

CDON AB Södergatan 22, 6 tr, 211 34 Malmö

Diarienummer: DI-2020-10549

Datum: 2023-03-31

Beslut efter tillsyn enligt dataskyddsförordningen – CDON AB

Integritetsskyddsmyndigheten beslut

Integritetsskyddsmyndigheten konstaterar att CDON AB har behandlat personuppgifter i strid med:

- artiklarna 5.1 c och 12.6 i dataskyddsförordningen¹ genom att ha begärt in ytterligare information av klagandena i klagomål 1–3 och 6-7 när de begärt att få sina personuppgifter raderade, utan att behandlingen varit nödvändig för att bekräfta klagandenas identitet.
- artikel 12.2 i dataskyddsförordningen genom att använda sig av en betungande verifieringsmetod gentemot klagandena i klagomål 1–3 och 6-7. Bolaget har därmed inte i tillräcklig mån underlättat för klagandena att utöva sin rätt till radering enligt artikel 17 i dataskyddsförordningen.

IMY ger CDON AB en reprimand enligt artikel 58.2 b i dataskyddsförordningen för överträdelse av artiklarna 5.1 c, 12.6 och 12.2 i dataskyddsförordningen.

Redogörelse för tillsynsärendet

Handläggningen

IMY har inlett tillsyn beträffande CDON AB (CDON eller bolaget) med anledning av sju klagomål. Klagomålen har lämnats över till IMY, i egenskap av ansvarig tillsynsmyndighet enligt artikel 56 i dataskyddsförordningen. Överlämningen har skett från tillsynsmyndigheten i de länder där klagandena har lämnat in sina klagomål (Finland och Danmark) i enlighet med förordningens bestämmelser om samarbete vid gränsöverskridande behandling.

Handläggningen vid IMY har skett genom skriftväxling. Mot bakgrund av att det gäller klagomål rörande 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 Danmark, Norge och Finland.

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).

Diarienummer: DI-2020-10549

Datum: 2023-03-31

Klagomålen

Sammanfattning av klagomålen

Sammanfattningsvis framgår följande av klagomålen. Klagandena har begärt att deras personuppgifter ska raderas. Bolaget har svarat att en begäran endast kan hanteras om den enskilde inkommer med uppgift om födelsedatum, adress, kundnummer, information om senaste inköp såsom ordernummer och information om betalsätt inklusive de fyra sista siffrorna i kreditkortsnumret vid kortbetalning. Flera av de klagande menar att deras inköp ligger så långt tillbaka i tiden att de inte kunnat återfinna alla de efterfrågade uppgifterna. Klagandena ifrågasätter att samtliga av de efterfrågade uppgifterna är nödvändiga för att bekräfta deras identitet och hantera deras begäranden.

Vad klaganden och CDON har uppgett i respektive klagomål

Klagomål 1 (Finland med nationellt diarienummer 2529/182/2018)

Klaganden har den 28 maj 2018 inkommit med en begäran om radering av sina personuppgifter. Bolaget har svarat att en begäran endast kan hanteras om den klaganden inkommer med födelsedatum, adress, kundnummer, ordernummer och beroende på betalningsmetod för senaste beställningen följande uppgift:

- om faktura: pris och referensnummer
- om kortbetalning: de fyra sista siffrorna i kreditkortsnumret
- om direktbetalning: referensnummer och kvitto

Klaganden uppger sammanfattningsvis att hon inte kan komma ihåg eller återfinna de av bolaget begärda uppgifterna eftersom beställningen gjordes för 5–10 år sedan.

Klagomål 2 (Finland med nationellt diarienummer 2537/154/2018)

Klaganden har den 25 maj 2018 inkommit med en begäran om radering av sina kunduppgifter. Bolaget har svarat att det kräver uppgift om födelsedatum, kundnummer, ordernummer och betalningsmetod för den senaste beställningen. Klaganden anser att det är orimligt att behöva svara på dessa frågor för att kunna tillvarata sina rättigheter. Klaganden har inte kvar de av bolaget begärda uppgifterna och har använt den e-post vid begäran om radering som var kopplad till klagandens kundkonto.

