfte. Det är således fråga om behandling av personuppgifter för vilka de registrerade har berättigade förväntningar på en hög grad av konfidentialitet och ett robust skydd mot obehörig och otillåten behandling. Denna typ av personuppgiftsbehandling sker dessutom inom ramen för Verisures kärnverksamhet, något som medför ännu högre krav på skyddsnivå.

Med hänsyn bland annat till att de uppgifter som Verisure behandlat har varit av integritetskänslig karaktär och berört ett stort antal personer har bolagets behandling av personuppgifter sammantaget inneburit en hög risk för fysiska personers rättigheter och friheter. Behandlingens art, omfattning och sammanhang har därmed medfört ett krav på en hög skyddsnivå för uppgifterna. Åtgärderna ska bland annat säkerställa att personuppgifter skyddas mot obehörigt röjande och obehörig åtkomst.

Uppgifterna har inte skyddats på ett lämpligt sätt

IMY ska därefter bedöma om Verisure har säkerställt den höga skyddsnivå som krävts. För att kunna upprätthålla säkerheten för de personuppgifter som behandlas i en verksamhets system är det grundläggande att kunna ha kontroll över vad som sker, och vad som har skett med uppgifterna. För den registrerade finns även en rätt att få tillgång till sina personuppgifter och information om hur uppgifterna har behandlats. För att den registrerade ska kunna utöva denna rättighet och därigenom bland annat kunna kontrollera lagligheten av behandlingen är det grundläggande att den

² Enligt Verisures webbplats har bolaget ca 500 000 svenska kunder, se Verisure, "Om oss".
<https://www.verisure.se/om-oss> [2024-11-27]

personuppgiftsansvarige har kontroll över hur uppgifterna behandlas eller har behandlats.³ Detta kan exempelvis ske genom loggföring.

Av utredningen i ärendet framgår att bildmaterialet lagras i en viss på förhand bestämd tid och raderas därefter från systemet. Efter denna period går det inte att eftersöka operatörers hantering av enskilda bilder. Inom ramen för bildhantering loggas däremot även andra uppgifter med nära anknytning till bildhanteringen under en något längre tid. Innan augusti 2022 sparades logguppgifter i form av bildernas filnamn i sammanlagt 100 dagar. Denna logguppgift gör det möjligt att kontrollera hur många gånger en viss operatör har öppnat en bild.

Vad gäller lagringstiden för Verisures logguppgifter gör IMY följande bedömning. Bildmaterial från kunders kameror i hemmet är som tidigare konstaterats förknippade med ett tungt vägande integritetsintresse. Mot bakgrund av detta samt de ändamål med behandlingen som Verisure har beskrivit och vad bolaget i övrigt uppgett anser IMY att den tid Verisure lagrar bildmaterialet är proportionerlig.

Det finns dock andra mindre integritetskänsliga logguppgifter som kan användas för att kontrollera att bildmaterial inte hanteras på ett otillbörligt sätt och därmed säkerställa att personuppgifter skyddas mot obehörigt röjande och obehörig åtkomst. Logguppgifter i form av bildernas filnamn är en sådan logguppgift med vilken man kan eftersöka hur många gånger en viss bild har öppnats i systemet. Enligt Verisure har dock dessa logguppgifter endast lagrats i 100 dagar vilket gjort att någon eftersökning av eventuell felhantering av bildmaterial inte kunnat göras efter denna period. Med beaktande av den höga skyddsnivå som har krävts för personuppgifterna bedömer IMY att den aktuella lagringstiden för logguppgifter om bildernas filnamn har varit för kort för att skydda uppgifterna mot obehörigt röjande eller obehörig åtkomst i tillräcklig grad och att säkerställa konfidentialiteten för personuppgifterna som behandlas i deras system.

IMY bedömer därför att Verisure inte har vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som var lämplig i förhållande till risken med behandlingen. Anledningen till detta är att Verisure inte lagrat logguppgifter om bildernas filnamn tillräckligt länge för att kunna eftersöka eventuell felhantering av personuppgifter i form av bildmaterial från kunders kameror. Genom detta har Verisure också saknat förmåga att i tillräcklig grad säkerställa skyddet för de registrerades rättigheter.

Verisure har dock inom ramen för en generell översyn av lagringstider under tiden för IMY:s tillsyn, implementerat en ny lagringstid för bildernas filnamn som innebär att logguppgifter om filnamnen sedan augusti 2022 sparas i fem år. Verisure har uppgett att justeringen av lagringstiden för filnamnen delvis är ett resultat av behovet att kunna utreda bildhantering under en längre period bakåt i tiden. Genom denna justering anser IMY att Verisure sedan augusti 2022 inte längre brister i efterlevnaden av dataskyddsförordningen på det sätt som beskrivits ovan.

