Rekommendationer 02/2021 om den rättsliga grunden för lagring av kreditkortsuppgifter endast i syfte att underlätta ytterligare elektroniska transaktioner

Antagna den 19 maj 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Europeiska dataskyddsstyrelsen har antagit dessa rekommendationer

med beaktande av artikel 70.1 e i 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 (*den allmänna dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018, och

med beaktande av artiklarna 12 och 22 i arbetsordningen.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1. Under covid-19-pandemin har den digitala ekonomin och e-handeln fortsatt att utvecklats. Riskerna med att använda kreditkortsuppgifter på internet har ökat i samma utsträckning. Såsom anges i artikel 29-arbetsgruppens riktlinjer om konsekvensbedömning avseende dataskydd kan kreditkortsincidenter entydigt få ”*allvarliga konsekvenser för den registrerades dagliga liv*” eftersom finansiella uppgifter kan användas för betalningsbedrägerier[1].

2. Det är därför mycket viktigt att den personuppgiftsansvarige inför lämpliga skyddsåtgärder för de registrerade och ser till att de registrerade får kontroll över sina egna personuppgifter för att minska risken för otillåten behandling och för att stärka förtroendet för den digitala miljön. Europeiska dataskyddsstyrelsen (EDPB) anser att detta förtroende är avgörande för en hållbar utveckling av den digitala ekonomin.

3. För detta ändamål strävar dessa rekommendationer efter att uppmuntra en harmoniserad tillämpning av dataskyddsreglerna om behandling av kreditkortsuppgifter inom Europeiska ekonomiska samarbetsområdet (EES) och att garantera ett enhetligt skydd för registrerades rättigheter med fullt beaktande av de grundläggande dataskyddsprinciperna i enlighet med den allmänna dataskyddsförordningen.

4. Dessa rekommendationer avser närmare bestämt den lagring av kreditkortsuppgifter som leverantörer av varor och tjänster på internet genomför enbart och uteslutande i syfte att underlätta registrerades fortsatta köp[2]. Rekommendationerna omfattar situationer när registrerade köper produkter eller betalar för tjänster via en webbplats eller applikation och anger sina kreditkortsuppgifter, vanligen via ett särskilt formulär, för att slutföra den unika transaktionen.

5. Den personuppgiftsansvarige måste ha en giltig rättslig grund i enlighet med artikel 6 i den allmänna dataskyddsförordningen för att lagra dessa uppgifter, precis som för all annan

[1] ARTIKEL 29-GRUPPENS riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679.

[2] Det bör noteras att rekommendationerna inte omfattar vare sig betalningsinstitut som är verksamma via nätbutiker eller offentliga myndigheter. De omfattar inte heller lagring av kreditkortsuppgifter för något annat ändamål, exempelvis för fullgörande av rättsliga förpliktelser, för att etablera en återkommande betalning för fortlöpande avtal eller prenumerationer för långvariga tjänster (t.ex. kontrakt om leverans av särskilda varor varje månad eller prenumeration av tjänster för direktuppspelning av musik eller film).

behandling. I detta avseende bör det noteras att ett antal av de rättsliga grunder som anges i artikel 6 i den allmänna dataskyddsförordningen inte är tillämpliga i det här fallet och ska uteslutas. Lagring av kreditkortsuppgifter efter en transaktion för att underlätta ytterligare köp kan varken anses vara nödvändigt för att fullgöra en rättslig förpliktelse (artikel 6.1 c i den allmänna dataskyddsförordningen) eller för att skydda intressen som är av grundläggande betydelse för en fysisk person (artikel 6.1 d i den allmänna dataskyddsförordningen). Det kan inte heller anses att utförandet av en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e) utgör en lämplig rättslig grund.

6. Lagringen av kreditkortsuppgifter efter betalning av varor eller tjänster är dessutom inte i sig nödvändig för att fullgöra ett avtal (artikel 6.1 b i den allmänna dataskyddsförordningen). Medan behandlingen av de avgifter som avser det kreditkort som kunden använt för att betala är nödvändig för att i första hand uppfylla avtalet, och därmed aktivera artikel 6.1 b i den allmänna dataskyddsförordningen, är lagringen av dessa uppgifter endast användbar för att underlätta en eventuell efterföljande transaktion och för att underlätta försäljningen. Ett sådant syfte kan inte anses vara absolut nödvändigt för fullgörandet av avtalet om leverans av de varor eller tjänster som den registrerade redan har betalat för[3].

7. Vad gäller behandling som är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen[4] konstaterar EDPB att de tre villkor som fastställs i artikel 6.1 f i den allmänna dataskyddsförordningen måste uppfyllas för att den personuppgiftsansvarige ska kunna åberopa den artikeln[5]. För denna rättsliga grund krävs för det första att den personuppgiftsansvariges eller en tredje parts berättigade intressen identifieras och kvalificeras. Den personuppgiftsansvariges eller en tredje parts berättigade intressen kan gå utöver syftet för behandlingen och måste utgöra faktiska intressen vid tidpunkten för behandlingen[6].

8. För denna rättsliga grund krävs för det andra att behandlingen av personuppgifter är nödvändig för det berättigade intresse som eftersträvas. Vad gäller det sistnämnda villkoret är det inte uppenbart att lagringen av kreditkortsuppgifterna för att underlätta ytterligare köp är nödvändigt för att eftersträva ett berättigat intresse, förutsatt att den personuppgiftsansvarige har ett berättigat intresse i enlighet med vad som nämns ovan. Det faktiska genomförandet av ett ytterligare köp beror på kundens val och det avgörs inte av möjligheten att genomföra köpet med ett klick.