Klagomål 3 (Finland med nationellt diarienummer 2648/182/2018)

Klaganden har den 31 maj 2018 kontaktat den finska dataskyddsmyndigheten efter att ha begärt tillgång till och radering av sina uppgifter hos bolaget. Bolaget har den 29 maj 2018 som svar på klagandens begäran angett att för att kunna verifiera klaganden som kund behövs av säkerhetsskäl uppgift om klagandens adress, kundnummer, ordernummer från senaste beställningen och beroende på betalningsmetod för den senaste beställningen följande uppgift:

- om faktura: pris och referensnummer
- om kortbetalning: de fyra sista siffrorna i kreditkortsnumret
- om direktbetalning: referensnummer och kvitto

Klaganden anför att det var länge sedan klaganden köpte något från bolaget och att klaganden inte har kvar de uppgifter som bolaget kräver. Vidare uppges att bolaget inte verkar radera uppgifterna utan att få svar på sina detaljerade frågor vid en begäran om radering.

Datum: 2023-03-31

Klagomål 4 (Finland med nationellt diarienummer 2664/182/2018)

Klaganden har den 31 maj 2018 vänt sig till den finska dataskyddsmyndigheten efter att ha begärt radering hos bolaget. Det var 5–10 år sedan klaganden beställde något från bolaget. För att få sina uppgifter raderade behöver klaganden tillhandahålla uppgifter från sitt köp som genomfördes för flera år sedan. Klaganden behöver även uppge personuppgifter som inte tidigare behövts för att genomföra ett köp. Bolaget har i sitt svar till klaganden informerat om att det finns en rätt att få tillgång till och att radera personuppgifter men att bolaget har rätt att bevara vissa personuppgifter för bokföringsändamål. För att tillmötesgå en begäran behöver bolaget av säkerhetsskäl få uppgift om klagandens födelsedatum, adress, kundnummer, ordernummer från senaste beställningen och beroende på betalningsmetod för den senaste beställningen följande uppgift:

- om faktura: pris och referensnummer
- om kortbetalning: de fyra sista siffrorna i kreditkortsnumret
- om direktbetalning: referensnummer och kvitto

Bolaget har uppgett att de inte kan verifiera vilket datum klagomålet inkom till bolaget eller vilket datum bolaget begärde kompletterande uppgifter från den klagande. Eftersom klaganden inte varit aktiv kund hos CDON under de två till fem senaste åren bekräftar CDON även att klagandenas personuppgifter gallrats från CDON:s system och att inga uppgifter om klaganden finns kvar.

Klagomål 5 (Finland med nationellt diarienummer 2478/153/2018)

Klaganden har kontaktat den finska dataskyddsmyndigheten efter att ha begärt radering av sina uppgifter hos bolaget. Bolaget har informerat klaganden om att det finns en rätt att få tillgång till och att radera personuppgifter men att bolaget har rätt att bevara vissa personuppgifter för bokföringsändamål. För att tillmötesgå en begäran behöver bolaget av säkerhetsskäl få uppgift om klagandens födelsedatum, adress, kundnummer, ordernummer från senaste beställningen och beroende på betalningsmetod för den senaste beställningen följande uppgift:

- om faktura: pris och referensnummer
- om kortbetalning: de fyra sista siffrorna i kreditkortsnumret
- om direktbetalning: referensnummer och kvitto

Klaganden kommer inte ihåg när en beställning gjordes från bolaget och hur köpet betalades. Det är över ett år sedan något beställdes.

Bolaget har uppgett att de inte kan verifiera vilket datum klagomålet inkom till bolaget eller vilket datum bolaget begärde kompletterande uppgifter från den klagande. Eftersom klaganden inte varit aktiv kund hos CDON under de två till fem senaste åren bekräftar CDON även att klagandenas personuppgifter gallrats från CDON:s system och att inga uppgifter om klaganden finns kvar.

Klagomål 6 (Finland med nationellt diarienummer 2814/154/2018)

Klaganden har vänt sig med ett klagomål till den finska dataskyddsmyndigheten efter en begäran om radering hos bolaget den 21 maj 2018. Klaganden uppger att bolaget gör det svårt att utöva rätten till radering genom att efterfråga information som man inte ska behöva spara som kund. Processen bidrar till att det tar lång tid att få personuppgifter raderade. Bolaget har i sitt svar till klaganden den 29 maj 2018 krävt information om födelsedatum, adress, kundnummer samt ett av följande:

