Integritetsskyddsmyndigheten

Apotea AB

Diarienummer:
IMY-2022-3271

Datum:
2024-12-19

Beslut efter tillsyn enligt dataskyddsförordningen – Apotea AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Apotea AB, med organisationsnummer 556651-6489, behandlat personuppgifter i strid med 32.1 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 22 juni 2020–9 maj 2022.

Integritetsskyddsmyndigheten ger Apotea AB en reprimand enligt artikel 58.2 b dataskyddsförordningen för överträdelsen.

Redogörelse för tillsynsärendet

Bakgrund

Den 11 maj 2022 lämnade Apotea AB (Apotea) in en anmälan om personuppgifts-incident till Integritetsskyddsmyndigheten (IMY). Av anmälan framgick bland annat att Apotea använt Meta Platforms Ireland Limiteds (Metas) analysverktyg Meta-pixeln på sin webbplats www.apotea.se (webbplatsen) för att förbättra sin annonsering mot kunder och mäta trafik på webbplatsen. Apotea uppgav att en potentiell person-uppgiftsincident inträffat eftersom mer information än bolaget haft kännedom om förts över till Meta. Apotea upptäckte incidenten genom information från en utomstående.

IMY inledde tillsyn i maj 2022 mot bakgrund av de uppgifter som förekom i incident-anmälan. Tillsynen har avgränsats till frågan om Apotea har vidtagit lämpliga tekniska och organisatoriska åtgärder i enlighet med artikel 32 i dataskyddsförordningen.

Handläggningen vid IMY har skett genom skriftväxling.

Vad Apotea har uppgett

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

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).

Personuppgiftsansvar
Apotea är personuppgiftsansvarig för den behandling av personuppgifter som förekommit i samband med användandet av Meta-pixeln (tidigare Facebook-pixeln) och den efterföljande delningen av personuppgifter till Meta (tidigare Facebook).

Ändamålet med behandlingen
Personuppgiftsbehandlingen vid användandet av Meta-pixeln har skett för ändamålen intressebaserad annonsering och analys. Marknadsföringen avsåg Apoteas sortiment av icke läkemedelsprodukter genom kampanjerbjudanden och handlade således om ett begränsat urval av produkter från Apoteas produktkatalog. Marknadsföringen har uteslutande skett genom annonser på Metas sociala plattformar Facebook och Instagram och endast skett på gruppnivå. Apoteas syfte har varit att använda en begränsad version av Meta-pixeln på webbsidan men den 22 juni 2020 utökades behandlingen, genom aktivering av Meta-pixelns funktion för automatisk avancerad matchning (AAM-funktionen), på grund av ett handhavandefel. Den 9 maj 2022 tog Apotea omedelbart bort analysverktyget från webbsidan efter att bolaget fått information om den oavsiktliga delningen.

Vilka uppgifter som förts över till Meta
Den utökade personuppgiftsbehandlingen har inneburit ett potentiellt röjande av fler personuppgifter än som var avsett. Apoteas avsikt var att samla in uppgifter om kunders och webbplatsbesökares IP-adresser samt interna produkt-id för produkter som placerades i kundkorgen. Den utökade användningen av Meta-pixeln har lett till att behandlingen även omfattat uppgifter om namn, adress, mejladress, telefonnummer och IP-adress om ett begränsat antal kunder. Apotea har inte delat känsliga personuppgifter, uppgifter om ekonomi, personnummer eller andra integritetskänsliga personuppgifter. Apotea har inte heller fört över uppgifter om kunder som nekat användning av kakor eller använt sig av annonsblockerare. Samtliga uppgifter, utom produkt-id, har krypterats genom hashning[2] innan de fördes över till Meta. Meta har försökt matcha informationen med sin egen hashade information, vilket enbart kunnat ske om individen haft ett konto på Facebook. Efter matchningsprocessen har uppgifterna raderats.

