Integritetsskydds myndigheten

Polismyndigheten
Skickas endast per e-post

Diarienummer:
DI-2020-3904

Ert diarienummer:
A194.851/2020

Datum:
2023-01-16

Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens personuppgiftsbehandling vid användning av e-post

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Polismyndigheten under perioden den 1 augusti till den 27 augusti 2018 behandlat personuppgifter i strid med 3 kap. 2 och 8 §§ brottsdatalagen (2018:1177). Detta genom att personuppgifter, som vid en spridning till obehöriga utanför myndigheten kan medföra en allvarlig negativ påverkan på den personliga integriteten, har fått skickas internt via e-post utan att myndigheten vidtagit tillräckliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att personuppgiftsbehandlingen är författningsenlig och för att skydda de personuppgifter som behandlas från obehörig eller otillåten behandling.

Integritetsskyddsmyndigheten konstaterar att det finns en risk för att de tekniska och organisatoriska åtgärderna som Polismyndigheten vidtagit inte är tillräckliga för att leva upp till kravet på lämplig skyddsnivå i 3 kap. 8 § brottsdatalagen. Integritetsskyddsmyndigheten rekommenderar därför, med stöd av 5 kap. 6 § första stycket brottsdatalagen, Polismyndigheten att vidta ytterligare åtgärder för att höja skyddsnivån kring hanteringen.

Vidare konstaterar Integritetsskyddsmyndigheten att det finns en risk för att Polismyndigheten inte fullgör den skyldighet att underrätta de registrerade som följer av 3 kap. 10 § brottsdatalagen när en personuppgiftsincident har inträffat, om inte åtgärder vidtas för att motverka risken. Integritetsskyddsmyndigheten rekommenderar därför Polismyndigheten, med stöd av 5 kap. 6 § första stycket brottsdatalagen, att se över sin hantering av när myndigheten är skyldig att underrätta berörda registrerade om en personuppgiftsincident.

Redogörelse för tillsynsärendet

Integritetsskyddsmyndigheten (IMY) mottog i september 2018 och februari 2020 två anmälningar om personuppgiftsincidenter enligt brottsdatalagen (ref.nr PUI-2018-859 och PUI-2020-428) från Polismyndigheten. Den första incidentanmälan avsåg e-postmeddelanden som oavsiktligt hade skickats till obehörig person under perioden mars 2016 till augusti 2018. Enligt myndighetens uppgifter innehöll cirka tio av dessa knappt sextio meddelanden integritetskänsliga personuppgifter, t.ex. uppgifter om

Postadress:
Box 8114
104 20 Stockholm
Webbplats:
www.imy.se
E-post:
imy@imy.se
Telefon:
08-657 61 00

misstänkt och brottsoffer, eller uppgifter som i sin tur gav åtkomst till den typen av uppgifter. Den andra incidentanmälan avsåg behörighet till en möteskalender som skickats via e-post. Mot bakgrund av dessa personuppgiftsincidenter inledde IMY en granskning av orsaken till incidenterna, om Polismyndigheten har tillräckliga rutiner för när personuppgifter får skickas via e-post samt om myndigheten i övrigt har vidtagit lämpliga åtgärder för att liknande incidenter inte ska upprepas. I granskningen har det också ingått att kontrollera om Polismyndighetens överväganden och bedömningar avseende frågan om det förelåg en skyldighet att underrätta berörda registrerade om de inträffade personuppgiftsincidenterna har varit förenliga med brottsdatalagen.

Information som polisanställda skickar via e-post kan hänföras till såväl den brottsbekämpande verksamheten som till Polismyndighetens övriga verksamhet. I det förra fallet ska brottsdatalagens bestämmelser tillämpas medan dataskyddsförordningens[1] bestämmelser gäller i det senare fallet. Denna tillsyn har avgränsats till en granskning enligt brottsdatalagen.

