Integritetsskyddsmyndigheten

Spotify AB
Org.nr: 556703-7485
Regeringsgatan 19
111 53 Stockholm

Diarienummer:
DI-2020-10541

Datum:
2021-03-24

Beslut efter tillsyn enligt dataskyddsförordningen – Spotify AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Spotify AB har behandlat personuppgifter i strid med

- artikel 12.4 dataskyddsförordningen[1] genom att bolaget i sitt svar av den 8 juni 2018 på klagandens invändning mot behandlingen av den 24 maj 2018 enligt artikel 21 inte på ett klart och tydligt sätt har redogjort för vilka uppgifter som behandlas, att uppgifterna behandlas med stöd av ett berättigat intresse och vad det berättigade intresset är samt att svaret inte innehållit information om möjligheten att lämna in ett klagomål till tillsynsmyndigheten och begära rättslig prövning.

Integritetsskyddsmyndigheten ger Spotify AB en reprimand enligt artikel 58.2 b dataskyddsförordningen.

Redogörelse för tillsynsärendet

Integritetsskyddsmyndigheten (IMY) har inlett tillsyn beträffande Spotify AB (Spotify eller bolaget) med anledning av ett klagomål. Klagomålet har lämnats över till IMY, i egenskap av ansvarig tillsynsmyndighet enligt artikel 56 dataskyddsförordningen. Överlämnandet har skett från tillsynsmyndigheten i det land där klaganden har lämnat in sitt klagomål (Danmark) i enlighet med förordningens bestämmelser om samarbete vid gränsöverskridande behandling.

I *klagomålet* anförs i huvudsak följande. Klaganden har tidigare haft ett konto och en betalprenumeration på bolagets musiktjänst. Klaganden har flera gånger begärt att bolaget ska radera hans kortuppgifter. Enligt bolaget har klaganden registrerat sig via PayPal och bolaget behandlar därför inte klagandens kortuppgifter. Klaganden ifrågasätter detta, eftersom klagandens son har nekats att registrera sig för en kostnadsfri provperiod där klagandens kortuppgifter använts, med motiveringen att kortet redan har använts.

Spotify AB har i huvudsak uppgett följande.

[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).

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Klaganden har begärt radering av sina kredit- eller betalkortsuppgifter. Spotify behandlar dock inte kortuppgifter när en användare betalar via PayPal, såsom klaganden gjort, utan behandlar istället unika identifierare för de betalkort eller ”instrument” (”unika betalningsinstrumentidentifierare”) som används av en kund vid registrering av kostnadsfria provperioder. Den rättsliga grunden för behandlingen är berättigade intressen. Att klaganden skrivit att han drar tillbaka sitt samtycke får tolkas som en invändning mot behandlingen. Den fortsatta behandlingen är inte föremål för rätten till radering eftersom Spotify har ett starkt, berättigat intresse att fortsätta behandlingen som väger tyngre än klagandens rättigheter och friheter.

För att registrera sig för en kostnadsfri provperiod måste potentiella kunder tillhandahålla Spotify betalkortsuppgifter som kommer användas för fakturering när den kostnadsfria provperioden har löpt ut. För att motverka missbruk av de kostnadsfria provperioder som bolaget erbjuder använder bolaget unika betalningsinstrumentidentifierare. Detta gör att samma betalningsinstrument inte kan användas flera gånger. Utan denna funktion skulle det vara enkelt för en kund att starta nya kostnadsfria Spotify-konton för ytterligare provperioder varje gång deras kostnadsfria provperiod löper ut, genom att variera uppgifter såsom e-postadress, och därmed bedrägligt utnyttja Spotify. Den unika betalningsinstrumentidentifieraren är en alfanumerisk kedja som genereras av Spotifys betalningsbehandlare PayPal. Den möjliggör den unika identifieringen av kreditkort, men den innehåller inte kreditkortsnumret eller andra kortdetaljer. Spotify kan inte genom betalningsinstrumentidentifieraren få tillgång till betalkortsuppgifter via baklängeskonstruktion (s.k. reverse engineering). Denna process är förenlig med PCI DSS[2].

