Pokyny 06/2020 týkající se vzájemného působení druhé směrnice o platebních službách a GDPR

Verze 2.0

Přijato dne 15. prosince 2020

Historie verzí

Verze 2.0	15. 12. 2020	Přijetí pokynů po veřejné konzultaci
Verze 1.0	17. 7. 2020	Přijetí pokynů pro veřejnou konzultaci

Obsah

Evropský sbor pro ochranu osobních údajů (EDPB)

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 „GDPR“),

s ohledem na Dohodu o EHP, a zejména na přílohu XI této dohody a protokol 37 k této dohodě, ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[1],

s ohledem na články 12 a 22 svého jednacího řádu,

vzhledem k těmto důvodům:

(1) Obecné nařízení o ochraně osobních údajů stanoví ucelený soubor pravidel pro zpracování osobních údajů v celé EU.

(2) Druhá směrnice o platebních službách (směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 23. prosince 2015, dále jen „směrnice PSD2“) ruší směrnici 2007/64/ES a stanoví nová pravidla pro zajištění právní jistoty spotřebitelů, obchodníků a společností v rámci platebního řetězce a modernizace právního rámce pro trh platebních služeb[2]. Členské státy měly směrnici PSD2 provést ve svém vnitrostátním právu do 13. ledna 2018.

(3) Důležitým prvkem směrnice PSD2 je zavedení právního rámce pro nové služby iniciování platby a služby informování o účtu. Směrnice PSD2 umožňuje poskytovatelům těchto nových platebních služeb získat přístup k platebním účtům subjektů údajů pro účely poskytování uvedených služeb.

(4) Pokud jde o ochranu údajů, podle čl. 94 odst. 1 směrnice PSD2 musí veškeré zpracování osobních údajů, včetně poskytování informací o tomto zpracování, pro účely směrnice PSD2 probíhat v souladu s GDPR[3] a nařízením (EU) 2018/1725.

(5) V 89. bodě odůvodnění směrnice PSD2 se uvádí, že dochází-li ke zpracování osobních údajů pro účely směrnice PSD2, měl by být stanoven přesný účel, uveden příslušný právní základ a měly by být dodržovány příslušné požadavky na bezpečnost stanovené v GDPR a současně by měly být respektovány zásady nutnosti, proporcionality, účelového omezení a přiměřené doby uchovávání údajů. Součástí všech systémů zpracovávání osobních údajů, které jsou v rámci směrnice PSD2 vytvořeny a používány, by měla být rovněž ochrana údajů již od návrhu a standardní nastavení ochrany údajů[4].

(6) V 93. bodě odůvodnění směrnice PSD2 se uvádí, že poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu na jedné straně a poskytovatel platebních služeb, který vede účet, na straně druhé by měli dodržovat nezbytné požadavky na ochranu údajů a bezpečnostní požadavky stanovené nebo uvedené v této směrnici nebo obsažené v návrzích regulačních technických norem.

[1] Odkazy na „členské státy“ v celém tomto dokumentu je třeba chápat jako odkazy na „členské státy EHP“.
[2] 6. bod odůvodnění směrnice PSD2.
[3] Jelikož směrnice PSD2 předchází GDPR, odkazuje ještě na směrnici 95/46. V článku 94 GDPR se stanoví, že odkazy na zrušenou směrnici 95/46 se považují za odkazy na GDPR.
[4] 89. bod odůvodnění směrnice PSD2.

PŘIJAL TYTO POKYNY:

1. ÚVOD

1. Druhá směrnice o platebních službách (dále jen „směrnice PSD2“) přinesla řadu novinek v oblasti platebních služeb. Ačkoli směrnice PSD2 vytváří nové příležitosti pro spotřebitele a zvyšuje transparentnost v této oblasti, její provádění vyvolává i určité otázky a obavy ohledně nutnosti zachování plné kontroly subjektů údajů nad svými osobními údaji. Obecné nařízení o ochraně osobních údajů (dále jen „GDPR“) se vztahuje na zpracování osobních údajů včetně činností zpracování prováděných v souvislosti s platebními službami, jak je definováno ve směrnici PSD2[5]. Proto musí správci údajů jednající v oblasti, na kterou se směrnice PSD2 vztahuje, vždy zajistit soulad s požadavky GDPR, včetně zásad ochrany údajů stanovených v článku 5 GDPR, i příslušnými ustanoveními směrnice o soukromí a elektronických komunikacích[6]. Vzhledem k tomu, že směrnice PSD2[7] a regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace (dále jen „regulační technické normy“[8]) obsahují určitá ustanovení týkající se ochrany a zabezpečení údajů, vyvstala nejistota ohledně výkladu těchto ustanovení i vzájemného působení obecného rámce ochrany údajů a směrnice PSD2.

2. Dne 5. července 2018 vydal EDPB dopis týkající se směrnice PSD2, ve kterém poskytl vysvětlení k otázkám ochrany osobních údajů z hlediska směrnice PSD2, zejména pokud jde o zpracování osobních údajů nesmluvních stran (tzv. „údajů tichých stran“) poskytovateli služeb informování o účtu a poskytovateli služeb iniciování platby, postupy týkající se udělení a odvolání souhlasu, regulační technické normy a spolupráci mezi poskytovateli platebních služeb, kteří vedou účet, ve vztahu k bezpečnostním opatřením. Aby bylo možné určit nejnaléhavější problémy, bylo součástí přípravných prací na těchto pokynech shromáždění podnětů zúčastněných stran, a to jak podnětů písemných, tak podnětů získaných na akci zúčastněných stran.

3. Cílem těchto pokynů je poskytnout další vodítka týkající se různých aspektů ochrany údajů z hlediska směrnice PSD2, zejména pokud jde o vztah mezi příslušnými ustanoveními nařízení GDPR a směrnice PSD2. Hlavní pozornost je v těchto pokynech věnována zpracování osobních údajů ze strany poskytovatelů služeb informování o účtu a poskytovatelů služeb iniciování platby. Proto se tento dokument zaměřuje na podmínky udělování přístupu k informacím o platebním účtu ze strany poskytovatelů platebních služeb, kteří vedou účet, a zpracování osobních údajů ze strany poskytovatelů služeb iniciování platby a poskytovatelů služeb informování o účtu, včetně požadavků a záruk v souvislosti se zpracováním osobních údajů ze strany poskytovatelů služeb iniciování platby a poskytovatelů služeb informování o účtu pro jiné účely, než jsou původní účely, pro které byly údaje shromážděny, zejména pokud byly shromážděny v souvislosti s poskytováním

[5] Ustanovení čl. 1 odst. 1 GDPR.
[6] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).
[7] Článek 94 směrnice o platebních službách atd.
[8] Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace (Text s významem pro EHP), C/2017/7782 (Úř. věst. L 69, 13.3.2018, s. 23), dostupné na https://eur-lex.europa.eu/legal-content/cs/TXT/PDF/?uri=CELEX:32018R0389&from=cs

služby informování o účtu[9]. Tento dokument také pojednává o různém pojetí výslovného souhlasu podle směrnice PSD2 a GDPR, o zpracování „údajů tichých stran“, o zpracování zvláštních kategorií osobních údajů ze strany poskytovatelů služeb iniciování platby a poskytovatelů služeb informování o účtu, o uplatňování hlavních zásad ochrany údajů stanovených v GDPR, včetně minimalizace údajů, transparentnosti, odpovědnosti a bezpečnostních opatření. Součástí směrnice PSD2 je také interdisciplinární odpovědnost, mimo jiné v oblastech ochrany spotřebitele a práva hospodářské soutěže. Úvahy týkající se těchto oblastí práva přesahují rámec těchto pokynů.

4. K usnadnění čtení těchto pokynů jsou níže uvedeny hlavní definice použité v tomto dokumentu.

1.1 Definice

„Poskytovatelem služeb informování o účtu“ se rozumí poskytovatel služby on-line, jejímž cílem je poskytnout konsolidované informace o jednom nebo více platebních účtech uživatele platebních služeb vedených buď u jiného poskytovatele platebních služeb, nebo u více než jednoho poskytovatele platebních služeb;

„poskytovatelem platebních služeb, který vede účet“ se rozumí poskytovatel platebních služeb, který pro plátce poskytuje a vede platební účty;

„minimalizace údajů“ je zásada ochrany osobních údajů, podle které musí být osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány;

„plátcem“ se rozumí fyzická nebo právnická osoba, která je majitelem platebního účtu a umožní platební příkaz z tohoto platebního účtu, nebo v případě neexistence platebního účtu plátce fyzická nebo právnická osoba, která dá platební příkaz;

„příjemcem“ se rozumí fyzická nebo právnická osoba, která je zamýšleným příjemcem peněžních prostředků, jež jsou předmětem platební transakce;

„platebním účtem“ se rozumí účet vedený na jméno jednoho nebo více uživatelů platebních služeb, který je využíván k provádění platebních transakcí;

„poskytovatelem služeb iniciování platby“ se rozumí poskytovatel služby iniciování platebního příkazu na žádost uživatele platebních služeb ve vztahu k platebnímu účtu vedenému u jiného poskytovatele platebních služeb;

„poskytovatelem platebních služeb“ se rozumí subjekt uvedený v čl. 1 odst. 1 směrnice PSD2[10] nebo fyzická či právnická osoba, na níž se vztahují výjimky podle článků 32 nebo 33 směrnice PSD2;

---

[9] Služba informování o účtu je služba on-line, jejímž cílem je poskytnout konsolidované informace o jednom nebo více platebních účtech uživatele platebních služeb vedených buď u jiného poskytovatele platebních služeb, nebo u více než jednoho poskytovatele platebních služeb.

