Statens Servicecenter, SSC

Statens servicecenters hantering av en personuppgiftsincident - Tillsyn enligt dataskyddsförordningen

Innehållsförteckning

Datainspektionens beslut

Datainspektionen konstaterar att Statens servicecenter **i egenskap av personuppgiftsbiträde** först den 20 augusti 2019 underrättade personuppgiftsansvariga myndigheter om en personuppgiftsincident som myndigheten fick vetskap om den 28 mars 2019. Detta innebär att Statens servicecenter överträtt artikel 33.2 i dataskyddsförordningen, då underrättelserna inte skedde utan onödigt dröjsmål efter att Statens servicecenter fått vetskap om personuppgiftsincidenten.

Datainspektionen beslutar med stöd av 6 kap. 2 § dataskyddslagen och artiklarna 58.2 och 83 dataskyddsförordningen att Statens servicecenter ska betala en administrativ sanktionsavgift på 150 000 kronor för överträdelsen av artikel 33.2 i dataskyddsförordningen, det vill säga för underlåtenheten att utan onödigt dröjsmål underrätta de personuppgiftsansvariga myndigheterna om den i tillsynsärendet aktuella personuppgiftsincidenten.

Datainspektionen konstaterar att Statens servicecenter **i egenskap av personuppgiftsansvarig** först den 25 juni 2019 till Datainspektionen kom in med en anmälan om en personuppgiftsincident som myndigheten fick vetskap om den 28 mars 2019. Detta innebär att Statens servicecenter överträtt artikel 33.1 i dataskyddsförordningen, då anmälan om personuppgiftsincidenten inte skedde inom 72 timmar efter att Statens servicecenter fått vetskap om den.

Vidare har Statens servicecenter som personuppgiftsansvarig inte dokumenterat väsentliga omständigheter kring personuppgiftsincidenten

och de korrigerande åtgärder som vidtagits och därmed överträtt artikel 33.5 i dataskyddsförordningen.

Datainspektionen beslutar med stöd av 6 kap. 2 § dataskyddslagen och artiklarna 58.2 och 83 i dataskyddsförordningen att Statens servicecenter ska betala en administrativ sanktionsavgift om 50 000 kronor för överträdelsen av artikel 33.1 i dataskyddsförordningen, det vill säga för underlåtenheten att anmäla personuppgiftsincidenten till Datainspektionen inom 72 timmar efter att ha fått vetskap om den.

Datainspektionen beslutar att med stöd av artikel 58.1 d i dataskyddsförordningen förelägga Statens servicecenter att:

1. Upprätta rutiner för dokumentation av personuppgiftsincidenter som gör det möjligt för Datainspektionen att kontrollera efterlevnaden av artikel 33 i dataskyddsförordningen. Rutinerna ska svara mot kraven i artikel 33.5 i dataskyddsförordningen, som föreskriver att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits, och därefter
2. löpande kontrollera och se till att rutinerna följs.

Datainspektionen konstaterar att Statens servicecenter som personuppgiftsbiträde respektive personuppgiftsansvarig vid inspektionstillfället saknade personuppgiftsbiträdesavtal som överensstämde med kraven i artikel 28.4 respektive artikel 28.3 i dataskyddsförordningen, men att Statens servicecenter nu har personuppgiftsbiträdesavtal som uppfyller förordningens krav. Datainspektionen vidtar i detta fall ingen ytterligare korrigerande åtgärd med anledning av denna inledningsvis konstaterade brist.

Redogörelse för tillsynsärendet

En anmälan om en personuppgiftsincident avseende personuppgifter som rörde personal på Statens servicecenter (härefter SSC) och som behandlades i systemet Primula inkom till Datainspektionen den 25 juni 2019. Enligt anmälan upptäcktes incidenten den 28 mars 2019. Datainspektionen fick också in, från den 13 augusti 2019 och fram till det att tillsynen inleddes, 37 anmälningar om personuppgiftsincidenter i Primula från myndigheter som

SSC är personuppgiftsbiträde åt, det vill säga personuppgiftsansvariga myndigheter. Var och en av de personuppgiftsansvariga myndigheterna fick kännedom om incidenten genom en underrättelse från SSC. Enligt anmälningarna inträffade incidenten från och med den 14 mars till och med den 30 maj 2019. En av de personuppgiftsansvariga myndigheterna bifogade till sin anmälan nämnda underrättelse från SSC, vilken var daterad den 12 augusti 2019.

Datainspektionen har inlett tillsyn i syfte att granska SSC:s hantering av personuppgiftsincidenter i systemet Primula. Tillsynen inleddes med en skrivelse till SSC den 18 september 2018 och följdes upp med begäran om komplettering den 5 november 2019 respektive den 17 januari 2020.

