Integritetsskyddsmyndigheten

Apoteket AB

Diarienummer:
IMY-2022-3270

Datum:
2024-08-29

Beslut efter tillsyn enligt dataskyddsförordningen – Apoteket AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Apoteket AB (556138-6532) 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 19 januari 2020–25 april 2022.

Integritetsskyddsmyndigheten beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att Apoteket AB ska betala en administrativ sanktionsavgift på 37 000 000 kronor.

Redogörelse för tillsynsärendet

Bakgrund m.m.

Den 25 april 2022 lämnade Apoteket AB (Apoteket) in en anmälan om personuppgiftsincident till Integritetsskyddsmyndigheten (IMY). Av anmälan framgick att Apoteket använt Meta Platforms Ireland Limiteds (Metas) analysverktyg Meta-pixeln på sin webbplats www.apoteket.se (webbplatsen) för att förbättra annonseringen mot kunder och därigenom tillåtit överföring av data gällande kunder och webbplatsbesökare till Meta som inte var tänkta att överföras. Apoteket upptäckte incidenten genom information från en utomstående. Incidentanmälan föregicks av uppgifter i media om att Apoteket fört över vissa uppgifter om sina kunders webbköp till Meta.

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

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).

Handläggningen vid IMY har skett genom skriftväxling med Apoteket. IMY har även inhämtat utredning i form av information från Meta om hur Meta-pixeln och dess filtreringsmekanism fungerar.

Vad Apoteket har uppgett

Apoteket har i huvudsak uppgett följande gällande den fråga som är föremål för granskning.

Personuppgiftsansvar
Apoteket är personuppgiftsansvarig i den del som avser införandet av Meta-pixeln (tidigare Facebook-pixeln) och överföringen av uppgifter till Meta (tidigare Facebook).

Ändamålet med behandlingen
Apoteket har använt sig av Meta-pixeln sedan 2017. Behandlingen har övergripande sett skett för marknadsföringsändamål. Det primära syftet var att mäta effekten av bolagets marknadsföring på Metas sociala medieplattformar Facebook och Instagram. Det sekundära syftet var att marknadsföra produkter till besökare som besökt produktsidor för egenvård utan att handla, för att få dessa kunder att handla vid ett senare tillfälle. Pixeln användes för det sekundära syftet i begränsad omfattning, under begränsade perioder. Den 19 januari 2020 aktiverades den automatiska typen av Meta-pixelns funktion för avancerad matchning (AAM-funktionen) vilket innebar att fler uppgifter än tidigare kom att behandlas. Aktiveringen av AAM-funktionen var inte nödvändig för att uppfylla ändamålen med behandlingen. Aktiveringen av Meta-pixeln och AAM-funktionen har skett av enskilda medarbetare utan föregående riskbedömning i strid med Apotekets rutiner. Apoteket blev medvetet om att uppgifter som skulle kunna anses känsliga delats först efter att media rapporterat om det. Apoteket beslutade att omedelbart inaktivera Meta-pixeln och AAM-funktionen den 25 april 2022 efter att bolaget uppmärksammats på omfattningen av uppgifter som förts över.

Vilka personuppgifter som förts över till Meta
Överföringen till Meta har inte sett likadan ut för alla kunder, utan har berott på kundens agerande på webbplatsen. Apoteket har inte fört över uppgifter om kunder som nekat till marknadsföringskakor. För kunder som har samtyckt till marknadsföringskakor har generellt sett följande händelsedata förts över genom Meta-pixeln:

- URL
- value (värde på produkt eller total kundkorg)
- currency (=”SEK”)
- content IDs (ProduktID, Apotekets interna produktnummer)
- content Type (=”Product”)
- IP-adress.

Sedan AAM-funktion aktiverades har därutöver följande kontaktinformation förts över:

- för- och efternamn
- e-postadress
- telefonnummer
- personnummer
- kön
- stad
- postnummer
- land.

Kontaktinformationen har bara förts över vid genomförda köp och då i hashad form, vilket innebar att Meta bara har kunnat läsa informationen om de har haft motsvarande information sedan tidigare. Meta har sedan försökt matcha den överförda kontaktinformationen med ett användar-ID på Facebook och därefter raderat den. Om en kund loggat in på ”Mina sidor” med mobilt BankID har personnumret överförts eftersom det tolkats som ett telefonnummer.