Inom ramen för denna tillsyn har Verisure även redogjort för andra tekniska och organisatoriska säkerhetsåtgärder som bolaget har vidtagit för att skydda kunders personuppgifter vid den interna hanteringen av bildmaterial. Med anledning av vad

³ Jfr EU-domstolens dom Pankki S, C-579/21, EU:C:2023:501, punkt 37-83.

Verisure uppgett i denna del konstaterar IMY att det inte framkommit annat än att de övriga skyddsåtgärderna framstår som lämpliga.

Sammantaget bedömer IMY att Verisure har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen. Av utredningen i ärendet kan utläsas att den begränsade lagringstiden för de aktuella logguppgifterna har förelegat åtminstone sedan tiden för tillsynens inledande den 20 april 2022 fram till augusti 2022. IMY bedömer därför att Verisure har behandlat personuppgifter i strid med dataskyddsförordningen under tiden den 20 april 2022 till augusti 2022.

Val av ingripande

Av artikel 58.2 i och artikel 83.2 i dataskyddsförordningen framgår att IMY har befogenhet att påföra administrativa sanktionsavgifter i enlighet med artikel 83. Beroende på omständigheterna i det enskilda fallet ska administrativa sanktionsavgifter påföras utöver eller i stället för de andra åtgärder som avses i artikel 58.2, som till exempel förelägganden och förbud. Vidare framgår av artikel 83.2 vilka faktorer som ska beaktas vid beslut om administrativa sanktionsavgifter ska påföras och vid bestämmande av avgiftens storlek. Om det är fråga om en mindre överträdelse får IMY enligt vad som anges i skäl 148 i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

Vid bedömningen av valet av ingripande beaktar IMY följande. IMY har bedömt att Verisure har överträtt artikel 32.1 i dataskyddsförordningen genom att under tiden den 20 april 2022 till augusti 2022 inte ha lagrat logguppgifter om bildernas filnamn tillräckligt länge för att kunna eftersöka eventuell felhantering av personuppgifter och på så sätt bland annat kunna säkerställa att personuppgifterna skyddades mot obehörigt röjande och obehörig åtkomst. En överträdelse av den bestämmelsen kan föranleda en sanktionsavgift.

Bildmaterial innehållandes personer i deras hemmiljö är mycket integritetskänsliga personuppgifter. Ett obehörigt röjande eller åtkomst till sådana personuppgifter medför en hög risk för de registrerades fri- och rättigheter. Verisure har saknat förmåga att eftersöka eventuell felhantering av personuppgifterna längre tillbaka i tiden än 100 dagar vilket innebär en risk för att obehörigt röjande eller åtkomst har kunnat ske utan att Verisure haft förmåga att kontrollera detta och vidta eventuella lämpliga åtgärder.

Verisure har dock inom ramen för en intern översyn, bland annat för att göra det möjligt att utreda bildhantering längre tillbaka i tiden, ändrat lagringstiden för de aktuella logguppgifterna på så sätt att de nu lagras i fem år. Detta gjordes visserligen efter att IMY inlett den nu aktuella tillsynen men innebär att Verisure därmed åtgärdat bristen. Vidare har den konstaterade bristen i sig inte inneburit att personuppgifter har behandlats på ett otillåtet sätt utan rör möjligheten att i efterhand kunna kontrollera behandlingen av uppgifterna.

IMY finner vid en samlad bedömning av omständigheterna i ärendet att det är fråga om en sådan mindre överträdelse i den mening som avses i skäl 148 att det finns anledning att avstå från att påföra Verisure en sanktionsavgift för den konstaterade överträdelsen. Verisure ska därför, med stöd av artikel 58.2 b i dataskyddsförordningen, i stället ges en reprimand för den konstaterade överträdelsen.

Detta beslut har fattats av enhetschefen Jenny Bård efter föredragning av avdelningsjuristen Sarah Bodlander. Vid den slutliga handläggningen av ärendet har även avdelningsjuristen Andreas Persson och it- och informationssäkerhetsspecialisten Petter Flink medverkat.

Jenny Bård

Kopia till
Dataskyddsombudet

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till IMY. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till IMY inom tre veckor från den dag ni fick del av beslutet. Om ni är en part som företräder det allmänna ska överklagandet dock ha kommit in inom tre veckor från den dag då beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder IMY det vidare till Förvaltningsrätten i Stockholm för prövning.

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