Statens servicecenters uppgifter
SSC har i huvudsak uppgett följande som svar på Datainspektionens frågor.

Den 28 mars 2019 fick SSC via dataskyddsombudet på en personuppgifts-ansvarig myndighet in en anmälan från en anställd på samma myndighet (härefter ”anmälaren”) om att det gick att komma åt personuppgifter som tillhörde andra personuppgiftsansvariga myndigheter. En intern incident-rapport upprättades av SSC inom tolv timmar från denna tidpunkt. Den bugg som antogs vara källan till problemet ansågs ha åtgärdats den 29 mars 2019. Det visade sig dock att buggen inte lösts eller att nya buggar uppkommit. Anmälaren påpekade detta för SSC under april. SSC lyckades inte återskapa incidenten såsom den beskrivits av anmälaren. Den 21 maj 2019 lämnade anmälaren ytterligare information om hur buggen visat sig och det framkom även att anmälaren vidtagit ytterligare programmeringsåtgärder i Primula. SSC anmälde ärendet till personuppgiftsbiträdet EVRY, som den 3 juni meddelade att ärendet var löst. SSC polisanmälde anmälaren den 24 maj 2019 eftersom det enligt SSC stod klart att denne själv utvecklat och verkställt kod i Primula i syfte att bereda sig tillgång till uppgifter.

Den 12 augusti 2019 skickade SSC en underrättelse om personuppgiftsincidenten till de 47 personuppgiftsansvariga myndigheter som använde sig av Primula. Ett kompletterande utskick till samma myndigheter gjordes den 29 augusti 2019.

Cirka 282 000 registrerade, varav 1 800 var anställda hos SSC, berördes av personuppgiftsincidenten. Följande kategorier av personuppgifter

omfattades: personnummer, namn, uppgift om kön, uppgift om skyddad adressuppgift (dock inte de skyddade uppgifterna), ekonomisk eller finansiell information (underlag för att räkna ut rätt skatt såsom skattetabell, skattekolumn, jämkning, procentuell skatt, medborgar- och arbetsland och så vidare), anställningstid, tjänstgöringsort, arbetstillstånd, nyckelperson, beräknad NOR, anteckning om anhörig (dock inte uppgift om vem den anhörige är).

Angående uppgifternas grad av känslighet kan enligt SSC uppgifter om personnummer dels anses skyddsvärda i sig, dels vara reglerade av stark sekretess enligt 39 kap. 3 § offentlighets- och sekretesslagen (2009:400), OSL. Den senare sekretessen gäller för nio av de myndigheter som använde sig av Primula. En uppgift om att någon har skyddade adressuppgifter kan omfattas av sekretess enligt 21 kap. 3 § och 39 kap. 3 § första stycket OSL, sekretessen är då extra svag eller svag. SSC:s bedömning var därför att vissa av personuppgifterna omfattades av sekretess och var av integritetskänsligt slag.

Anledningen till att SSC dröjde med att underrätta, var att SSC ville ha bekräftat om och hur incidenten inträffat innan de berörda myndigheterna underrättades, vilket enligt SSC är en förutsättning för att anses ha kunskap/vetskap om incidenten enligt artikel 33.2. Samma skäl låg bakom att SSC i egenskap av personuppgiftsansvarig dröjde med att anmäla personuppgiftsincidenten till Datainspektionen. Det angavs också i anmälan om personuppgiftsincidenten att det fortsatt var oklart hur den obehöriga åtkomsten faktiskt sett ut och om obehöriga hade tillgång till personuppgifter som SSC var personuppgiftsansvarig för, vilket inte hade kunnat bekräftas vid tidpunkten för anmälan.

SSC uppfattade de svar som lämnades från systemleverantören, EVRY, som vaga. Kort efter incidenten frågade SSC systemleverantören om användare kunde ta del av personuppgifter för personer utanför den egna myndigheten. Därefter höll SSC återkommande uppföljningsmöten och fortsatte ställa samma fråga utan att få ett konkret svar från systemleverantören. SSC fick inte heller svar efter att myndigheten ställt frågan mejlledes. Efter sommaren bedömde SSC att det var nödvändigt att underrätta de berörda myndigheterna, även om uppgifterna (om incidenten) fortfarande inte hade bekräftats. Vid det tillfället ansåg inte heller SSC att det fanns någon oro för att exponera pågående säkerhetsbrister i systemet genom att lämna underrättelse om den misstänkta incidenten.