Behandlingen är nödvändig för Spotify för att kunna motverka bedrägeri. Detta är både ett berättigat intresse för Spotify och bolagets breda kundbas, eftersom bolaget inte skulle kunna fortsätta erbjuda kostnadsfria provperioder av bolagets tjänst om bedrägerier inte kunde motverkas på det här sättet. Det ligger också i allmänhetens berättigade intresse.

Spotify har svarat på klagandens begäranden men inte raderat uppgifterna eftersom rätten till radering inte är tillämplig. Bolaget svarade den 7 december 2017 på klagandens ursprungliga begäran av den 6 december 2017 och den 8 juni 2018 på klagandens senaste begäran av den 24 maj 2018 och således inom tidsfristen i dataskyddsförordningen. Gällande klagandens skrivelse från den 15 mars 2018 tolkade bolaget inte det som en begäran om radering enligt dataskyddsförordningen, men besvarade skrivelsen den 4 maj 2018. Bolaget har i flera av dessa svar informerat klaganden om att bolaget inte lagrar hans betalkortsuppgifter och att bolaget inte kunde radera betalningsinstrumentreferensen som identifierar att hans kort redan har använts för att ta del av ett av bolagets erbjudanden eller tjänster.

Gällande vilken information som lämnades till klaganden den 8 juni 2018 med anledningen av dennes invändning anser Spotify att bolaget svarade på klagandens fråga genom att förklara att det inte lagrar några kortuppgifter utan endast använder en algoritm för att se om ett kreditkort har använts för att ta del av ett Spotify-erbjudande tidigare. Om bolaget hade haft anledning att tro att klaganden önskade mer detaljer om dessa kategorier av personuppgifter hade bolaget tillhandahållit det. När bolagets kundtjänstrådgivare kommunicerar med användare försöker bolaget alltid att tillhandahålla den information som användarna frågar efter i ett format som är relevant

[2] PCI DSS står för Payment Card Industry Data Security Standard och är en allmänt accepterad uppsättning riktlinjer och rutiner som syftar till att optimera säkerheten kring användningen av kredit- och bankkort.

för användarna och som även någon som inte känner till bestämmelserna i dataskyddsförordningen skulle förstå. Eftersom klaganden varken nämnde förordningen eller frågade efter den rättsliga grunden för behandlingen gick bolaget inte in på legala detaljer i sitt svar såsom bolagets intresseavvägning. Därtill hade bolaget i sin integritetspolicy kommunicerat till sina användare att det på förfrågan gärna tillhandahåller mer information om den intresseavvägning som bolaget har gjort för att förlita sig på berättigat intresse som legal grund och informerat om möjligheten att lämna in klagomål till tillsynsmyndigheterna. Vidare bör det beaktas att ärendet påbörjades mer än fem månader innan dataskyddsförordningen trädde i kraft och att den enda korrespondensen som ägt rum i tiden efter var bolagets svar två veckor därefter. Sedan dess har bolagets kundtjänstrådgivare genomgått ytterligare utbildning i hur de ska svara användare på ett klart och tydligt sätt, vilka frågor som ska betraktas som förfrågningar enligt dataskyddsförordningen samt vilka frågor som ska vidarebefordras till bolagets dataskyddsteam och dataskyddsombud. Slutligen ska det beaktas att bolaget får in över 11.000 kundtjänstärenden dagligen. Även om bolagets kundtjänst får kontinuerliga utbildningar i dataskydd kan den mänskliga faktorn ibland leda till att ett ärende besvaras som ett kundtjänstärende istället för ett svar på en förfrågan enligt dataskyddsförordningen som avses i artikel 12.4, särskilt när användaren inte nämner personuppgifter eller dataskyddsförordningen i sin kommunikation med bolaget.

Handläggningen har skett genom skriftväxling. Mot bakgrund av att det gäller gränsöverskridande behandling har IMY använt sig av de mekanismer för samarbete och enhetlighet som finns i kapitel VII i dataskyddsförordningen. Berörda tillsynsmyndigheter har varit dataskyddsmyndigheterna i Portugal, Belgien, Cypern, Österrike, Frankrike, Tyskland, Slovakien, Italien, Spanien, Danmark, Norge och Finland.