[10] Ustanovení čl. 1 odst. 1 směrnice PSD2 uvádí, že směrnice PSD2 stanoví pravidla, podle nichž členské státy rozlišují tyto kategorie *poskytovatelů platebních služeb*:
a) úvěrové instituce ve smyslu čl. 4 odst. 1 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 575/2013, včetně jejich poboček ve smyslu bodu 17 uvedeného článku, pokud se tyto pobočky nacházejí v Unii, bez ohledu na to, zda se jedná o pobočky úvěrových institucí se sídlem v Unii, nebo o pobočky úvěrových institucí se sídlem mimo Unii podle článku 47 směrnice 2013/36/EU a vnitrostátních právních předpisů;
b) instituce elektronických peněz ve smyslu čl. 2 bodu 1 směrnice 2009/110/ES, včetně jejich poboček podle článku 8 uvedené směrnice a vnitrostátních právních předpisů, pokud se takové pobočky nacházejí v Unii a jejich sídlo se nachází mimo Unii, a v případě, že platební služby poskytované těmito pobočkami jsou spojeny s vydáváním elektronických peněz;

„uživatelem platebních služeb“ se rozumí fyzická nebo právnická osoba, která využívá platební službu jakožto plátce, příjemce, nebo obojí;

„osobními údaji“ se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelná fyzická osoba je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

„záměrnou ochranou osobních údajů“ se rozumí technická a organizační opatření začleněná do určitého produktu nebo služby, jejichž účelem je účinným způsobem provádět zásady ochrany údajů a začlenit do jejich zpracování nezbytné záruky tak, aby byly splněny požadavky GDPR a aby byla chráněna práva subjektů údajů;

„standardní ochranou osobních údajů“ se rozumí vhodná technická a organizační opatření zavedená u produktu nebo služby k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné;

„regulačními technickými normami“ se rozumí regulační technické normy ve smyslu nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace;

„poskytovateli z řad třetích stran“ se rozumí jak poskytovatelé služeb iniciování platby, tak poskytovatelé služeb informování o účtu.

1.2 Služby poskytované ve smyslu směrnice PSD2

5. Směrnice PSD2 zavádí dva nové druhy (poskytovatelů) platebních služeb: poskytovatele služeb iniciování platby a poskytovatele služeb informování o účtu. V příloze 1 směrnice PSD2 je uvedeno osm platebních služeb, které směrnice PSD2 upravuje.

6. Poskytovatelé služeb iniciování platby poskytují služby k iniciování platebních příkazů na žádost uživatele platebních služeb ve vztahu k platebnímu účtu uživatele vedenému u jiného poskytovatele platebních služeb[11]. Poskytovatel služeb iniciování platby může požádat poskytovatele platebních služeb, který vede účet (obvykle banku), aby inicioval transakci jménem uživatele platebních služeb. Uživatelem (platebních služeb) může být fyzická osoba (subjekt údajů) nebo právnická osoba.

7. Poskytovatelé služeb informování o účtu poskytují služby on-line, jejichž cílem je poskytnout konsolidované informace o jednom nebo více platebních účtech uživatele platebních služeb vedených buď u jiného poskytovatele platebních služeb, nebo u více než jednoho poskytovatele platebních služeb[12]. Podle 28. bodu odůvodnění směrnice PSD2 má uživatel platebních služeb možnost získat v kterémkoli daném okamžiku celkový přehled o své okamžité finanční situaci.

c) poštovní žirové instituce, jež jsou v souladu s vnitrostátními právními předpisy oprávněny poskytovat platební služby;
d) platební instituce;
e) ECB a národní centrální banky, pokud nejednají jako měnový orgán nebo jako jiné veřejné orgány;
f) členské státy a jejich regionální a místní orgány, pokud nejednají jako veřejné orgány.

[11] Ustanovení čl. 4 odst. 15 směrnice PSD2.

[12] Ustanovení čl. 4 odst. 16 směrnice PSD2.

8. Pokud jde o služby informování o účtu, může být nabízeno několik odlišných typů služeb s důrazem na různé prvky a účely. Někteří poskytovatelé mohou například uživatelům nabízet služby, jako je plánování rozpočtu a sledování výdajů. Zpracování osobních údajů v souvislosti s těmito službami upravuje směrnice PSD2. Služby, které zahrnují posuzování úvěruschopnosti uživatele platebních služeb nebo auditorské služby prováděné na základě shromažďování informací prostřednictvím služby informování o účtu, směrnice PSD2 neupravuje, a proto spadají do oblasti působnosti GDPR. Směrnice PSD2 se navíc nevztahuje ani na jiné účty než platební (např. spořicí, investiční). Platným právním rámcem pro zpracování osobních údajů je v každém případě GDPR.

Příklad 1:

HappyPayments je společnost, která nabízí službu on-line, která spočívá v poskytování informací o jednom nebo více platebních účtech prostřednictvím mobilní aplikace s cílem podat finanční přehled (služba informování o účtu). Díky této službě může uživatel platebních služeb okamžitě zjistit zůstatky a nedávné transakce na dvou nebo více platebních účtech v různých bankách. Tato služba také nabízí možnost, pokud se tak uživatel platebních služeb rozhodne, třídění výdajů a příjmů podle různých kritérií (plat, volný čas, energie, hypotéka atd.), čímž uživateli platebních služeb pomáhá s finančním plánováním. V rámci této aplikace nabízí společnost HappyPayments také službu iniciování plateb přímo z platebního účtu určeného (platebních účtů určených) uživateli (služba iniciování platby).

9. Aby bylo možné tyto služby poskytovat, reguluje směrnice PSD2 právní podmínky, za kterých mohou poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu získat přístup k platebním účtům, aby mohli uživateli platebních služeb poskytovat služby.

10. V čl. 66 odst. 1 a čl. 67 odst. 1 směrnice PSD2 se stanoví, že uživatel má právo na přístup k platebním službám a službám informování o účtu a jejich využívání. To znamená, že uživatel platebních služeb by měl mít při uplatnění tohoto práva naprostou volnost a neměl by být k jeho využití nucen.

11. Přístup k platebním účtům a používání informací o platebním účtu částečně upravují články 66 a 67 směrnice PSD2, ve kterých jsou uvedeny záruky týkajíce se ochrany (osobních) údajů. V čl. 66 odst. 3 písm. f) směrnice PSD2 se stanoví, že poskytovatel služeb iniciování platby nesmí od uživatele platebních služeb vyžadovat žádné jiné údaje než ty, které jsou nezbytné k poskytnutí služby iniciování platby, a v čl. 66 odst. 3 písm. g) směrnice PSD2 se uvádí, že poskytovatel služeb iniciování platby nesmí používat a uchovávat žádné údaje a využívat přístupu k nim pro jiné účely než k poskytnutí služby iniciování platby podle výslovné žádosti plátce. Dále čl. 67 odst. 2 písm. d) směrnice PSD2 omezuje přístup poskytovatele služeb informování o účtu pouze k informacím z určených platebních účtů a souvisejícím platebním transakcím, zatímco čl. 67 odst. 2 písm. f) směrnice PSD2 stanoví, že poskytovatelé služeb informování o účtu nesmějí používat a uchovávat žádné údaje a využívat přístupu k nim pro jiné účely než k poskytnutí služby informování o účtu podle výslovné žádosti uživatele platebních služeb v souladu s pravidly pro ochranu údajů. Ta zdůrazňují, že v rámci služeb informování o účtu mohou být osobní údaje shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely. Poskytovatel služeb informování o účtu by proto měl ve smlouvě výslovně uvést, pro jaké konkrétní účely budou osobní údaje o účtu v souvislosti s poskytovanou službou informování o účtu zpracovávány. Podle článku 5 GDPR by smlouva měla být zákonná, korektní a transparentní a také v souladu s dalšími zákony na ochranu spotřebitele.

12. V závislosti na konkrétních okolnostech mohou být poskytovatelé platebních služeb podle GDPR buď správci, nebo zpracovateli. V těchto pokynech se „správci“ rozumí takoví poskytovatelé platebních služeb, kteří sami nebo společně s ostatními stanovují účely a prostředky zpracování

osobních údajů. Bližší objasnění této problematiky se nachází v pokynech EDPB 07/2020 týkajících se pojmů správce a zpracovatel v GDPR.

2 ZÁKONNÉ DŮVODY A DALŠÍ ZPRACOVÁNÍ PODLE SMĚRNICE PSD2

2.1 Zákonné důvody pro zpracování

13. Podle GDPR musí mít správci pro zpracování osobních údajů právní základ. Ustanovení čl. 6 odst. 1 GDPR představuje taxativní a omezující výčet šesti právních základů pro zpracování osobních údajů podle GDPR[13] Za stanovení vhodného právního základu a zajištění toho, aby byly všechny podmínky tohoto právního základu splněny, odpovídá správce. Určení příslušného a pro konkrétní situaci nejvhodnějšího základu závisí na okolnostech, za kterých zpracování probíhá, mimo jiné na účelu zpracování a vztahu mezi správcem a subjektem údajů.

2.2 Ustanovení čl. 6 odst. 1 písm. b) GDPR (zpracování je nezbytné pro splnění smlouvy)

14. Platební služby jsou poskytovány na základě smlouvy mezi uživatelem platebních služeb a poskytovatelem platebních služeb. Jak je uvedeno v 87. bodě odůvodnění směrnice PSD2, *„[t]ato směrnice by se měla týkat pouze smluvních závazků a odpovědnosti mezi uživatelem platebních služeb a poskytovatelem platebních služeb“*. Podle GDPR je hlavním právním základem pro zpracování osobních údajů pro poskytování platebních služeb čl. 6 odst. 1 písm. b) GDPR, což znamená, že zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů.