Polismyndigheten har under tillsynen besvarat ett antal frågor från IMY och skickat in relevanta interna styrdokument. Av myndighetens svar framgår att bakgrunden till incidenterna huvudsakligen varit att e-postmeddelanden av misstag har skickats till obehöriga mottagare genom att anställda vid myndigheten råkat stava fel på ”...@polisen.se” när mottagaradressen har angetts. Vidare har Polismyndigheten uppgett att en utomstående person har registrerat internetdomäner med snarlika stavningar till polisen.se och med en s.k. catch-all funktion[2] obehörigen tagit del av e-postmeddelanden som alltså egentligen varit avsedda till polisanställda. Detta har enligt myndigheten kommit till dess kännedom genom att domänägaren kontaktat myndigheten och berättat.

Polismyndigheten har uppgett att det av de interna riktlinjer som fanns redan innan incidentanmälan i september 2018 framgår att information inom informationsklasserna *öppen* till och med *högt skyddsvärde* får skickas internt via e-post inom myndigheten. Däremot tillåts inte att information med *mycket högt skyddsvärde* skickas på det sättet. Därutöver framgår att endast information som klassats såsom öppen får skickas till externa mottagare via vanlig e-post (dvs. utan någon form av krypteringslösning).

Av riktlinjerna framgår att informationsklassen högt skyddsvärde avser information som kan innebära allvarlig skada eller kränkning för Polismyndigheten, annan myndighet eller enskild fysisk eller juridisk person om den kommer till obehörigas kännedom. Vidare anges, som exempel på information med ett högt skyddsvärde, känsliga personuppgifter enligt personuppgiftslagen (dvs. den lag som gällde innan dataskyddsförordningen trädde i kraft), uppgifter som avser lagöverträdelser eller liknande uppgifter.

I riktlinjerna beskrivs informationsklassen mycket högt skyddsvärde som information som kan innebära mycket allvarlig skada eller kränkning för någon om uppgiften kommer till obehörigas kännedom.

Den 1 oktober 2022 ersattes de äldre riktlinjerna av nya. Av dessa följer att det fortsatt är tillåtet att skicka information i informationsklasserna öppen till och med högt

[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)
[2] Funktionen innebär att all e-post kommer till domänägaren oavsett vad som anges före @-tecknet.

skyddsvärde internt inom myndigheten via e-post, men det rekommenderas att gemensamma kataloger i första hand används vid delning av filer och vikten av att kontrollera mottagaradressen understryks. I de nya riktlinjerna används begreppet negativ konsekvens istället för skada/kränkning och det har förtydligats att det bland annat ska göras en bedömning av om ett röjande av uppgiften kan innebära en negativ påverkan på integriteten. Informationen har ett högt skyddsvärde om ett röjande bedöms medföra en allvarlig negativ påverkan på den personliga integriteten respektive ett mycket högt skyddsvärde om det bedöms medföra en mycket allvarlig sådan påverkan. Känsliga personuppgifter eller personuppgifter om lagöverträdelser nämns inte särskilt under någon av informationsklasserna.

Polismyndigheten har beskrivit att myndigheten har vidtagit ett antal säkerhetsåtgärder för att förhindra att e-postmeddelanden av misstag skickas till obehöriga personer. Redan innan den första incidentanmälan fanns det krav på att en anställd måste ansöka om behörighet för att kunna skicka e-post externt och det kom, precis som nu, upp ett automatiskt varningsmeddelande i form av en notis ovanför mottagaradressen med uppgift om att mottagaren finns utanför organisationen när en anställd skriver in en extern mottagaradress. Vidare har myndigheten uppgett att en e-postadress till en mottagare utanför organisationen, sedan innan den första incidentanmälan, automatiskt får en annan färg än om mottagaradressen går till en anställd inom myndigheten. Den 28 augusti 2018 har Polismyndigheten infört en teknisk spärr, i form av ett filter i polisens it-miljö, som stoppar möjligheten för anställda inom polisen att skicka e-postmeddelanden till bl.a. ett antal olika domännamn som liknar @polisen.se. Det framgår av inlämnat material att denna spärr har uppdaterats kontinuerligt med andra tänkbara felskrivningar.