Diarienummer: DI-2020-10549 Datum: 2023-03-31

- ordernummer från senaste beställningen,
- beroende på betalningsmetod för den senaste beställningen följande uppgift:
 - o m faktura: pris och referensnummer
 - om kortbetalning: de fyra sista siffrorna i kreditkortsnumret
 - o m direktbetalning: referensnummer och kvitto

Klagomål 7 (Danmark med nationellt diarienummer 2018-31-0638)

Klaganden uppger sig ha försökt radera sitt kundkonto online på cdon.dk genom att använda sig av en hyperlänk http://cdon.dk/. Bolaget har svarat klaganden den 29 maj 2018 och krävt information om födelsedatum, adress, kundnummer, ordernummer från senaste beställningen och betalningsmetod för den senaste beställningen inklusive de fyra sista siffrorna i kreditkortsnumret. Klaganden uppger bl.a. att bolaget kräver fler uppgifter vid utövandet av rätten till radering än vid skapandet av kundkontot. Klaganden har använt samma e-postadress vid begäran om radering som vid skapandet av kundkontot hos bolaget.

Vad CDON AB har uppgett i övrigt

CDON AB har i huvudsak uppgett följande.

Klagomålen

Av de inkomna klagomålen har CDON kunnat identifiera sex av sju klaganden mot upplysningar i sina system. Vad gäller dessa sex klagande konstaterar CDON att de är personuppgiftsansvarig för den behandling av personuppgifter som klagomålen avser. Vad avser det sjunde klagomålet (2478/153/2018) har bolaget uppgett att klaganden inte kunnat identifieras men att det är möjligt att den klagande har haft en kundrelation med CDON under en annan e-postadress än den som angivits i det klagomål som sänts till tillsynsmyndigheten.

I samband med att klagandena har begärt radering har de till CDON inkommit med namn och e-postadress. CDON har dock bedömt att endast dessa två uppgifter inte är tillräckliga för att säkerställa klagandenas identitet. CDON har, med stöd av artikel 12.6 i dataskyddsförordningen, därför begärt kompletterande uppgifter från samtliga klagande. Utöver namn och e-postadress har CDON begärt följande uppgifter för att säkerställa klagandenas identitet:

- födelsedatum,
- · folkbokföringsadress,
- kundnummer,
- ordernummer för senaste order, och
- betalsätt vid senaste order.

Därutöver har klagandena behövt lämna följande information om betalsätt:

- vid fakturaköp: pris samt referensnummer,
- vid kortbetalning: kortets fyra sista siffror,
- vid direktbetalning: referens- eller fakturanummer.

Befintliga rutiner

CDON ser i sammanhanget mycket allvarligt på de klagomål som inkommit gällande svårigheter för registrerade att utöva sina rättigheter enligt dataskyddsförordningen och har löpande arbetat med att förbättra sina rutiner för identifiering vid begäran om registerutdrag eller radering. Sedan 2018, då klagomålen inkom, har identifieringsprocessen granskats och förtydligats. Under årens gång har CDON arbetat för att förbättra hanteringen och säkerställa en enkel och säker process vid

Diarienummer: DI-2020-10549 5(11)

Datum: 2023-03-31

förfrågningar om radering. Kunder som vill begära radering eller tillgång hänvisas till att kontakta bolaget på kunddata@cdon.com. I samband med att en registrerad kontaktar bolaget med en begäran om radering meddelar bolaget den registrerade att den registrerades e-post inom kort kommer att avregistreras från CDON:s nyhetsbrev (om sådan prenumeration är aktiverad). För att få sitt konto raderat efterfrågar i dagsläget CDON att kunden besvarar två säkerhetsfrågor (en vardera från kategori 1 respektive 2) för att CDON ska kunna säkerställa att den person som hör av sig är rätt registrerad. De registrerade får välja att besvara en fråga från respektive säkerhetskategori av frågor som CDON tillhandahåller. Detta innebär att de registrerade behöver besvara endast en av följande säkerhetsfrågor i kategori 1. Enligt kontrollfrågorna i kategori 1 ska kunder uppge födelsedatum², folkbokföringsadress eller kundnummer hos CDON.com. Därefter behöver de registrerade besvara endast en av följande säkerhetsfrågor i kategori 2. Kontrollfrågorna i kategori 2 är kopplade till senaste ordern där kunden antingen uppger ordernummer eller beroende på betalsätt anger en av följande uppgifter: vid faktura; summa samt OCR-nummer, vid kortbetalning: de fyra sista siffrorna på kortet och vid direktbetalning; transaktions-id eller faktura-id.

