

Henstillinger



Henstilling 02/2021 om retsgrundlaget for opbevaring af kreditkortoplysninger med det ene formål at lette yderligere onlinetransaktioner

Vedtaget den 19. maj 2021

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

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (i det følgende benævnt "GDPR"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 til EØS-aftalen, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018, og

under henvisning til artikel 12 og artikel 22 i forretningsordenen —

VEDTAGET FØLGENDE HENSTILLING

1. I forbindelse med covid-19-pandemien har den digitale økonomi og e-handelen udviklet sig løbende. Det betyder samtidigt, at risikoen ved at bruge kreditkortoplysninger på nettet er steget. Som det fremgår af Artikel 29-Gruppens retningslinjer for konsekvensanalyser vedrørende databeskyttelse, påvirker misbrug af kreditkortoplysninger "*tydeligt den registreredes liv i alvorlig grad*", da finansielle oplysninger kan bruges til "*betalingssvindel*"¹.
2. Derfor er det meget vigtigt, at de dataansvarlige indfører passende garantier for de registrerede og sikrer dem kontrol over deres personoplysninger for at mindske risikoen for ulovlig behandling og skabe tillid til det digitale miljø. EDPB anser denne tillid for afgørende for den digitale økonomis bæredygtige vækst.
3. Derfor har denne henstilling til formål at tilskynde til en harmoniseret anvendelse af databeskyttelsesreglerne vedrørende behandling af kreditkortoplysninger inden for Det Europæiske Økonomiske Samarbejdsområde (EEA) og garantere en ensartet beskyttelse af den registreredes rettigheder med fuld efterlevelse af de grundlæggende beskyttelsesprincipper, der kræves i GDPR.
4. Mere specifikt vedrører denne henstilling den opbevaring af kreditkortoplysninger, der sker hos onlineudbydere af varer og tjenester, med det eneste og specifikke formål at lette de registreredes videre køb². Den omfatter situationen, hvor en registreret person køber et produkt eller betaler for en tjeneste via en hjemmeside eller en app, og indtaster sine kreditkortoplysninger, normalt i en dertil indrettet formular, for at foretage denne ene transaktion.
5. Som med enhver behandling skal den dataansvarlige i henhold til artikel 6 i GDPR have et gyldigt retsgrundlag for opbevaring af sådanne oplysninger. I den henseende skal det bemærkes, at en række af de retsgrundlag, der er nævnt i artikel 6 i GDPR, ikke ville være anvendelige i denne

¹ ARTIKEL 29-GRUPPEN VEDRØRENDE BESKYTTELSE AF PERSONOPLYSNINGER - Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen i henhold til forordning (EU) 2016/679 "sandsynligvis indebærer en høj risiko".

² Det skal bemærkes, at den ikke omfatter betalingsinstitutter, der opererer i onlinebutikker, eller offentlige myndigheder. Hverken opbevaring af kreditkortoplysninger til andre formål, for eksempel i forbindelse med overholdelse af en juridisk forpligtelse eller for at oprette en tilbagevendende betaling i tilfælde af kontrakt om fortsat levering af eller abonnement på en langsigtet tjeneste (f.eks. en kontrakt om månedlig levering af en bestemt vare eller abonnement på en musik- eller filmstreamingtjeneste).

situation og skal udelukkes. Opbevaring af kreditkortoplysninger efter en transaktion for at lette yderligere køb kan ikke betragtes som nødvendig for at overholde en retlig forpligtelse (artikel 6, stk. 1, litra c), i GDPR) eller for at beskytte en fysisk persons vitale interesser (artikel 6, stk. 1, litra d), i GDPR). Udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt (artikel 6, stk. 1, litra e), i GDPR), kan heller ikke betragtes som et passende retsgrundlag.