Apoteket har gjort ett aktivt val att inte föra över uppgifter om receptbelagda varor. Exkluderingen har skett genom att den del av webbplatsen där en kund kan lägga en receptbelagd vara i varukorgen inte innehöll Meta-pixeln. Vidare har orderrader som innehåller receptbelagda varor filtrerats bort vid köptillfället från själva produktdatan av Apotekets server innan den förts över till Meta. Om en besökare accepterat marknadsföringskakor och genomfört ett köp har uppgifter om följande produkter och/eller produktkategorier delats via Meta-pixeln med AAM-funktionen aktiverad:

a) självtester och behandling för könssjukdomar
b) preventivmedel och dagen-efter-piller
c) sexleksaker
d) produkter för vaginal hälsa (t.ex. torra slemhinnor, klimakteriebesvär och svamp i underlivet)
e) produkter för prostatabesvär och urineringsbesvär
f) graviditetstest, ägglossningstest och graviditetsprodukter
g) produkter för behandling av svamp (t.ex. fotsvamp eller nagelsvamp)
h) produkter för behandling och kontroll av diabetes
i) produkter för behandling av ändtarmsbesvär (t.ex. analsprickor och hemorrojder)
j) produkter för behandling av magbesvär (t.ex. IBS, förstoppning och diarré)
k) produkter för behandling av migrän
l) produkter för behandling av allergi
m) tillbehör till hörapparater
n) produkter för behandling av bakteriella infektioner
o) produkter för behandling av psoreasis
p) produkter för behandling av rosacea
q) stomiprodukter.

Meta är i grund och botten en behörig mottagare och all överföring av webbplatsbesökarnas uppgifter har inte varit otillåten. Det som utgjort en personuppgiftsincident är den eventuella överföringen av känsliga personuppgifter. Alla produkter i Apotekets sortiment kan dock inte anses ge information om en persons hälsa eller sexualliv, utan enbart produkter ur ett så kallat integritetskänsligt sortiment i kombination med en direkt personuppgift. En persons agerande på webbplatsen behöver inte heller indikera något om den enskildes hälsa eller sexualliv, förrän kunden lagt en integritetskänslig produkt i varukorgen eller genomfört ett köp av en sådan produkt. Det är dock inte självklart att heller det säger något om den enskilde kunden eftersom många handlar produkter åt andra, i preventivt syfte eller till ett ”husapotek”. Därtill tillhör de egenvårdsprodukter som Apoteket säljer med säkerhet inte det så kallade integritetskänsliga sortimentet. Rättsläget är oklart på området och det är svårt att kategoriskt säga att känsliga personuppgifter har överförts.

Om överföring av känsliga personuppgifter har skett så har det inte varit Apotekets avsikt. Apoteket har dock ett personuppgiftsbiträdesavtal med Meta och det är inte fråga om en okänd mottagare av uppgifterna. Överföringen har inte skett på ett okontrollerat sätt i den mening att obehöriga har kommit åt informationen genom en hackerattack med uppenbart ont uppsåt. Den faktiska risken för de registrerade bedöms därför som måttlig. Överföringen av personnummer har inte ökat risken för de

registrerade eftersom uppgifterna förts över i förvrängd form, hashade[2] med SHA256, och sedan raderats av Meta eftersom uppgifterna inte kunnat matchas. Den primära bristen består av att de registrerade i viss mån förlorat kontrollen över sina personuppgifter, men Apotekets agerande i sig ökade inte risken för de registrerade. Det bör ses som förmildrande att Meta har haft en aktiv signalfiltreringsmekanism som filtrerat bort känsliga uppgifter. Informationen har därmed inte delats vidare eller använts av Apoteket eller Meta. Skadan för de registrerade är därmed begränsad.

Incidentens omfattning
Incidenten uppskattades vid tidpunkten för anmälan ha påverkat 500 001–1 000 000 registrerade. Apoteket har därefter uppgett att det inte går att ge en exakt siffra på antalet registrerade som drabbats av händelsen. Detta bland annat med hänsyn till att det inte handlar om en läcka från ett register eller en databas som Apoteket har haft full kontroll och insyn över samt att överföring av data skett direkt mellan användarens webbläsare och Meta. Kretsen av potentiellt berörda registrerade påverkas av flera faktorer. Det maximala antalet påverkade individer är 930 000. Beräkningen baserar sig på antalet köp från webben under den aktuella perioden, med hänsyn tagen till att en viss andel av köpen görs av återkommande kunder och kunder som använder sig av annonsblockerare eller har nekat till användningen av kakor. Apotekets uppfattning är att incidenten endast omfattar genomförda köp och inte uppgifter om att en person klickat på produkter, lagt produkter i varukorgen eller påbörjat betalning. Nio procent av den totala andelen av webbförsäljningen under den aktuella perioden som incidenten pågick bestod av produkter som tillhör de kategorier som räknas upp ovan under punkt a–q. Vad gäller mängden överförda personuppgifter har Apoteket bland annat framfört att antalet unika produkter för varje köp som genomfördes under perioden uppgår till 1,41 produkter per kund. Vid bedömningen av hur många känsliga personuppgifter som överförts måste dock beaktas att vissa av köpen har omfattat egenvårdsprodukter (som inte avslöjar uppgifter om hälsa), gjorts åt andra eller avsett flera förpackningar av samma produkt.