15. Platební služby poskytované podle směrnice PSD2 jsou definovány v příloze 1 směrnice PSD2. Poskytování těchto služeb definovaných ve směrnici PSD2 je požadavkem pro uzavření smlouvy, ve které mají smluvní strany přístup k údajům o platebním účtu uživatele platebních služeb. Tito poskytovatelé platebních služeb musí být rovněž provozovateli s povolením. Pokud jde o služby iniciování platby a služby informování o účtu podle směrnice PSD2, mohou smlouvy obsahovat podmínky, které rovněž ukládají podmínky týkající se doplňkových služeb, jež směrnice PSD2 neupravuje. *Pokyny EDPB 2/2019 o zpracovávání osobních údajů podle čl. 6 odst. 1 písm. b) GDPR v souvislosti s poskytováním on-line služeb subjektům údajů* jasně stanoví, že správci musí posoudit, jaké zpracování osobních údajů je pro plnění smlouvy objektivně nezbytné. V těchto pokynech je zdůrazněno, že odůvodnění nezbytnosti závisí na povaze služby, na vzájemných perspektivách a očekáváních smluvních stran, na odůvodnění smlouvy a na podstatných náležitostech smlouvy.

[13] Podle článku 6 je zpracování osobních údajů zákonné pouze tehdy, pokud je splněna nejméně jedna z těchto podmínek:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

16. Pokyny EDPB 2/2019 rovněž objasňují, že na základě čl. 7 odst. 4 GDPR se rozlišuje mezi činnostmi zpracování nezbytnými pro plnění smlouvy a podmínkami, které službu podmiňují určitými činnostmi zpracování, jež ve skutečnosti nejsou pro plnění smlouvy nezbytné. „Nezbytné pro plnění“ nepochybně vyžaduje něco více než jen smluvní podmínku[14]. Správce by měl být schopen prokázat, proč není možné ve skutečnosti splnit hlavní předmět dané smlouvy se subjektem údajů, pokud nedojde k danému zpracování dotčených osobních údajů. Pouhý odkaz na zpracování údajů nebo zmínka o něm ve smlouvě nestačí k tomu, aby dotčené zpracování spadalo do působnosti čl. 6 odst. 1 písm. b) GDPR.

17. V čl. 5 odst. 1 písm. b) GDPR se stanoví zásada účelového omezení, která vyžaduje, že osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Při posuzování toho, zda je čl. 6 odst. 1 písm. b) vhodným právním základem pro on-line (platební) službu, je třeba zohlednit konkrétní cíl, účel nebo záměr této služby[15]. Účely zpracování musí být jasně určeny a sděleny subjektu údajů v souladu s povinnostmi správce údajů týkajícími se účelového omezení a transparentnosti. Posuzování toho, co je „nezbytné“, zahrnuje provedení kombinovaného, fakticky podloženého posouzení zpracování „pro dosažení sledovaného cíle a toho, zda toto zpracování představuje menší zásah do soukromí ve srovnání s jinými alternativami“. Ustanovení čl. 6 odst. 1 písm. b) se nevztahuje na zpracování, které je užitečné, ale není objektivně nezbytné pro poskytnutí smluvní služby nebo k provedení příslušných předsmluvních kroků na žádost subjektu údajů, i když je nezbytné pro další obchodní účely správce údajů[16].

18. Pokyny EDPB 2/2019 jasně stanoví, že ve smlouvách nelze uměle rozšiřovat kategorie osobních údajů nebo typy operací zpracování, které správce potřebuje provést za účelem plnění smlouvy ve smyslu čl. 6 odst. 1 písm. b)[17]. Tyto pokyny se také zabývají případy, v nichž by mohla pro subjekty údajů, jež mohou mít zájem pouze o jednu ze služeb, nastat situace „ber, nebo nech být“. Ta by mohla nastat, pokud by chtěl správce seskupit několik samostatných služeb nebo prvků služby s různými základními účely, vlastnostmi nebo odůvodněním do jedné smlouvy. Pokud smlouvu tvoří několik samostatných služeb nebo prvků služby, které lze ve skutečnosti v přiměřeném rozsahu provádět nezávisle na sobě, je třeba použitelnost uvedenou v čl. 6 odst. 1 písm. b) posoudit u každé z těchto služeb samostatně na základě toho, co je k provedení každé z těchto jednotlivých služeb, o něž subjekt údajů aktivně požádal nebo se k nim přihlásil, objektivně nutné[18].

19. V souladu s výše uvedenými pokyny musí správci posoudit, co je pro plnění smlouvy objektivně nezbytné. Pokud správci nemohou prokázat, že zpracování osobních údajů o platebním účtu je objektivně nezbytné pro poskytování každé z těchto služeb samostatně, není čl. 6 odst. 1 písm. b) GDPR platným právním důvodem pro jejich zpracování. V těchto případech by správce měl zvážit jiný právní základ pro zpracování.

2.3 Předcházení podvodům

20. V čl. 94 odst. 1 směrnice PSD2 se stanoví, že členské státy umožní zpracování osobních údajů platebními systémy a poskytovateli platebních služeb, je-li to nezbytné z důvodu předcházení

[14] Pokyny 2/2019 o zpracovávání osobních údajů podle čl. 6 odst. 1 písm. b) GDPR v souvislosti s poskytováním on-line služeb subjektům údajů, EDPB, strana 8.
[15] Tamtéž.
[16] Tamtéž, strana 7.
[17] Tamtéž, strana 10.
[18] Tamtéž, strana 11.

platebním podvodům, jejich vyšetřování a odhalování. Zpracování osobních údajů, které je nezbytně nutné pro účely předcházení podvodům, by mohlo představovat oprávněný zájem dotčeného poskytovatele platebních služeb za předpokladu, že nad těmito zájmy nepřevažují zájmy nebo základní práva a svobody subjektu údajů[19]. Činnosti zpracování pro účely předcházení podvodům by měly vycházet z pečlivého posouzení jednotlivých případů správcem v souladu se zásadou odpovědnosti. Kromě toho mohou správci za účelem předcházení podvodům podléhat také konkrétním právním povinnostem, které vyžadují zpracování osobních údajů.

2.4 Další zpracování (poskytovatelé služeb informování o účtu a poskytovatelé služeb iniciování platby)

21. V čl. 6 odst. 4 GDPR se stanoví podmínky pro zpracování osobních údajů pro jiný účel, než pro který byly osobní údaje shromážděny. Konkrétně může toto další zpracování proběhnout tehdy, je-li založeno na právu Unie nebo členského státu, které v demokratické společnosti představuje nutné a přiměřené opatření k zajištění cílů uvedených v čl. 23 odst. 1, pokud k němu subjekt údajů udělil souhlas nebo pokud je zpracování za jiným účelem než za účelem, pro který byly osobní údaje shromážděny, slučitelné s původním účelem.

22. Je třeba náležitě zohlednit čl. 66 odst. 3 písm. g) a čl. 67 odst. 2 písm. f) směrnice PSD2. Jak bylo uvedeno výše, čl. 66 odst. 3 písm. g) směrnice PSD2 stanoví, že poskytovatel služeb iniciování platby nesmí používat a uchovávat žádné údaje a využívat přístupu k nim pro jiné účely než k poskytnutí služby iniciování platby podle výslovné žádosti plátce. V čl. 67 odst. 2 písm. f) směrnice PSD2 stanoví, že poskytovatel služeb informování o účtu nesmí používat a uchovávat žádné údaje a využívat přístupu k nim pro jiné účely než k poskytnutí služby informování o účtu podle výslovné žádosti uživatele platebních služeb v souladu s pravidly pro ochranu údajů.

23. Ustanovení čl. 66 odst. 3 písm. g) a čl. 67 odst. 2 písm. f) směrnice PSD2 tedy možnosti zpracování pro jiné účely značně omezují, což znamená, že zpracování pro jiný účel není povoleno, pokud k němu subjekt údajů neudělil souhlas podle čl. 6 odst. 1 písm. a) GDPR nebo pokud toto zpracování neukládá právo Unie nebo právo členského státu, které se na správce údajů vztahuje podle čl. 6 odst. 4 GDPR. Není-li zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, založeno na souhlasu subjektu údajů nebo na právu Unie nebo členského státu, omezení uvedená v čl. 66 odst. 3 písm. g) a čl. 67 odst. 2 písm. f) směrnice PSD2 jasně stanoví, že žádný jiný účel není slučitelný s účelem, pro který byly osobní údaje původně shromážděny. Test slučitelnosti podle čl. 6 odst. 4 GDPR nemůže vést k vytvoření právního základu pro zpracování.

24. Ustanovení čl. 6 odst. 4 GDPR umožňuje další zpracování na základě práva Unie nebo členského státu. Například všichni poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu jsou povinnými osobami podle čl. 3 odst. 2 písm. a) směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení zneužití finančního systému k praní peněz nebo financování terorismu nebo směrnice o boji proti praní peněz. Tyto povinné osoby jsou tedy nuceny uplatňovat opatření hloubkové kontroly klienta, jak je stanoveno ve směrnici. Osobní údaje zpracovávané v souvislosti se službou směrnice PSD2 jsou proto dále zpracovávány na základě nejméně jedné právní povinnosti, kterou má poskytovatel služeb[20].

25. Jak je uvedeno v bodě 20, čl. 6 odst. 4 GDPR uvádí, že zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, může být založeno na souhlasu subjektu údajů, pokud jsou splněny

[19] 47. bod odůvodnění GDPR.
[20] Upozorňujeme, že důkladné posouzení otázky, zda je směrnice o boji proti praní peněz v souladu s čl. 6 odst. 4 GDPR, nespadá do rozsahu působnosti tohoto dokumentu.

všechny podmínky udělení souhlasu podle GDPR. Jak je stanoveno výše, správce musí prokázat, že souhlas lze odmítnout nebo odvolat, aniž by byl subjekt údajů poškozen (42. bod odůvodnění GDPR).