Det stod klart relativt snabbt efter att anmälan kom in till SSC att det fanns säkerhetsbrister i Primula, men inte nödvändigtvis att det inträffat en personuppgiftsincident, utom för den myndighet som anmälde bristen. Den 20 augusti 2019 fick SSC bekräftelse på att det varit möjligt att ta del av personuppgifter på andra myndigheter som SSC var personuppgiftsbiträde åt. SSC har uppgivit att servicecentret inte utredde händelsen tillräckligt skyndsamt och att avsaknaden av tydliga och dokumenterade rutiner för att hantera dessa frågor på ett samordnat sätt har bidragit till förseningen med att underrätta de berörda myndigheterna.

SSC har ett personuppgiftsbiträdesavtal med EVRY som gjordes under tiden för personuppgiftslagen (1998:204), PUL. Redan före dataskyddsförordningens ikraftträdande har dock SSC sökt ändring i befintligt PUB-avtal för att ersätta detta med ett som följer dataskyddsförordningens terminologi och formkrav i övrigt.

SSC har dokumenterat personuppgiftsincidenten genom polisanmälan, SSC:s anmälan till Datainspektionen, underrättelserna till de personuppgiftsansvariga myndigheterna, den incidentrapport som upprättades och kommunikationen med anmälaren som upptäckte och utnyttjade säkerhetshålet. Dokumentationen finns diarieförd i tre olika ärenden, varav underrättelserna, incidentrapporten och kommunikationen med anmälaren är ett eget ärende.

Efter slutkommunicering har SSC framfört följande synpunkter.

Personuppgiftsbiträdet EVRY har avtalsmässigt förbundit sig till att leverera en tjänst som är förenlig med gällande lagstiftning. Som ett uttryck för det avtalade kravet att tjänsten ska vara förenlig med gällande lagstiftning har SSC före dataskyddsförordningens ikraftträdande ställt ett antal frågor till EVRY om hur de nya kraven som följer av dataskyddsförordningen hanteras och säkerställs i Primula. EVRY har såväl lämnat svar som ändrat funktionalitet i tjänsten, som en följd av de nya kraven. De åtaganden som finns i det då gällande PUB-avtalet, tillsammans med andra säkerhetskrav och avtalsmässiga åtaganden, innebar en fullgod reglering vad gäller det materiella skyddet och behandlingen av personuppgifter. Den inträffade personuppgiftsincidenten, och de brister som därefter funnits i hanteringen, var inte en konsekvens av det då gällande personuppgiftsbiträdesavtalet eller

andra avtalade åtaganden. SSC har dock numera ett uppdaterat personuppgiftsbiträdesavtal med EVRY avseende Primula.

Datainspektionens blankett för anmälan av personuppgiftsincidenter har använts av SSC. Det vore anmärkningsvärt om Datainspektionen vid sin kontroll av efterlevnaden av artikel 33 ställer krav på ytterligare dokumentation än det underlag som personuppgiftsansvariga enligt Datainspektionens egna underlag är skyldiga att rapportera.

Övrigt som framkommit i tillsynen
Datainspektionen har tagit del av den incidentrapport som SSC upprättade i samband med anmälan från en person på en myndighet den 28 mars 2019. I rapporten beskrivs hur personen som anmälde incidenten kunde se bland annat personnummer för alla anställda på vissa myndigheter. Rapporten anger vidare att incidenten utifrån skador, kostnader och konsekvenser är att se som mycket allvarlig ”då känsliga uppgifter blev tillgängliga för användare som inte ska ha åtkomst till dessa”.

Datainspektionen har noterat att SSC i underrättelsen till myndigheterna den 12 augusti 2019 anger att SSC bedömt det som nödvändigt att säkerställa att nödvändiga säkerhetsåtgärder har vidtagits innan sådan underrättelse lämnades. Detta eftersom ”informationen berör ett flertal myndigheter som därigenom får kunskap om säkerhetsbrister hos varandra”.

Datainspektionen har begärt in den polisanmälan som SSC gjorde den 24 maj 2019. Av polisanmälan framgår att SSC anmält att en person som var anställd på en av de myndigheter som anlitar SSC för sin lönehantering, vid två olika tillfällen olovligen tagit sig in i systemet och på så sätt tagit del av information tillhörande andra myndigheter samt att informationen bestått i personuppgifter och ”löneuppgifter”.

Motivering av beslut

Rättslig bakgrund

Allmänt om ansvaret för personuppgiftsbehandlingar
En personuppgiftsansvarig ansvarar för att den följer dataskyddsförordningens bestämmelser vid behandling av personuppgifter, och för att säkerställa att anlitade personuppgiftsbiträden följer dataskyddsförordningen när de behandlar personuppgifter. I dataskyddsförordningen framgår detta av att dess bestämmelser i huvudsak

riktar sig till personuppgiftsansvariga, att denne enligt artikel 24 ansvarar för att genomföra tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandling av personuppgifter sker i enlighet med dataskyddsförordningen och att den enligt artikel 28 endast ska anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga sådana åtgärder.

