

Doporučení



Doporučení 02/2021 k právnímu základu pro ukládání údajů z kreditních karet za výhradním účelem usnadnění dalších on-line transakcí

Přijato dne 19. května 2021

Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. e) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů“),

s ohledem na Dohodu o EHP a zejména přílohu XI a protokol 37 k uvedené dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018,

s ohledem na články 12 a 22 svého jednacího řádu,

PŘIJAL TATO DOPORUČENÍ:

1. V souvislosti s pandemií COVID-19 zaznamenaly digitální ekonomika a elektronický obchod pokračující rozvoj. Obdobně došlo i k nárůstu rizik používání údajů z kreditních karet na internetu. Jak uvedla pracovní skupina zřízená podle článku 29 ve svých pokynech pro posouzení vlivu na ochranu údajů, porušení zabezpečení údajů z kreditních karet „*má jednoznačně závažný vliv na každodenní život subjektu údajů*“, neboť finanční údaje lze použít k „*podvodům s platbami*“¹.
2. Je proto velmi důležité, aby správci zavedli vhodné záruky pro subjekty údajů a zajistili subjektům údajů kontrolu nad jejich osobními údaji s cílem snížit riziko protiprávního zpracování a posílit důvěru v digitální prostředí. Evropský sbor pro ochranu osobních údajů považuje tuto důvěru za naprosto zásadní pro udržitelný růst digitální ekonomiky.
3. Za tím účelem je cílem těchto doporučení povzbudit harmonizované uplatňování pravidel ochrany údajů, pokud jde o zpracování údajů z kreditních karet v rámci Evropského hospodářského prostoru (EHP), a zaručit jednotnou ochranu práv subjektu údajů při plném dodržování základních zásad ochrany údajů, jak je vyžaduje obecné nařízení o ochraně osobních údajů.
4. Konkrétně se tato doporučení zabývají ukládáním údajů z kreditních karet ze strany on-line dodavatelů zboží a poskytovatelů služeb, a to za výhradním a konkrétním účelem, kterým je usnadnit další nákupy subjektů údajů². Týkají se situace, kdy subjekt údajů nakupuje výrobek nebo platí za službu prostřednictvím internetových stránek nebo aplikace a za účelem uzavření takové jedinečné transakce poskytuje údaje ze své kreditní karty, obvykle pomocí zvláštního formuláře.
5. Stejně jako u jakéhokoli jiného zpracování musí mít správce pro ukládání těchto údajů platný právní základ podle článku 6 obecného nařízení o ochraně osobních údajů. V této souvislosti je třeba upozornit, že řada právních základů uvedených v článku 6 obecného nařízení o ochraně osobních údajů by na tuto situaci nebyla použitelná a musí být vyloučena. Ukládání údajů z kreditních karet

¹ PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29 – Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679.

² Je třeba upozornit, že doporučení se nevztahují na platební instituce působící v rámci internetových obchodů, ani na orgány veřejné moci. Nevztahují se ani na ukládání údajů z kreditních karet pro jakýkoli jiný účel, například za účelem splnění zákonné povinnosti nebo zadání opakované platby v případě smlouvy o pokračujícím plnění nebo předplatného dlouhodobé služby (např. smlouva, která stanoví dodávku určitého zboží každý měsíc, nebo předplatné hudební či filmové streamovací služby).

po transakci za účelem usnadnění dalších nákupů nelze považovat za nezbytné pro splnění právní povinnosti (čl. 6 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů), ani pro ochranu životně důležitého zájmu fyzické osoby (čl. 6 odst. 1 písm. d) obecného nařízení o ochraně osobních údajů). Za vhodný právní základ nelze považovat ani splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce (čl. 6 odst. 1 písm. e) obecného nařízení o ochraně osobních údajů).

6. Ukládání údajů z kreditních karet po provedení platby za zboží nebo služby není jako takové nezbytné pro splnění smlouvy (čl. 6 odst. 1 písm. b) obecného nařízení o ochraně osobních údajů). Zatímco zpracování údajů týkajících se kreditní karty, kterou zákazník používá k zaplacení, je v první řadě nezbytné pro splnění smlouvy, což aktivuje použití čl. 6 odst. 1 písm. b) obecného nařízení o ochraně osobních údajů, uložení těchto údajů je užitečné pouze k usnadnění případné další transakce a usnadnění prodeje. Takový účel nelze považovat za naprosto nezbytný pro splnění smlouvy o dodávce zboží nebo poskytnutí služeb, za které již subjekt údajů zaplatil³.
7. Pokud jde o zpracování nezbytné pro účely oprávněného zájmu správce nebo třetí strany⁴, Evropský sbor pro ochranu osobních údajů upozorňuje, že k tomu, aby se správce mohl opřít o čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, musí být splněny tři podmínky stanovené v uvedeném článku⁵. Tento právní základ vyžaduje, za prvé, určení a kvalifikaci oprávněného zájmu správce nebo třetí strany. Zájem správce nebo třetí strany může být širší než účel zpracování a tento zájem musí existovat a být účinný ke dni zpracování údajů⁶.
8. Za druhé, právní základ spočívající v oprávněném zájmu vyžaduje nezbytnost zpracování osobních údajů pro účely oprávněného zájmu. Pokud jde o tuto druhou podmínku, má-li správce oprávněný zájem, jak je uvedeno výše, není zřejmé, že ukládání údajů z kreditních karet k usnadnění budoucích nákupů je pro sledování tohoto oprávněného zájmu nezbytné. Vlastní uzavření jiného nákupu totiž závisí na volbě spotřebitele a není určováno možností uskutečnit je „jedním kliknutím“.
9. A konečně třetí podmínka vyžaduje provedení testu vyváženosti: oprávněný zájem správce nebo třetí strany musí být v rovnováze se zájmy nebo základními právy a svobodami subjektu údajů, včetně práv subjektu údajů na ochranu údajů a soukromí. Test vyváženosti vyžaduje zohlednění konkrétních okolností daného zpracování⁷. Nezbytným prvkem vyvažování je možný vliv na práva

³ Viz také EDPB, Pokyny 2/2019 o zpracovávání osobních údajů podle čl. 6 odst. 1 písm. b) nařízení GDPR v souvislosti s poskytováním on-line služeb subjektům údajů, konkrétně s. 10.