2.5 Právní základ pro udělení přístupu k účtu (poskytovatelé platebních služeb, kteří vedou účet)

26. Jak je uvedeno v bodě 10, mohou uživatelé platebních služeb uplatnit své právo na využití služeb iniciování platby a informování o účtu. S cílem zajistit účinné uplatňování práva uživatele platebních služeb na využití výše uvedených platebních služeb by měly být povinnosti uložené členským státům v čl. 66 odst. 1 a čl. 67 odst. 1 směrnice PSD2 provedeny ve vnitrostátním právu. Účinné uplatňování těchto práv by nebylo možné bez existence odpovídající povinnosti poskytovatele platebních služeb, který vede účet, obvykle banky, udělit poskytovateli platebních služeb přístup k účtu pod podmínkou, že splnil všechny požadavky pro získání přístupu k účtu uživatele platebních služeb. Ustanovení čl. 66 odst. 5 a čl. 67 odst. 4 směrnice PSD2 dále jednoznačně stanoví, že poskytování služeb iniciování platby a služeb informování o účtu nesmí být závislé na existenci smluvního vztahu mezi poskytovatelem služeb iniciování platby / poskytovatelem služeb informování o účtu a poskytovatelem platebních služeb, který vede účet.

27. Zpracování osobních údajů poskytovatelem platebních služeb, který vede účet, spočívající v udělení přístupu k osobním údajům požadovaným poskytovatelem služeb iniciování platby a poskytovatelem služeb informování o účtu za účelem poskytnutí jejich platební služby uživateli platebních služeb, je založeno na zákonné povinnosti. Za účelem splnění cílů směrnice PSD2 musí poskytovatelé platebních služeb, kteří vedou účet, poskytovat osobní údaje pro účely služeb poskytovatelů služeb iniciování platby a poskytovatelů služeb informování o účtu, což je nezbytnou podmínkou k tomu, aby mohli poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu poskytovat své služby a tím zajistit práva stanovená v čl. 66 odst. 1 a čl. 67 odst. 1 směrnice PSD2. Proto je v tomto případě platným právním důvodem ustanovení čl. 6 odst. 1 písm. c) GDPR.

28. Vzhledem k tomu, že GDPR uvádí, že zpracování založené na právní povinnosti by mělo být jasně stanoveno právem Unie nebo členského státu (viz čl. 6 odst. 3 GDPR), měla by povinnost poskytovatelů platebních služeb, kteří vedou účet, poskytnout přístup vyplývat z vnitrostátního práva, kterým se směrnice PSD2 provádí.

3 VÝSLOVNÝ SOUHLAS

3.1 Souhlas podle GDPR

29. Podle GDPR je souhlas jedním ze šesti právních důvodů pro zákonnost zpracování osobních údajů. Podle čl. 4 odst. 11 GDPR je souhlas definován jako „jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“. Tyto čtyři podmínky – svobodný, konkrétní, informovaný a jednoznačný – jsou pro platnost souhlasu zásadní. Podle pokynů EDPB 05/2020 k souhlasu podle nařízení 2016/679 může být souhlas vhodným právním základem pouze tehdy, je-li subjektu údajů nabídnuta kontrola a skutečná možnost volby, pokud jde o přijetí nebo odmítnutí nabízených podmínek, nebo o jejich odmítnutí, aniž by byl subjekt poškozen. Při žádosti o souhlas má správce povinnost posoudit, zda bude splňovat všechny požadavky pro získání platného souhlasu. Je-li souhlas získán v plném souladu s GDPR, je souhlas nástroj, který dává subjektům údajů kontrolu nad tím, zda budou osobní údaje, které se jich týkají, zpracovávány, či nikoli. Pokud tomu tak není, kontrola subjektu údajů je pouze zdánlivá a souhlas je neplatným právním základem pro zpracování, čímž se činnost zpracování stává protiprávní[21].

30. GDPR obsahuje další záruky také v článku 7, který stanoví, že správce údajů musí být schopen prokázat, že platný souhlas byl k dispozici v okamžiku zpracování. Žádost o souhlas musí být rovněž předložena způsobem, který je od jiných skutečností jasně odlišitelný a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Kromě toho musí být subjekt údajů informován o právu souhlas kdykoli odvolat stejně jednoduchým způsobem, jako tomu bylo při udělení souhlasu.

31. Podle článku 9 GDPR je souhlas jednou z výjimek z obecného zákazu zpracování zvláštních kategorií osobních údajů. V takovém případě však musí být souhlas subjektu údajů „výslovný“[22].

32. Podle pokynů EDPB 05/2020 k souhlasu podle nařízení 2016/679 označuje výslovný souhlas podle GDPR způsob, jakým je souhlas vyjádřen subjektem údajů. To znamená, že subjekt údajů by měl vyjádřit výslovné prohlášení o souhlasu pro konkrétní účel(y) zpracování. Nejjednodušším způsobem, jak zajistit, aby byl souhlas výslovný, by bylo výslovné potvrzení souhlasu v písemném prohlášení. Případně by správce mohl zajistit, aby subjekt údajů písemné prohlášení podepsal s cílem odstranit veškeré možné pochybnosti a předejít možnému nedostatku důkazů v budoucnu.

33. V žádném případě nelze souhlas odvozovat z potenciálně nejednoznačných prohlášení nebo jednání. Správce musí mít také na paměti, že souhlas nelze získat prostřednictvím stejného úkonu jako souhlas se smlouvou nebo přijetím všeobecných podmínek služby.

3.2 Souhlas podle směrnice PSD2

34. EDPB poznamenává, že právní rámec týkající se výslovného souhlasu je komplexní, protože pojem „výslovný souhlas“ je uveden jak ve směrnici PSD2, tak v GDPR. To vyvolává otázku, zda by měl být „výslovný souhlas“ uvedený v čl. 94 odst. 2 směrnice PSD2 vykládán stejným způsobem jako výslovný souhlas podle GDPR.

[21] Pokyny 05/2020 k souhlasu podle nařízení 2016/679, EDPB, bod 3.
[22] Viz také stanovisko č. 15/2011 k definici souhlasu (WP 187), s. 6–8, a/nebo stanovisko č. 06/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES (WP 217), s. 9, 10, 13 a 14.

3.2.1 Výslovný souhlas podle čl. 94 odst. 2 směrnice PSD2

35. Směrnice PSD2 obsahuje řadu zvláštních pravidel týkajících se zpracování osobních údajů, zejména v čl. 94 odst. 1 směrnice PSD2, který stanoví, že zpracování osobních údajů pro účely směrnice PSD2 musí být v souladu s právem EU v oblasti ochrany údajů. V čl. 94 odst. 2 směrnice PSD2 se dále stanoví, že poskytovatelé platebních služeb mohou zpracovávat a uchovávat pouze osobní údaje nezbytné pro poskytování svých platebních služeb a mít k nim přístup, a to s výslovným souhlasem uživatele platebních služeb. Podle čl. 33 odst. 2 směrnice PSD2 se tento požadavek výslovného souhlasu uživatele platebních služeb nevztahuje na poskytovatele platebních služeb informování o účtu. Výslovný souhlas s poskytováním služby poskytovateli služeb informování o účtu však i přesto stanoví čl. 67 odst. 2 písm. a) směrnice PSD2.

36. Jak bylo uvedeno výše, výčet právních základů pro zpracování údajů podle GDPR je taxativní. Jak bylo uvedeno v odstavci 14, právním základem pro zpracování osobních údajů pro poskytování platebních služeb je v zásadě čl. 6 odst. 1 písm. b) GDPR, což znamená, že zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů. Z toho vyplývá, že čl. 94 odst. 2 směrnice PSD2 nelze považovat za dodatečný právní základ pro zpracování osobních údajů. EDPB se domnívá, že s ohledem na výše uvedené by se měl tento bod vykládat jednak v souladu s platným právním rámcem pro ochranu údajů, jednak způsobem, kterým se zachová jeho užitečný účinek. Výslovný souhlas podle čl. 94 odst. 2 směrnice PSD2 by proto měl být považován za dodatečný požadavek smluvní povahy[23], pokud jde o přístup k osobním údajům a jejich následné zpracovávání a uchovávání za účelem poskytování platebních služeb, a není tedy stejný jako (výslovný) souhlas podle GDPR.

37. „Výslovný souhlas“ uvedený v čl. 94 odst. 2 směrnice PSD2 je smluvní souhlas. To znamená, že čl. 94 odst. 2 směrnice PSD2 by měl být vykládán tak, že při uzavírání smlouvy s poskytovatelem platebních služeb podle směrnice PSD2 musí být subjekty údajů plně informovány o konkrétních kategoriích osobních údajů, které budou zpracovávány. Dále musí být informovány o konkrétním účelu (platební služby), pro který budou jejich osobní údaje zpracovávány, a musí s těmito ustanoveními výslovně souhlasit. Tato ustanovení by měla být jasně odlišitelná od ostatních záležitostí, které jsou předmětem smlouvy, a subjekt údajů s nimi musí výslovně souhlasit.

38. Základem pojmu „výslovný souhlas“ podle čl. 94 odst. 2 směrnice PSD2 je získání přístupu k osobním údajům za účelem následného zpracování a uchovávání těchto údajů pro účely poskytování platebních služeb. To znamená, že poskytovatel platebních služeb[24] osobní údaje dosud nezpracovává, ale potřebuje získat přístup k osobním údajům, které byly zpracovávány v odpovědnosti jiného správce. Pokud uživatel platebních služeb uzavře smlouvu například s poskytovatelem služeb iniciování platby, musí tento poskytovatel získat přístup k osobním údajům tohoto uživatele platebních služeb, za jejichž zpracování odpovídá poskytovatel platebních služeb, který vede účet. Předmětem výslovného souhlasu podle čl. 94 odst. 2 směrnice PSD2 je povolení k získání přístupu k uvedeným osobním údajům, aby bylo možné tyto osobní údaje, které jsou nezbytné pro účely poskytování platební služby, zpracovávat a uchovávat. Pokud subjekt údajů udělí výslovný souhlas, je poskytovatel platebních služeb, který vede účet, povinen poskytnout k uvedeným osobním údajům přístup.