Ett personuppgiftsbiträde, inklusive underbiträden, är ansvarigt för att följa de bestämmelser i dataskyddsförordningen som riktar sig direkt till personuppgiftsbiträden, däribland artikel 33.2. Dessutom kan personuppgiftsbiträden bli ansvariga för överträdelser av dataskyddsförordningen som är en följd av att de inte följt den personuppgiftsansvariges instruktioner.

Skyldighet att ha ett personuppgiftsbiträdeavtal
Enligt artikel 28.3 i dataskyddsförordningen ska ett personuppgiftsbiträdes behandling av personuppgifter för den personuppgiftsansvariges räkning regleras av ett personuppgiftsbiträdesavtal (eller annan bindande rättsakt). Avtalet ska bland annat föreskriva en skyldighet för personuppgiftsbiträden att se till att skyldigheterna i artiklarna 32–36 i dataskyddsförordningen fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

Personuppgiftsbiträden som anlitas av personuppgiftsbiträden, så kallade underbiträden, ska enligt artikel 28.4 i dataskyddsförordningen åläggas samma skyldigheter i fråga om dataskydd som anges i personuppgifts-biträdesavtalet med den personuppgiftsansvariga. Framförallt ska avtalet ge tillräckliga garantier om att underbiträdet ska genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen. Skyldigheterna ska åläggas genom ett avtal (eller annan bindande rättsakt).

Skyldighet att underrätta personuppgiftsansvariga
Personuppgiftsbiträden ska utan dröjsmål underrätta den personuppgifts-ansvarige efter att biträdet fått vetskap om att en personuppgiftsincident har ägt rum, se artikel 33.2 i dataskyddsförordningen. Personuppgiftsbiträdet ska därmed inte göra någon sannolikhetsbedömning vad gäller riskerna för de registrerades fri- och rättigheter. Det är den personuppgiftsansvarige som ska bedöma om personuppgiftsincidenten är sådan att den ska anmälas till

tillsynsmyndigheten. För att den personuppgiftsansvarige ska kunna uppfylla sin anmälningsskyldighet krävs att personuppgiftsbiträdet snabbt underrättar den ansvarige.

Skyldighet att anmäla till Datainspektionen
Det framgår av artikel 33.1 i dataskyddsförordningen att den personuppgifts-ansvarige vid en personuppgiftsincident ska anmäla incidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den. Om det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter behöver den inte anmälas. Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål, se artikel 33.4 i dataskyddsförordningen.

Enligt Artikel 29-gruppens vägledning WP250 får den personuppgifts-ansvarige vid en potentiell incident genomföra en kort undersökning för att fastställa huruvida en incident verkligen har ägt rum. Under denna undersökningsperiod kan den personuppgiftsansvarige inte anses ha fått ”vetskap” om incidenten. I de flesta fall bör, enligt samma vägledning, riskbedömning och anmälan till tillsynsmyndigheten slutföras så snart som möjligt efter den inledande varningen/misstanken om att en säkerhetsincident har ägt rum som kan inbegripa personuppgifter. Endast i undantagsfall bör detta ta längre tid. [1]

Skyldighet att dokumentera personuppgiftsincidenter
Enligt artikel 33.5 i dataskyddsförordningen ska den personuppgiftsansvarige dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av artikel 33 i dataskyddsförordningen.

[1] Artikel 29 – Arbetsgruppen för uppgiftsskydd, WP250rev.01; Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679; antagna den 3 oktober 2017; senast granskade och antagna den 6 februari 2018; antagna av EDPB under det första plenarsammanträdet den 25 maj 2018; s. 11–12. *Arbetsgruppen inrättades enligt artikel 29 i direktiv 95/46/EG och var ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet.*

Dokumentationsskyldigheten i artikel 33.5 är kopplad till ansvarsskyldigheten i artikel 5.2 i dataskyddsförordningen, det vill säga att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna för dataskydd efterlevs. Det finns även en koppling mellan artikel 33.5 och artikel 24 i dataskyddsförordningen. Den senare bestämmelsen innebär att den personuppgiftsansvarige ska vidta tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att den utför personuppgiftsbehandlingar i enlighet med dataskyddsförordningens bestämmelser.[2]

Datainspektionens bedömning

Rollfördelning och sammanfattning av händelseförloppet

SSC har beträffande de överträdelser av dataskyddsförordningen som detta beslut rör uppträtt i olika roller, som personuppgiftsansvarig respektive personuppgiftsbiträde. SSC har agerat i egenskap av personuppgiftsbiträde gentemot 47 personuppgiftsansvariga myndigheter som, genom anslutningen till SSC, använder sig av systemet Primula för hantering av personuppgifter om sin personal. Däremot har SSC agerat i egenskap av personuppgiftsansvarig vid behandling av personuppgifter om den egna myndighetens personal i samma system. SSC har anlitat företaget EVRY som personuppgiftsbiträde för driften av systemet Primula. EVRY har därmed varit personuppgiftsbiträde för behandlingen av såväl personuppgifter om anställda hos de 47 personuppgiftsansvariga myndigheterna som personuppgifter om anställda hos SSC.