Myndigheten har vidare framfört att den efter den första incidentanmälan lagt ut information på den interna hemsidan i syfte att göra de anställda medvetna om vikten av att skriva rätt mottagaradress. Myndigheten har också efter den första incidentanmälan infört en obligatorisk utbildning om bl.a. säkerhet vid e-posthantering som samtliga anställda med behörighet till myndighetens it-system, t.ex. behörighet att skicka e-post externt, måste genomföra. Därtill har det beskrivits att ytterligare information om säkerheten vid utskick av e-post har publicerats på den interna hemsidan sedan den senare incidenten och att fler åtgärder ska vidtas, t.ex. fler informationsinsatser och utbildningar, samt fastställande av en ny riktlinje för hur medarbetare ska agera vid personuppgiftsincidenter. Riktlinjen uppges kunna öka myndighetens möjligheter att upptäcka och hantera liknande incidenter samt att kunna vidta ytterligare konkreta åtgärder i syfte att förhindra sådana incidenter. Myndigheten har även anfört att de har en riktlinje för dataskydd vid verksamhetsutveckling, bl.a. för att säkerställa att det görs en rättslig bedömning av i vilken utsträckning e-post får användas vid ny eller förändrad behandling av personuppgifter.

Polismyndigheten har beträffande båda personuppgiftsincidenterna bedömt att det inte funnits någon skyldighet att underrätta berörda registrerade om det inträffade enligt 3 kap. 10 § första stycket brottsdatalagen, eftersom incidenterna inte kunde antas medföra särskild risk för otillbörligt intrång i de registrerades personliga integritet. Vad myndigheten närmare har framfört avseende denna bedömning framgår nedan.

Motivering av beslutet

Polismyndighetens skyldighet att vidta tekniska och organisatoriska åtgärder för att skydda de personuppgifter som skickas via e-post

Tillämpliga bestämmelser
Polismyndigheten är enligt 3 kap. 1 § brottsdatalagen och 1 kap. 4 § lagen (2018:1693) om polisens behandling inom brottsdatalagens område personuppgiftsansvarig för all behandling av personuppgifter som utförs under myndighetens ledning eller på myndighetens vägnar. Som personuppgiftsansvarig ansvarar Polismyndigheten för att behandlingen av personuppgifter inom myndigheten är författningsenlig och följer de grundläggande principerna för behandling av personuppgifter. Som ett led i det ansvaret ska Polismyndigheten enligt 3 kap. 2 § brottsdatalagen genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och visa att behandlingen utförs i enlighet med brottsdatalagens bestämmelser. Det innebär till exempel att det måste finnas tydliga rutiner och riktlinjer för anställdas behandling av personuppgifter vid användning av e-post. Av 3 kap. 1 § brottsdataförordningen (2018:1202) framgår att de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige ska vidta ska vara rimliga med hänsyn till behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen.

Vidare föreskrivs i 3 kap. 8 § brottsdatalagen en skyldighet att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas mot bl.a. obehörig eller otillåten behandling. Sådana åtgärder kan till exempel vara kontroller, utbildning i datasäkerhet och information om vikten av att följa gällande säkerhetsrutiner.[3] Åtgärderna ska enligt 3 kap. 11 § brottsdataförordningen åstadkomma en skyddsnivå som är lämplig med hänsyn till tekniska möjligheter, kostnader för åtgärderna, behandlingens art, omfattning, sammanhang och ändamål, de särskilda riskerna med behandlingen och hur integritetskänsliga personuppgifterna som behandlas är. Av 3 kap. 3 § brottsdatalagen följer även en skyldighet att se till att skyddsåtgärder integreras i behandlingen, när medlen för behandlingen bestäms och under själva behandlingen.

IMY:s bedömning
Av den incidentanmälan som skedde i september 2018 framgår att medarbetare vid Polismyndigheten utan avsikt har röjt personuppgifter avseende bland annat individer som varit föremål för brottsmisstankar eller ingått i brottsutredningar, i samband med att uppgifterna har behandlats i e-post. Av anmälan framgår att incidenten inträffade mellan den 28 mars 2016 och den 9 augusti 2018. Incidenten har således till väldigt stor del inträffat innan brottsdatalagen trädde ikraft den 1 augusti 2018.