[23] Dopis EDPB týkající se směrnice PSD2, 5. července 2018, strana 4.
[24] To se týká služeb 1 až 7 v příloze 1 směrnice PSD2.

39. Přestože souhlas podle čl. 94 odst. 2 směrnice PSD2 není právním důvodem pro zpracování osobních údajů, týká se tento souhlas konkrétně osobních údajů a ochrany údajů a pro uživatele platebních služeb zajišťuje transparentnost a určitou míru kontroly[25]. Přestože směrnice PSD2 nespecifikuje věcné podmínky pro udělení souhlasu podle čl. 94 odst. 2 směrnice PSD2, je třeba ji chápat, jak je uvedeno výše, v souladu s platným právním rámcem pro ochranu údajů a způsobem, který zachová jeho užitečný účinek.

40. Pokud jde o informace, které mají správci poskytnout, a požadavek transparentnosti, v pokynech k transparentnosti pracovní skupiny zřízené podle článku 29 se uvádí, že *„základní úvaha stojící za zásadou transparentnosti popsanou v těchto ustanoveních je taková, že subjekt údajů by měl být schopen předem rozpoznat rozsah a důsledky zpracování a neměl by být následně zaskočen tím, jak jsou jeho osobní údaje používány“*[26].

41. Osobní údaje musí být navíc shromažďovány, jak vyžaduje zásada účelového omezení, pro určité, výslovně vyjádřené a legitimní účely (čl. 5 odst. 1 písm. b) GDPR). Jsou-li osobní údaje shromažďovány pro více než jeden účel, *„měli by se správci vyhnout tomu, aby pro odůvodnění různých činností dalšího zpracování stanovili pouze jeden široce pojatý účel, který se skutečným původním účelem fakticky souvisí pouze vzdáleně“*[27]. EDPB poukazuje, naposledy v souvislosti se smlouvami o poskytování on-line služeb, na riziko zahrnutí všeobecných podmínek zpracování do smlouvy a uvádí, že účel shromažďování údajů by měl být jasně a konkrétně uveden: měl by být dostatečně podrobný, aby určoval, jaký druh zpracování spadá a jaký nespadá pod stanovený účel, a aby bylo možné posoudit dodržení právních předpisů a uplatnit záruky ochrany údajů[28].

42. Při posouzení v souvislosti s dodatečným požadavkem výslovného souhlasu podle čl. 94 odst. 2 směrnice PSD2 to znamená, že správci musí subjektům údajů poskytnout přesné a jasné informace o konkrétních účelech určených správcem, pro které lze jejich osobní údaje zpracovávat, uchovávat a mít k nim přístup. V souladu s čl. 94 odst. 2 směrnice PSD2 musí subjekty údajů tyto konkrétní účely výslovně přijmout.

43. Jak je navíc uvedeno výše v bodě 10, poukazuje EDPB na to, že uživatel platebních služeb musí mít možnost se rozhodnout, zda službu využije, nebo nikoli, a nesmí k tomu být nucen. Proto musí být souhlas podle čl. 94 odst. 2 směrnice PSD2 také souhlasem svobodným.

3.3 Závěr

44. Výslovný souhlas podle směrnice PSD2 se liší od (výslovného) souhlasu podle GDPR. Výslovný souhlas podle čl. 94 odst. 2 směrnice PSD2 je dodatečným požadavkem smluvní povahy. Pokud poskytovatel platebních služeb potřebuje pro účely poskytování platebních služeb přístup k osobním údajům, je nutný výslovný souhlas uživatele platebních služeb podle čl. 94 odst. 2 směrnice PSD2.

[25] Ustanovení čl. 94 odst. 2 směrnice PSD2 spadá pod kapitolu 4 „Ochrana údajů“.
[26] Pracovní skupina zřízená podle článku 29, Pokyny k transparentnosti podle nařízení 2016/679, bod 10 (přijaté dne 11. dubna 2018) – schválené EDPB.
[27] Stanovisko č. 03/2013 pracovní skupiny zřízené podle článku 29 o účelovém omezení (WP203), strana 16.
[28] Pokyny 2/2019 o zpracovávání osobních údajů podle čl. 6 odst. 1 písm. b) GDPR v souvislosti s poskytováním on-line služeb subjektům údajů, bod 16 (verze pro veřejnou konzultaci) a Stanovisko č. 03/2013 pracovní skupiny zřízené podle článku 29 o účelovém omezení (WP203), strany 15–16.

4 ZPRACOVÁNÍ ÚDAJŮ TICHÉ STRANY

4.1 Údaje tiché strany

45. Problémem ochrany údajů, který je třeba pečlivě zvážit, je zpracování tzv. „údajů tiché strany“. Pro účely tohoto dokumentu se údaji tiché strany rozumí osobní údaje týkající se subjektu údajů, který není uživatelem konkrétního poskytovatele platebních služeb, ale jehož osobní údaje uvedený konkrétní poskytovatel platebních služeb zpracovává za účelem plnění smlouvy mezi poskytovatelem a uživatelem platebních služeb. Jedná se například o případ, kdy uživatel platebních služeb, subjekt údajů A, využije služeb poskytovatele služeb informování o účtu a subjekt údajů B provede řadu platebních transakcí ve prospěch platebního účtu subjektu údajů A. V tomto případě se subjekt údajů B považuje za „tichou stranu“ a osobní údaje (jako je číslo účtu subjektu údajů B a peněžní částka, která s těmito transakcemi souvisela) týkající se subjektu údajů B se považují za „údaje tiché strany“.

4.2 Oprávněný zájem správce

46. Ustanovení čl. 5 odst. 1 písm. b) GDPR vyžaduje, aby byly osobní údaje shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely a aby nebyly dále zpracovávány způsobem, který je s těmito účely neslučitelný. GDPR dále stanoví, že veškeré zpracování osobních údajů musí být jednak nezbytné, jednak přiměřené a v souladu se zásadami ochrany údajů, jako jsou zásady účelového omezení a minimalizace údajů.

47. GDPR umožňuje zpracování údajů tiché strany, pokud je takové zpracování nezbytné pro účely oprávněných zájmů správce nebo třetí strany (čl. 6 odst. 1 písm. f) GDPR). K takovému zpracování však může dojít jen tehdy, pokud před oprávněným zájmem správce nemají „přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů“.

48. Právním základem pro zpracování údajů tiché strany poskytovateli služeb iniciování platby a poskytovateli služeb informování o účtu – v souvislosti s poskytováním platebních služeb podle směrnice PSD2 – by tedy mohl být oprávněný zájem správce údajů nebo třetí strany na plnění smlouvy s uživatelem platebních služeb. Nutnost zpracování osobních údajů tiché strany je omezená a určuje se na základě rozumných očekávání těchto subjektů údajů. V souvislosti s poskytováním platebních služeb, na něž se vztahuje směrnice PSD2, je třeba zavést účinná a vhodná opatření, která zaručí, že nebudou potlačeny zájmy nebo základní práva a svobody tichých stran a že budou respektována rozumná očekávání těchto subjektů údajů týkající se zpracování jejich osobních údajů. V tomto ohledu musí správce (poskytovatel služeb informování o účtu nebo poskytovatel služeb iniciování platby) zavést nezbytné záruky pro zpracování za účelem ochrany práv subjektů údajů. To znamená i technická opatření k zajištění toho, aby údaje tiché strany nebyly zpracovávány pro jiný účel, než pro jaký byly tyto osobní údaje poskytovateli služeb iniciování platby a poskytovateli služeb informování o účtu původně shromážděny. Je-li to možné, je třeba pro dosažení odpovídající úrovně zabezpečení a minimalizace údajů použít také šifrování nebo jiné techniky.

4.3 Další zpracování osobních údajů tiché strany

49. Jak je uvedeno v odstavci 29, mohou být osobní údaje zpracovávané v souvislosti s platební službou, kterou upravuje směrnice PSD2, dále zpracovávány na základě zákonných povinností, které se vztahují na poskytovatele služeb. Tyto zákonné povinnosti se mohou týkat i osobních údajů tiché strany.

50. Pokud jde o další zpracování údajů tiché strany na základě oprávněného zájmu, EDPB je toho názoru, že tyto údaje nelze použít pro jiný účel, než pro který byly tyto osobní údaje shromážděny, nebo pro účel stanovený podle práva EU nebo členského státu. Získání souhlasu tiché strany není z právního hlediska možné, protože pro získání souhlasu by bylo nutné osobní údaje tiché strany shromažďovat nebo zpracovávat, k čemuž však podle článku 6 GDPR nelze nalézt žádný právní důvod. Ani test slučitelnosti podle článku čl. 6 odst. 4 GDPR neposkytuje důvod pro zpracování pro jiné účely (např. činnosti přímého marketingu). Pokud nový správce údajů použije osobní údaje subjektů údajů tiché strany pro jiné účely, nebudou respektována práva a svobody těchto subjektů údajů vzhledem k souvislostem, v nichž byly tyto osobní údaje shromážděny, zejména vzhledem k neexistenci jakéhokoli vztahu se subjekty údajů, které jsou tichými stranami[29]; vzhledem k neexistenci jakékoli souvislosti mezi jiným účelem a účelem, pro který byly tyto osobní údaje původně shromážděny (tj. skutečnost, že poskytovatelé platebních služeb potřebují údaje tiché strany pouze pro plnění smlouvy s druhou smluvní stranou); vzhledem k povaze dotčených osobních údajů[30], vzhledem k okolnosti, že subjekty údajů nemohou důvodně očekávat žádné další zpracování nebo si být dokonce vědomi toho, který správce může jejich osobní údaje zpracovávat, a vzhledem k zákonným omezením zpracování stanoveným v čl. 66 odst. 3 písm. g) a čl. 67 odst. 2 písm. f) směrnice PSD2.