En incident inträffade den 14 mars 2019 och den 28 mars 2019 tog SSC emot en anmälan om det inträffade från anmälaren. Anmälaren menade att den kunde se personuppgifter från andra myndigheter än den egna i Primula. En incidentrapport upprättades av SSC den 28 mars 2019. Efter att anmälan kompletterats med ytterligare uppgifter från anmälaren den 21 maj 2019 upprättade SSC en polisanmälan mot denne den 24 maj 2019.

I egenskap av personuppgiftsansvarig anmälde SSC den ovan beskrivna personuppgiftsincidenten till Datainspektionen den 25 juni 2019. Anmälan avsåg obehörig åtkomst till personuppgifter om myndighetens egen personal.

[2] WP250, rev01, s. 28.

I egenskap av personuppgiftsbiträde underrättade SSC de 47 personuppgiftsansvariga myndigheterna den 12 augusti 2019.

Den 20 augusti 2019 bekräftade EVRY för SSC att personuppgiftsincidenten innebar att det var möjligt för anställda på någon av de myndigheter som använde sig av Primula att komma åt personuppgifter från de andra myndigheter som använde sig av systemet.

Underrättelserna till myndigheterna gjordes för sent

Datainspektionen konstaterar att det dröjde närmare fem månader från det att incidenten upptäcktes den 28 mars 2019 till det att SSC underrättade de personuppgiftsansvariga myndigheterna den 12 augusti 2019. Det är betydligt mer tid än vad som kan anses krävas för en kortare undersökning för att tillägna sig vetskap om att en personuppgiftsincident inträffat. Till detta kommer att SSC gjorde en anmälan för egen del omkring sex veckor innan kundmyndigheterna underrättades. Det är tydligt att SSC inte visste mer om hur incidenten drabbat personuppgifterna för den egna personalen än hur den drabbat anställda på de personuppgiftsansvariga myndigheterna. Större kunskap kan därför inte motivera att SSC inte skickade underrättelser till de personuppgiftsansvariga myndigheterna trots att de gjorde en anmälan till Datainspektionen för egen del.

Dataskyddsförordningen kräver att den personuppgiftsansvarige blir underrättad utan onödigt dröjsmål så att den kan vidta de åtgärder som behövs med anledning av en inträffad incident. Datainspektionen bedömer att SSC hade tillräcklig vetskap för att vara skyldig att underrätta de personuppgiftsansvariga myndigheterna redan efter den första anmälan från ett dataskyddsombud på en av myndigheterna. Det saknades då enligt Datainspektionens bedömning anledning för SSC att vänta med underrättelsen till de personuppgiftsansvariga myndigheterna för att ”säkerställa att nödvändiga säkerhetsåtgärder vidtagits”.

Datainspektionen konstaterar att SSC genom att först den 20 augusti 2019 ha underrättat de personuppgiftsansvarige myndigheterna har överträtt artikel 33.2 i dataskyddsförordningen.

Anmälan till Datainspektionen gjordes för sent

Datainspektionen konstaterar att det dröjde nästan tre månader från det att incidenten kom till SSC:s kännedom den 28 mars 2019 till det att SSC

lämnade in en anmälan om incidenten till Datainspektionen den 25 juni 2019. Detta överstiger vida den tidsgräns om 72 timmar som anges i artikel 32.1 i dataskyddsförordningen. Det är också betydligt mer tid än vad som kan anses krävas för en kortare undersökning för att tillägna sig vetskap om att en personuppgiftsincident inträffat.

SSC har till Datainspektionen uppgett att de, i den bemärkelse som avses i artikel 33 i dataskyddsförordningen, fick vetskap om incidenten den 20 augusti 2019 då EVRY bekräftade att personuppgifter kunnat nås sinsemellan de myndigheter som använde sig av Primula. Datainspektionen har i detta avseende tagit fasta på SSC:s agerande både som personuppgiftsansvarig och som personuppgiftsbiträde eftersom SSC agerade utifrån samma händelse i båda rollerna.

