Integritetsskyddsmyndigheten

Kry International AB

**Diarienummer:**
IMY-2022-3822

**Datum:**
2024-12-19

# Beslut efter tillsyn enligt dataskyddsförordningen – Kry International AB

## Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Kry International AB, med organisationsnummer 556967-0820, har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1] genom att inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifter vid användning av analysverktyget Meta-pixeln under perioden 28 maj 2020–17 maj 2022.

IMY ger Kry en reprimand med stöd av artikel 58.2 b i dataskyddsförordningen för överträdelsen.

## Redogörelse för tillsynsärendet

### Bakgrund m.m.

Kry International AB (Kry) har den 18 maj 2022 lämnat in en anmälan om personuppgiftsincident till Integritetsskyddsmyndigheten (IMY). Av anmälan framgår bland annat att Kry har erbjudit en tjänst för företag emellan (business-to-business tjänst) i syfte att underlätta distanskontakt genom en säker och krypterad videoanslutning (tjänsten). Användarna har typiskt sett varit företag inom vård och hälsa (användare) som kunnat registrera ett konto och därefter bjuda in andra organisationer, kollegor, kunder, patienter och personer som representerar patienter (slutanvändare) genom att skicka ut en länk till ett videomöte via bland annat sms och mejl. Genom att använda Meta Platforms Ireland Limiteds (Metas) analysverktyg Meta-pixeln på webbplatserna där tjänsten erbjöds har hashade[2] kontaktuppgifter om slutanvändarna oavsiktligen förts över till Meta. Incidenten har upptäckts genom information från en utomstående.

IMY har inlett tillsyn i maj 2022 mot bakgrund av de uppgifter som förekom i incidentanmälan. Tillsynen har avgränsats till frågan om Kry vidtagit lämpliga tekniska och

**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).
[2] Hashning är en kryptografisk envägsfunktion som kan användas för att åstadkomma pseudonymisering, som är en möjlig säkerhetsåtgärd enligt artikel 32 i dataskyddsförordningen, genom att personuppgifter ersätts med en så kallad hashsumma. Det innebär att de ersatta personuppgifterna inte är tillgängliga i klartext och att det behövs kompletterande uppgifter för att det ska gå att identifiera den registrerade.

organisatoriska åtgärder i enlighet med artikel 32 i dataskyddsförordningen vad avser slutanvändarnas personuppgifter.

På grund av att tillsynsärendet har gränsöverskridande karaktär har IMY använt sig av de mekanismer för samarbete och enhetlighet som finns i kapitel VII i dataskyddsförordningen. Berörda tillsynsmyndigheter har varit dataskyddsmyndigheterna i Danmark, Finland, Frankrike, Luxemburg, Nederländerna, Norge, Polen, Tyskland, Ungern och Österrike.

## Vad Kry har uppgett

Kry har i huvudsak uppgett följande gällande den fråga som IMY granskar.

**Personuppgiftsansvar**
Kry är personuppgiftsansvarigt för den oavsiktliga insamlingen och delningen av slutanvändarnas personuppgifter. Implementeringen av Meta-pixeln har skett av Kry i syfte att marknadsföra Krys egna tjänster. Kry har därmed bestämt ändamål och medel för den aktuella behandlingen.

**Ändamålet med behandlingen**
Kry har använt sig av Meta-pixeln i marknadsföringssyfte. Avsikten har varit att samla in en begränsad mängd uppgifter om webbplatsbesökare och användare i syfte att rikta annonser, på Metas sociala plattform Facebook, mot de besökare som ännu inte registrerat ett konto eller användare som registrerat ett konto utan att börja använda tjänsten. Syftet var också att utvärdera behovet och mäta effektiviteten av sådan marknadsföring. Kry har inte avsett att samla in information om eller rikta marknadsföring till slutanvändarna. På grund av att Meta-pixelns automatiska funktion för avancerad matchning (AAM-funktionen) varit aktiverad har dock kontaktuppgifter som användarna angett om slutanvändarna för att skicka ut en inbjudan till videomöte samlats in och förts över till Meta. Överföringen av uppgifterna startade den 28 maj 2020 och upphörde den 17 maj 2022.