[29] 87. bod odůvodnění směrnice PSD2 uvádí, že směrnice PSD2 se vztahuje pouze na „smluvní závazky a odpovědnosti mezi uživatelem platebních služeb a poskytovatelem platebních služeb“. Údaje tiché strany proto do oblasti působnosti směrnice PSD2 nespadají.

[30] Zvláštní pozornost je třeba věnovat zpracování finančních osobních údajů, protože jejich zpracování lze podle pokynů pro posouzení vlivu na ochranu osobních údajů považovat za zvýšení možného rizika pro práva a svobody osob.

5 ZPRACOVÁVÁNÍ ZVLÁŠTNÍCH KATEGORIÍ OSOBNÍCH ÚDAJŮ PODLE SMĚRNICE PSD2

5.1 Zvláštní kategorie osobních údajů

51. Ustanovení čl. 9 odst. 1 GDPR zakazuje zpracování „osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby“.

52. Je třeba zdůraznit, že v některých členských státech jsou elektronické platby již obecně rozšířené a mnoho lidí jim při každodenních transakcích dává přednost před hotovostí. Finanční transakce mohou zároveň odhalit citlivé informace o konkrétním subjektu údajů, mimo jiné informace týkající se zvláštních kategorií osobních údajů. Například z darů politickým stranám nebo organizacím, církvím nebo farnostem by v závislosti na podrobnostech transakce mohly být odhaleny politické názory a náboženské vyznání. Odečtením ročního členského příspěvku z bankovního účtu by mohlo být odhaleno členství dané osoby v odborech. Analýzou účtů za zdravotní péči, které subjekt údajů uhradil zdravotníkovi (například psychiatrovi), by mohly být získány osobní údaje o zdravotním stavu. A konečně informace o některých nákupech mohou odhalit informace týkající se sexuálního života nebo sexuální orientace dané osoby. Jak dokládají tyto příklady, mohou i jednotlivé transakce obsahovat zvláštní kategorie osobních údajů. Služby informování o účtu by navíc mohly vycházet z profilování, jak je definováno v čl. 4 odst. 4 GDPR. Jak již bylo uvedeno v Pokynech k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 pracovní skupiny zřízené podle článku 29, schválených EDPB, „profilování může vytvořit zvláštní kategorie údajů prostřednictvím dedukce z údajů, které nejsou samy o sobě zvláštními kategoriemi údajů, ale stávají se jimi, když se zkombinují s jinými údaji“[31]. To znamená, že prostřednictvím souhrnu finančních transakcí lze odhalit různé druhy vzorců chování, ke kterým mohou patřit i zvláštní kategorie osobních údajů. Proto je velká pravděpodobnost, že poskytovatel služeb, který zpracovává informace o finančních transakcích subjektů údajů, zpracovává také zvláštní kategorie osobních údajů.

53. Pokud jde o pojem „citlivé údaje o platbách“, uvádí EDPB následující skutečnosti. Definice pojmu citlivé údaje o platbách ve směrnici PSD2 se značně liší od způsobu, jakým se běžně používá pojem „citlivé osobní údaje“ v souvislosti s GDPR a ochranou údajů (právními předpisy v dané oblasti). Zatímco směrnice PSD2 definuje „citlivé údaje o platbách“ jako „údaje, včetně osobních bezpečnostních údajů, které by mohly být použity k podvodu“, GDPR zdůrazňuje potřebu specifické ochrany zvláštních kategorií osobních údajů, které jsou podle článku 9 GDPR svou povahou zvláště citlivé, pokud jde o vztah k základním právům a svobodám, jako jsou zvláštní kategorie osobních údajů[32]. Proto se doporučuje přinejmenším zmapovat a přesně kategorizovat, jaký druh osobních údajů bude zpracováván. S největší pravděpodobností bude nutné provést posouzení vlivu na ochranu osobních údajů v souladu s článkem 35 GDPR, což při tomto mapování pomůže. Bližší informace o posouzení vlivu na ochranu osobních údajů se nacházejí v Pokynech pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů

[31] Pracovní skupina zřízená podle článku 29, Pokyny k automatizovanému individuálnímu rozhodování a profilování
pro účely nařízení 2016/679, WP251 rev. 01, strana 15.

[32] Například v 10. bodě odůvodnění GDPR jsou zvláštní kategorie osobních údajů označovány jako „citlivé údaje“.

bude mít za následek vysoké riziko“ pro účely nařízení 2016/679 pracovní skupiny zřízené podle článku 29, schválených EDPB.

5.2 Možné výjimky

54. Zákaz uvedený v článku 9 GDPR není absolutní. Zejména vzhledem k tomu, že výjimky uvedené v čl. 9 odst. 2 písm. b) až f) a h) až j) GDPR zjevně nelze použít na zpracování osobních údajů v kontextu směrnice PSD2, lze zvážit následující dvě výjimky v čl. 9 odst. 2 GDPR:

a) Zákaz se nepoužije, pokud subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů (čl. 9 odst. 2 písm. a) GDPR).

b) Zákaz se nepoužije, je-li zpracování nezbytné z důvodů významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů (čl. 9 odst. 2 písm. g) GDPR).

55. Je třeba zdůraznit, že seznam výjimek v čl. 9 odst. 2 GDPR je taxativní. Poskytovatel služeb musí vzít na vědomí možnost, že do osobních údajů zpracovávaných za účelem poskytování jakékoli služby, na kterou se vztahuje směrnice PSD2, jsou zahrnuty zvláštní kategorie osobních údajů. Vzhledem k tomu, že pro tyto poskytovatele služeb se použije zákaz uvedený v čl. 9 odst. 1 GDPR, musí tito poskytovatelé zajistit, aby se na ně vztahovala některá z výjimek podle čl. 9 odst. 2 GDPR. Je třeba zdůraznit, že pokud poskytovatel služeb nemůže prokázat, že je některá z výjimek splněna, použije se zákaz podle čl. 9 odst. 1.

5.3 Významný veřejný zájem

56. V rámci platebních služeb mohou být zpracovávány zvláštní kategorie osobních údajů z důvodů významného veřejného zájmu, ale pouze tehdy, jsou-li splněny všechny podmínky čl. 9 odst. 2 písm. g) GDPR. To znamená, že zpracování zvláštních kategorií osobních údajů musí být v právu Unie nebo členského státu řešeno zvláštní výjimkou z čl. 9 odst. 1 GDPR. Toto ustanovení bude muset zohledňovat přiměřenost ve vztahu ke sledovanému cíli zpracování a obsahovat vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů. Toto ustanovení podle práva Unie nebo členského státu bude navíc muset dodržovat podstatu práva na ochranu údajů. A konečně bude muset být prokázáno, že zpracování zvláštních kategorií údajů je nezbytné z důvodu významného veřejného zájmu, včetně zájmů systémového významu. Pouze tehdy, jsou-li všechny tyto podmínky zcela splněny, může se u daných druhů platebních služeb použít tato výjimka.

5.4 Výslovný souhlas

57. V případech, kdy se výjimka z čl. 9 odst. 2 písm. g) GDPR neuplatní, je pravděpodobně jedinou možnou zákonnou výjimkou pro zpracování zvláštních kategorií osobních údajů ze strany poskytovatelů z řad třetích stran získání výslovného souhlasu v souladu s podmínkami pro platný souhlas uvedenými v GDPR. V Pokynech EDPB 05/2020 k souhlasu podle nařízení 2016/679 je uvedeno,[33] že: „ustanovení čl. 9 odst. 2 neuznává „nezbytnost pro plnění smlouvy“ jako výjimku z obecného zákazu zpracování zvláštních kategorií údajů. Správci a členské státy, které se s touto situací setkají, by proto měly prozkoumat zvláštní výjimky uvedené v čl. 9 odst. 2 písm. b) až j).“ Pokud poskytovatelé služeb vycházejí z čl. 9 odst. 2 písm. a) GDPR, musí před zahájením zpracování

[33] Pokyny 05/2020 k souhlasu podle nařízení 2016/679, EDPB, bod 99.

zajistit, aby jim byl udělen výslovný souhlas. Výslovný souhlas, jak je stanovený v čl. 9 odst. 2 písm. a) GDPR, musí splňovat všechny požadavky GDPR.

5.5 Žádná vhodná výjimka

58. Jak bylo uvedeno výše, pokud poskytovatel služeb nemůže prokázat, že je splněna některá z výjimek, použije se zákaz podle čl. 9 odst. 1. V tom případě lze zavést technická opatření, která by zabránila zpracování zvláštních kategorií osobních údajů, například tím, že by zabránila zpracování určitých datových bodů. V tomto ohledu mohou poskytovatelé platebních služeb prozkoumat technické možnosti vyloučení zvláštních kategorií osobních údajů a umožnění selektivního přístupu, který by zabránil zpracování zvláštních kategorií osobních údajů souvisejících s tichými stranami poskytovateli z řad třetích stran.