Datainspektionens bedömning är att SSC måste ha vetat om att en personuppgiftsincident hade inträffat, i den bemärkelsen att SSC trodde på den information som lämnats till myndigheten om personuppgiftsincidenten den 28 mars 2019 och den 21 maj 2019. Den tydligaste indikationen på detta är att det som uppgavs i anmälan till Polismyndigheten den 24 maj 2019 var att en person tagit del av personuppgifter tillhörande andra myndigheter. Att döma av internrapporten ifrågasatte inte SSC uppgifterna om incidenten när den upprättades den 28 mars 2019.

Datainspektionen konstaterar mot bakgrund av ovanstående att SSC har överträtt artikel 33.1 i dataskyddsförordningen genom att inte anmäla personuppgiftsincidenten inom 72 timmar från den tidpunkt då anmälan kom in till SSC den 28 mars 2019.

Inget giltigt personuppgiftsbiträdesavtal
Under perioden 28 mars 2019 till och med 20 augusti 2019 hade SSC, i egenskap av personuppgiftsbiträde, inte ett personuppgiftsbiträdesavtal med EVRY som motsvarade kraven på vad ett personuppgiftsbiträdesavtal ska innehålla enligt artikel 28.4 i dataskyddsförordningen. SSC i egenskap av personuppgiftsansvarig saknade under samma period ett personuppgiftsbiträdesavtal med EVRY som motsvarade kraven på vad ett personuppgiftsbiträdesavtal ska innehålla enligt artikel 28.3.

Som personuppgiftsansvarig har SSC att se till att den personuppgiftsbehandling som utförs för myndighetens räkning omfattas av ett personuppgiftsbiträdesavtal.

Ett avtal mellan personuppgiftsbiträden ska ha ett innehåll som motsvarar kraven i artikel 28.3. Det framgår av artikel 28.4, som föreskriver att avtalet framförallt ska ”ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning”. Det är det personuppgiftsbiträde som anlitar ett annat biträde, i detta fall SSC, som ska se till att det finns ett avtal som uppfyller de angivna kraven. Detta eftersom det förstnämnda personuppgiftsbiträdet ansvarar för personuppgiftsbehandlingen gentemot den personuppgiftsansvarige för de underbiträden denne anlitat.

Datainspektionen konstaterar att SSC i egenskap av personuppgiftsansvarig respektive i egenskap av personuppgiftsbiträde överträtt artiklarna 28.3 och 28.4 i dataskyddsförordningen genom att ha anlitat ett personuppgiftsbiträde utan att i ett avtal eller annan rättsakt föreskriva sådana skyldigheter som krävs enligt artikel 28 i dataskyddsförordningen.

Brister i dokumentationen i rollen som personuppgiftsansvarig
Datainspektionen konstaterar att den dokumentation av personuppgiftsincidenten som SSC kommit in med inte klargör hur SSC ställde sig till den underrättelse som kom frånanmälaren och som gav SSC kännedom om incidenten. Det framgår inte hur SSC:s försök att återskapa incidenten gick till och vad det fanns för skäl att ifrågasätta uppgifterna som anmälaren lämnat. Därmed saknas de delar av omständigheterna kring personuppgiftsincidenten som krävs för att kunna visa varför incidenten inte anmäldes inom 72 timmar. Det framgår inte heller av dokumentationen vad SSC har gjort för att få svar på de frågor om incidenten som SSC anfört att myndigheten hade. Det saknas information om omständigheterna kring personuppgiftsincidenten som hade kunnat förklara dröjsmålet med anmälan. Vidare har SSC förklarat att dokumentationen av personuppgiftsincidenten såvitt rör SSC som personuppgiftsansvarig – i form av polisanmälan, anmälan till Datainspektionen, upprättad incidentrapport och kommunikation med den användare som underrättade SSC, finns i tre ärenden i SSC:s diarium. Det ärende som har den mesta dokumentationen – underrättelserna till myndigheterna, incidentrapporten och kommunikationen med användaren, finns i ett ärende som avser SSC:s roll

som personuppgiftsbiträde. Dokumentationen visar inte att den har gjorts för att uppfylla skyldigheten enligt artikel 33.5 i dataskyddsförordningen utan framstår som motiverad och ordnad efter andra principer.

En förutsättning för att Datainspektionen ska kunna följa upp en personuppgiftsincident baserat på dokumentationen är att den är samlad och ger en rättvisande bild av händelseförloppet. Dokumentationen har i det här fallet inte gjort det möjligt för Datainspektionen att kontrollera efterlevnaden av artikel 33 i dataskyddsförordningen.

Datainspektionen konstaterar att SSC i egenskap av personuppgiftsansvarig har överträtt artikel 33.5 i dataskyddsförordningen genom att inte dokumentera personuppgiftsincidenten på ett sätt som gjort det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av artikel 33 i dataskyddsförordningen.