Motivering av beslut

Integritetsskyddsmyndighetens bedömning

Har bolaget haft rätt att fortsätta behandla klagandens uppgifter efter att klaganden invänt mot behandlingen?
Enligt artikel 17.1 c dataskyddsförordningen ska den registrerade ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om den registrerade invänder mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre. Enligt artikel 21.1 ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 f. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa avgörande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter.

Klagandens skrivelse av den 24 maj 2018 får förstås som en invändning mot behandlingen enligt artikel 21.1, av skäl som hänför sig till hans specifika situation på så sätt att den medför att kortnumret inte kan återanvändas för att registrera nya kostnadsfria provperioder på bolagets tjänster. Eftersom begäran inte hade hanterats innan dataskyddsförordningen började tillämpas den 25 maj 2018 så ska bolagets hantering av begäran bedömas enligt dataskyddsförordningen, det vill säga om

bolaget har påvisat avgörande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter.

För att behandling ska kunna stödja sig på artikel 6.1 f krävs att samtliga tre villkor som föreskrivs där är uppfyllda, nämligen för det första att den personuppgiftsansvarige eller tredje part har ett berättigat intresse (*berättigat intresse*), för det andra att behandlingen är nödvändig för ändamål som rör det berättigade intresset (*nödvändig*) och för det tredje att inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter (*intresseavvägning*).

Bolaget har bland annat anfört att bolagets *berättigade intresse* med behandlingen är att motverka bedrägerier avseende kostnadsfria provperioder. I skäl 47 dataskyddsförordningen anges att sådan behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier utgör ett *berättigat intresse* för berörd personuppgiftsansvarig. IMY anser därmed att bolaget har ett berättigat intresse.

Vidare anser IMY att behandlingen är absolut *nödvändig* för ändamål som rör det berättigade intresset. Av utredningen framgår nämligen att uppgifterna har minimerats i den mån det är möjligt för att bolaget ska kunna uppnå ändamålet som rör det berättigade intresset.

Vid den *intresseavvägning* som ska göras mellan bolagets berättigade intresse och klagandens intressen, rättigheter och friheter, konstaterar IMY att *bolagets berättigade intresse* väger tungt. Behandlingen framstår som något som klaganden rimligen kan förvänta sig vid registrering av en kostnadsfri provperiod och inte särskilt integritetskränkande. Uppgifterna i sig är inte heller att betrakta som integritetskänsliga. Vid en sammanvägd bedömning anser IMY att bolaget har visat avgörande berättigade skäl som väger tyngre än *klagandens intresse* av att hans kortuppgifter kan återanvändas för att registrera nya kostnadsfria provperioder på bolagets tjänster och att hans personuppgifter inte ska behandlas.

IMY anser mot bakgrund av de skäl som bolaget fört fram att bolaget har visat avgörande berättigade skäl som väger tyngre än klagandens intressen, friheter och rättigheter. Bolaget har därmed haft fog för att fortsätta behandla uppgifterna efter att klaganden har invänt mot behandlingen och klaganden har därför inte haft rätt till radering enligt artikel 17.1 c dataskyddsförordningen.

Har bolaget hanterat klagandens begäranden på ett formellt korrekt sätt enligt dataskyddsförordningen?
Enligt artikel 12.1 dataskyddsförordningen ska den personuppgiftsansvarige vidta lämpliga åtgärder för att till den registrerade tillhandahålla all kommunikation enligt artikel 17 och 21 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, Enligt artikel 12.3 dataskyddsförordningen ska den personuppgiftsansvarige på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt artikel 17 och 21. Enligt artikel 12.4 ska den personuppgiftsansvarige, om denne inte vidtar åtgärder på den registrerades begäran, utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning. Enligt skäl 59 dataskyddsförordningen bör personuppgiftsansvariga utan onödigt dröjsmål och senast inom en månad vara

skyldiga att besvara registrerades önskemål och lämna en motivering, om de inte avser att uppfylla sådana önskemål.

I ärendet ska endast bedömas bolagets agerande under den tid som dataskyddsförordningen har varit tillämplig, det vill säga sedan den 25 maj 2018. Vid bedömningen av om bolaget uppfyllt sina informationsskyldigheter gentemot klaganden genom sitt svar den 8 juni 2018 ska dock de svar som bolaget tidigare lämnat till klaganden beaktas till bolagets fördel.