Teknisk och organisatorisk säkerhet
Innan den aktuella incidenten hade Apoteket proaktiva processer på plats för att säkerställa korrekt hantering av personuppgifter, inklusive ingående riskbedömningar och granskningar av dataskyddsombudet avseende frågor som rör personuppgifter. Apotekets utvecklingsprocess innehåller flera kontrollpunkter för att fånga upp risker och säkerställa en korrekt behandling av personuppgifter. Kontrollpunkterna består av att nya lösningar eller funktioner på webbplatsen granskas ur informationssäkerhets- och dataskyddsperspektiv (genom en informationsanalys), arkitekturellt perspektiv och avtalsmässigt (om lösningen köps in) samt kodgranskas innan lösningen går i produktion på webbplatsen. Apoteket genomför också revisioner och penetrationstester av webbplatsen för att kunna upptäcka och åtgärda sårbarheter.

I det aktuella fallet har Apotekets fastställda rutiner för IT-utveckling och riskbedömning inte följts av enskilda medarbetare. En möjlig orsak, vilket inte är ett försvar, kan ha varit att funktionaliteten var mycket enkel att aktivera utan någon egentlig utvecklingsinsats. Vid tidpunkten för aktiveringen av AAM-funktionen krävdes adminbehörighet i verktyget Meta Business Manager vilket två yrkesroller, omfattande totalt tre personer, hade. Enligt rutin ses behörigheter till verktyget Meta Business Manager, inklusive AAM-funktionen, över och kontrolleras regelbundet för att säkerställa att

[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.

endast personer med behov har tillgång. Några andra önskvärda rutiner för översyn och uppföljning har inte satts upp till följd av att aktiveringen pixeln och AAM-funktionen inte har följt Apotekets ordinarie rutiner.

Efter att Meta-pixeln och AAM-funktionen avaktiverats har Apoteket haft en dialog med Meta kring radering av data. Meta har uppgett att data äldre än två år redan raderats, men att bolaget inte kan radera datan från de två senaste åren manuellt. Apoteket har tagit fram generell information till de registrerade om händelsen som var publicerad på webbplatsen under slutet av april och i maj 2022. För att kunna bemöta specifika frågor och svar från kunder togs ett informationsunderlag fram till Apotekets medarbetare. Apoteket har även vidtagit åtgärder för att långsiktigt minska risken för liknande händelser. Bolaget har genomfört en inventering och analys av cookies- och analysverktyg på webbplatsen, infört en yrkesroll med övergripande ansvar för marknadsavdelningen i syfte att säkerställa efterlevnad av regler och riktlinjer samt förbättrat sin styrmodell för informationssäkerhet. Medarbetarna genomförde sedan tidigare en årlig e-utbildning inom säkerhet som inkluderar ett kapitel om dataskydd och informationssäkerhet. För att ytterligare stärka medvetenheten efter incidenten har korta e-utbildningar inom IT- och informationssäkerhet införts.

Val av korrigerande åtgärd
Apoteket har fört över uppgifter till Meta som inte borde ha delats. Skadan har dock varit begränsad. Överträdelsen har inte heller påverkat kärnan i uppfyllandet av Apotekets skyldigheter enligt artikel 32 i dataskyddsförordningen. Apoteket har omedelbart anmält överträdelsen till IMY och vidtagit de åtgärder som varit möjliga för att minska konsekvenserna av överträdelsen. Dessa omständigheter, tillsammans med att överträdelsen skett genom oaktsamhet, medför att det är fråga om en överträdelse av mindre betydelse och det är därför tillräckligt att meddela en reprimand.

Vad gäller överträdelsens allvarlighet så har den endast i liten utsträckning hindrat en effektiv tillämpning av artikel 32 i dataskyddsförordningen. Vidare har överträdelsen genomförts inom affärsverksamhet och behandlingens karaktär har därför inte medfört några särskilda risker. Det har inte heller funnits något beroendeförhållande mellan de registrerade och Apoteket. Behandlingen har skett för marknadsföringsändamål vilket inte är en del av Apotekets kärnverksamhet som består av att tillhandahålla receptbelagda och receptfria läkemedel. Personuppgiftsincidenten har förvisso omfattat ett förhållandevis stort antal registrerade, men nivån av skada som överträdelsen medfört är låg. Överträdelsen bör som högst anses vara av medelhög allvarlighetsgrad.