**Vilka personuppgifter som förts över till Meta**
Uppgifterna som förts över om användarna har omfattat teknisk information om användarens enhet, IP-adress, hashad kontaktinformation i form av mejladress och telefonnummer samt interaktionsdata såsom knapptryck och händelser (exempelvis registrering av konto, öppning av sidor eller skapande av möteslänkar). Överföringen av slutanvändarnas kontaktuppgifter har omfattat *antingen* deras mejladresser eller telefonnummer. Det har inte skett någon insamling och överföring av uppgifter om slutanvändarnas användning av tjänsten såsom exempelvis uppgifter om att personen klickat på en möteslänk, anslutit till ett möte eller avslutat ett möte.

Det ska uppmärksammas att flera överförda kontaktuppgifter med största sannolikhet inte utgör personuppgifter enligt dataskyddsförordningen eftersom de bestått av gemensamma mejladresser såsom info@vårdgivare.se eller växelnummer. En granskning av pilotprojektet för tjänsten och feedback från användare visar vidare att tjänsten använts genom att en vårdgivare bjudit in en juridisk person, exempelvis en vårdcentral eller ett boende, som slutanvändare till videomötet. I sådana fall har kontakten med patienten skett via den juridiska personens enhet och bokningen har inte omfattat behandling av patientens personuppgifter.

Uppgifterna om slutanvändarna har inte omfattat särskilda kategorier av personuppgifter enligt artikel 9 i dataskyddsförordningen bland annat av följande skäl. Det har

inte varit möjligt att knyta uppgifter om slutanvändaren till händelser eller åtgärder som användaren vidtagit på tjänsten såsom inbjudningar eller möten. Det är mycket osannolikt att Meta överhuvudtaget kunnat uppfatta att uppgifterna som förts över om användaren och slutanvändaren tillhört olika parter, eftersom det inte förts över några uppgifter som antyder vem uppgifterna avsett. Aktiveringen av AAM-funktionen har lett till att slutanvändarens mejladress eller telefonnummer har knutits till händelsen i stället för användarens mejladress och telefonnummer. För Meta har det därmed sett ut som att användaren ändrat sina kontaktuppgifter. Enligt det avtal och person-uppgiftsbiträdesavtal som gäller mellan Kry och Meta har Meta vidare endast haft tillåtelse att matcha kontaktuppgifterna mot personer med konton på Metas plattformar. Meta har därmed inte heller haft rätt att försöka koppla ihop de hashade kontaktuppgifterna. Även om Meta skulle kunnat kunnat avgöra att uppgifterna gällt olika parter har det inte varit möjligt för Meta att dra slutsatsen att det rört sig om vare sig en patient eller vårdgivare. Det skulle kräva långtgående antaganden av Meta eftersom det finns många andra tänkbara kopplingar mellan de olika plattforms-kontona än att det skulle röra sig om en vårdgivare respektive patient. Därtill har uppgifterna som förts över om användarna varit professionella uppgifter och konton på Metas plattformar är typiskt sett av privat karaktär. Det är därför osannolikt att de hashade kontaktuppgifterna om användarna matchar uppgifter hos Meta och Meta har då inte kunnat översätta den hashade mejladressen till en läsbar adress.

**Incidentens omfattning**
En viktig princip för plattformen och tjänsten har varit att inte samla in, lagra eller annars behandla personuppgifter om slutanvändare. Slutanvändarnas kontaktuppgifter har därför omedelbart raderats från Krys system efter att inbjudan skickats ut. Av den anledningen finns det inga register eller lagring av data som kan användas för att beräkna det exakta antalet unika slutanvändare. Baserat på antalet inbjudningar som genomförts genom plattformen och intern statistik från Krys andra tjänster uppskattar Kry att cirka 90 000 slutanvändare kan ha påverkats. En stor del av kontaktuppgifterna för dessa slutanvändare har dock sannolikt inte utgjort personuppgifter, vilket medför att antalet registrerade som berörts av incidenten är lägre än den redovisade siffran.

Krys utredning visar även att Metas personuppgiftsbehandling har varit begränsad. Kontaktuppgifterna har endast, och under mycket kort tid, använts till att identifiera Metas plattformsanvändare som potentiella mottagare av riktade annonser och har inte använts på något annat sätt. I Sverige genomfördes ingen marknadsföring via Meta under perioden för incidenten eller efteråt. När Kry blev medvetet om incidenten togs pixeln omedelbart bort från webbplatserna där tjänsten erbjöds och marknads-föringen genom Meta stoppades på samtliga marknader.