Samtliga produkter hos Apotea är klassificerade baserat på typ av produkt. Dessa klassificeringar består av exempelvis handelsvaror, medicintekniska produkter (inklusive självtester), receptfria läkemedel och receptbelagda läkemedel. Utöver klassificeringen kategoriseras produkterna i samband med att en ny produkt läggs till i produktkatalogen genom val av en av de kategorier som finns inlagda i systemet. Det är något som sker oaktat användningen av Meta-pixeln och utgör en del av Apoteas interna rutiner för att underlätta regelefterlevnad. Kategoriseringen sköts direkt i det digitala systemet av en särskild grupp inom Apotea.

Apotea har gett Meta tillgång till ett varuregister med utvalda interna artikel-ID för varor som Apotea säljer. Det har på så sätt varit möjligt för Meta att i begränsad utsträckning koppla kundernas personuppgifter till köp av produkter med dessa artikel-id. Varuregistret innehöll dock enbart uppgifter om handelsvaror och hade rensats från produktkategorier som bedömdes känsliga. Registret innehöll inga uppgifter om varor som klassificerats som medicintekniska produkter såsom självtester och kondomer,

[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.

receptbelagda läkemedel och icke receptbelagda läkemedel. Meta har därmed endast kunnat koppla personuppgifterna till köp av varor som inte ingår i dessa kategorier.

Det går inte att utesluta en mindre felmarginal i den begränsade produktkatalogen där exempelvis enstaka felkategoriserade produkter skulle kunna förekomma. Det är dock osannolikt att en sådana felkategoriserade produkter skulle matchas mot en kund eftersom Meta har ett automatiserat system som tar bort sådana produkter och de utesluts därför innan matchningsprocessen vilket innebär att de inte kan kopplas till en kunds köp.

Incidentens omfattning
Det är inte möjligt att uppge ett exakt antal registrerade som berörts av händelsen då en stor del av underlaget som skulle behövas för en sådan uträkning har gallrats eller endast lagras av Meta. Uppskattningsvis har maximalt 238 234–379 959 kunder påverkats av händelsen. Beräkningen utgår från antalet kunder under den aktuella perioden, uppgifter från Meta om urvalet vid användning av AAM-funktionen och en uppskattning av hur många kunder som använder sig av annonsblockerare. I praktiken kan antalet påverkade vara lägre eftersom ett visst antal kunder nekat till användningen av cookies och andra har saknat konto på Facebook och Instagram vilkets krävts för att en matchning skulle vara möjlig.

Det är inte självklart att händelsen utgör en personuppgiftsincident eftersom det inte är klarlagt att det skett en obehörig åtkomst till personuppgifter. Apotea har haft ett avtal med Meta om överföringen och Meta är därmed behörigt att ta emot uppgifterna. Såväl den begränsade som utökade överföringen till Meta är tillåten enligt dataskyddsförordningen. Eftersom beslutet om att utvidga behandlingen inte skett i enlighet med Apoteas interna rutiner har bolaget valt att anmäla händelsen som en personuppgiftsincident.

Teknisk och organisatorisk säkerhet
Apotea har både före och efter incidenten haft tekniska och organisatoriska åtgärder på plats för att förebygga obehörig och otillåten behandling av personuppgifterna. Åtgärderna har bestått av tekniska säkerhetsåtgärder, åtkomstbegränsningar, interna riskbedömningar och rutiner för beslutsfattande. Endast tre personer, som behövt sådan åtkomst för att utföra för sina arbetsuppgifter, har haft behörighet och åtkomst till inställningarna för Meta-pixeln.

Beslut om att inleda en ny eller förändrad personuppgiftsbehandling måste förankras med Apoteas dataskyddsombud. Apotea har även rutiner för riskanalyser och konsekvensbedömningar samt anlitar regelbundet externa jurister för rådgivning i dataskyddsfrågor. Det initiala beslutet om att använda Meta-pixeln fattades innan dataskyddsförordningen trädde ikraft. Apotea har tidigare tagit ställning till att AAM-funktionen inte skulle användas.