⁴ Viz stanovisko pracovní skupiny zřízené podle článku 29 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/, na jehož revizi v současné době Evropský sbor pro ochranu osobních údajů pracuje (viz pracovní program EDPB na období 2021/2022 přijatý dne 16. března 2021).

⁵ Viz rozsudek SDEU ze dne 4. května 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme“, věc C-13/16, ECLI:EU:C:2017:336, bod 28.

⁶ Viz rozsudek SDEU ze dne 11. prosince 2019, TK v. Asociația de Proprietari bloc M5A-ScaraA, věc C-708/18, ECLI:EU:C:2019:1064, bod 44.

⁷ Viz rozsudek SDEU ze dne 24. listopadu 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEDM) v. Administración del Estado, věci C-468/10 a C-469/10, ECLI:EU:C:2011:777, body 47 a 48; rozsudek SDEU ze dne 19. října 2016, Patrick Breyer v. Bundesrepublik Deutschland, věc C-582/14, ECLI:EU:C:2016:779, bod 62.

a svobody subjektu údajů vyplývající ze zpracování⁸. Tento vliv může záviset na povaze údajů, konkrétní metodě zpracování a na přístupu třetích stran k těmto údajům. Pokud jde o povahu kritéria týkajícího se údajů, je třeba upozornit, že pracovní skupina zřízená podle článku 29 vyhodnotila finanční údaje jako údaje vysoce osobní povahy, neboť porušení jejich zabezpečení má jednoznačně závažný vliv na každodenní život subjektu údajů⁹. Bez ohledu na povinnost správce zavést technická a organizační opatření k zajištění náležitého zabezpečení údajů z kreditních karet podle čl. 5 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů a na skutečnost, že tyto údaje mohou být ukládány pro jiné účely, může být jejich zpracování za účelem usnadnění dalších nákupů spojeno se zvýšeným rizikem porušení zabezpečení údajů z kreditních karet, neboť znamená zpracování v jiných systémech. Dalším důležitým prvkem testu vyváženosti, který by mohl být zohledněn při posuzování vlivu zpracování na subjekty údajů, jsou přiměřená očekávání subjektů údajů na základě jejich vztahu se správcem údajů, okolností a účelu shromažďování osobních údajů¹⁰. Zdá se však, že při poskytování údajů z kreditní karty pro platbu subjekt údajů v okamžiku nákupu přiměřeně neočekává, že jeho údaje z kreditní karty budou ukládány po dobu delší, než je nezbytné k úhradě za zboží nebo služby, které subjekt údajů nakupuje. V důsledku toho by základní práva a svobody osoby dotčené z hlediska ochrany údajů za těchto konkrétních okolností pravděpodobně převažovaly nad zájmem správce.

10. Uvedené aspekty vedou k závěru, že jediným vhodným právním základem pro zákonnost výše uvedeného zpracování je patrně udělení souhlasu (čl. 6 odst. 1 písm. a) obecného nařízení o ochraně osobních údajů). Aby byla řešena bezpečnostní rizika, aby si subjekt údajů mohl ponechat kontrolu nad svými údaji a aby se mohl aktivně rozhodovat o použití svých údajů z kreditní karty, měl by být před uložením jeho údajů z kreditní karty po nákupu skutečně získán konkrétní souhlas subjektu údajů. Tento souhlas umožní správci prokázat ochotu dané osoby usnadnit si další nákupy prostřednictvím konkrétní internetové stránky nebo aplikace, kterou nelze předpokládat na základě pouhé skutečnosti, že daná osoba uzavřela jednu nebo více jednotlivých transakcí.
11. Tento souhlas nesmí být předpokládán, musí být svobodný, konkrétní, informovaný a jednoznačný¹¹. Musí být poskytnut zjevným potvrzením a měl by být vyžádán uživatelsky vstřícným způsobem, například prostřednictvím zaškrtačacího políčka, které by nemělo být předem zaškrtnuto¹², a to přímo na formuláři používaném pro shromažďování údajů. Tento konkrétní souhlas musí být odlišen od souhlasu uděleného k podmínkám služby nebo prodeje a nesmí být podmínkou uskutečnění transakce.
12. Podle čl. 7 odst. 3 obecného nařízení o ochraně osobních údajů má subjekt údajů právo svůj souhlas s uložením údajů z kreditních karet za účelem usnadnění dalších nákupů kdykoli odvolat. Odvolání souhlasu musí být pro subjekt údajů bezplatné a stejně snadné, jako bylo jeho poskytnutí.

⁸ Viz výše uvedený rozsudek SDEU ze dne 24. listopadu 2011, bod 44; výše uvedený rozsudek SDEU ze dne 11. prosince 2019, bod 56.

⁹ PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29 – Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679.

¹⁰ Viz 47. bod odůvodnění obecného nařízení o ochraně osobních údajů.

¹¹ Viz EDPB, Pokyny č. 05/2020 k souhlasu podle nařízení 2016/679.

¹² *Tamtéž*.

Musí vést k tomu, že správce údaje z kreditních karet uložené za výhradním účelem usnadnění dalších nákupů účinně vymaže.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)