6. Derudover er opbevaring af kreditkortoplysninger efter betaling for varer eller tjenester som sådan ikke nødvendig for opfyldelse af en kontrakt (artikel 6, stk. 1, litra b), i GDPR). Hvor behandlingen af de oplysninger, der er relateret til det kreditkort, som kunden bruger til at betale med, i første omgang er nødvendig for at opfylde kontrakten, hvorved artikel 6, stk. 1, litra b), i GDPR udløses, har opbevaringen af disse data kun til formål at lette den potentielle næste transaktion og lette handelen. Et sådant formål kan ikke betragtes som strengt nødvendigt for opfyldelsen af kontrakten om levering af den vare eller tjeneste, som den registrerede allerede har betalt³.
7. Hvad angår behandling, der er nødvendig med henblik på den dataansvarliges eller en tredjeparts legitime interesse⁴, bemærker EDPB, at for at den dataansvarlige kan henholde sig til artikel 6, stk. 1, litra f), i GDPR, skal de tre betingelser, der er fastsat i denne artikel, være opfyldt⁵. Dette retsgrundlag kræver for det første identifikation og afgrænsning af en legitim interesse, der forfølges af den dataansvarlige eller af en tredjepart. Den dataansvarliges eller tredjepartens interesse kan være bredere end formålet med behandlingen og skal være til stede og gældende på datoen for databehandlingen⁶.
8. Retsgrundlaget for den legitime interesse kræver for det andet behovet for at behandle personoplysninger med henblik på den forfulgte legitime interesse. For så vidt angår denne sidste betingelse, er det ikke, forudsat at den dataansvarlige har en legitim interesse som beskrevet ovenfor, tydeligt, at opbevaring af kreditkortoplysninger for at lette fremtidige køb er nødvendig for at forfølge den legitime interesse. Faktisk afhænger den faktiske afslutning af et andet køb af forbrugers valg og afgøres ikke af muligheden for at gennemføre det "med et enkelt klik".
9. Endelig kræver den tredje betingelse udførelse af en afbalanceringstest: Den dataansvarliges eller tredjepartens legitime interesse skal afvejes mod den registreredes interesser eller grundlæggende rettigheder og friheder, herunder den registreredes rettigheder til databeskyttelse og privatlivets fred. Afbalanceringstesten kræver, at man tager hensyn til de særlige omstændigheder ved behandlingen⁷. En væsentlig del af afbalanceringsøvelsen er den

³ Se også EDPB's retningslinjer 2/2019 for behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i GDPR i forbindelse med leveringen af onlinetjenester til registrerede, særlig side 10.

⁴ Se Artikel 29-Gruppens udtalelse om begrebet dataansvarliges legitime interesse i henhold til artikel 7 i direktiv 95/46/EF, der i øjeblikket revideres af EDPB (se EDPB's arbejdsprogram 2021/2022 vedtaget den 16. marts 2021).

⁵ Se EU-Domstolens dom af 4. maj 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde mod Rīgas pašvaldības SIA 'Rīgas satiksme', sag C-13/16, ECLI:EU:C:2017:336, præmis 28.

⁶ Se Domstolens dom af 11. december 2019, TK mod Asociația de Proprietari bloc M5A-ScaraA, sag C-708/18, ECLI:EU:C:2019:1064, præmis 44.

⁷ Se Domstolens dom af 24. november 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEDM) mod Administración del Estado, sag C-468/10 og C-469/10, ECLI:EU:C:2011:777, præmis 47 og 48; Domstolens dom af 19. oktober 2016, Patrick Breyer mod Bundesrepublik Deutschland, sag C-582/14, ECLI:EU:C:2016:779, præmis 62.