I tillsynen har det framkommit att Polismyndigheten vid den första incidentanmälan hade riktlinjer som redogör för hur och när uppgifter får skickas via e-post. Riktlinjerna har nyligen ersatts av nya. Enligt både de äldre och de nya riktlinjerna är bedömningen av hur informationen klassas utifrån sitt skyddsvärde avgörande för frågan hur uppgifterna får skickas och hanteras i e-postsystemet. Av båda riktlinjerna följer att information med en informationsklass från öppen till och med högt skyddsvärde får

[3] Se prop. 2017/18:232 Brottsdatalag s. 457 f.

skickas internt via e-post inom myndigheten. Som beskrivits ovan definieras informationsklassen högt skyddsvärde på olika sätt i de två riktlinjerna. IMY har dock uppfattat det som att den nya definitionen inte innebär någon väsentlig skillnad i förhållande till den tidigare avseende bedömningen av hur personuppgifter får skickas. De nya riktlinjerna tydliggör dock att eventuell påverkan på integriteten är en av faktorerna som ska tas med i bedömningen.

IMY konstaterar utifrån detta att Polismyndigheten, både enligt sina tidigare och nuvarande riktlinjer, tillåter att personuppgifter, som vid ett röjande kan medföra en allvarlig negativ påverkan på någons personliga integritet, får skickas internt via e-post. Således tillåts personuppgifter som är särskilt integritetskänsliga att skickas via e-post internt, såvida uppgifterna i det enskilda fallet inte bedöms ha ett mycket högt skyddsvärde, trots att det i samma system är möjligt att skicka e-post till externa mottagare. Det kan t.ex. röra sig om känsliga personuppgifter[4], personuppgifter om lagöverträdelser[5] eller liknande kategorier av personuppgifter såsom personnummer, skyddade personuppgifter eller uppgift om att någon är målsägande eller vittne. De anmälda incidenterna visar också att personuppgifter inom dessa kategorier behandlades i interna e-postmeddelanden. Behandlingen av sådana personuppgifter är särskilt känslig när behandlingen sker inom Polismyndighetens operativa verksamhet, dvs. för brottsbekämpande och brottsutredande ändamål. En spridning av sådana uppgifter kan få långtgående konsekvenser för enskilda genom att det exempelvis kan leda till skadat anseende, hot och våld, diskriminering, identitetsbedrägeri eller brott mot regelverket om sekretess.

Det bör även framhållas att personuppgiftsincidenter ofta orsakas just av den mänskliga faktorn.[6] I och med att Polismyndigheten tillåter att personuppgifter som vid ett röjande kan medföra en allvarlig negativ påverkan på någons personliga integritet får skickas internt via e-post har myndigheten också ett stort ansvar för att vidta åtgärder som säkerställer en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen.

Detta innebär sammantaget att det måste ställas mycket höga krav på de tekniska och organisatoriska åtgärder som Polismyndigheten behöver vidta enligt 3 kap. 2 och 8 §§ brottsdatalagen för att skydda de registrerades rättigheter och de personuppgifter som behandlas.

Av Polismyndighetens svar till IMY framgår att det som avgör om ett e-postmeddelande går via e-post internt till en intern mottagare, eller via det öppna nätet till en extern mottagare är angivandet av mottagaradressen. Mottagaradressen har alltså en avgörande betydelse för vilket skydd uppgifterna i e-postmeddelandet får.

Polismyndigheten har angett att den innan incidentanmälan i september 2018 hade vidtagit ett antal säkerhetsåtgärder för att motverka att anställda av misstag skickar e-post till obehörig extern mottagare genom att felaktigt uppge en extern mejladress istället för en intern. Åtgärderna som beskrivs närmare ovan innebär att ett automatiskt varningsmeddelande uppkommer och att mejladressen får en avvikande färg när en

[4] Känsliga personuppgifter är bland annat uppgifter om etniskt ursprung, politiska åsikter, hälsa eller biometriska uppgifter, Se 2 kap. 11-12 §§ brottsdatalagen.
[5] Personuppgifter rörande lagöverträdelser är t.ex. att någon misstänks för ett brott eller har blivit föremål för straffprocessuella tvångsmedel. Se även IMY:s rättsliga ställningstagande IMYRS 2021:1 - innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen.
[6] Se IMY:s rapport Anmälda personuppgiftsincidenter 2022:1 s. 19

extern mejladress anges samt att särskild behörighet krävs för att kunna skicka e-post externt.

