Apohem AB

Diarienummer:
IMY-2022-3272

Datum:
2024-08-29

Beslut efter tillsyn enligt dataskyddsförordningen – Apohem AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Apohem AB (559094–8401) 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 15 april 2021–26 april 2022.

Integritetsskyddsmyndigheten beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att Apohem AB ska betala en administrativ sanktionsavgift på 8 000 000 kronor.

Redogörelse för tillsynsärendet

Bakgrund m.m.

Integritetsskyddsmyndigheten (IMY) mottog den 14 maj 2022 en anmälan om personuppgiftsincident från Apohem AB (Apohem eller bolaget). Av anmälan framgick att Apohem hade överfört fler personuppgifter än vad som avsetts till Meta Platforms Limited Ireland (Meta) för kunder som godkänt marknadsföringskakor i bolagets cookie consent manager (samtyckeshanterare). Överföringen hade skett genom en Meta-pixel som fanns implementerad på bolagets webbplats. Den data som hade förts över till Meta omfattade kontaktuppgifter och köpinformation men inga uppgifter om receptbelagda läkemedel. Bolaget fick kännedom om överföringen genom en extern källa och valde då att stänga av pixeln.

IMY inledde tillsyn mot Apohem den 31 maj 2022 mot bakgrund av de uppgifter som förekom i anmälan. Tillsynen har avgränsats till frågan om Apohem 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 Apohem. IMY har även inhämtat utredning i form av information från Meta om hur Meta-pixeln och dess filtreringsmekanism fungerar.

Vad Apohem har uppgett

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

Personuppgiftsansvar
Det är Apohems uppfattning att bolaget är gemensamt personuppgiftsansvarig med Meta för införandet av pixeln och den efterföljande överföringen av personuppgifter till Meta. Apohem är personuppgiftsansvarig genom att ha infört pixeln på sin webbplats och därefter överfört personuppgifter till Meta. Meta har ett personuppgiftsansvar eftersom de har utvecklat och erbjuder programkoden för pixeln.

Ändamålet med behandlingen
Meta-pixeln har implementerats och använts på webbplatsen www.apohem.se för att kunna marknadsföra produkter på Metas plattformar (Facebook och Instagram). Med hjälp av pixeln har Apohem samlat in information om köp och beteenden på webbplatsen för att sedan dela informationen med Meta, med avsikt att kunna attribuera beteenden och genomförda köp på webbplatsen till marknadsföringen som gjorts via Meta . Syftet har varit att utforma och rikta personligt anpassade annonser till webbplatsbesökare och därmed göra erbjudanden mer relevanta för dem än vad som är fallet med generell annonsering. Annonserna skulle avse mer allmänt hållen marknadsföring av Apohem och dess produkter eller en kampanj avseende en specifik produkt/varumärke.

Apohem har inte haft för avsikt att använda sig av pixelns delfunktion Automatic Advanced Matching (AAM) som var orsaken till den oavsiktliga överföringen av personuppgifter till Meta. Bolagets interna utredning har inte kunnat visa att en enskild person har aktiverat funktionen eller datumet för aktiveringen. Det bedöms dock som mest sannolikt att funktionen aktiverades i samband med ett byte av bolagets e-handelsplattform den 15 april 2021, vilket innebär att den oavsiktliga överföringen av uppgifter pågick under perioden 15 april 2021–26 april 2022.

Vilka personuppgifter som förts över till Meta
För webbplatsbesökare, som godkänt marknadsföringskakor på Apohems webbplats och som inte haft annonsblockerande webbläsartillägg (ad blocker) installerade, har följande personuppgifter förts över till Meta genom pixeln:

- IP-adresser
- köpinformation (kategori, produktgrupp och namn på handelsvaror och andra icke receptbelagda produkter, produktkod, antal och pris), och
- webbplatsbeteende/aktiverade händelser (besökt sida, besökt produktsida, lagt i varukorgen, gått till kassan, genomfört köp).