För det fall en kund inte vill eller kan besvara de säkerhetsfrågor som efterfrågas erbjuds den registrerade också möjligheten att kontakta kundtjänst för uppföljning och utredning av alternativa säkerhetsfrågor för att försöka hitta ett annat sätt att verifiera kundens identitet. CDON anser att det är nödvändigt med minst två ytterligare upplysningar utöver namn och e-postadress från kunder enligt bolagets nya rutin för att med tillräcklig säkerhet kunna verifiera att det är rätt person som framställer en begäran. CDON:s rutin för identifiering och verifiering av den registrerade innebär inte att ny information samlas in om den registrerade. CDON begär endast att få två olika uppgifter verifierade mot de uppgifter som CDON redan behandlar om den registrerade med laglig grund för att kunna verifiera den registrerades identitet.

Bolagets gallringsrutiner

CDON har redogjort för att de har en rutin för gallring av mejl och en annan rutin för gallring av personuppgifter. CDON:s rutin för gallring av mejl innebär att samtliga mejl inkomna till CDON:s kunddata-box dvs. kunddata@cdon.com, dit kunder blir hänvisade om de har önskemål om radering eller registerutdrag, gallras och raderas efter 14 månader från det datum då mejlen inkom till CDON. Gallring av kundprofiler på CDON sker för närvarande baserat på konsumenträttsliga förpliktelser i olika länder till exempel efter tre år i Sverige. CDON bekräftar därmed att samtliga klagandes personuppgifter raderats hos CDON.

Motivering av beslut

Tillämpliga bestämmelser

För att personuppgiftbehandling ska vara förenlig med dataskyddsförordningen krävs bland annat att behandlingen uppfyller kraven gällande de principer om behandling av personuppgifter som anges i artikel 5 i dataskyddsförordningen,³ bland annat principen om uppgiftsminimering (artikel 5.1 c) och principen om ansvarsskyldighet (artikel 5.2).

² Sedan den 22 januari 2021 samlar CDON endast in födelsenummer (om den registrerade väljer att komplettera med den uppgiften i säkerhetsfråga 1) och inte det fulla personnumret (dnr DI-2020-10549-18 s.2).

³ Se EU-domstolens dom Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, punkt 50, med där angiven rättspraxis.

Diarienummer: DI-2020-10549 6(11)

Datum: 2023-03-31

Enligt artikel 5.1 c i dataskyddsförordningen ska personuppgifterna vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (principen om uppgiftsminimering).

I enlighet med den ansvarsprincip som stadgas i artikel 5.2 i dataskyddsförordningen måste den personuppgiftsansvarige kunna visa att punkt 1 i denna artikel efterlevs, dvs. har bevisbördan för detta.⁴

Enligt artikel 11.2 i dataskyddsförordningen gäller att om den personuppgiftsansvarige, i de fall som avses i punkt 1 i denna artikel, kan visa att denne inte är i stånd att identifiera den registrerade, ska den personuppgiftsansvarige om möjligt informera den registrerade om detta. I sådana fall ska artiklarna 15–20 inte gälla, förutom när den registrerade för utövande av sina rättigheter i enlighet med dessa artiklar tillhandahåller ytterligare information som gör identifieringen möjlig.

Enligt artikel 12.2 i dataskyddsförordningen ska den personuppgiftsansvarige underlätta utövandet av den registrerades rättigheter i enlighet med artiklarna 15–22. I de fall som avses i artikel 11.2 i dataskyddsförordningen får den personuppgiftsansvarige inte vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter enligt artiklarna 15–22, om inte den personuppgiftsansvarige visar att han eller hon inte är i stånd att identifiera den registrerade.

I artikel 12.6 i dataskyddsförordningen anges att utan att det påverkar tillämpningen av artikel 11 i dataskyddsförordningen får den personuppgiftsansvarige, om denne har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 15–21, begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet tillhandahålls. I Europeiska dataskyddsstyrelsens (EDPB) riktlinjer 01/2022 om rätten till tillgång⁵ framgår följande.