**Teknisk och organisatorisk säkerhet**
Kry har vidtagit ett antal organisatoriska och tekniska åtgärder utifrån den specifika risk som identifierats med behandlingen av personuppgifter inom ramen för tjänsten. Vid tidpunkten för implementeringen av tjänsten har Kry haft interna policyer och processer på plats. Innan driftsättningen av tjänsten gjordes bland annat en riskanalys som resulterade i ett en konsekvensbedömning genomfördes. Konsekvensbedöm-ningen ledde bland annat till att behandlingen av slutanvändarnas personuppgifter begränsats till att avse de kontaktuppgifter som varit nödvändiga för att skicka ut en mötesinbjudan. Genom inbyggt dataskydd har Kry så långt som möjligt begränsat i vilken mån användarna överhuvudtaget kunde tillföra uppgifter till systemet. Vidare har beslutats att kontaktuppgifter till slutanvändare samt andra uppgifter som behövt hanteras för att tillhandahålla tjänsten, såsom videosamtal, tekniska data och metadata om videomöten, endast skulle behandlas i realtid och således inte sparas i

Krys system. När marknadsföringsavdelningen skulle implementera pixeln på de aktuella webbsidorna har det inte bedömts nödvändigt att genomföra en ytterligare konsekvensbedömning eftersom riskerna ansågs låga.

Krys utredning visar att det tekniska team som implementerat Meta-pixeln inte fullt ut har förstått en del av dess funktionalitet. Kry har implementerat en kunddataplattform för att säkerställa kontroll över vilka uppgifter som samlades in på webbplatserna där tjänsten erbjudits och för att kunna genomföra övergripande dataskyddsinställningar för all spårning. Kry har gjort ett antal inställningar i kunddataplattformen för att skydda personuppgifter, bland annat genom att ingen spårning skulle ske av slutanvändar-sidan och att direktidentifierad information skulle hashas. AAM-funktion, som orsakade den oavsiktliga överföringen, var avstängd i kunddataplattformen på grund av integritetsskäl. Incidenten inträffade för att det gjorts motsatta inställningar i Metas eget utvecklarverktyg som gavs företräde. Eftersom syftet med kunddataplattformen är att instruera tredjepartscookies och pixlar, förutsåg inte Kry att pixelns inställningar skulle ges företräde framför inställningarna i kunddataplattformen och därmed orsaka överföringen av personuppgifter. En funktion som hashade identifierade uppgifter har varit aktiverad i kunddataplattformen som gjorde att automatiskt konverterade uppgifterna från klartext till hashad form. Meta har därmed endast fått tillgång till hashade personuppgifter. Bristen på förståelse kring konsekvensen av att slå på AAM-funktionen, i kombination med att de tekniska inställningar som gjorts för pixeln gavs företräde framför inställningarna i kunddataplattformen resulterade alltså i att hashade kontaktuppgifter till slutanvändare överförts till Meta trots att det aldrig var avsikten.

Kry tillämpar principen om lägsta behörighet vilket innebär att ingen användarroll tilldelas högre behörighet än som behövs för att utföra sina arbetsuppgifter. Endast 3–4 personer på marknadsföringsavdelningen har kunnat läsa och konfigurera verktyget för Meta-pixeln. Marknadsföringsavdelningen har löpande och regelbundet utvärderat statistiken kring de datapunkter och händelser som bolaget bestämt att samla in genom pixeln. Dessutom har en extern part genomfört penetrationstester av tjänsten vid två olika tillfällen. Någon uppföljning av vilka personuppgifter som samlades in genom pixeln och skickades till Meta gjordes inte eftersom Kry konfigurerat kunddata-plattformen för att säkerställa en begränsad och säker behandling av personuppgifter. Kry hade bland annat vidtagit åtgärder så att inga direkt identifierande personuppgifter från händelsedatan skulle delas med Meta. Vidare hade Kry inte förstått att AAM-funktionen aktiverats och därmed kringgått integritetsinställningarna i kunddataplatt-formen. I maj 2022 genomfördes en mer ingående granskning av vilken data som samlades in och skickades till Meta, som bekräftade att vissa uppgifter om slut-användarna av misstag skickats till Meta genom AAM-funktionen.