IMY:s bedömning är att de tekniska åtgärder som hade vidtagits före den första incidentanmälan, dvs. varningsmeddelande och avvikande färg på mottagaradressen, är sådana att de lätt kan förbigås omedvetet av den anställde. Det kan konstateras att det under denna period inte fanns någon teknisk spärr mot utskick till externa mejladresser som liknar Polismyndighetens egna mejladresser. Det fanns därför en påtaglig risk för att anställda, genom att oavsiktligt ange en extern mejladress istället för en intern, spred personuppgifter som var menade att gå till en intern mottagaren till obehöriga personer. Enligt de anmälda personuppgiftsincidenterna har detta också inträffat vid flera tillfällen, vilket påvisar att åtgärderna inte har varit tillräckligt effektiva för att begränsa risken för att personuppgifter av misstag skickas till extern mottagare. IMY gör mot den bakgrunden bedömningen att de tekniska och organisatoriska åtgärder som Polismyndigheten hade vidtagit vid brottsdatalagens ikraftträdande den 1 augusti 2018 och fram till slutet av augusti 2018 inte var tillräckliga för att uppfylla kraven i 3 kap. 2 och 8 §§ brottsdatalagen.

Polismyndigheten har beskrivit att man efter incidentanmälan i september 2018 genomfört ett antal ytterligare säkerhetsåtgärder. Myndigheten har t.ex. genomfört utbildnings- och informationsinsatser för att medvetandegöra medarbetarna om vikten av att skriva rätt mottagaradress. Det framhålls också särskilt i de nya riktlinjerna. Därutöver har myndigheten enligt vad som framgår närmare ovan infört en teknisk spärr i slutet av augusti 2018 som fångar upp och stoppar e-postmeddelanden som har skickats till domännamn som liknar @polisen.se. Myndigheten har uppgett att spärren kontinuerligt utökas med fler tänkbara felskrivningar av domäner. Vidare har myndigheten förklarat att den tekniska spärren inte aktualiserades vid den incident som skedde under 2020 eftersom e-postmeddelandet vid det tillfället inte skickades från Polismyndighetens e-postsystem.

De åtgärder som Polismyndigheten vidtagit efter den första incidentanmälan har höjt säkerhetsnivån och IMY lägger särskild vikt vid den tekniska spärr, dvs. funktionen som fångar upp och stoppar e-postmeddelande, som har införts för att motverka risken för att personuppgifter oavsiktligt sprids till obehöriga mottagare. Enligt IMY finns det emellertid en kvarvarande osäkerhet kring om de vidtagna åtgärderna sammantaget säkerställer en lämplig skyddsnivå och är tillräckligt effektiva för att förhindra nya liknande incidenter. Som IMY konstaterat ovan ställs mycket höga krav på de tekniska och organisatoriska åtgärder som Polismyndigheten behöver vidta för den aktuella behandlingen.

IMY konstaterar vidare att det finns ytterligare säkerhetsåtgärder som kan vara rimliga att överväga. Det kan t.ex. vara fråga om att helt separera den e-post som går internt inom myndigheten från den e-post som går externt eller att införa tekniska kontroller som innebär att den anställde aktivt måste bekräfta att denne är medveten om att meddelandet kommer att skickas till en extern mottagare via öppet nät och bekräfta att det säkerställts att informationen är sådan att den får skickas externt. Ett annat alternativ kan vara att myndigheten inte tillåter att sådana personuppgifter som bedöms omfattas av ett högt skyddsvärde får skickas internt via e-post. Det har i ärendet inte framkommit några tekniska hinder eller kostnadsaspekter som talar emot att Polismyndigheten skulle ha möjlighet att vidta ytterligare säkerhetsåtgärder för att förstärka skyddet.

IMY bedömer mot den bakgrunden att det finns skäl som talar för att Polismyndigheten behöver vidta ytterligare åtgärder för att leva upp till kravet på lämplig skyddsnivå i 3 kap. 8 § brottsdatalagen och 3 kap 11 § brottsdataförordningen. Det finns således en risk för att Polismyndigheten kommer att behandla personuppgifter i strid med dessa bestämmelser. Enligt IMY ger dock inte utredningen i ärendet tillräckligt stöd för att konstatera en överträdelse av bestämmelserna.