Om den personuppgiftsansvarige har rimliga skäl att tvivla på den begärande personens identitet får denne, såsom anges ovan, begära ytterligare information för att bekräfta den registrerades identitet. Den personuppgiftsansvarige måste dock samtidigt se till att den inte samlar in fler personuppgifter än vad som är nödvändigt för att möjliggöra identifiering av den begärande personen. Därför ska den personuppgiftsansvarige göra en proportionalitetsbedömning, som måste ta hänsyn till den typ av personuppgifter som behandlas (t.ex. särskilda kategorier av uppgifter eller inte), begärans art, det sammanhang i vilket begäran görs samt eventuell skada som kan uppstå till följd av otillbörligt utlämnande. Vid bedömningen av proportionaliteten bör överdriven uppgiftsinsamling undvikas samtidigt som en lämplig nivå av säkerhet vid behandling ska säkerställas.⁶

Den personuppgiftsansvarige bör införa ett autentiseringsförfarande (kontroll av den registrerades identitet) för att vara säker på identiteten på de personer som begär tillgång till sina uppgifter, och säkerställa säkerheten vid behandlingen av en

⁴ Se EU-domstolens dom Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, punkt 77 och 81.

⁵ Guidelines 01/2022 on data subject rights - Right of access Version 2.0 Adopted on 28 March 2023 (EDPB:s Riktlinjer 01/2022 om rätten till tillgång).

⁶ EDPB: s Riktlinjer 01/2022, punkt 70, IMY:s översättning; original: "As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable authentication of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security."

Diarienummer: DI-2020-10549 7(11)

Datum: 2023-03-31

begäran om tillgång i enlighet med artikel 32, till exempel en säker kanal för de registrerade att tillhandahålla ytterligare information. Den metod som används för autentisering bör vara relevant, lämplig, proportionerlig och respektera principen om uppgiftsminimering. Om den personuppgiftsansvarige inför åtgärder som syftar till att identifiera den registrerade som är betungande måste den på lämpligt sätt motivera detta och säkerställa efterlevnad av alla grundläggande principer, inbegripet uppgiftsminimering och skyldigheten att underlätta utövandet av de registrerades rättigheter (artikel 12.2 i dataskyddsförordningen).⁷

Integritetsskyddsmyndigheten bedömning

Klagomålen

IMY ska enligt artikel 57.1 f i dataskyddsförordningen behandla klagomål och där så är lämpligt undersöka den sakfråga klagomålet gäller. Ärendet omfattar sju klagomål. IMY har begärt att CDON ska yttra sig över vilka uppgifter bolaget har begärt, nödvändigheten av varje enskild uppgift, datum för när begäran om radering mottogs i respektive klagomål, datum för när bolaget begärde kompletterande uppgifter för att bekräfta identiteten i respektive klagomål samt om klagandena kontaktat bolaget efter 25 maj 2018.

Av klagomål 4 (Finland med nationellt diarienummer 2664/182/2018) samt 5 (Finland med nationellt diarienummer 2478/153/2018) framgår inget datum för när klagandena gjort en begäran om radering hos bolaget eller när bolaget begärde den kompletterande informationen. Bolaget har uppgett att de har raderat klagandenas personuppgifter i de två enskilda klagomålen i enlighet med sin rutin och kan inte verifiera datum för när begäran i respektive klagomål mottogs eller hanterats. IMY finner inte skäl att betvivla att CDON har saknat möjlighet att hitta någon information om klaganden och deras begäranden om radering. Det har passerat flera år sedan klagomålen lämnades till den finska dataskyddsmyndigheten.

IMY konstaterar att det inte går att dra några säkra slutsatser av vad som har förevarit i de två klagandenas fall utifrån vad som har varit möjligt att utreda i klagomålen. Det har bland annat, särskilt mot bakgrund av att klagandenas begäranden är hänförliga till tiden i nära anslutning till att dataskyddsförordningen började tillämpas, inte varit möjligt att utreda om dessa två klagomål omfattas av dataskyddsförordningen. CDON har vidare bekräftat att inga personuppgifter om dessa två klaganden längre behandlas av bolaget. Mot denna bakgrund finner IMY att sakfrågan i de två klagomålen är utredd i den omfattning som är lämplig enligt artikel 57.1 f i dataskyddsförordningen. IMY finner därmed inte skäl att utreda dessa två klagomål vidare. IMY har följaktligen med utgångspunkt i de resterande fem aktuella klagomålen i ärendet dels granskat bolagets agerande i dessa enskilda fall, dels om bolagets nuvarande rutin är förenlig med dataskyddsförordningen.