potentielle indvirkning af behandlingen på den registreredes rettigheder og friheder⁸. En sådan indvirkning kan afhænge af oplysningernes art, den specifikke metode til behandling og tredjeparters adgang til sådanne oplysninger. Med hensyn til kriteriet for arten af oplysninger bør det bemærkes, at finansielle oplysninger er blevet afgrænset af Artikel 29-Gruppen som oplysninger af meget personlig karakter, fordi misbrug af dem klart indebærer alvorlige indvirkninger på den registreredes liv⁹. Uanset den dataansvarliges forpligtelse til at træffe tekniske og organisatoriske foranstaltninger for at sikre passende sikkerhed for kreditkortoplysningerne i henhold til artikel 5, stk. 1, litra f), i GDPR og det faktum, at disse oplysninger kan opbevares til andre formål, kan behandlingen af dem for at lette yderligere køb medføre en stigende risiko for brud på kreditkortoplysningssikkerheden, da det indebærer behandling i andre systemer. Et andet vigtigt element i afbalancerings testen, der kan tages i betragtning for at vurdere indvirkningen af behandlingen på registrerede, er de registreredes rimelige forventninger baseret på deres forhold til den dataansvarlige, sammenhængen og formålet med indsamling af personoplysninger¹⁰. Alligevel ser det ud til, at den registrerede på købstidspunktet, hvor kreditkortoplysningerne gives, ikke med rimelighed forventer, at hans eller hendes kreditkortoplysninger opbevares i længere tid, end hvad der er nødvendigt for at betale de varer eller tjenester, som han/hun køber. Derfor vil de grundlæggende rettigheder og friheder for den person, der er berørt af databeskyttelsen, sandsynligvis gå forud for den dataansvarliges interesse i denne specifikke sammenhæng.

10. Disse aspekter fører til den konklusion, at samtykke (artikel 6, stk. 1, litra a), i GDPR) synes at være det eneste passende retsgrundlag for, at den ovenfor beskrevne behandling kan være lovlig. For at imødegå sikkerhedsrisici, så den registrerede kan bevare kontrollen over sine data og aktivt tage beslutning om brugen af sine kreditkortoplysninger, skal den registreredes specifikke samtykke opnås inden opbevaring af vedkommendes kreditkortoplysninger efter et køb. Dette samtykke vil gøre det muligt for den dataansvarlige at godtgøre den enkeltes vilje til at lette sine videre køb på den specifikke hjemmeside eller app, hvilket ikke kan antages blot på grundlag af, at vedkommende afsluttede en eller flere enkeltransaktioner.
11. Dette samtykke kan ikke formodes, det skal være gratis, specifikt, oplyst og utvetydigt¹¹. Det skal gives i form af en tydeligt bekræftende handling, der skal kunne foretages på en brugervenlig måde, f.eks. ved et afkrydsningsfelt, der ikke bør være afkrydset på forhånd¹², og direkte på den formular, der bruges til indsamlingen af oplysninger. Det skal være muligt at skelne dette specifikke samtykke fra det samtykke, der gives til servicevilkår eller salg, og det må ikke være en betingelse for gennemførelsen af transaktionen.
12. I henhold til artikel 7, stk. 3, i GDPR har den registrerede til enhver tid ret til tilbagetrækning af sit samtykke til opbevaring af kreditkortoplysninger, der havde til formål at lette yderligere køb. Tilbagetrækningen skal være gratis, enkel og lige så let for den registrerede, som det var at give

⁸ Se Domstolens dom af 24. november 2011, jf. ovenfor, præmis 44; EU-Domstolens dom af 11. december 2019, jf. ovenfor, præmis 56.

⁹ ARTIKEL 29-GRUPPEN VEDRØRENDE BESKYTTELSE AF PERSONOPLYSNINGER - Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen i henhold til forordning (EU) 2016/679 "sandsynligvis indebærer en høj risiko".

¹⁰ Se betragtning 47 i GDPR.

¹¹ Se EDPB's retningslinje 05/2020 vedrørende samtykke i henhold til forordning (EF) nr. 2016/679.

¹² *Ibid.*

samtykket. Det skal føre til, at den dataansvarlige faktisk sletter de kreditkortoplysninger, der er gemt med det ene formål at lette yderligere transaktioner.

For Det Europæiske Databeskyttelsesråd

Formanden

(Andrea Jelinek)