Genom AAM-funktionen har Apohem dessutom oavsiktligt fört över uppgifter till Meta avseende webbplatsbesökare som godkänt marknadsföringskakor, lagt produkter i varukorgen samt gått vidare och fyllt i formuläret i kassan i form av:

- för- och efternamn
- e-postadress

- telefonnummer och
- adressuppgifter (ort, postnummer, land).

Det har inte förts över uppgifter om receptbelagda läkemedel, utan endast information om handelsvaror (produkter för kropp och välmående, kosmetika, hygienartiklar samt olika typer av hushållsprodukter) och icke receptbelagda produkter i bolagets sortiment. Pixelkoden har funnits installerad på de delar av webbplatsen där följande produkter och/eller produktkategorier har funnits:

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 och 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.

Uppgifter om dessa produkter/produktkategorier har inte behandlats av Metas annonssystem trots pixelkoden. Meta har en policy om vilken typ av information som användare av pixeln får överföra till dem. Det finns därför en filtreringsmekanism kopplad till pixeln som ska upptäcka och radera uppgifter om bland annat sjukdomar, hälsotillstånd, sexuell och reproduktiv hälsa, medicinska procedurer/behandlingar/tester, tillskott/mediciner (receptfria och receptbelagda), biologiska cyklar m.m. Apohem har inte fått någon information från Meta att sådan data har förts över till Meta. Om Apohem hade fått sådan information hade orsaken undersökts och åtgärder vidtagits. För det fall att sådana uppgifter har förts över till Meta, som Apohem inte fått någon underrättelse om, har det inte funnits någon risk att uppgifterna har behandlats av Metas annonssystem utan endast i syfte att raderas.

Apohem anser inte att produkterna/produktkategorierna ovan utgör uppgifter om hälsa eller annan känslig information. Den person som köper handelsvaror och andra icke receptbelagda produkter hos bolaget är nödvändigtvis inte den som också slutligen använder produkten. Köp av icke receptbelagda produkter behöver inte heller ge direkt information om en persons hälsostatus då en och samma produkt kan tas i flera olika syften och fylla olika funktioner för olika personer. Många av produkterna kan dessutom köpas och användas utan att personer som sedan använder produkten har några hälsoproblem.

Apohem har vidare gjort urval och kategorisering av produkter som skulle behandlas av pixeln och därmed marknadsföras i Metas kanaler. Detta gjordes utifrån att följande produkter/kategorier valdes bort:

- produkter som regleras av specifika marknadsföringsbestämmelser och regler, t.ex. OTC, kosttillskott och medicintekniska produkter,
- produkter som inte får marknadsföras gentemot konsumenter enligt lag, t.ex. modersmjölksersättning och receptbelagda läkemedel, och
- produkter som inte får marknadsföras på Metas plattformar, t.ex. sexleksaker.

För att säkerställa att de produkter Apohem tillgängliggjorde för Meta följde detta urval, implementerade Apohem ett filter i sin produkt-feed. Denna produkt-feed uppdateras dagligen utifrån tillgängliga produkter i bolagets sortiment och hämtas sedan dagligen av Meta. Det är alltså endast dessa produkter som har marknadsförts för de webbplatsbesökare som har ett konto på Facebook eller Instagram.

Den totala andelen av bolagets försäljning som utgjordes av produkter som räknas upp under punkt a–q uppgick till 5,7 procent under perioden 15 april 2021–26 april 2022.

Incidentens omfattning
Apohem bedömer att personuppgifter kopplat till ca 15 000 registrerade har överförts till Meta under den aktuella perioden. Detta baseras på antalet unika kunder som (1) accepterat kakor enligt bolagets cookie consent manager, (2) som inte haft annonsblockerande webbläsartillägg (ad blocker) installerat, (3) inte haft en aktiv kaka från Facebook eller Instagram i sin browser men (4) innehaft ett konto på Facebook eller Instagram och därmed har kunnat matchas genom AAM-funktionen. Enligt uppgift från Meta har andelen kunder som kunnat matchas genom AAM uppgått till ca 3 procent.