9. För det tredje villkoret krävs slutligen att ett avvägningstest genomförs. De berättigade intressena hos den registeransvarige eller tredje parter måste vägas mot den registrerades intressen eller grundläggande fri- och rättigheter, däribland den registrerades rätt till dataskydd och integritet. I

[3] Se även EDPB:s riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, framför allt sida 10.
[4] Se artikel 29-arbetsgruppens yttrande om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG, som EDPB håller på att se över (se EDPB:s arbetsprogram 2021/2022 som antogs den 16 mars 2021).
[5] Se EU-domstolens dom av den 4 maj 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde mot Rīgas pašvaldības SIA ”Rīgas satiksme”, mål C-13/16, ECLI:EU:C:2017:336, punkt 28.
[6] Se EU-domstolens dom av den 11 december 2019, TK mot Asociaţia de Proprietari bloc M5A-ScaraA, mål C-708/18, ECLI:EU:C:2019:1064, punkt 44.

avvägningstestet måste de särskilda omständigheterna för behandlingen beaktas[7]. En viktig del i avvägningen är behandlingens möjliga inverkan på den registrerades fri- och rättigheter[8]. Denna inverkan kan bero på arten av uppgifter, den särskilda behandlingsmetoden och tredje parters tillgång till sådana uppgifter. Vad gäller arten av uppgifter bör det noteras att artikel 29-arbetsgruppen har förklarat att finansiella uppgifter är uppgifter av mycket personlig karaktär eftersom överträdelser mot dessa uppgifter entydigt får allvarliga konsekvenser för den registrerades dagliga liv[9]. Trots att den personuppgiftsansvarige är skyldig att införa tekniska eller organisatoriska åtgärder för att säkerställa kreditkortsuppgifternas säkerhet i enlighet med artikel 5.1 f i den allmänna dataskyddsförordningen och det faktum att dessa uppgifter skulle kunna lagras för andra ändamål kan behandlingen av dessa uppgifter för att underlätta ytterligare köp därför medföra en ökad risk för säkerhetsöverträdelser mot kreditkortsuppgifter. En annan viktig del av avvägningstestet som kan beaktas vid bedömningen av behandlingens inverkan på registrerade är de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige, sammanhanget och syftet med insamlingen av personuppgifterna[10]. Ändå verkar det som att de registrerade inte rimligen förväntar sig att deras kreditkortsuppgifter vid köptillfället ska lagras längre än vad som är nödvändigt för att betala för de köpta varorna eller tjänsterna, trots att de anger sina kreditkortsuppgifter för betalningen. I detta särskilda sammanhang skulle de grundläggande fri- och rättigheterna för de personer som dataskyddet avser därmed antagligen ha företräde framför den personuppgiftsansvariges intressen.

10. Dessa aspekter leder till slutsatsen att samtycke (artikel 6.1 a i den allmänna dataskyddsförordningen) verkar vara den enda lämpliga rättsliga grunden till att ovannämnda behandling ska vara laglig. För att hantera riskerna, låta den registrerade behålla kontrollen över sina egna uppgifter samt för att denne aktivt ska fatta beslut om användningen av hans/hennes kreditkortsuppgifter bör den registrerades specifika samtycke erhållas innan kreditkortsuppgifterna lagras efter ett köp. Detta samtycke gör det möjligt för den personuppgiftsansvarige att bevisa att individens vill underlätta sina ytterligare köp via den särskilda webbplatsen eller applikationen, vilket inte kan förutsättas baserat på att individen helt enkelt har genomfört ett eller flera enskilda transaktioner.

11. Detta samtycke kan inte förutsättas, och det måste vara frivilligt, specifikt, informerat och otvetydigt[11]. Det måste lämnas i form av en tydlig bekräftelse och bör begäras på ett användarvänligt sätt, såsom med hjälp av en ruta, som inte bör vara ikryssad på förhand[12], direkt i det formulär som används för att samla in uppgifterna. Detta specifika samtycke måste särskiljas

[7] Se EU-domstolens dom av den 24 november 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado, förenade målen C-468/10 och C-469/10, ECLI:EU:C:2011:777, punkterna 47 och 48, och EU-domstolens dom av den 19 oktober 2016, Patrick Breyer mot Bundesrepublik Deutschland, mål C-582/14, ECLI:EU:C:2016:779, punkt 62.

[8] Se EU-domstolens ovannämnda dom av den 24 november 2011, punkt 44, och EU-domstolens ovannämnda dom av den 11 december 2019, punkt 56.

[9] ARTIKEL 29-GRUPPENS riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679.

[10] Se skäl 47 i den allmänna dataskyddsförordningen.

[11] Se Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679.

[12] *Ibid*.

från det samtycke som ges för tjänste- eller försäljningsvillkoren och får inte utgöra ett villkor för att transaktionen ska genomföras.

12. Enligt artikel 7.3 i den allmänna dataskyddsförordningen ska de registrerade ha rätt att när som helst återkalla sitt samtycke till lagringen av kreditkortsuppgifterna för att underlätta ytterligare köp. Det måste vara gratis, lätt och lika enkelt för den registrerade att återkalla sitt samtycke som det var att ge det. Detta ska leda till att den personuppgiftsansvarige omedelbart raderar de kreditkortsuppgifter som har lagrats endast i syfte att underlätta ytterligare transaktioner.

På Europeiska dataskyddsstyrelsens vägnar

Ordförande

(Andrea Jelinek)