Det finns skäl att beakta hur omsättning beräknas inom andra EU-rättsliga områden, främst konkurrensrätten. Detta eftersom huvuddelen av Apotekets omsättning härrör från andra delar av Apotekets verksamhet, såsom exempelvis traditionell butikshandel samt vård- och dosaffärer, än den överträdelsen skett inom. Enligt Kommissionens Riktlinjer för beräkning av böter som döms ut enligt artikel 23.2 a i förordning nr 1/2003[3] anges att grundbeloppet för beräkningen ska fastställas genom att utgå från försäljningsvärdet för de varor eller tjänster som har ett direkt eller indirekt samband med överträdelsen och som företaget sålt i det berörda geografiska området inom EES. Analogt skulle den del av Apotekets omsättning som avser den del av verksamheten där överträdelsen skett beaktas, det vill säga omsättningen som avser onlineförsäljning av receptfria läkemedel, egenvårdsprodukter, hygienartiklar och hudvård.

[3] Rådets förordning (EG) nr 1/2003 av den 16 december 2002 om tillämpning av konkurrensreglerna i artiklarna 81 och 82 i fördraget.

Det föreligger flera förmildrande omständigheter kring överträdelsen bland annat i form av de åtgärder Apoteket vidtagit för att lindra konsekvenserna för de registrerade, att Apoteket samarbetat fullt ut med IMY och att uppgifter filtrerats bort och därmed inte nått Meta för vidarebehandling. Apoteket har även anmält händelsen på eget initiativ till IMY. Eftersom ekonomisk vinst genom överträdelsen kan ses som en försvårande faktor vid beräkningen av sanktionsavgift, vill Apoteket förtydliga att den ökning av försäljningen som eventuellt kan kopplas till användningen av AAM-funktionen är näst intill obefintlig.

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 Apoteket 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 19 januari 2020–25 april 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[4]. eDataskyddsdirektivet har genomförts i svensk rätt genom lagen (2003:389) 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 dataskydds-förordningen behörig tillsynsmyndighet för den behandling som inte regleras särskilt i eDataskyddsdirektivet.[5]

---

[4] 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).
[5] 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.

IMY:s bedömning
IMY:s granskning tar sikte på en situation då registrerade har använt sig av en tjänst på Apotekets webbsida i syfte att beställa en vara och själv lämnat den information som Meta-pixeln har fångat upp. Denna informationshantering innebär inte att uppgifter lagras i eller hämtas från en abonnents eller användares terminalutrustning och omfattas därmed inte av 9 kap. 28 § i LEK eller tidigare gällande motsvarande bestämmelse i lagen om om elektronisk kommunikation. Det innebär att regleringen i dataskyddsförordningen är tillämplig på den aktuella personuppgiftsbehandlingen och att IMY är behörig tillsynsmyndighet. Därtill kan konstateras att IMY:s granskning avser om Apoteket vidtagit tillräckliga säkerhetsåtgärder, vilket inte är något som regleras särskilt i LEK. Även det förhållandet medför således att IMY är 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
Apoteket har uppgett att bolaget är personuppgiftsansvarigt vad gäller införandet av Meta-pixeln och den överföring av uppgifter som har skett till Meta.

Av utredningen i ärendet framgår att Apoteket har infört Meta-pixeln, ett scriptbaserat verktyg i form av ett kodstycke som registrerar besökares agerande och överför informationen till Meta, på sin webbplats och därefter aktiverat AAM-funktionen. Syftet med Meta-pixeln har varit att öka effektiviteten av bolagets marknadsföring samt i viss mån rikta annonser mot tidigare besökare på webbplatsen. Apoteket har därmed bestämt hur behandlingen ska gå till och för vilket ändamål personuppgifterna ska behandlas. IMY bedömer därför att Apoteket är personuppgiftsansvarig för den behandling av personuppgifter som har skett genom användandet av Meta-pixeln med AAM-funktionen aktiverad.

Har Apoteket 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 säkerhets-nivå som är lämplig i förhållande till risken med behandlingen. Det ska, enligt samma bestämmelse, ske med beaktande av den senaste utvecklingen, genomförande-kostnaderna 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.

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

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.

Behandling av 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 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[6] (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.[7] EU-domstolen har i det senare avgörandet Vyriausioji tarnybinės etikos komisija

[6] 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.
[7] EU-domstolens dom den 6 november 2003, Lindqvist, C-101/01, EU:C:2003:596, punkt 50–51.

konstaterat att begreppet känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen ska tolkas brett och bedömt att även personuppgifter som indirekt, efter en intellektuell slutledning eller avstämning, avslöjar en fysisk persons sexuella läggning utgör känsliga personuppgifter enligt den aktuella bestämmelsen.[8]

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 ska inledningsvis ta ställning till vilka personuppgifter Apoteket har fört över till Meta genom Meta-pixeln med AAM-funktionen aktiverad.