Val av ingripande

Rättslig reglering

I artikel 58 i dataskyddsförordningen anges Datainspektionens samtliga befogenheter. Datainspektionen har vid överträdelser av dataskyddsförordningen ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a - j, bland annat reprimand, föreläggande och sanktionsavgifter. Av artikel 58.2 i dataskyddsförordningen följer att Datainspektionen i enlighet med artikel 83 ska påföra sanktionsavgifter utöver eller i stället för andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall. Om det är fråga om en mindre överträdelse får tillsynsmyndigheten, enligt skäl 148 i dataskyddsförordningen, utfärda en reprimand i stället för att påföra en sanktionsavgift.

Datainspektionen har ovan bedömt att SSC i de aktuella behandlingarna av personuppgifter har överträtt artiklarna 33 och 28 i dataskyddsförordningen. Dessa artiklar omfattas av artikel 83.4, som innebär att sanktionsavgifter som huvudregel ska påföras. Det är frågan om en myndighet. Sanktionsavgiften kan därför enligt 6 kap. 2 § dataskyddslagen (2018:218) bestämmas till högst 5 000 000 kronor.

Enligt artikel 83.1 i dataskyddsförordningen ska varje tillsynsmyndighet säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt

fall är effektivt, proportionellt och avskräckande.

I artikel 83.2 i dataskyddsförordningen anges samtliga faktorer som ska beaktas vid bestämmande av sanktionsavgiftens storlek. Vid bedömningen av storleken på sanktionsavgiften ska hänsyn tas till bland annat a) överträdelsens karaktär, svårighetsgrad och varaktighet, b) uppsåt eller oaktsamhet, samt g) de kategorier av personuppgifter som påverkas av överträdelsen.

Sanktionsavgifter ska påföras

De personuppgiftsincidenter som SSC inte underrättade de 47 personuppgiftsansvariga myndigheterna om i tid omfattade personuppgifter om cirka 280 000 registrerade. Personuppgifterna som riskerade att bli röjda omfattade bland annat personnummer, uppgift om att personer har skyddad adress (dock inte de skyddade uppgifterna i sig) och uppgifter om anställning. Det dröjde nästan fem månader innan de personuppgiftsansvariga myndigheterna underrättades från det att SSC fått vetskap om personuppgiftsincidenten. Det är därmed inte fråga om mindre överträdelser och det finns inte skäl att ersätta sanktionsavgiften med en reprimand.

Den personuppgiftsincident som SSC i egenskap av personuppgiftsansvarig inte anmälde till tillsynsmyndigheten Datainspektionen i tid omfattade personuppgifter om cirka 1 800 registrerade. Personuppgifterna som riskerade att blir röjda omfattade bland annat personnummer, uppgift om att personer har skyddad adress och uppgifter om anställning. Det dröjde närmare tre månader innan SSC kom in med en anmälan till Datainspektionen från det att SSC fick vetskap om personuppgiftsincidenten. Datainspektionen finner att det inte är fråga om en mindre överträdelse och att det inte finns skäl att ersätta sanktionsavgiften med någon annan korrigerande åtgärd.

SSC ska därför påföras administrativa sanktionsavgifter för dessa överträdelser.

Personuppgiftsbiträdesavtal

Datainspektionen har också konstaterat att SSC inte hade personuppgiftsbiträdesavtal som överensstämde med kraven i artiklarna 28.3 och 28.4 i dataskyddsförordningen. SSC har emellertid uppgett att SSC hade

personuppgiftsbiträdesavtal som var upprättade i enlighet med personuppgiftslagen, att det pågick ett arbete att uppdatera avtalen och att SSC numera har personuppgiftsbiträdesavtal med EVRY som överensstämmer med dataskyddsförordningens krav. Mot den bakgrunden finner Datainspektionen att det i det här fallet finns skäl att inte påföra en särskild sanktionsavgift eller annan korrigerande åtgärd med anledning av den brist som tidigare förelåg.

Omständigheter av betydelse för att fastställa sanktionsavgiftens storlek

Personuppgiftsincidenten rörde cirka 280 000 anställda hos 47 personuppgiftsansvariga myndigheter vad avser SSC:s roll som personuppgiftsbiträde och cirka 1 800 anställda hos SSC vad avser SSC:s roll som personuppgiftsansvarig.

Datainspektionen har, vid bedömningen av den sanktionsavgift som gäller underlåtenheten att i tid underrätta de personuppgiftsansvariga myndigheterna, bedömt att fördröjningen står i en tydlig konflikt med vikten av att de personuppgiftsansvariga snabbt får information om inträffade personuppgiftsincidenter så att de kan vidta lämpliga åtgärder.