Apotea har genomfört en intern utredning av händelsen och haft kontakt med ett externt rättsligt ombud för juridisk analys. Personuppgiftsincidenten har uppkommit till följd av ett handhavandefel i strid med Apoteas interna rutiner. Apotea har säkerhetssystem och rutiner implementerade som kan identifiera en förändring av informationsinsamling via webbplatsen. Däremot har inte Apotea haft motsvarande möjlighet att identifiera förändringar i det aktuella fallet eftersom de berott på ändrade inställningar på Apoteas Facebooksida.

Efter incidenten har Apotea inlett arbete med att förbättra och förtydliga befintliga rutiner för att undvika framtida incidenter. Apotea har bland annat vidtagit följande åtgärder:

- Implementerat nya tekniska säkerhetsåtgärder, åtkomstbegränsningar, interna riskbedömningar och rutiner för beslutsfattande.
- Infört ytterligare åtgärder och rutiner för förändringar, som nu även omfattar förändringar som görs via tredjepartsinställningar på webbsidan.
- Utvärdering av behovet av att upphandla en tjänst som bl.a. kan identifiera oavsiktlig delning av information från webbsidan.
- Utbildat samtlig personal som behandlar personuppgifter om dataskydds-förordningen.
- Upphört med all överföring av personuppgifter till Meta. Meta har bekräftat att all tidigare överförd data har raderats.
- Uppdaterat all information till kunder och webbplatsbesökare.
- Informerat samtliga kunder om den utökade överföringen av personuppgifter via Meta-pixeln.

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 Apotea är personuppgiftsansvarig och om bolaget har vidtagit lämpliga säkerhetsåtgärder enligt artikel 32 i dataskyddsförordningen för att skydda de personuppgifter som behandlats genom Meta-pixeln, med AAM-funktionen aktiverad, under perioden 22 juni 2020–9 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).

[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).

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 dataskydds-förordningen 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 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 parten 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 den insamlande parten 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 Apoteas användning av Meta-pixeln, ett scriptbaserat verktyg i form av ett kodstycke, på sin webbplats, där den så kallade AAM-funktionen senare kom att aktiveras. Aktiveringen av AAM-funktionen har medfört att pixeln instruerat kundernas webbläsare att samla in och hasha information i form av de personuppgifter som de angett på sidan. 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 Apotea 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

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

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 ansvarsskyldighet).

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

Av utredningen framgår att Apotea har beslutat att införa Meta-pixeln, ett scriptbaserat verktyg i form av ett kodstycke som registrerar besökares agerande och överför informationen till Meta, på sin webbsida och därefter aktiverat AAM-funktionen. Syftet med användningen av Meta-pixeln har varit att möjliggöra intressebaserad annonsering och analys. Apotea har därmed bestämt hur behandlingen ska gå till och för vilket ändamål personuppgifterna ska behandlas. IMY bedömer därför att Apotea är personuppgiftsansvarig för den behandling av personuppgifter som har skett genom användandet av Meta-pixeln med AAM-funktionen aktiverad.

Har Apotea säkerställt en lämplig säkerhetsnivå för personuppgifterna?

Tillämpliga bestämmelser

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 och sexualliv utgör sådana 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.