6 MINIMALIZACE ÚDAJŮ, ZABEZPEČENÍ, TRANSPARENTNOST, ODPOVĚDNOST A PROFILOVÁNÍ

6.1 Minimalizace údajů a záměrná a standardní ochrana osobních údajů

59. Zásada minimalizace údajů je zakotvena v čl. 5 odst. 1 písm. c) GDPR: „Osobní údaje musí být […] přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány“. Podle zásady minimalizace údajů by správci v podstatě neměli zpracovávat více osobních údajů, než je pro dosažení daného konkrétního účelu nezbytné. Jak je uvedeno v kapitole 2, množství a druh osobních údajů, které jsou nezbytné k poskytování platební služby, jsou dány objektivním a vzájemně srozumitelným smluvním účelem[34]. Zásada minimalizace údajů platí pro každé zpracování (např. každé shromáždění osobních údajů nebo přístup k nim a žádost o osobní údaje). Pokyny EDPB 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů uvádějí, že „zpracovatelé a poskytovatelé technologií jsou také považováni za klíčové faktory záměrné a standardní ochrany osobních údajů a měli by si být rovněž vědomi toho, že správci údajů musí osobní údaje zpracovávat pouze pomocí systémů a technologií s integrovanou ochranou údajů[35]“.

60. Článek 25 GDPR stanoví povinnosti uplatňovat záměrnou a standardní ochranu osobních údajů. Tyto povinnosti jsou zvlášť důležité v případě zásady minimalizace údajů. Tento článek stanoví, že správci zavedou jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jejichž účelem je provádět zásady ochrany údajů účinným způsobem a začlenit do zpracování nezbytné záruky, aby splnili požadavky GDPR a ochránili práva subjektů údajů. Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. K těmto opatřením mohou patřit šifrování, pseudonymizace a další technická opatření.

61. Při uplatnění povinnosti podle článku 25 GDPR je třeba zohlednit aspekty, jako je stav techniky, náklady na zavedení a povaha, rozsah, kontext a účely zpracování, jakož i různě pravděpodobná a různě závažná rizika pro práva a svobody fyzických osob, jež sebou zpracování nese. Bližší vysvětlení týkající se této povinnosti je poskytnuto ve výše uvedených Pokynech EDPB 4/2019 týkajících se článku 25 Záměrná a standardní ochrana osobních údajů.

6.2 Opatření k minimalizaci údajů

62. Poskytovatelé z řad třetích stran, kteří mají přístup k údajům o platebním účtu za účelem poskytování požadovaných služeb, musí rovněž zohledňovat zásadu minimalizace údajů a musí shromažďovat pouze osobní údaje nezbytné k poskytování konkrétních platebních služeb požadovaných uživatelem platebních služeb. Přístup k osobním údajům by měl být v zásadě omezen na údaje, které jsou nezbytné pro poskytování platebních služeb. Jak bylo uvedeno v kapitole 2, vyžaduje směrnice PSD2, aby poskytovatelé platebních služeb, kteří vedou účet, na žádost uživatele platebních služeb sdělili informace o uživateli platebních služeb, pokud si uživatel platebních služeb přeje použít službu iniciování platby nebo službu informování o účtu.

[34] Pokyny 2/2019 o zpracovávání osobních údajů podle čl. 6 odst. 1 písm. b) GDPR v souvislosti s poskytováním on-line služeb subjektům údajů, EDPB, bod 32.
[35] Pokyny 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, strana 29.

63. Pokud nejsou pro plnění smlouvy nezbytné všechny údaje o platebním účtu, měl by poskytovatel služeb informování o účtu před shromážděním údajů vybrat relevantní kategorie údajů. Ke kategoriím údajů, které nemusí být nezbytné, mohou patřit totožnost tiché strany a charakteristiky transakce. Stejně tak nemusí být nezbytné zobrazovat IBAN bankovního účtu tiché strany, ledaže to vyžadují právní předpisy členského státu nebo EU.

64. V této souvislosti by se mohlo zvážit případné uplatnění technických opatření, která by poskytovatelům z řad třetích stran umožňovala přístup pouze k takovým osobním údajům a jejich vyhledávání, jež jsou nezbytné pro poskytování jejich služeb, nebo by je v této jejich povinnosti podporovala, a to v rámci provádění vhodných politik na ochranu údajů v souladu s čl. 24 odst. 2 GDPR. EDPB v tomto ohledu doporučuje používání digitálních nástrojů na podporu poskytovatelů služeb informování o účtu v jejich povinnosti shromažďovat pouze osobní údaje, které jsou pro účely, pro které jsou zpracovávány, nezbytné. Pokud například poskytovatel služeb nepotřebuje pro poskytování svých služeb charakteristiky transakce (v poli popisu záznamů transakcí), mohl by jako prostředek poskytovatelů z řad třetích stran pro vyloučení tohoto pole z operací celkového zpracování prováděných poskytovateli platebních služeb z řad třetích stran fungovat nástroj pro digitální výběr.

Příklad 2:

Společnost HappyPayments, náš poskytovatel služeb informování o účtu z příkladu 1, si přeje zajistit, aby zpracovával pouze osobní údaje o platebním účtu, o které mají jeho uživatelé zájem. Získání přístupu k dalším údajům o platebním účtu by pro poskytování služby nebylo nezbytné. Umožní tedy uživatelům zvolit si konkrétní typy informací, o které mají zájem.

Uživatel A požaduje přehled svých výdajů za poslední dva měsíce. Proto si ke svým dvěma bankovním účtům vedeným u dvou různých poskytovatelů platebních služeb, kteří vedou účet, vyžádá informace o všech transakcích za poslední dva měsíce, částku transakce, datum provedení a jméno příjemce a zaškrtne odpovídající políčka v uživatelském rozhraní na stránkách společnosti HappyPayments.

Společnost HappyPayments si pak od příslušných poskytovatelů platebních služeb, kteří vedou účet, vyžádá pouze informace odpovídající polím nastaveným uživatelem A a pouze za dobu posledních dvou měsíců. Informace jako „oznámení“ o převodu nebo dokonce IBAN požadovány nejsou, protože uživatel A o tyto informace nepožádal.

Aby poskytovatelé platebních služeb, kteří vedou účet, umožnili společnosti HappyPayments splnit její povinnosti týkající se minimalizace údajů, umožňují jí vyžádat si informace v konkrétních polích pro vymezené časové období.

65. V této souvislosti je třeba také poznamenat, že podle směrnice PSD2 mají poskytovatelé platebních služeb, kteří vedou účet, povoleno poskytovat přístup pouze k informacím o platebním účtu. V rámci směrnice PSD2 neexistuje žádný právní základ pro poskytování přístupu k osobním údajům obsaženým v jiných účtech, jako jsou spořicí, hypoteční nebo investiční účty. Proto je podle směrnice PSD2 nutné zavést technická opatření, která zajistí, aby byl přístup omezen na nezbytné informace o platebním účtu.

66. Kromě toho, že má poskytovatel služeb shromažďovat co nejméně údajů, musí zavést také omezení doby uchovávání. Poskytovatel služeb nesmí osobní údaje uchovávat po dobu delší, než je nezbytné pro účely požadované uživatelem platebních služeb.

67. Pokud smlouva mezi subjektem údajů a poskytovatelem služeb informování o účtu vyžaduje předání osobních údajů třetím stranám, mohou být předány pouze ty osobní údaje, které jsou

nezbytné pro plnění smlouvy. Subjekty údajů by měly být o předání i o osobních údajích, které budou této třetí straně předány, rovněž konkrétně informovány.

6.3 Bezpečnost

68. EDPB již poukázal na to, že porušení ochrany finančních osobních údajů *„má jednoznačně závažný vliv na každodenní život subjektu údajů*“, a jako příklad uvedl rizika podvodu s platbami[36].

69. Pokud se porušení bezpečnosti údajů týká finančních údajů, může být subjekt údajů vystaven značným rizikům. V závislosti na tom, jaké informace uniknou, mohou být subjekty údajů vystaveny riziku krádeže identity, krádeže finančních prostředků na svém účtu i krádeže dalších aktiv. Navíc může expozice údajů o transakcích souviset se značnými riziky narušení soukromí, protože údaje o transakcích mohou obsahovat odkazy na všechny aspekty soukromého života subjektu údajů. Zároveň jsou finanční údaje samozřejmě cenné pro zločince a jsou pro ně tedy i atraktivním cílem.

70. Poskytovatelé platebních služeb jsou jako správci povinni zavést přiměřená opatření na ochranu osobních údajů subjektů údajů (čl. 24 odst. 1 GDPR). Čím vyšší jsou rizika spojená s činností zpracování prováděnou správcem, tím vyšší bezpečnostní normy je třeba uplatňovat. Vzhledem k tomu, že zpracování finančních údajů je spojeno s řadou závažných rizik, měla by tomu odpovídat výše úrovně bezpečnostních opatření.

71. Poskytovatelé služeb by měli dodržovat vysoké standardy, včetně mechanismů silného ověření klienta a vysokých bezpečnostních standardů pro technické vybavení[37]. Důležité jsou i další postupy, jako je prověřování zpracovatelů z hlediska bezpečnostních norem a zavádění postupů proti neoprávněnému přístupu.

6.4 Transparentnost a odpovědnost

72. Transparentnost a odpovědnost jsou dvě základní zásady GDPR.

73. Pokud jde o transparentnost (čl. 5 odst. 1 písm. a) GDPR), článek 12 GDPR stanoví, že správci musí přijmout vhodná opatření k poskytnutí veškerých informací uvedených v článcích 13 a 14 GDPR. Dále vyžaduje, aby informace nebo sdělení o zpracování osobních údajů byly stručné, transparentní, srozumitelné a snadno přístupné. Informace musí být sdělovány pomocí jasných a jednoduchých jazykových prostředků, a to písemně „nebo jinými prostředky, včetně ve vhodných případech v elektronické formě“. Pokyny k transparentnosti podle nařízení 2016/679 pracovní skupiny zřízené podle článku 29, schválené EDPB, uvádějí konkrétní doporučení pro dodržování zásady transparentnosti v digitálním prostředí.