Bolaget anser inte att den oavsiktliga överföringen av personuppgifter till Meta har påverkat de registrerade negativt. Detta eftersom varken känsliga personuppgifter, personnummer eller uppgifter om ekonomi har omfattats av överföringen.

Teknisk och organisatorisk säkerhet
Apohem vidtar regelmässigt åtgärder för att säkerställa en korrekt behandling av personuppgifter inför, i samband med och efter införandet av nya funktioner på webbplatsen. Bolaget har styrdokument och fastställda rutiner på plats för att säkerställa det interna dataskyddsarbetet. Dessa innebär bland annat att en kartläggning ska göras innan en ny funktionalitet implementeras som ställer krav på dokumentering, korrekt laglig grund, gallringsrutiner och information till de registrerade. Det finns lagringstider för de system som används av bolaget och en angiven produktägare för varje system med ansvar för att personuppgifter i systemet hanteras korrekt. Utöver detta finns styrdokument avseende personuppgiftsincidenter och hantering av de registrerades rättigheter.

Apohem följer gemensamt utarbetade branschvägledningar på området från Svensk Handel. Dessa är *Vägledning om personuppgifter, cookies och annan spårningsteknik* samt *Dataskyddsförordningen och personuppgifter – en tolkningsguide i det praktiska dataskyddsarbetet för Svensk Handels medlemsföretag*. Bolaget följer även E-hälsomyndighetens instruktioner, bland annat i enlighet med den kompletterande apoteksdatalagen (2009:367).

Vid införandet av Meta-pixeln bedömde Apohem att det inte förelåg hög risk för de registrerades fri- och rättigheter samt att personuppgiftsbehandlingen var proportionerlig i förhållande till de åtgärder som vidtogs av bolaget. De organisatoriska skyddsåtgärder som vidtogs för att skydda uppgifterna som behandlades via pixeln var behörighetsstyrning. Det innebar att endast en person hos bolaget hade full administrativ behörighet i ett särskilt konto hos Meta för att hantera pixeln. Den

utsedda personen bestämde i sin tur vilka enstaka personer med personligt inlogg på marknads- och IT-avdelningen på Apohem samt anlitad partner för marknadsföring som haft behov av åtkomst för att hantera den. Eftersom det inte var aktuellt att ändra vilken information som skulle samlas in genom Meta-pixeln genomförde Apohem inga regelbundna uppföljningar av vilka personuppgifter som samlades in och behandlades. Apohem förlitade sig i stället på Metas filtreringsmekanism som innebär att ingen information utöver den som godkänns enligt Metas policy ska inhämtas via pixeln.

Bolaget har inte haft för avsikt att använda AAM-funktionen och har därför inte aktivt vidtagit några åtgärder specifikt kopplat till funktionen. Inte heller har det gjorts någon riskbedömning avseende funktionen. De personuppgifter som behandlades i AAM var däremot hashade genom hashningsalgoritmen SHA-256[2] innan de överfördes till Meta.

När Apohem upptäckte den oavsiktliga överföringen av personuppgifter stängde bolaget omedelbart av pixeln, inklusive AAM-funktionen, och gjorde en anmälan om personuppgiftsincident till IMY. I samband med detta kontaktade Apohem även Meta med frågor om det inträffade men Meta har inte besvarat Apohems frågor. Efter att anmälan om personuppgiftsincidenten gjordes har bolaget vidtagit ett flertal organisatoriska skyddsåtgärder för att kunna upptäcka otillåten utgående trafik. Dessa har bestått av att utarbeta nya interna styrdokument och rutiner samt utökat legalt stöd av DSO, Head of legal and Compliance och anlitade advokatbyråer.

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 Apohem 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 15 april 2021–26 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[3]. 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

[2] IMY:s tillägg: 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.
[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).