Bolaget har bland annat fört fram att anledningen till att bolaget i sitt svar till klaganden inte informerat om sin rättsliga grund för behandlingen, sin intresseavvägning eller möjligheten att klaga till tillsynsmyndigheter berott på att klaganden inte nämnt personuppgifter eller dataskyddsförordningen i sin kommunikation med bolaget och att klaganden kort där innan fått information om detta genom bolagets integritetspolicy som började gälla den 25 maj 2018. IMY konstaterar dock att klaganden uttryckligen angett att det gällt kreditkortsuppgifter och för vilka ändamål han menade att uppgifterna får behandlas, vilket svårligen kan förstås som annat än som personuppgifter och hänvisningar till dataskyddsreglerna. Som IMY ovan konstaterat och bolaget också själv angett ska klagandens begäran dessutom uppfattas som en invändning enligt artikel 21, vilket därmed har inneburit en skyldighet för bolaget att meddela ett för klaganden individualiserat beslut enligt dataskyddsförordningen. Eftersom bolagets beslut var negativt skulle bolagets svar enligt skäl 59 varit motiverat och enligt artikel 12.4 innehållit orsaken till detta och klagohänvisning, vilket det inte gjorde. Vad bolaget anfört om att information om detta framgått av bolagets integritetspolicy är inte tillräckligt. Detta eftersom det rört sig om ett individualiserat beslut och den enskilde inte kan förväntas ta del av en sådan policy i sin helhet för att dra slutsatser om vilken typ av beslut som bolaget därmed fattat, särskilt när bolaget varken angett vilken rättslig grund behandlingen baserats på eller att klagandens invändning hade avslagits.

Mot denna bakgrund finner IMY att bolagets svar av den 8 juni 2018 inte varit tillräckligt motiverat enligt artikel 12.4 eftersom bolaget inte på ett klart och tydligt sätt har redogjort för vilka uppgifter som behandlas, att uppgifterna behandlas med stöd av ett berättigat intresse och vad det berättigade intresset är samt att svaret inte innehållit information om möjligheten att lämna in ett klagomål till tillsynsmyndigheten och begära rättslig prövning. Spotify har därigenom behandlat personuppgifter i strid med artikel 12.4 dataskyddsförordningen.

Val av ingripande

Av artikel 58.2 i och artikel 83.2 dataskyddsförordningen framgår att IMY har befogenhet att påföra administrativa sanktionsavgifter i enlighet med artikel 83. Beroende på omständigheterna i det enskilda fallet ska administrativa sanktionsavgifter påföras utöver eller i stället för de andra åtgärder som avses i artikel 58.2, som till exempel förelägganden och förbud. Vidare framgår av artikel 83.2 vilka faktorer som ska beaktas vid beslut om administrativa sanktionsavgifter ska påföras och vid bestämmande av avgiftens storlek. 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. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

Bolaget har till sitt försvar i huvudsak anfört att det rör sig om en engångsföreteelse och att bolaget hanterar en stor mängd kundtjänstärenden. Vidare har sedan det inträffade bolagets kundtjänstrådgivare genomgått ytterligare utbildning i hur de ska svara användare på ett klart och tydligt sätt, vilka frågor som ska betraktas som förfrågningar enligt dataskyddsförordningen samt vilka frågor som ska vidarebefordras till bolagets dataskyddsteam och dataskyddsombud.

IMY finner vid en samlad bedömning av omständigheterna att det är fråga om en sådan mindre överträdelse i den mening som avses i skäl 148 och att Spotify AB därför ska ges en reprimand enligt artikel 58.2 b dataskyddsförordningen för den konstaterade överträdelsen.

Ärendet avslutas.

Detta beslut har fattats av enhetschefen Catharina Fernquist efter föredragning av juristen Olle Pettersson.

Catharina Fernquist, 2021-03-24 (Det här är en elektronisk signatur)

Kopia till
Dataskyddsombudet

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Integritetsskyddsmyndigheten senast tre veckor från den dag ni fick del av beslutet. Om överklagandet har kommit in i rätt tid sänder Integritetsskyddsmyndigheten det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Integritetsskyddsmyndigheten om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.