Att informationen når ut snabbt är särskilt viktigt om personuppgiftsincidenten innebär en hög risk för fysiska personers rättigheter och friheter, eftersom den personuppgiftsansvarige då ska informera de registrerade utan dröjsmål (se artikel 34 i dataskyddsförordningen). Datainspektionen konstaterar att det i detta fall inte har varit fråga om en personuppgiftsincident som sannolikt inneburit en sådan hög risk. Datainspektionen bedömer att detta medför att förseningen kan bedömas som mindre allvarlig än vad som annars hade kunnat vara fallet.

Datainspektionen väger samtidigt in att incidenten omfattade ett stort antal registrerade, att den rörde myndighetens kärnverksamhet och att det har dröjt flera månader från det att SSC fick vetskap om den till dess att SSC underrättade myndigheterna. Dessa omständigheter är försvårande. Det ska också betonas att det rör sig om ett större antal överträdelser, genom i grunden samma felaktiga handlande, eftersom var och en av de 47 drabbade myndigheterna skulle ha underrättats utan onödigt dröjsmål.

Vad gäller sanktionsavgiften för underlåtenheten att i tid anmäla personuppgiftsincidenten till tillsynsmyndigheten, det vill säga till Datainspektionen, omfattade denna underlåtelse ett mindre antal registrerade än underlåtelsen att underrätta de personuppgiftsansvariga myndigheterna. En försvårande omständighet är även i detta fall att det dröjde flera månader innan SSC kom in med en anmälan till Datainspektionen.

När det gäller personuppgifternas karaktär har Datainspektionen inte anledning att anta någon annan ståndpunkt än SSC vad gäller personuppgifternas skyddsvärde, det vill säga att vissa av dem omfattades av sekretess och var integritetskänsliga.

Vad gäller om förseningarna med att anmäla och underrätta om incidenten skett med uppsåt eller av oaktsamhet finner Datainspektionen att SSC har haft uppsåt till förseningarna. Av utredningen framgår att SSC, i den bemärkelse som avses i artikel 33 i dataskyddsförordningen, haft vetskap om att en personuppgiftsincident inträffat som omfattat såväl SSC:s anställda som de personuppgiftsansvariga myndigheternas anställda. Detta har framgått dels genom den interna personuppgiftsincidentsrapport som upprättades den 28 mars 2019, dels genom den polisanmälan som SSC gjorde den 24 maj 2019. SSC har trots vetskapen om incidenten inte anmält den till Datainspektionen i tid eller underrättat myndigheterna utan obehörigt dröjsmål. Bestämmelserna i artikel 33 i dataskyddsförordningen är tydliga vad gäller tidsaspekten och det rör sig, under de omständigheter som kommit fram i tillsynen, inte om ett ursäktligt bedömningsfel.

Datainspektionen bestämmer utifrån en samlad bedömning att SSC ska betala en administrativ sanktionsavgift på 150 000 kronor för underlåtelsen att underrätta de personuppgiftsansvariga myndigheterna om personuppgiftsincidenten utan onödigt dröjsmål och att SSC ska betala en administrativ sanktionsavgift på 50 000 kronor för underlåtelsen att anmäla personuppgiftsincidenten till Datainspektionen utan onödigt dröjsmål. Beloppen är ägnade att vara effektiva, proportionella och avskräckande.

Föreläggande på grund av brister i dokumentation

Att personuppgiftsincidenten inte dokumenterades i enlighet med kriterierna i artikel 33.5 har inte utgjort en mindre överträdelse eftersom dokumentationen inte har kunnat användas av Datainspektionen för att

kontrollera efterlevnaden av artikel 33. Vid en prövning i enlighet med artikel 83.2 a) bedömer dock Datainspektionen att dokumentationen ändå inte har varit bristfällig till en sådan grad att det är befogat att påföra en sanktionsavgift. En sanktionsavgift framstår inte heller som proportionell. Däremot ska SSC, i egenskap av personuppgiftsansvarig, föreläggas att upprätta rutiner för dokumentation av personuppgiftsincidenter som gör det möjligt för Datainspektionen att kontrollera efterlevnaden av artikel 33 och framledes kontrollera och se till att dessa rutiner följs. Rutinerna ska åtminstone svara mot kraven i artikel 33.5 i dataskyddsförordningen, som föreskriver att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Elin Hallström. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Malin Blixt och enhetschefen Katarina Tullstedt medverkat. It-säkerhetsspecialisten Johan Ma har medverkat i de bedömningar som rör informationssäkerhet.

Lena Lindgren Schelin, 2020-04-28 (Det här är en elektronisk signatur)

Bilaga
Hur man betalar sanktionsavgift

Kopia för kännedom till:
Dataskyddsombud för Statens servicecenter

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.