Av utredningen i ärendet framgår att aktiveringen av Meta-pixelns AAM-funktion har inneburit att Apoteket, såvida en kund accepterat marknadsföringskakor och inte använt sig av annonsblockerare, har fört över uppgifter om genomförda köp till Meta. Uppgifterna som förts över har omfattat information köpta produkter (bland annat URL-adressen till produkter på webbplatsen, produkt-ID samt produkttyp) samt kontaktinformation om kunden (bland annat för- och efternamn, adress och telefonnummer).

Uppgifterna som förts över till Meta har inte omfattat receptbelagda produkter, men däremot följande produkter och produktkategorier:

a) självtester och behandling för könssjukdomar
b) preventivmedel och dagen-efter-piller
c) sexleksaker
d) produkter för vaginal hälsa (t.ex. torra slemhinnor, klimakteriebesvär och svamp i underlivet)
e) produkter för prostatabesvär och urineringsbesvär
f) graviditetstest, ägglossningstest och graviditetsprodukter
g) produkter för behandling av svamp (t.ex. fotsvamp eller nagelsvamp)
h) produkter för behandling och kontroll av diabetes
i) produkter för behandling av ändtarmsbesvär (t.ex. analsprickor och hemorrojder)
j) produkter för behandling av magbesvär (t.ex. IBS, förstoppning och diarré)
k) produkter för behandling av migrän
l) produkter för behandling av allergi
m) tillbehör till hörapparater
n) produkter för behandling av bakteriella infektioner
o) produkter för behandling av psoreasis
p) produkter för behandling av rosacea
q) stomiprodukter.

I ärendet har framkommit att Meta har implementerat en så kallad filtreringsmekanism vars syfte är att upptäcka och radera information som förts över till Meta i strid med bolagets policy. IMY har med anledning av detta inhämtat information från Meta om hur filtreringsmekanismen fungerar. Av Metas yttrande den 16 februari 2024 framgår

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

att mekanismen är utformad för att upptäcka och radera potentiellt otillåten information, till exempel uppgifter om hälsa och ekonomi, i data som användare av pixeln överför till Meta innan den lagras och används i Metas annonssystem. När sådana uppgifter upptäcks och raderas får användaren en notifikation om det, men filtreringsmekanismen fungerar även om ett sådant meddelande inte skickas till användaren. Mot bakgrund av detta konstaterar IMY att pixeln i sig inte innehåller en filtreringsmekanism som förhindrar en överföring av uppgifter till Meta. Filtreringsmekanismen är utformad för att filtrera bort potentiellt integritetskänsliga uppgifter först efter att de har överförts till Meta och om Metas system har kunnat identifiera att överförda uppgifter innehåller sådan otillåten information. Avsaknaden av notifikationer om otillåten och raderad information kan inte heller i sig anses vara en bekräftelse på att potentiellt integritetskänsliga uppgifter inte har överförts till Meta. Förekomsten av filtreringsfunktionen har sammanfattningsvis inte förhindrat den konstaterade överföringen av personuppgifter till Meta.

IMY gör följande bedömning av riskerna med den aktuella personuppgiftsbehandlingen.

Behandling som omfattar känsliga personuppgifter medför normalt sett högre risker. Begreppet känsliga personuppgifter ska tolkas brett och omfattar även uppgifter som indirekt avslöjar sådana uppgifter. Apoteket har fört över uppgifter till Meta om vilken produkt som en kund har köpt samt uppgifter som identifierar kunden i form av bland annat namn, adress och telefonnummer. IMY anser att kombinationen av uppgifter som förts över till Meta har gjort det möjligt att utläsa att en specifik person har köpt en viss utpekad produkt.