⁷ EDPB:s Riktlinjer 01/2022,punkt 71, IMY:s översättning, original; "The controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data, and ensure security of the processing throughout the process of handling an access requests in accordance with Art. 32 GDPR, including for instance a secure channel for the data subjects to provide additional information. The method used for authentication should be relevant, appropriate, proportionate and respect the data minimisation principle. If the controller imposes measures aimed at authentifying the data subject which are burdensome, it needs to adequately justify this and ensure compliance with all fundamental principles, including data minimisation and the obligation to facilitate the exercise of data subjects' rights (Art. 12(2) GDPR).

Diarienummer: DI-2020-10549 8(11)

Datum: 2023-03-31

Allmänna utgångpunkter

Det kan konstateras att den personuppgiftsansvarige, för att identifiera en registrerad, får begära ytterligare information som är nödvändig, om den personuppgiftsansvarige har rimliga skäl att betvivla identiteten hos den person som lämnar in en begäran.

Dataskyddsförordningen reglerar inte explicit vilka uppgifter som får efterfrågas eller hur den ytterligare informationen ska samlas in. Den personuppgiftsansvarige måste göra en proportionalitetsbedömning för att fastställa vad som är lämpligt med hänsyn till förordningens krav bland annat avseende säkerhet, men även mot bakgrund av kravet i artikel 12.2 i dataskyddsförordningen, enligt vilket den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter. Att slentrianmässigt kräva uppgifter för identifiering utan hänsyn till om uppgifterna är nödvändiga på så vis som beskrivs i artikel 12.6 i dataskyddsförordningen strider enligt IMY mot både denna bestämmelse och även mot principen om uppgiftsminimering i artikel 5.1 c i dataskyddsförordningen.

Som följer av ordalydelsen i dessa bestämmelser och som bekräftas av EDPB:s riktlinje 01/2022 om rätten till tillgång ska den personuppgiftsansvarige genomföra en proportionalitetsbedömning och kunna motivera den verifieringsmetod som används. För att undvika överdriven uppgiftssamling måste en begäran om ytterligare information vara proportionell i förhållande till den typ av uppgifter som behandlas och den skada som kan uppstå. Även detta bekräftas av riktlinjerna.8

Har det skett en överträdelse av dataskyddsförordningen avseende vad som framförts i klagomålen i detta ärende?

Frågan är om de uppgifter som bolaget krävt för att tillmötesgå begärandena i de enskilda fallen där dataskyddsförordningen är tillämplig (dvs. klagomål 1-3 och 6 -7) har varit nödvändiga för att identifiera respektive klaganden och därmed i enlighet med dataskyddsförordningen. De uppgifter som bolaget har krävt i de enskilda klagomålen, utöver namn och e-post, har varit födelsedatum, folkbokföringsadress, kundnummer, ordernummer och betalsätt vid senaste order, samt, beroende på betalsätt, pris samt referensnummer vid fakturabetalning, kortets fyra sista siffror vid kortbetalning, referens- eller fakturanummer vid direktbetalning.

Bolaget har getts tillfälle att motivera på vilket sätt respektive uppgift som begärts in varit nödvändig för att identifiera klagandena i de enskilda fallen. Bolaget har utan att närmare förklara nödvändigheten av respektive begärd uppgift svarat att det inte varit tillräckligt med namn och e-post för att identifiera klagandena och verifiera att det är rätt person som framställer en begäran. Enligt IMY ger bolagets redogörelse inte tillräckligt stöd för att slå fast att samtliga av de övriga aktuella uppgifterna varit nödvändiga för att identifiera de registrerade i enlighet med artikel 12.6 i dataskyddsförordningen och principen om uppgiftsminimering i artikel 5.1 c i dataskyddsförordningen. Det är CDON, i egenskap av personuppgiftsansvarig, som ska kunna visa att behandlingen utförs i enlighet med förordningen (artikel 5.2 i dataskyddsförordningen). IMY anser att CDON inte har gjort detta. IMY konstaterar därmed att CDON AB behandlat personuppgifter i strid med artikel 5.1 c och 12.6 i dataskyddsförordningen.

De klagande har i detta fall behövt inkomma med förhållandevis många personuppgifter för att kunna utöva sin rätt till radering bl.a. ordernummer och pris för senaste order samt referensnummer vid fakturaköp tillsammans med ytterligare

⁸ EDPB:s Riktlinjer 01/2022, General considerations on the assessment of the data subject's request, sid.2-3.