Vid tillfället för incidenten har Kry haft ett gällande generellt revisionsprogram för dataskydd samt årliga interna kontroller på dataskyddsområdet, baserat på kraven i dataskyddsförordningen och som särskilt beaktade riskerna i samband med databehandlingen. Risken för Meta-pixeln inom ramen för detta program har dock bedömts som relativt låg, bland annat till följd av den målgrupp som Kry avsåg att samla in uppgifter om och åtgärderna som vidtagits för att följa tillämplig lagstiftning. Det ansågs därför inte finnas en risk för AAM-funktionen som krävde ytterligare åtgärder eftersom flera lämpliga åtgärder redan hade vidtagits.

När incidenten upptäckts togs Meta-pixeln bort från webbsidorna där tjänsten erbjöds. Kry har därefter vidtagit flera åtgärder i form av att bland annat utreda incidenten och informera de registrerade om den på webbplatserna där tjänsten erbjöds. Kry har även kontaktat Meta och bett bolaget radera överförda uppgifter. Meta informerade om att

all hashad data som delas med Meta raderas inom 48 timmar. Kry har även vidtagit åtgärder för att förbättra sin hantering av spårningsteknik. Vidare har andra framåtblickande åtgärder vidtagits i form av exempelvis översyn av befintliga krav och riktlinjer, utbildningsåtgärder och planering av granskning av funktionalitet i kunddataplattformen. Kry har inte sökt eller haft någon finansiell fördel av den oavsiktliga delningen av uppgifter.

# Motivering av beslutet

IMY ska inledningsvis ta ställning till om dataskyddsförordningen är tillämplig och om IMY är behörig tillsynsmyndighet. Om så är fallet ska IMY pröva frågan om Kry är personuppgiftsansvarig och om bolaget har vidtagit lämpliga säkerhetsåtgärder enligt artikel 32 i dataskyddsförordningen för att skydda de personuppgifter som behandlats om slutanvändarna genom Meta-pixeln, med AAM-funktionen aktiverad, under perioden 28 maj 2020–17 maj 2022.

## IMY:s behörighet

**Tillämpliga bestämmelser**
Av artikel 95 i dataskyddsförordningen följer att dataskyddsförordningen inte ska innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter, för sådana områden som redan omfattas av skyldigheter enligt det så kallade eDataskyddsdirektivet[3]. eDataskyddsdirektivet har genomförts i svensk rätt genom lagen (2022:482) om elektronisk kommunikation (LEK), där bland annat insamling av uppgifter genom webbkakor regleras.

Enligt 9 kap. 28 § LEK, som genomför artikel 5.3 i eDataskyddsdirektivet, får uppgifter lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Vidare framgår att detta inte hindrar sådan lagring eller åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som är nödvändig för att tillhandahålla en tjänst som användaren eller abonnenten uttryckligen har begärt. LEK trädde i kraft den 22 augusti 2022. Under den i ärendet aktuella tiden gällde dock samma krav enligt 6 kap. 18 § lagen om (2003:389) om elektronisk kommunikation. Det är Post- och telestyrelsen (PTS) som är tillsynsmyndighet enligt LEK (1 kap 5 § förordningen [2022:511] om elektronisk kommunikation).

Europeiska dataskyddsstyrelsen (EDPB) har yttrat sig över samspelet mellan eDataskyddsdirektivet och dataskyddsförordningen. Av yttrandet följer bland annat att den nationella tillsynsmyndighet som utsetts enligt eDataskyddsdirektivet är ensamt behörig att övervaka efterlevnaden av direktivet. Däremot är IMY enligt dataskyddsförordningen behörig tillsynsmyndighet för den behandling som inte regleras särskilt i eDataskyddsdirektivet.[4]

EDPB har den 7 oktober 2024 antagit riktlinjer gällande den tekniska omfattningen av artikel 5.3 eDataskyddsdirektivet. I riktlinjerna anges bland annat att ett vanligt tillvägagångssätt för företag är användningen av unika identifierare eller beständiga

[3] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).
[4] Yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter, antaget den 12 mars 2019, punkt 68 och 69.