Apoteket har inte fört över uppgifter om receptbelagda produkter. Flertalet av produkterna i Apotekets övriga sortiment (se punkt a–q ovan) är dock av sådan karaktär att uppgift om att en person köpt en sådan produkt skulle kunna avslöja uppgifter om den enskildes hälsotillstånd eller sexualliv. Apoteket har invänt att det inte är säkert att köparen är den faktiska användaren av produkten och det är svårt att kategoriskt säga att känsliga personuppgifter har överförts. IMY anser dock att det är sannolikt att i vart fall vissa av köpen av till exempel stomiprodukter, produkter för ändtarms-, urinerings- och prostatabesvär, vaginala besvär samt behandling av könssjukdomar och diabetes har gjorts för eget bruk i syfte att behandla ett visst hälsotillstånd. IMY bedömer därför att det är sannolikt att behandlingen har omfattat uppgifter om hälsa i den mening som avses i artikel 4.15 i dataskyddsförordningen. IMY gör samma bedömning avseende köpen av exempelvis dagen-efter-piller och sexleksaker, det vill säga att det är sannolikt att köpen i åtminstone några fall har skett för eget bruk och att behandlingen därmed avslöjat uppgifter om den enskildes sexualliv. Vid bedömningen av lämplig skyddsnivå skulle Apoteket därför beaktat att behandlingen skulle kunna komma att omfatta känsliga personuppgifter.

IMY bedömer vidare att uppgifter om köp av de utpekade varorna i punkt a–q, oaktat om uppgifterna utgör känsliga personuppgifter eller inte, är av sådan integritetskänslig art att de kräver ett starkt skydd enligt dataskyddsförordningen. Det har även framgått att Apoteket i vissa fall har överfört andra skyddsvärda personuppgifter i form av personnummer.[9] Därtill har behandlingen utförts av ett apotek 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

[9] Personnummer omfattas av ett särskilt skydd enligt artikel 87 i dataskyddsförordningen och 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

sammanhang som de behandlats i har medfört ökade risker för de registrerades fri- och rättigheter.

IMY konstaterar även att behandlingen har varit omfattande. Apoteket har haft ett stort antal kunder under den period Meta-pixelns AAM-funktion varit aktiverad och bolaget uppskattar att upp till 930 000 personer har omfattats av den aktuella incidenten. Beräkningen baseras på antalet köp från webben under den aktuella perioden med hänsyn tagen till att en viss andel köp gjorts av återkommande kunder och av individer som använder sig av annonsblockerare eller har nekat till kakor. Apoteket har även uppgett att 9 procent av de totala webköpen som genomfördes under perioden har omfattat de integritetskänsliga produkter som listats under punkt a–q. IMY bedömer att det utifrån dessa uppgifter, även om det inte går att fastställa exakt hur många av dessa köp som gjorts av registrerade som inte använt sig av annonsblockerare eller nekat till marknadsföringskakor, i vart fall kan konstateras att incidenten har berört ett stort antal registrerade.

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 obehörigt röjande och förlust av kontroll.

Apoteket har inte vidtagit tillräckliga säkerhetsåtgärder

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

Apoteket har uppgett att bolaget hade proaktiva processer på plats innan incidenten för att säkerställa en korrekt hantering av personuppgifter. I det aktuella fallet har dock fastställda rutiner för IT-utveckling och riskbedömning, som bland annat inkluderar översyn och uppdatering av informationsanalyser vid alla förändringar av system och verktyg, inte följts av enskilda medarbetare. Av utredningen framgår att Apoteket därför inte har analyserat vilka risker och konsekvenser som den personuppgifts-behandling som införandet av Meta-pixeln och aktiveringen av AAM-funktionen skulle innebära, innan behandlingen påbörjades. Apoteket har inte heller gjort ett urval och kategorisering av vilka produkter som skulle komma att behandlas. Det har lett till att det, utöver exkluderingen av receptbelagda varor, inte funnits någon teknisk begränsning av vilka uppgifter som skulle omfattas av behandlingen och att integritets-känsliga uppgifter om exempelvis köp av receptfria läkemedel och medicinsktekniska produkter har förts över till Meta.

En grundläggande förutsättning för att Apoteket ska kunna uppfylla sina skyldigheter enligt dataskyddsförordningen är att bolaget är medvetet om vilken behandling som sker under dess ansvar. Apoteket har under en lång period från den 19 januari 2020, då AAM-funktionen aktiverades, till och med den 25 april 2022, då Meta-pixeln togs bort, fört över fler uppgifter än som var avsett till Meta utan att själva upptäcka det. Apoteket har framfört att aktiveringen av Meta-pixelns AAM-funktion inte har följt Apotekets ordinarie rutiner och att några önskvärda rutiner för översyn och uppföljning därför inte satts upp. Eftersom Apoteket endast har haft rutiner för att följa upp dokumenterade förändringar, som utförts enligt uppsatta rutiner, har Apoteket saknat förmåga att upptäcka och åtgärda andra förändringar som faktiskt genomförts eller uppstått på annat sätt. Mot denna bakgrund konstaterar IMY att Apoteket har saknat organisatoriska rutiner för att systematisk följa upp oavsiktliga förändringar i sina system.