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 tillsynsmyndigheten enligt dataskyddsförordningen behörig tillsynsmyndighet för den behandling som inte regleras särskilt i eDataskyddsdirektivet. Om endast en del av behandlingen faller under eDataskyddsdirektivet, begränsar inte detta dataskyddsmyndighetens befogenhet att pröva andra delar av behandlingen enligt dataskyddsförordningen.[4]

IMY:s bedömning
IMY:s granskning tar sikte på en situation då kunder har använt sig av en tjänst på Apohems 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 därför inte av 9 kap. 28 § i LEK eller tidigare gällande motsvarande bestämmelse i lagen om (2003:389) om elektronisk kommunikation. IMY konstaterar därmed att dataskyddsförordningen är tillämplig på den aktuella personuppgifts-behandlingen och att IMY är behörig tillsynsmyndighet. Det kan vidare konstateras att IMY:s granskning avser om bolaget vidtagit tillräckliga säkerhetsåtgärder, vilket inte är något som regleras särskilt i LEK. Även det förhållandet medför att IMY är behörig tillsynsmyndighet.

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).

EU-domstolen har i målet Fashion-ID konstaterat att en webbplatsinnehavare som använder så kallade insticksprogram från sociala nätverk på sin webbplats kan bli gemensamt personuppgiftsansvarig med det sociala nätverket. Detta gäller för den insamling och det utlämnande genom översändande av webbplatsbesökarnas personuppgifter som sker med hjälp av det sociala nätverkets insticksprogram. Domstolen uttalade även att respektive part bara är ansvarig för de delar av behandlingskedjan som den faktiskt bestämt ändamål och medel för.[5]

---

[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 68–69.
[5] EU-domstolens dom den 29 juli 2019, Fashion ID, C-40/17, EU:C:2019:629, punkt 64–85.

IMY:s bedömning
Apohem har uppgett att det föreligger ett gemensamt personuppgiftsansvar tillsammans med Meta för införandet av pixeln på bolagets webbplats och den efterföljande överföringen av personuppgifter till Meta.

Inom ramen för detta ärende tar IMY endast ställning till om Apohem har ett personuppgiftsansvar för den insamling och överföring av personuppgifter som skedde genom användandet av Meta-pixeln med AAM-funktionen aktiverad. IMY tar därmed inte ställning till om det föreligger ett gemensamt personuppgiftsansvar tillsammans med Meta för den aktuella behandlingen.

Av utredningen i ärendet framgår att Apohem 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 webbplats. Syftet har varit att öka effektiviteten i bolagets marknadsföring och kunna rikta annonser mot tidigare besökare på webbplatsen. Apohem har därmed bestämt för vilket ändamål personuppgifterna ska behandlas och hur behandlingen ska gå till. IMY bedömer mot denna bakgrund att Apohem är personuppgiftsansvarig för den behandling av personuppgifter som skedde genom användandet av Meta-pixeln med AAM-funktionen aktiverad.

Har Apohem 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.

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 vidare i ett senare avgörande, 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 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 säkerställa 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. Vid bedömningen ska särskild hänsyn tas till de

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

risker som behandlingen medför, bland annat obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

Av utredningen i ärendet framgår att användningen av Meta-pixeln och aktiveringen av AAM-funktionen har inneburit att Apohem fört över uppgifter till Meta om kunder som har påbörjat eller genomfört köp på bolagets webbplats. De påbörjade köpen har omfattat situationen då kunder manuellt har fyllt i sina personuppgifter i formuläret i kassan och gått vidare i köpprocessen men inte slutfört köpet. De överförda uppgifterna har bestått av exempelvis namn på handelsvaror och icke receptbelagda produkter samt kontaktinformation om kunden i form av för- och efternamn, postadress, e-postadress och telefonnummer. Uppgifter om receptbelagda läkemedel har inte överförts. Apohem har även haft pixelkoden installerad på de delar av webbplatsen som bland annat avsett preventivmedel, dagen-efter-piller, sexleksaker, självtester och behandling av könssjukdomar, produkter för vaginal hälsa, prostata-, ändtarms- och urineringsbesvär, stomiprodukter samt produkter för kontroll och behandling av diabetes.