identifierare. Sådana identifierare kan härledas från beständiga personuppgifter (namn, efternamn, mejladress, telefonnummer etc.), som hashas på användarens enhet, insamlad och delad mellan flera personuppgiftsansvariga för att unikt identifiera en person genom olika datamängder (användardata som samlats in genom användandet av en webbsida eller applikation, kundrelationshantering som avser online- eller offlineköp eller prenumerationer etc.). I riktlinjerna klargörs att omständigheten att informationen matas in av användaren inte utesluter tillämpligheten av artikel 5.3 i eDataskyddsdirektivet eftersom informationen tillfälligt lagras på terminalen innan den samlas in. När det gäller insamling genom unika identifierare på webbsidor eller mobilapplikationer ger den insamlande enheten instruktioner till webbläsaren (genom kod som distribueras till terminalen/klienten) som skickar informationen. Därmed sker en hämtning av uppgifter och artikel 5.3 är tillämplig.[5] Den omständigheten att enheten som instruerar terminalen att skicka tillbaka informationen inte är densamma som den som tar emot informationen utesluter inte tillämpligheten av artikel 5.3 i eDataskyddsdirektivet.[6]

**IMY:s bedömning**
IMY:s granskning tar sikte på Krys användning av Meta-pixeln, ett scriptbaserat verktyg i form av ett kodstycke, på webbplatsen där tjänsten erhölls. Aktiveringen av Meta-pixelns AAM-funktion har medfört att pixeln instruerat användarnas webbläsare att samla in och hasha information som användarna angett på webbsidan om sig själva och slutanvändaren. Utifrån dessa uppgifter har en unik identifierare skapats som tillfälligt lagrats i användarens terminal och sedan förts över till, och därmed hämtats av, Meta för matchning. Den aktuella behandlingen har därmed omfattat både lagring i och hämtning från användares terminalutrustning som avses i 9 kap. 28 § i LEK, och motsvarande bestämmelse i 6 kap. 18 § lagen om (2003:389) om elektronisk kommunikation.

PTS är ensamt behörig att utöva tillsyn över tillämpningen av LEK. IMY:s granskning avser dock om Kry vidtagit tillräckliga säkerhetsåtgärder, vilket inte är något som regleras särskilt i LEK. IMY är därmed behörig att utreda den fråga som tillsynsärendet gäller.

## Personuppgiftsansvar

**Tillämpliga bestämmelser**
Personuppgiftsansvarig är enligt artikel 4.7 i dataskyddsförordningen den som ensamt eller tillsammans med andra bestämmer ändamål och medel för behandlingen av personuppgifter. Att ändamål och medel kan bestämmas av mer än en aktör innebär att flera aktörer kan vara personuppgiftsansvariga för samma behandling.

Den personuppgiftsansvarige ska enligt artikel 5.2 i dataskyddsförordningen ansvara för och kunna visa att principerna i artikel 5.1 efterlevs (principen om ansvars-skyldighet).

**IMY:s bedömning**
Kry har uppgett att bolaget är personuppgiftsansvarigt för den behandling av person-uppgifter som förekommit vid användningen av Meta-pixeln och för överföringen av personuppgifter till Meta.

[5] EDPB:s riktlinjer Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, punkt 61–63.
[6] Ibid, punkt 34.

Av utredningen framgår att Kry har beslutat att införa Meta-pixeln, ett verktyg som registrerar besökares agerande och överför informationen till Meta, på de webbsidor där tjänsten erbjudits och därefter aktiverat AAM-funktionen genom inställningarna i Metas verktyg. Syftet med användningen av Meta-pixeln har varit att marknadsföra Krys tjänst och följa upp den marknadsföringen. Kry har därmed bestämt hur behandlingen ska gå till och för vilket ändamål personuppgifterna ska behandlas. IMY bedömer därför att Kry är personuppgiftsansvarig för den behandling av personuppgifter som har skett genom användandet av Meta-pixeln med AAM-funktionen aktiverad.

## Har Kry säkerställt en lämplig säkerhetsnivå för personuppgifterna?

### Tillämpliga bestämmelser

*Definitionen av personuppgifter*

En personuppgift är enligt artikel 4.1 i dataskyddsförordningen varje upplysning som avser en identifierad eller identifierbar fysisk person. Av samma bestämmelse framgår att en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

*Kravet på att vidta lämpliga skyddsåtgärder*

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. Det ska, enligt samma bestämmelse, ske med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, 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.