IMY bedömer därmed att Apoteket, även med beaktande av vad som anförts om de rutiner som förelåg vid tidpunkten för överträdelsen, inte kan anses ha vidtagit lämpliga tekniska och organisatoriska åtgärder i förhållande till de höga risker som behandlingen har inneburit. Apoteket har därför behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Val av ingripande

Tillämpliga bestämmelser m.m.
Vid överträdelser av dataskyddsförordningen har IMY ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 i dataskyddsförordningen. Av artikel 58.2 i dataskyddsförordningen följer att IMY i enlighet med artikel 83 ska påföra sanktionsavgifter utöver eller i stället för andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall.

Varje tillsynsmyndighet ska säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Det anges i artikel 83.1 i dataskyddsförordningen.

I artikel 83.2 anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras, men också vad som ska påverka sanktionsavgiftens storlek. Av betydelse för bedömningen av överträdelsens allvar är bland annat dess karaktär, svårighetsgrad och varaktighet. EDPB har antagit riktlinjer om beräkning av administrativa sanktionsavgifter enligt dataskyddsförordningen som syftar till att skapa en harmoniserad metod och principer för beräkning av sanktionsavgifter.[10]

Enligt artikel 83.4 ska det vid överträdelser av bland annat artikel 32 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Om det är fråga om en mindre överträdelse får IMY enligt vad som anges i skäl 148 i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b i förordningen.

IMY:s bedömning

Sanktionsavgift ska påföras

IMY har gjort bedömningen att Apoteket behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Överträdelsen har skett genom att Apoteket behandlat personuppgifter med en otillräcklig säkerhetsnivå, vilket har medfört att personuppgifter av integritetskänslig och skyddsvärd karaktär om ett stort antal registrerade oavsiktligen har förts över till Meta. Obehörig åtkomst till den här typen av uppgifter medför en hög risk för de registrerades fri- och rättigheter. Överföringen har pågått under en lång tid och har inte upptäckts och åtgärdats förrän Apoteket informerats om bristen av en utomstående. IMY anser att det inte är fråga om en sådan mindre allvarlig överträdelse som kan medföra att en reprimand utfärdas i stället för en sanktionsavgift.

[10] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

EU-domstolen har klargjort att det krävs att den personuppgiftsansvarige har begått en överträdelse uppsåtligen eller av oaktsamhet för att administrativa sanktionsavgifter ska kunna påföras enligt dataskyddsförordningen. EU-domstolen har uttalat att personuppgiftsansvariga kan påföras sanktionsavgifter för ageranden om de inte kan anses ha varit okunniga om att agerandet utgjorde en överträdelse, oavsett om de varit medvetna om att de åsidosatte bestämmelserna i dataskyddsförordningen.[11]

Enligt principen om ansvarsskyldighet som bland annat kommer till uttryck i artikel 5.2 i dataskyddsförordningen ska den som ansvarar för behandlingen av personuppgifter säkerställa och kunna visa att behandlingen är förenlig med dataskyddsförordningen. IMY konstaterar således att Apoteket ansvarar för att de personuppgifter som behandlas i verksamheten, behandlas på ett sätt som säkerställer en lämplig säkerhetsnivå. IMY har vid sin prövning konstaterat att Apoteket inte levt upp till de krav som dataskyddsförordningen ställer i detta avseende. Apoteket kan inte anses ha varit okunnig om att dess agerande inneburit en överträdelse av förordningen.[12]

IMY bedömer därmed att förutsättningarna för att påföra Apoteket en administrativ sanktionsavgift för överträdelserna är uppfyllda. Vid bestämmande av sanktionsavgiftens storlek ska IMY beakta de omständigheter som anges i artikel 83.2 samt säkerställa att den administrativa sanktionsavgiften är effektiv, proportionell och avskräckande.

Utgångspunkter för beräkningen av sanktionsavgiften

IMY bedömer att det är årsomsättningen för Apoteket som ska läggas till grund för beräkningen av de administrativa sanktionsavgifter i det aktuella fallet.[13] Den maximala sanktionsavgiften som gäller för företag vid överträdelser av artikel 32 uppgår till det belopp som är högst av 10 000 000 EUR respektive 2 procent av den totala globala årsomsättningen under föregående budgetår.

Av Apotekets årsredovisning för år 2023 framgår att årsomsättningen för det året var 23 270 000 000 kronor. Det högsta sanktionsbelopp som kan fastställas i ärendet uppgår därmed till 2 procent av det beloppet vilket är 465 400 000 kronor. IMY konstaterar att det saknas stöd i tillämplig lagstiftning för att beräkna sanktionsavgiften utifrån ett annat belopp på det sätt som Apoteket framfört görs vid tillämpning av annan EU-rättslig lagstiftning.