9(11)

Datum: 2023-03-31

uppgifter. I något fall var det längesedan sedan klaganden handlat något hos CDON. Detta har inneburit att klagandena inte kunnat tillvarata sin rätt till radering enligt artikel 17 i dataskyddsförordningen utan att behöva anstränga sig för att leta efter i vissa fall gamla uppgifter och i varje fall många uppgifter. Genom att utan motivering använda sig av en sådan betungande verifieringsmetod vid begäran om radering har bolaget därmed inte underlättat utövande av de registrerades rättigheter på det sätt som krävs enligt artikel 12.2 i dataskyddsförordningen. CDON AB har därmed behandlat personuppgifter i strid med artikel 12.2 i dataskyddsförordningen.

Är bolagets nuvarande rutin förenlig med dataskyddsförordningen?

Av utredningen framgår att bolaget kontinuerligt har sett över sina rutiner för hanteringen av förfrågningar om radering sedan 2018, då samtliga aktuella klagomål i ärendet inkom. De generella rutiner som granskats är de som varit gällande från 22 januari 2021 fram till och med dagen för IMY:s beslut i det aktuella ärendet.

För att säkerställa identiteten på den registrerade som begär radering behöver den registrerade numera besvara två frågor (en fråga i kategori 1 och en fråga i kategori 2) som exempelvis födelsedatum och ordernummer. I kategori 1 behöver registrerade sedan 22 januari 2021 inte uppge personnummer utan endast födelsedatum om den registrerade väljer att komplettera med den uppgiften. Det är inga nya personuppgifter som begärs för att bekräfta den registrerades identitet utan två olika uppgifter för att jämföra dem mot uppgifter som bolaget redan behandlar om den registrerade för att verifiera den registrerade. Att CDON verifierar den registrerades identitet innan radering av personuppgifter sker är även ett skydd för den registrerade som inte ska behöva få sina personuppgifter raderade av misstag. Bolaget erbjuder även en alternativ väg för den registrerade som inte kan eller vill besvara säkerhetsfrågorna nämligen att kontakta kundtjänsten för att hitta ett annat sätt att verifiera den registrerades identitet. För en kund som inte har gjort en beställning finns därmed alternativet att kontakta kundtjänsten istället.

Mot denna bakgrund finner IMY att CDON:s befintliga rutin inte är oproportionerlig och därmed inte i strid med dataskyddsförordningen under förutsättning att bolaget endast inhämtar de uppgifter som framgår av rutinen i situationer där det finns anledning att betvivla identiteten hos den registrerade och att då endast de uppgifter som är nödvändiga för att identifiera den registrerade begärs in.

Val av ingripande

Av artikel 58.2 i och artikel 83.2 i 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 i dataskyddsförordningen, som till exempel förelägganden och förbud. Vidare framgår av artikel 83.2 i dataskyddsförordningen 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 i dataskyddsförordningen. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

IMY konstaterar följande relevanta omständigheter. Den aktuella tillsynen omfattar CDON AB:s hantering av fem enskilda klagandens begäranden i den situation som klagomålen avser.

Integritetsskyddsmyndigheten

Diarienummer: DI-2020-10549 10(11)

Datum: 2023-03-31

Bolaget har vidtagit åtgärder i syfte att underlätta för registrerade att utöva sina rättigheter i enlighet med dataskyddsförordningen och ändrat sina rutiner så att de är förenliga med dataskyddsförordningen. Vissa åtgärder hade vidtagits redan innan detta tillsynsärendet inleddes. Vidare inträffade de konstaterade överträdelserna relativt långt tillbaka i tiden. Bolaget har inte tidigare erhållit någon korrigerande åtgärd för överträdelse av dataskyddsbestämmelserna. Mot denna bakgrund finner IMY att det är fråga om en sådan mindre överträdelse i den mening som avses i skäl 148 och att CDON AB ska ges en reprimand enligt artikel 58.2 b i dataskyddsförordningen för de konstaterade överträdelserna.

Detta beslut har fattats av enhetschefen Catharina Fernquist efter föredragning av juristen Salli Fanaei. *Catharina Fernquist*, 2023-03-31 (Det här är en elektronisk signatur)

Kopia till

Dataskyddsombudet

Diarienummer: DI-2020-10549 11(11)

Datum: 2023-03-31

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.