I skäl 75 till dataskyddsförordningen anges faktorer som ska beaktas vid bedömningen av risken för fysiska personers rättigheter och friheter. Bland annat nämns förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt samt om behandlingen avser uppgifter om hälsa eller sexualliv. Vidare ska beaktas om behandlingen gäller personuppgifter om sårbara fysiska personer, framförallt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

I skäl 76 till dataskyddsförordningen anges att hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller hög risk.

*Känsliga personuppgifter*

Uppgifter om hälsa tillhör de särskilda kategorier av personuppgifter, så kallade känsliga personuppgifter, som ges ett särskilt starkt skydd enligt dataskyddsförordningen. Det är som huvudregel förbjudet att behandla sådana personuppgifter enligt artikel 9.1 i dataskyddsförordningen, om inte behandlingen omfattas av något av undantagen i artikel 9.2 i förordningen.

Uppgifter om hälsa definieras i artikel 4.15 i dataskyddsförordningen som personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa vilka ger information om dennes hälsostatus. I skäl 35 till dataskyddsförordningen anges att personuppgifter om hälsa bör innefatta alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd.

**IMY:s bedömning**

*Behandlingen har innefattat en risk*

Den personuppgiftsansvarige ska vidta åtgärder för att säkerhetsställa en skyddsnivå 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. På grundval av en objektiv bedömning ska fastställas huruvida behandlingen innebär en risk eller hög risk.

Av utredningen i ärendet framgår att Kry har fört över uppgifter till Meta om användarna av tjänsten i form av bland annat mejladress och information om hur denne agerat exempelvis i form av att registrera konto, öppna sidor eller skapat möteslänkar. Vidare har de kontaktuppgifter, i form av mejladress eller telefonnummer, som användaren lagt in om slutanvändaren för att skapa en mötesinbjudan förts över till Meta.

IMY gör följande bedömning av riskerna med behandlingen av slutanvändarnas personuppgifter.

Sådana uppgifter som överförts till Meta i det aktuella fallet kan, i vart fall vad gäller personliga mejladresser och telefonnummer, utgöra uppgifter som direkt eller indirekt kan identifiera en fysisk person och därmed utgöra personuppgifter. IMY konstaterar vidare att det inte kan uteslutas att det har gått att utläsa av de överförda uppgifterna att en inbjudan till möte mellan användaren och slutanvändaren har skickats ut. Vidare måste det i många fall ha framgått av användarens mejladress att denne representerat en vårdgivare.

Den aktuella överföringen har dock inte omfattat några uppgifter om relationen mellan användaren och slutanvändaren eller några uppgifter om vad bokningen gällt. Det har därmed inte gått att utläsa att slutanvändaren varit patient och inte heller att mötet

utgjort ett vårdbesök eller vilka hälsobesvär det i så fall skulle gälla. IMY bedömer därför att de överförda uppgifterna inte omfattar någon information om slutanvändarens hälsotillstånd och utgör således inte känsliga personuppgifter enligt dataskyddsförordningen.

Mot bakgrund av att tjänsten har använts inom vården konstaterar IMY dock att behandlingen, även om den inte har omfattat känsliga personuppgifter om hälsa, har förekommit i ett sammanhang där de registrerade måste ha kunnat förvänta sig en hög grad av konfidentialitet. Detta inte minst när tjänsten använts för möten mellan en vårdgivare och patient. Därtill kan konstateras att det rört sig om en omfattande behandling då Kry uppskattat att upp till 90 000 slutanvändare har påverkats av incidenten.

Sammanfattningsvis bedömer IMY att behandlingen, med hänsyn till sin art, omfattning och sammanhanget, har inneburit en risk som medfört ett krav på Kry att säkerställa en skyddsnivå som är lämplig i förhållande till den aktuella risken. Åtgärderna skulle bland annat säkerställa att personuppgifterna skyddades mot förlust av kontroll.

*Kry har inte vidtagit tillräckliga säkerhetsåtgärder*

IMY ska därefter bedöma om Kry har säkerställt den skyddsnivå som krävts för att skydda slutanvändarnas personuppgifter.