Överträdelsens allvar

Av EDPB:s riktlinjer framgår att tillsynsmyndigheten ska bedöma om överträdelsen är av låg, medel, eller hög allvarlighetsgrad enligt artikel 83.2 a, b och g i dataskyddsförordningen.[14]

Den aktuella överträdelsen har omfattat ett stort antal registrerade och har pågått under en lång tid. Uppgifterna som förts över har omfattat personnummer och uppgifter om att direkt identifierbara personer köpt integritetskänsliga produkter. Den

[11] EU-domstolens dom den 5 december 2023, Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949, p. 81 och EU-domstolens dom den 5 december 2023, Deutsche Wohnen SE C-807/21, EU:C:2023:950, p. 76.
[12] Se för bedömningen av oaktsamhet även Kammarrätten i Stockholms dom den 11 mars 2024 i mål 2829-23 s.12.
[13] Apoteket är moderbolag i en koncern. Om företaget omfattas av skyldigheten att upprätta koncernredovisningar är dessa koncernredovisningar för koncernens moderbolag relevanta för att återspegla företagets sammanlagda omsättning, se EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 130.
[14] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 60.

obehöriga överföringen har därmed inneburit en hög risk för de registrerades fri- och rättigheter i form av risk för förlust av konfidentialitet för skyddsvärda uppgifter. Vidare har överträdelsen skett i en apoteksverksamhet där de registrerade måste anses haft en berättigad förväntan på hög konfidentialitet och att deras personuppgifter inte sprids till obehöriga. Försäljning av receptfria och andra hälsorelaterade produkter måste därtill anses omfattas av Apotekets kärnverksamhet, vilket gör att överträdelsen ska betraktas som mer allvarlig än om så inte varit fallet.[15]

I bedömningen av allvarlighetsgraden beaktar IMY även att Apoteket vid tidpunkten för överträdelsen hade vidtagit ett antal lämpliga tekniska och organisatoriska säkerhetsåtgärder. 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.

IMY bedömer mot bakgrund av ovanstående omständigheter att det sammantaget rör sig om en överträdelse av artikel 32.1 i datasskyddsförordningen av låg allvarlighetsgrad.

IMY ska vid sin bedömning av sanktionsavgiftens storlek även ta hänsyn till sådana försvårande och förmildrande faktorer som förtecknas i artikel 83.2 i dataskyddsförordningen. Efter överträdelsen har Apoteket bland annat fört en dialog med Meta om radering, gett information till de registrerade samt vidtagit åtgärder för att långsiktigt minska risken för liknande incidenter. IMY konstaterar dock att åtgärderna har vidtagits först efter att Apoteket uppmärksammats på föreliggande brister av en utomstående och att de inte kan anses gå utöver vad som förväntas av Apoteket i det aktuella fallet. De vidtagna åtgärderna är därmed inte sådana faktorer som påverkar IMY:s bedömning av sanktionsavgiftens storlek i förmildrande riktning. Detsamma gäller det faktum att Apoteket lämnade in en anmälan om personuppgiftsincident och samarbetat med IMY vid utredningen av den aktuella överträdelsen eftersom det utgör omständigheter som ska anses neutrala vid bestämmandet av sanktionsavgiften.[16] IMY konstaterar att det inte heller i övrigt framkommit några omständigheter som påverkar IMY:s bedömning av sanktionsavgiftens storlek i försvårande eller förmildrande riktning.

Sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande

Den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande. Det innebär att beloppet ska bestämmas så att den administrativa sanktionsavgiften leder till rättelse, att den ger en preventiv effekt och att den dessutom är proportionerlig i förhållande till såväl aktuell överträdelse som till tillsynsobjektets betalningsförmåga.

IMY bestämmer utifrån en samlad bedömning att Apoteket ska betala en administrativ sanktionsavgift på 37 000 000 kr. IMY bedömer att detta belopp är effektivt, proportionerligt och avskräckande.

---

[15] Ju mer central en behandling är för den personuppgiftsansvariges verksamhet, desto allvarligare blir oriktigheterna i behandlingen. Se EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 53.
[16] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkterna 95–98.

Detta beslut har fattats av den vikarierande generaldirektören David Törngren efter föredragning av juristen Maja Welander. Vid den slutliga handläggningen har även tillförordnade rättschefen Cecilia Agnehall, enhetschefen Nidia Nordenström, juristen Shirin Daneshgari Nejad samt it- och informationssäkerhetsspecialisten Petter Flink medverkat.

David Törngren, 2024-08-29 (Det här är en elektronisk signatur)

Bilaga
Information om betalning av sanktionsavgift

Kopia till
Dataskyddsombud för Apoteket

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 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 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.