Det har vidare framkommit att Meta har implementerat en så kallad filtreringsmekanism vars syfte är att försöka upptäcka och radera information som förts över till Meta i strid med Metas policy. Av yttrande från Meta den 16 februari 2024 framgår 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.

Apohem har invänt att Metas yttrande tycks utgå från nuvarande förhållanden om hur filtreringsmekanismen fungerar. IMY konstaterar dock att det inte finns något i utredningen som tyder på att filtreringsmekanismen har fungerat på ett annat sätt under den i ärendet aktuella tidsperioden.

IMY konstaterar därmed att det framgår av utredningen i ärendet att pixeln inte innehållit 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 deras 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 så kallade känsliga personuppgifter medför normalt högre risker. Begreppet känsliga personuppgifter ska tolkas brett och omfattar även uppgifter som indirekt avslöjar sådana uppgifter. Apohem har fört över uppgifter till Meta om vilken produkt som kunden har påbörjat eller genomfört köp av samt uppgifter som identifierar kunden i form av för- och efternamn, postadress, e-postadress och telefonnummer. IMY konstaterar att kombinationen av uppgifter som förts över har gjort det möjligt att utläsa att en specifik person har köpt en viss utpekad produkt.

Apohem har inte fört över några uppgifter om receptbelagda produkter. IMY anser dock att flertalet produkter i bolagets övriga sortiment, och som bolaget fört över uppgifter om, är av sådan karaktär att informationen om att en person köpt en sådan produkt skulle kunna avslöja uppgifter om den enskildes hälsotillstånd eller sexualliv. Det handlar till exempel om stomiprodukter, produkter för vaginal hälsa, prostata-, ändtarms- och urineringsbesvär, produkter för kontroll och behandling av diabetes, självtester och behandling av könssjukdomar, preventivmedel, dagen-efter-piller samt sexleksaker. Apohem har invänt att köparen inte nödvändigtvis är den faktiska användaren av produkten och att behandlingen därför inte har omfattat känsliga personuppgifter. 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 diabetes och könssjukdomar har gjorts för eget bruk i syfte att behandla ett visst hälsotillstånd. IMY bedömer därmed att behandlingen sannolikt har omfattat uppgifter om hälsa i den mening som avses i artikel 4.15 i dataskyddsförordningen. Samma bedömning görs med avseende på köpen av exempelvis dagen-efter-piller och sexleksaker, det vill säga att det är sannolikt att köpen i några fall har skett för eget bruk och att behandlingen därmed avslöjat uppgifter om den enskildes sexualliv. Vid bedömningen av lämplig skyddsnivå skulle Apohem därför beaktat att behandlingen skulle kunna komma att omfatta känsliga personuppgifter.

IMY bedömer att uppgifterna om köp av produkter, oaktat om uppgifterna utgör känsliga personuppgifter eller inte, är av sådan integritetskänslig art att de kräver ett starkt skydd enligt dataskyddsförordningen. Därutöver har behandlingen utförts av ett apotek där kunden får antas ha särskilda förväntningar på att deras personuppgifter hanteras med en hög grad av konfidentialitet. Mot denna bakgrund konstaterar IMY att såväl personuppgifternas karaktär som det sammanhang som de behandlats i har medfört ökade risker för de registrerades fri- och rättigheter.

Apohem beräknar att ca 15 000 registrerade har omfattats av personuppgiftsincidenten. Beräkningen baseras bland annat på antalet webbplatsbesökare som har haft ett konto på Facebook eller Instagram och kunnat matchas genom AAM-funktionen. Apohem har vidare räknat upp kategorier av produkter som funnits tillgängliga för köp på de delar av webbplatsen där pixelkoden funnits installerad och uppgett att den totala andelen av bolagets försäljning som avsett dessa produkter uppgått till 5,7 procent under den aktuella perioden. IMY bedömer att det utifrån dessa uppgifter, även om det inte går att fastställa exakt hur många påbörjade eller genomförda köp som gjorts för eget bruk eller den exakta mängden personuppgifter som förts över till Meta genom AAM-funktionen, i vart fall kan konstateras att det rör sig om en omfattande behandling av personuppgifter.