Polismyndighetens skyldighet att underrätta berörda registrerade om en personuppgiftsincident

Tillämpliga bestämmelser
Av 3 kap. 10 § första stycket brottsdatalagen följer att den personuppgiftsansvarige utan onödigt dröjsmål ska informera den registrerade om en incident om den har medfört eller kan antas medföra särskild risk för otillbörligt intrång i den registrerades personliga integritet. Det finns ett antal undantag från denna underrättelseskyldighet, vilka följer av paragrafens andra stycke och 3 kap. 11 § brottsdatalagen. Syftet med underrättelsen är framförallt att den registrerade ska kunna vidta nödvändiga åtgärder för att skydda sig själv.[7]

IMY:s bedömning
Denna tillsyn har inletts mot bakgrund av att Polismyndigheten har gjort två anmälningar om personuppgiftsincidenter till IMY och inom ramen för tillsynen har IMY granskat de överväganden och bedömningar som Polismyndigheten har gjort avseende frågan om det föreligger en skyldighet att underrätta berörda registrerade om incidenterna eller inte. Anmälningarna har i båda fallen gjorts mot bakgrund av brottsdatalagens bestämmelser, eftersom incidenterna huvudsakligen avsåg personuppgifter som Polismyndigheten behandlade inom ramen för den brottsbekämpande verksamheten.

Det åligger Polismyndigheten som personuppgiftsansvarig att i det enskilda fallet bedöma om det föreligger en skyldighet att underrätta de registrerade om en personuppgiftsincident. Vid bedömningen ska hänsyn tas till hur allvarliga konsekvenserna kan bli för den registrerade med anledning av incidenten och hur sannolikt det är att dessa konsekvenser inträffar, med beaktande av behandlingens art, omfattning, sammanhang och ändamål.[8] Den s.k. Artikel 29-gruppen, som numera är ersatt av Europeiska dataskyddstyrelsen, har tagit fram riktlinjer om anmälan av personuppgiftsincidenter enligt dataskyddsförordningen (WP250 rev0.1).[9] Riktlinjerna är i tillämpliga delar vägledande även för personuppgiftsbehandling enligt brottsdatalagen. I riktlinjerna rekommenderas att en personuppgiftsansvarig tar hänsyn till följande kriterier vid riskbedömningen: typen av incident, personuppgifternas natur, känslighet och volym, hur lätt det är att identifiera enskilda personer, konsekvensernas svårighetsgrad för enskilda personer, den enskildes speciella egenskaper, den

[7] Se skäl 62 till 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 (brottsdatadirektivet).
[8] Se skäl 52 till brottsdatadirektivet.
[9] EDPB har tagit fram kompletterande riktlinjer (Guidelines 01/2021 on Examples regarding Personal Data Breach Notification) innehållande ett flertal exempel på personuppgiftsincidenter och hur personuppgiftsansvarig bör hantera dessa.

personuppgiftsansvariges speciella egenskaper, antalet personer som påverkas och andra allmänna aspekter.[10]

Polismyndigheten har beträffande båda incidenterna bedömt att det inte funnits någon skyldighet att underrätta de registrerade om det inträffade eftersom incidenterna inte kunde antas medföra en särskild risk för otillbörligt intrång i de registrerades personliga integritet.

Enligt incidentanmälan 2018 fick en obehörig person kännedom om knappt sextio e-postmeddelanden, varav tio enligt Polismyndigheten innehöll integritetskänsliga personuppgifter bl.a. uppgift om brott. Myndigheten har framfört att bedömningen avseende underrättelseskyldigheten i det fallet gjordes mot bakgrund av att det inte fanns anledning att anta att den som obehörigen fått del av uppgifterna hade avsikt att använda eller sprida dessa, eftersom denne själv kontaktade Polismyndigheten och berättade om incidenten.