Kry har uppgett att bolaget gjort inställningar i sin kunddataplattform för att förhindra användningen av Meta-pixelns AAM-funktion. Bolagets utredning visar dock att den aktuella funktionen trots det har varit aktiverat eftersom motsatta inställningar gjorts i Metas utvecklarverktyg, som gavs företräde framför inställningarna i kunddata-plattformen. Aktiveringen av AAM-funktionen har medfört att Kry oavsiktligen fört över slutanvändarnas kontaktuppgifter till Meta. Kry har dock vidtagit säkerhetsåtgärder inför den aktuella behandlingen som begränsat de negativa konsekvenserna av den oavsiktliga överföringen. Kry har bland annat beslutat att begränsa behandlingen av slutanvändarnas uppgifter till vad som behövdes för att skicka ut mötesinbjudan och implementerat tekniska hinder som hindrat användaren från att lägga in fler uppgifter än så. Dessa begränsningar har medfört att det inte gått att utläsa vad den aktuella mötesinbjudan gällt eller några andra integritetskänsliga uppgifter om de registrerade.

IMY konstaterar dock att en grundläggande förutsättning för att Kry ska kunna uppfylla sina skyldigheter enligt dataskyddsförordningen är att bolaget är medvetet om vilken behandling som sker under dess ansvar. Kry har uppgett att bolaget har haft rutiner för att följa upp sin behandling av personuppgifter. Enligt bolaget gjordes dock ingen uppföljning av vilka personuppgifter som samlades in och fördes över till Meta genom pixeln, eftersom det gjorts inställningar i kunddataplattformen som skulle säkerställa en begränsad och säker behandling av personuppgifter.

Kry har under en lång period, från den 28 maj 2020 till den 17 maj 2022, fört över uppgifter om slutanvändarna till Meta som inte var avsedda att överföras. Först efter att bolaget fått information om incidenten från utomstående har bolaget gjort kontroller som bekräftat att sådan överföring skett. Mot denna bakgrund bedömer IMY att Kry inte kan anses ha haft de systematiska rutiner som krävts för att identifiera sådana oavsiktliga förändringar av behandling av personuppgifter som aktiveringen av Meta-pixelns AAM-funktion inneburit. Det har medfört att Kry saknat kontroll över behandlingen och förmåga att upptäcka den aktuella bristen. IMY bedömer därför att Kry, även med beaktande av de säkerhetsåtgärder som vidtagits vid tidpunkten för

överträdelsen, inte kan anses ha vidtagit lämpliga tekniska och organisatoriska åtgärder i förhållande till de risker som behandlingen har inneburit. Kry har därför behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

## Val av ingripande

IMY har möjlighet att rikta ett antal åtgärder, så kallade korrigerande befogenheter, mot den som brutit mot dataskyddsförordningen. Av artikel 58.2 i och artikel 83.2 i dataskyddsförordningen framgår att IMY bland annat har befogenhet att påföra administrativa sanktionsavgifter i enlighet med artikel 83 i samma förordning. Om det är fråga om en mindre överträdelse får IMY enligt vad som anges i skäl 148 till dataskyddsförordningen 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.

Den konstaterade överträdelsen har skett genom att Kry behandlat personuppgifter med en otillräcklig säkerhetsnivå, vilket har lett till att bolaget oavsiktligen fört över uppgifter om ett stort antal registrerade till Meta. Överföringen har pågått under en lång tid och har inte upptäckts och åtgärdats förrän en utomstående informerat Kry om bristen. Överträdelsen har vidare skett i inom vården där registrerade måste anses ha haft en berättigad förväntan på hög grad av konfidentialitet. Kry har dock vidtagit flera åtgärder som begränsat intrånget i kundernas personliga integritet och som bland annat medfört att den oavsiktliga överföringen inte omfattat uppgifter av integritetskänslig karaktär. Vidare har de av bolaget vidtagna åtgärderna medfört att personuppgifterna förts över i hashat, det vill säga oläsligt, format till en enda mottagare och det rör sig därmed inte om ett okontrollerat röjande där uppgifterna exempelvis delats till många obehöriga eller funnits publikt tillgängliga på webben.

Vid en sammantagen bedömning finner IMY att det är fråga om en sådan mindre överträdelse som avses i skäl 148 till dataskyddsförordningen och att Kry därför ska ges en reprimand.

---

Detta beslut har fattats av enhetschefen Nidia Nordenström efter föredragning juristen Maja Welander. Vid den slutliga handläggningen av ärendet har även it- och informationssäkerhetsspecialisten Petter Flink medverkat.

*Nidia Nordenström*

**Kopia till**
Krys dataskyddsombud

# 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.