Sammanfattningsvis bedömer IMY att behandlingens art, omfattning och sammanhang har inneburit höga risker som medfört ett krav på en hög skyddsnivå för personuppgifterna. Åtgärderna skulle bland annat säkerställa att personuppgifterna skyddades mot obehörigt röjande och förlust av kontroll.

Apohem har inte vidtagit tillräckliga säkerhetsåtgärder

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

Apohem har uppgett att bolaget har interna rutiner och styrdokument för att säkerställa en korrekt hantering av personuppgifter inför, i samband med och efter införandet av

nya funktioner på webbplatsen. Vid implementeringen av Meta-pixeln på webbplatsen har bolaget genomfört en riskanalys av pixeln och bedömt att personuppgifts-behandlingen inte skulle innebära en hög risk för de registrerades fri- och rättigheter. Bolaget har även gjort ett urval och kategorisering av vilka produkter som skulle marknadsföras i Metas kanaler. Apohem har dock haft pixelkoden installerad på sidor med integritetskänsliga produkter vilka inte skulle omfattas av marknadsföringen. Apohem har inte vidtagit tekniska säkerhetsåtgärder för att förhindra att uppgifter om kunders påbörjade och genomförda köp av dessa produkter inte skulle föras över till Meta.

Apohem har vidare uppgett att det inte har gjorts regelbundna uppföljningar av vilken information som samlades in och behandlades genom Meta-pixeln. I stället har bolaget förlitat sig på att Metas filtreringsmekanism ska upptäcka och radera information av integritetskänslig karaktär som behandlas genom pixeln. Det har medfört att den otillåtna överföringen av personuppgifter pågick under drygt ett år och att bolaget fick kännedom om, och stoppade, överföringen först när en extern källa påtalade vad som pågick.

Eftersom Apohem endast har haft rutiner för att följa upp dokumenterade förändringar, som utförts enligt uppsatta rutiner, har Apohem saknat förmåga att upptäcka och åtgärda andra förändringar som faktiskt genomförts eller uppstått på annat sätt. Mot denna bakgrund konstaterar IMY att bolaget har saknat organisatoriska rutiner för att systematisk följa upp oavsiktliga förändringar i sina system.

IMY bedömer därmed att Apohem inte har vidtagit lämpliga tekniska och organisatoriska åtgärder i förhållande till den höga risk som behandlingen har inneburit. Bolaget har därför behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Val av ingripande

Tillämpliga bestämmelser m.m.
Om det har skett en överträdelse 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 sanktions-avgifter 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.

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.

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.[9]

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.

IMY:s bedömning

Sanktionsavgift ska påföras

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

Överträdelsen har skett genom att Apohem behandlat personuppgifter med en otillräcklig säkerhetsnivå, vilket har medfört att integritetskänsliga personuppgifter om ett stort antal registrerade oavsiktligt förts över till Meta under perioden 15 april 2021–26 april 2022. Obehörig åtkomst till den typen av uppgifter medför en hög risk för de registrerades fri- och rättigheter. 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.

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.[10]

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 att Apohem därför 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 bolaget inte levt upp till de krav som dataskydds-förordningen ställer i detta avseende. Apohem kan inte anses ha varit okunnig om att dess agerande inneburit en överträdelse av förordningen.[11]

IMY bedömer därmed att förutsättningarna för att påföra Apohem en administrativ sanktionsavgift för överträdelsen 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

Av årsredovisningen för räkenskapsåret 2023 framgår att Apohem hade en års-omsättning på 603 000 000 kronor. Eftersom IMY har konstaterat en överträdelse av