74. Podle výše uvedených pokynů k transparentnosti podle nařízení 2016/679 by měl být článek 11 GDPR vykládán jako způsob prosazování skutečné minimalizace údajů, aniž by byl omezen výkon práv subjektu údajů, a výkon práv subjektu údajů by měl být umožněn pomocí dodatečných informací poskytnutých subjektem údajů. Mohou nastat situace, ve kterých správce údajů zpracovává informace způsobem, který nevyžaduje identifikaci subjektu údajů (například pseudonymizované údaje). V takových případech může být relevantní také čl. 11 odst. 1, který stanoví, že správce nemá povinnost uchovávat, získávat nebo zpracovávat dodatečné informace za účelem identifikace subjektu údajů výlučně kvůli dosažení souladu s obecným nařízením o ochraně osobních údajů.

---

[36] 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 pracovní skupiny zřízené podle článku 29, WP248 rev. 01 – schválené EDPB.

[37] Viz regulační technické normy.

75. V případě služeb podle směrnice PSD2 se na osobní údaje shromážděné od subjektu údajů použijí ustanovení článku 13 GDPR a na osobní údaje, které nebyly získány od subjektu údajů, ustanovení článku 14.

76. Subjekt údajů musí být zejména informován o době, po kterou budou osobní údaje uchovávány, nebo není-li ji možné určit, o kritériích použitých pro stanovení této doby a případně o oprávněných zájmech, které správce nebo případná třetí strana sledují. Pokud je zpracování založeno na souhlasu podle čl. 6 odst. 1 písm. a) GDPR nebo na výslovném souhlasu podle čl. 9 odst. 2 písm. a) GDPR, musí být subjekt údajů informován o tom, že má právo souhlas kdykoli odvolat.

77. Správce poskytne subjektu údajů informace s ohledem na zvláštní okolnosti, za nichž jsou osobní údaje zpracovávány. Mají-li být osobní údaje použity pro komunikaci se subjektem údajů[38], což bude pravděpodobně případ poskytovatelů služeb informování o účtu, musí být tato informace poskytnuta nejpozději v době první komunikace s tímto subjektem údajů. Mají-li být osobní údaje sděleny jinému příjemci, musí být tato informace sdělena nejpozději při prvním sdělení osobních údajů.

78. Pokud jde o on-line platební služby, výše uvedené pokyny uvádějí, že rozhodnou-li se správci údajů použít k zajištění transparentnosti kombinaci metod, mohou uplatňovat víceúrovňový přístup. Zejména se doporučuje používat víceúrovňová prohlášení/oznámení o ochraně soukromí k propojení s různými kategoriemi informací, jež musí být subjektu údajů poskytnuty, spíše než zobrazovat všechny tyto informace v jediném oznámení na obrazovce, aby nedošlo k únavě z informací a aby byla zároveň zajištěna účinnost těchto informací.

79. Ve výše uvedených pokynech je rovněž vysvětleno, že správci se mohou rozhodnout použít k poskytnutí informací jednotlivým subjektům údajů i další nástroje, například přehledy o ochraně soukromí. Přehled o ochraně soukromí (dashboard) je jedno místo, kde si subjekty údajů mohou prohlížet „informace o ochraně soukromí“ a spravovat své preference v této oblasti tím, že umožní použití svých údajů dotčeným správcem konkrétním způsobem, či toto použití zablokují[39]. Přehled o ochraně soukromí může poskytovat přehled o poskytovatelích z řad třetích stran, kteří získali výslovný souhlas subjektů údajů, a může také poskytovat relevantní informace o povaze a množství osobních údajů, k nimž měli poskytovatelé platebních služeb z řad třetích stran přístup. Poskytovatel platebních služeb, který vede účet, může prostřednictvím tohoto přehledu uživateli v zásadě nabídnout možnost odvolat konkrétní výslovný souhlas podle směrnice PSD2,[40] což by vedlo k zamítnutí přístupu k jeho platebním účtům pro jednoho nebo více poskytovatelů z řad třetích stran. Uživatel by také mohl požádat poskytovatele platebních služeb, který vede účet, aby odepřel přístup k jeho platebním účtům jednomu nebo více konkrétním poskytovatelům z řad třetích stran[41], protože uživatel má právo službu informování o účtu (ne)používat. Používají-li se

[38] Ustanovení čl. 14 odst. 3 písm. b) GDPR.

[39] Podle Pokynů k transparentnosti podle nařízení 2016/679 pracovní skupiny zřízené podle článku 29, schválených EDPB, jsou přehledy o ochraně soukromí užitečné zejména v případě, kdy subjekty údajů používají stejnou službu na mnoha různých zařízeních, protože jim poskytují přístup k jejich osobním údajům a kontrolu nad nimi bez ohledu na to, jak službu využívají. Mohou-li subjekty údajů ručně nastavit ochranu soukromí prostřednictvím uvedeného přehledu, zjednoduší se tak i personalizace prohlášení/oznámení o ochraně soukromí, protože pak jsou v něm uvedeny pouze druhy zpracování, které probíhají v souvislosti s daným subjektem údajů.

[40] Viz například „výslovný souhlas“ uvedený v čl. 67 odst. 2 písm. a) směrnice PSD2.

[41] Viz také EBA/OP/2020/10, bod 45.

k udělení nebo odebrání výslovného souhlasu přehledy o ochraně soukromí, měly by být vytvořeny a používány v souladu se zákonem a zejména by měly bránit vytváření překážek k právu poskytovatelů z řad třetích stran poskytovat služby v souladu se směrnicí PSD2. V této souvislosti a v souladu s platnými ustanoveními směrnice PSD2 má poskytovatel z řad třetích stran možnost získat výslovný souhlas uživatele znovu poté, co byl tento souhlas odvolán.

80. Zásady odpovědnosti vyžadují, aby správce stanovil vhodná technická a organizační opatření, pomocí kterých zajistí a bude moci prokázat, že zpracování probíhá v souladu s GDPR, zejména s hlavními zásadami ochrany údajů stanovenými v čl. 5 odst. 1. Tato opatření by měla zohledňovat povahu, rozsah, kontext a účely zpracování a riziko pro práva a svobody fyzických osob a v případě potřeby musí být přezkoumána a aktualizována[42].

6.5 Profilování

81. Součástí zpracování osobních údajů poskytovateli platebních služeb může být „profilování“ podle čl. 4 odst. 4 GDPR. Poskytovatelé služeb informování o účtu by například mohli vycházet z automatizovaného zpracování osobních údajů, aby mohli vyhodnotit určité osobní aspekty týkající se fyzické osoby. Podle specifik dané služby by mohla být posouzena osobní finanční situace subjektu údajů. Služby informování o účtu, které mají být poskytovány na žádost uživatelů, mohou zahrnovat rozsáhlé hodnocení osobních údajů o platebních účtech.

82. Správce musí subjektu údajů rovněž poskytnout transparentní informace, pokud jde o existenci automatizovaného rozhodování, včetně profilování. V těchto případech musí správce poskytnout smysluplné informace o použitém postupu i o významu a předpokládaných důsledcích tohoto zpracování pro subjekt údajů (čl. 13 odst. 2 písm. f) a čl. 14 odst. 2 písm. g) a 60. bod odůvodnění[43]). Podobně má subjekt údajů podle článku 15 GDPR právo vyžádat si a získat od správce informace o existenci automatizovaného rozhodování, včetně profilování, použitém postupu a důsledcích pro subjekt údajů, a za určitých okolností právo vznést námitku proti profilování, bez ohledu na to, zda se na základě profilování provádí výhradně automatizované individuální rozhodování[44].

83. V této souvislosti je také důležité právo subjektu údajů nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká, jak je stanoveno v článku 22 GDPR. Součástí této normy je za určitých okolností rovněž potřeba, aby správci údajů prováděli vhodná opatření na ochranu práv subjektu údajů, jako je poskytnutí konkrétních informací subjektu údajů, právo na lidský zásah do rozhodovacího procesu a na vyjádření svého názoru a napadnutí rozhodnutí. Jak je také uvedeno v 71. bodě odůvodnění GDPR, znamená to mimo jiné, že subjekty údajů mají právo nebýt předmětem rozhodnutí, jako je automatické odmítnutí on-line žádosti o úvěr bez jakéhokoli lidského zásahu[45].

84. Automatizované rozhodování, včetně profilování, které zahrnuje zvláštní kategorie osobních údajů, je povoleno pouze při splnění kumulativních podmínek čl. 22 odst. 4 GDPR:

- existuje použitelná výjimka podle čl. 22 odst. 2;

[42] Ustanovení čl. 5 odst. 2 a článku 24 GDPR.
[43] Pokyny k transparentnosti podle nařízení 2016/679, WP 260 rev. 01 – schválené EDPB.
[44] Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 pracovní skupiny zřízené podle článku 29, WP251 rev. 01.
[45] 71. bod odůvodnění GDPR.

- a použijí se ustanovení čl. 9 odst. 2 písm. a) nebo g) GDPR. V obou případech musí správce přijmout vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů[46].

85. Také je třeba dodržovat požadavky na další zpracování uvedené v těchto pokynech. Vysvětlení a pokyny k automatizovanému individuálnímu rozhodování a profilování uvedené v Pokynech k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 pracovní skupiny zřízené podle článku 29, schválených EDPB, jsou v souvislosti s platebními službami plně relevantní, a proto je nutné je náležitě zohledňovat.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)

[46] Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 pracovní skupiny zřízené podle článku 29, WP251 rev. 01, strana 24.