Enligt incidentanmälan 2020 var det fråga om ett e-postmeddelande innehållande inloggningsuppgifter till en bokningskalender av förhör som kom obehörig tillhanda. I kalendern fanns enligt Polismyndigheten vissa integritetskänsliga personuppgifter inskrivna. Beträffande denna händelse så har Polismyndigheten angett att det vid bedömningen av om underrättelseskyldighet föreligger beaktat att bokningskalendern innehöll endast en mycket liten del uppgifter som möjliggjorde identifiering av någon registrerad och att dessa uppgifter var mycket svåra att hitta för en vanlig användare samt att det ändå inte framgick vilken förhörsroll den registrerade hade eller vilket brott det rörde sig om. Vidare har myndigheten även tagit hänsyn till att uppgifterna fanns tillgängliga endast under en begränsad tid eftersom myndigheten raderade dessa strax efter att incidenten blev känd och att det, även i detta fall, saknades indikationer på att uppgifterna skulle sparas, spridas eller användas.

Enligt IMY ska följande beaktas vid bedömningen av risken för otillbörligt intrång i de registrerades personliga integritet med anledning av de aktuella incidenterna. Vid båda incidenterna har det rört sig om särskilt skyddsvärda personuppgifter, t.ex. personuppgifter avseende kontaktförbud eller kallelser till polisförhör, som obehöriga personer fått tillgång till. Det gäller framförallt vid den tidigare incidenten 2018, eftersom incidenten år 2020 enligt myndigheten omfattade ett begränsat antal uppgifter. Vid båda tillfällena har uppgifterna skickats okrypterat via ett öppet nät, vilket inneburit att andra än den direkta mottagaren kan ta del av de uppgifter som kommuniceras i nätet. Det är därför inte möjligt att, som Polismyndigheten har gjort, dra slutsatsen att uppgifterna genom incidenterna blivit tillgängliga för endast en obehörig person.

Det har vidare framgått att Polismyndigheten har beaktat mottagarens avsikter i sin riskbedömning. Artikel 29-gruppen nämner i sina riktlinjer att en mottagare som bedöms vara ”betrodd” kan göra incidenten mindre allvarlig. Med betrodd avses enligt riktlinjerna att den personuppgiftsansvarige i viss grad kan vara säker på att mottagaren inte kommer att läsa eller försöka få åtkomst till de uppgifter som felaktigt skickats till denne eller att vidta ytterligare åtgärder med uppgifterna, utan istället kommer följa den personuppgiftsansvariges instruktioner om att t.ex. förstöra uppgifterna. Som exempel på när en mottagare kan anses betrodd anges en situation där uppgifter av misstag skickats till fel avdelning inom en organisation eller en ofta använd leverantör och där den personuppgiftsansvarige har ett pågående

[10] Artikel 29-gruppens riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, WP250 rev.01, s. 25 ff.

förhållande med mottagaren samt känner till deras rutiner, historik och andra relevanta detaljer.[11] IMY kan konstatera att det inte har rört sig om en sådan situation i de aktuella fallen och inte heller en situation som kan jämföras med angivna exempel.

IMY finner mot denna bakgrund att det finns brister i de riskbedömningar som Polismyndigheten vidtagit som underlag för att avgöra om det i dessa fall funnits en skyldighet att underrätta registrerade om personuppgiftsincidenterna. Omständigheterna tyder på att detta utgör en systematisk brist i hur riskbedömningar görs hos Polismyndigheten. IMY konstaterar därför att det föreligger en risk för att Polismyndigheten inte fullgör sin underrättelseskyldighet enligt 3 kap. 10 § brottsdatalagen om inte myndigheten vidtar åtgärder för att motverka den risken.

Val av ingripande

Korrigerande befogenheter

Av 5 kap. 7 § brottsdatalagen framgår 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.

Ovan har IMY konstaterat att Polismyndigheten, under perioden 1 augusti till 27 augusti 2018, överträtt 3 kap. 2 och 8 §§ brottsdatalagen. Av 6 kap. 1 och 2 §§ brottsdatalagen följer att IMY kan utfärda sanktionsavgift vid överträdelse av dessa bestämmelser. I 6 kap. 4 § brottsdatalagen anges de faktorer som särskilt ska beaktas för att bestämma om en sanktionsavgift ska påföras samt vad som ska påverka sanktionsavgiftens storlek. Av denna bestämmelse följer att IMY särskilt ska ta hänsyn till om överträdelsen varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller kränkning som överträdelsen inneburit, överträdelsens karaktär, svårhetsgrad och varaktighet, vad den personuppgiftsansvarige gjort för att begränsa verkningarna av överträdelsen, och om den personuppgiftsansvarige tidigare ålagts att betala en sanktionsavgift. Uppräkningen är inte uttömmande utan anger de omständigheter som är särskilt viktiga.