EU-domstolen nyligen slagit fast att i situationen då en aktör som ägnar sig åt onlineförsäljning av läkemedel som endast får säljas av apotek utgör information som kunder anger när de köper läkemedel (såsom namn, adress och detaljer som individualiserar läkemedlet) uppgifter om hälsa, även när det gäller icke-receptbelagd medicin. Enligt EU-domstolen skulle uppgifterna i fråga kunna avslöja information om den registrerades hälsostatus i den mån det går att fastställa ett samband mellan läkemedlet, och dess terapeutiska indikationer eller användningsområden, och en identifierbar person. Att göra olika tolkningar beroende på om läkemedlet är receptbelagt eller inte anses inte vara förenligt med dataskyddsförordningens mål att säkerställa ett starkt skydd för de registrerades grundläggande fri- och rättigheter och skulle stå i strid med bland annat artikel 9.1 i dataskyddsförordningen. Således måste informationen som apotekskunder anger när de köper receptfria läkemedel som endast tillhandahålls av apotek anses utgöra uppgifter om hälsa, även när det bara med viss sannolikhet och inte absolut säkerhet går att konstatera att produkterna är avsedda för dessa kunder. Det är inte heller uteslutet att det, när produkterna är avsedda för andra, går att identifiera och dra slutsatser om dessa personers hälsostatus.[7]

EU-domstolen har i målet Lindqvist slagit fast att en uppgift om att en person skadat sin fot och är deltidssjukskriven utgör en personuppgift som rör hälsa enligt dataskyddsdirektivet[8] (direktivet upphävdes genom dataskyddsförordningen). EU-domstolen uttalade i målet att med hänsyn till syftet med dataskyddsdirektivet ska uttrycket "uppgifter som rör hälsa" ges en vid tolkning och anses omfatta uppgifter som rör alla aspekter av en persons hälsa, såväl fysiska som psykiska sådana.[9]EU-domstolen har i det senare avgörandet Vyriausioji tarnybinės etikos komisija konstaterat att begreppet känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen ska tolkas brett och bedömt att även personuppgifter som indirekt, efter

[7] EU-domstolens dom Lindenapotheke, C-21/23, EU:C:2024:846, punkt 84, 89–91 och 94.
[8] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
[9] EU-domstolens dom den 6 november 2003, Lindqvist, C-101/01, EU:C:2003:596, punkt 50–51.

en intellektuell slutledning eller avstämning, avslöjar en fysisk persons sexuella läggning utgör känsliga personuppgifter enligt den aktuella bestämmelsen.[10]

IMY:s bedömning

Behandlingen har inneburit en hög risk och krävt en hög skyddsnivå

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.

IMY gör följande bedömning av riskerna med den aktuella personuppgifts-behandlingen.

Apotea bedriver försäljning av en stor mängd varor av integritetskänslig natur, bland annat i form av receptbelagda och receptfria läkemedel samt medicintekniska produkter och självtester. Information om enskilda personers köp av sådana varor omfattar i många fall integritetskänsliga personuppgifter och skulle även, i de fall den aktuella informationen säger något om enskilda kunders hälsa, kunna omfattas av den breda definitionen av begreppet känsliga personuppgifter. IMY konstaterar därmed att den aktuella behandlingen omfattar personuppgifter som kräver ett starkt skydd enligt dataskyddsförordningen.

Behandlingen har vidare utförts i en apoteksverksamhet där kunden får antas ha särskilda förväntningar på att deras personuppgifter hanteras med en hög grad av konfidentialitet. IMY konstaterar därför att såväl personuppgifternas karaktär som det sammanhang som de behandlats i har medfört ökade risker för de registrerades fri-och rättigheter.

IMY konstaterar vidare att den aktuella behandlingen har varit omfattande, Apotea har haft ett stort antal kunder under den period Meta-pixelns AAM-funktion varit aktiverad och bolaget uppskattar att maximalt 238 234–379 959 kunder påverkats av incidenten.

Sammanfattningsvis bedömer IMY att behandlingen med hänsyn till sin art, omfattning och sammanhang har inneburit höga risker som medfört ett krav på hög skyddsnivå för personuppgifterna. Åtgärderna skulle bland annat säkerställa att personuppgifterna skyddades mot förlust av kontroll.

Apotea har inte vidtagit tillräckliga säkerhetsåtgärder

IMY ska därefter bedöma om Apotea har säkerställt den höga skyddsnivå som krävts för personuppgifterna.