[9] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under GDPR antagna den 24 maj 2023.
[10] EU-domstolens dom i mål C-683/21 Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos mot Valstybinė duomenų apsaugos inspekcija av den 5 december 2023, punkt 81 och dom i mål C 807/21 Deutsche Wohnen av den 5 december 2023, punkt 76.
[11] Se för bedömningen av oaktsamhet även Kammarrätten i Stockholms dom den 11 mars 2024 i mål 2829-23, s.12.

artikel 32 i dataskyddsförordningen ska det högsta sanktionsbelopp som kan fastställas i ärendet enligt artikel 83.4 uppgå till 10 000 000 EUR eller två procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst. Två procent av bolagets årsomsättning för 2023 är 12 060 000 kronor. Den högsta sanktionsavgiften som kan fastställas i ärendet är därför 10 000 000 EUR.

Överträdelsens allvar

Av EDPB:s riktlinjer framgår att tillsynsmyndigheten ska bedöma om överträdelsen är av låg, medelhög eller hög allvarlighetsgrad.[12]

Vid bedömningen av överträdelsens allvarlighetsgrad tar IMY hänsyn till följande omständigheter. De aktuella säkerhetsbristerna har lett till en incident som har berört ett stort antal registrerade och att Meta under en lång tid har kunnat ta del av en stor mängd personuppgifter som inte skulle ha förts över till dem. Uppgifterna har omfattat integritetskänsliga personuppgifter om direkt identifierbara kunder, det vill säga uppgifter som kräver en hög skyddsnivå. Därutöver har överträdelsen skett i en apoteksverksamhet där de registrerade måste anses ha haft en berättigad förväntan på hög konfidentialitet och att deras personuppgifter inte sprids till obehöriga. Försäljning av receptfria och andra hälsorelaterade produkter måste även anses omfattas av Apohems kärnverksamhet, vilket gör att överträdelsen ska betraktas som mer allvarlig än om så inte varit fallet.[13]

Vidare beaktar IMY att Apohem vid tidpunkten för överträdelsen hade vidtagit ett antal lämpliga tekniska och organisatoriska säkerhetsåtgärder. Personuppgifterna har dessutom 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 med många obehöriga eller funnits publikt tillgängliga på webben.

Vid en samlad bedömning mot bakgrund av ovanstående omständigheter anser IMY att det rör sig om en överträdelse av artikel 32.1 i dataskyddsförordningen 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 Apohem bland annat försökt kontakta Meta med frågor om överföringen av personuppgifter samt utarbetat nya styrdokument och rutiner för att minska risken för liknande incidenter. Apohem stängde även av pixeln i sin helhet när bolaget fick kännedom om överföringen. IMY konstaterar dock att dessa åtgärder har vidtagits först efter att bolaget har blivit uppmärksammad på de aktuella bristerna av en extern källa. De vidtagna åtgärderna kan enligt IMY inte anses gå utöver vad som förväntas av Apohem i det aktuella fallet. De är därmed inte av sådan karaktär att de påverkar IMY:s bedömning av sanktionsavgiftens storlek i förmildrande riktning. Detsamma gäller det faktum att Apohem lämnade in en anmälan om personuppgiftsincident till IMY eftersom det utgör en omständighet som ska anses neutral vid bestämmandet av sanktionsavgiften.[14] IMY konstaterar att det inte heller i övrigt framkommit några omständigheter som påverkar bedömningen av sanktionsavgiftens storlek, varken i försvårande eller förmildrande riktning.

---

[12] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 60.
[13] 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.
[14] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 98.

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 aktuella överträdelser som till tillsynsobjektets betalningsförmåga.

Mot bakgrund av överträdelsens allvar bestämmer IMY att Apohem ska betala en administrativ sanktionsavgift på 8 000 000 kronor för den konstaterade överträdelsen. IMY bedömer att detta belopp är effektivt, proportionerligt och avskräckande.

Detta beslut har fattats av den vikarierande generaldirektören David Törngren efter föredragning av juristen Shirin Daneshgari Nejad. Vid den slutliga handläggningen har även den tillförordnade rättschefen Cecilia Agnehall, enhetschefen Nidia Nordenström, juristen Maja Welander 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
DSO

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.