IMY ska beroende på omständigheterna i varje enskilt fall välja en korrigerande åtgärd som är effektiv, proportionell och avskräckande.

IMY konstaterar att överträdelsen av brottsdatalagens bestämmelser har pågått under knappt en månad och att den kan medföra allvarliga konsekvenser för de registrerade med hänsyn till att det är fråga om personuppgifter som, om de sprids, kan innebära stora risker för intrång i den personliga integriteten. Den konstaterade bristen har inneburit att åtminstone en obehörig person har tagit del av ett antal personuppgifter som var särskilt integritetskänsliga. Den omständigheten att Polismyndigheten fick kännedom om det inträffade först när personen självmant kontaktade myndigheten tyder på att myndigheten inte har haft full kontroll över hur ofta e-postmeddelanden felaktigt har skickats utanför myndigheten istället för internt, varför det kan ha skett vid fler tillfällen än vad som framgår av de incidenter som rapporterats till IMY. Det är mot den bakgrunden svårt att bedöma hur många registrerade som har drabbats av att deras personuppgifter oavsiktligt har skickats till en mejladress utanför myndigheten under tiden för den aktuella överträdelsen av brottsdatalagen. Beträffande eventuell

[11] Se föregående not s. 26.

skada så har det inte inom ramen för tillsynen funnits förutsättningar att närmare utreda om överträdelserna har lett till att enskild har lidit någon faktisk skada

Samtidigt bör beaktas att Polismyndigheten har vidtagit flera tekniska och organisatoriska åtgärder både innan och efter att incidenterna anmälts till IMY, vilket tyder på att myndigheten arbetar kontinuerligt och systematiskt med informationssäkerhetsarbetet avseende den behandling av personuppgifter som tillsynen avser.

Vid en samlad bedömning anser IMY att det inte är proportionerligt att påföra en sanktionsavgift för den konstaterade bristen. Inte heller är det aktuellt med ett föreläggande eller varning då den konstaterade bristen inte är pågående.

Förebyggande befogenheter

Om det finns en risk för att viss personuppgiftsbehandling kan komma att stå i strid med lag eller annan författning ska IMY genom de förebyggande befogenheterna som följer av 5 kap. 6 § brottsdatalagen försöka förmå den personuppgiftsansvarige att vidta åtgärder för att motverka den risken. Det kan ske genom råd, rekommendationer eller påpekanden. Om det inte bedöms tillräckligt har IMY även möjlighet att utfärda en varning.

IMY har ovan kommit fram till att det föreligger en risk för att de tekniska och organisatoriska åtgärderna som Polismyndigheten vidtagit inte är tillräckliga för att leva upp till kravet på lämplig skyddsnivå enligt 3 kap. 8 § brottsdatalagen och 3 kap 11 § brottsdataförordningen.

Vidare har IMY enligt vad som framgår ovan kommit fram till att det föreligger en risk för att Polismyndigheten inte fullgör den skyldighet att underrätta som följer av 3 kap. 10 § brottsdatalagen när en personuppgiftsincident har inträffat, om inte åtgärder vidtas för att motverka detta.

Ingen av riskerna är av sådan karaktär att det enligt IMY är motiverat att tilldela en varning. IMY finner däremot skäl att rekommendera Polismyndigheten dels att vidta ytterligare åtgärder för att höja skyddsnivån och förhindra att personuppgifter, som kan medföra en allvarlig negativ påverkan på den personliga integriteten, sprids via e-post till obehöriga utanför myndigheten och dels att se över sin hantering av när myndigheten är skyldig att underrätta berörda registrerade om en personuppgiftsincident.

Detta beslut har fattats av enhetschefen Charlotte Waller Dahlberg efter föredragning av juristen Jonas Agnvall. Vid den slutliga handläggningen av ärendet har även rättschefen David Törngren och juristen Lisa Zettervall samt it-säkerhetsspecialisten Magnus Bergström medverkat.

Charlotte Waller Dahlberg, 2023-01-16 (Det här är en elektronisk signatur)

Kopia för kännedom till:
Polismyndighetens dataskyddsombud

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.