Av utredningen i ärendet framgår att Apotea tagit ställning till frågan om Meta-pixelns AAM-funktion och beslutat att inte använda sig av den, men att så ändå skett till följd av ett handhavandefel i strid med Apoteas rutiner. Aktiveringen av AAM-funktionen har inneburit att Apotea har fört över fler uppgifter till Meta om kunders köp än som var avsett. Uppgifterna som förts över har omfattat kundernas namn, adress, mejladress och telefonnummer samt Apoteas interna produkt-id för produkter som kunderna köpt.

[10] EU-domstolens dom den 1 augusti 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, p. 123–127.

Apotea har dock gjort ett urval och kategorisering av vilka uppgifter som skulle behandlas av Meta-pixeln och försett Meta med ett varuregister som endast innehållit produkt-id för så kallade handelsvaror. Varuregistret har inte innehållit uppgifter om exempelvis medicintekniska produkter såsom självtester och kondomer, receptbelagda läkemedel eller icke receptbelagda läkemedel. Eftersom Apotea endast fört över uppgifter om produkternas interna produkt-id, och inga uppgifter om exempelvis namnet på produkten, har det bara gått att utläsa vilken produkt kunden köpt om den funnits med i varuregistret. Om en kund köpt en integritetskänslig produkt har det därmed, till följd av de säkerhetsåtgärder Apotea vidtagit inför behandlingen, inte framgått av de uppgifter som förts över till Meta vilken produkt som kunden köpt. Det finns inte stöd i utredningen för att det skett en felkategorisering av produkter som medfört att sådana integritetskänsliga uppgifter ändå har gått att utläsa.

IMY konstaterar dock att en grundläggande förutsättning för att Apotea ska kunna uppfylla sina skyldigheter enligt dataskyddsförordningen är att bolaget är medvetet om vilken behandling som sker under dess ansvar. Apotea har under en lång period från den 22 juni 2020, då AAM-funktionen aktiverades, till och med den 9 maj 2022, då Meta-pixeln togs bort, fört över fler uppgifter än som var avsett till Meta utan att själva upptäcka det. Vid tidpunkten för överträdelsen har Apotea haft säkerhetssystem och rutiner för identifiering av förändrad informationsinsamling på webbplatsen. Den förändring av behandling av personuppgifter som aktiveringen av Meta-pixeln innebar har inte kunnat identifieras eftersom den berodde på ändrade inställningar på Apoteas Facebooksida. IMY konstaterar att avsaknaden av åtgärder för att upptäcka förändringar på webbsidan som berott på tredjepartsinställningar har medfört att Apotea vare sig har haft kontroll över personuppgiftsbehandlingen eller förmåga att upptäcka den oavsedda överföringen. IMY bedömer att Apotea därmed, 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 höga risker som behandlingen har inneburit. Apotea 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 Apotea behandlat personuppgifter med en otillräcklig säkerhetsnivå vilket har lett till att bolaget fört över fler personuppgifter än som varit avsett om ett stort antal registrerade till Meta. Överföringen har pågått under en lång tid och har inte upptäckts och åtgärdats förrän en utomstående informerat Apotea om bristen. Överträdelsen har vidare skett i en apoteksverksamhet där de registrerade måste anses haft en berättigad förväntan på hög grad av konfidentialitet. Apotea har dock vidtagit flera åtgärder som begränsat intrånget i kundernas personliga integritet. Bolaget har bland annat vidtagit förebyggande säkerhetsåtgärder innan behandlingen påbörjades som medfört att den oavsiktliga överföringen inte omfattat uppgifter av integritetskänslig karaktär. Vidare

har 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 Apotea därför ska ges en reprimand.

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

Nidia Nordenström

Kopia till
Apoteas 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 senast tre veckor från den dag ni fick del av beslutet. Om överklagandet har kommit in i 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.