PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

16/CS
WP 242 rev.01

Pokyny týkající se práva na přenositelnost údajů

přijaté dne 13. prosince 2016
naposledy revidované a přijaté dne 5. dubna 2017

OBSAH

Shrnutí

Článek 20 obecného nařízení o ochraně osobních údajů vytváří nové právo na přenositelnost údajů, které úzce souvisí s právem na přístup k údajům, ale v mnoha směrech se od něj liší. Umožňuje subjektům údajů získat osobní údaje, které poskytli správci údajů, a to ve strukturovaném, běžně používaném a strojově čitelném formátu, a předat tyto údaje jinému správci údajů. Účelem tohoto nového práva je zmocnit subjekt údajů a dát mu větší kontrolu nad osobními údaji, které se ho týkají.

Jelikož právo na přenositelnost údajů umožňuje přímé předávání osobních údajů od jednoho správce druhému, jedná se rovněž o důležitý nástroj na podporu volného pohybu osobních údajů v EU a rozvoje hospodářské soutěže mezi správci údajů. Usnadní přechod mezi různými poskytovateli služeb, a tím podpoří rozvoj nových služeb v souvislosti se strategií pro jednotný digitální trh.

Toto stanovisko poskytuje pokyny týkající se způsobu, jak vykládat a provádět právo na přenositelnost údajů zavedené obecným nařízením o ochraně osobních údajů. Zaměřuje se na analýzu práva na přenositelnost údajů a jeho rozsahu. Vysvětlují se v něm podmínky, za kterých se toto nové právo uplatňuje se zřetelem na právní základ zpracování údajů (souhlas subjektu údajů, nebo nutnost plnění smlouvy) a na skutečnost, že toto právo se týká pouze osobních údajů poskytnutých subjektem údajů. Toto stanovisko rovněž poskytuje konkrétní příklady a kritéria vysvětlující okolnosti, za kterých se toto právo použije. Pracovní skupina WP29 se v této souvislosti domnívá, že právo na přenositelnost údajů se vztahuje na údaje vědomě a aktivně poskytnuté subjektem údajů, jakož i na osobní údaje, které vznikly v důsledku jeho činnosti. Toto nové právo nelze oslabit a omezit na osobní informace, které přímo sdělí subjekt údajů, například prostřednictvím on-line formuláře.

V rámci osvědčených postupů by správci údajů měli začít rozvíjet prostředky, které přispějí k poskytnutí reakcí na žádosti o uplatnění práva na přenositelnost údajů, jako jsou nástroje ke stahování a aplikační programové rozhraní. Měli by zaručit, že se osobní údaje budou předávat ve strukturovaném, běžně používaném a strojově čitelném formátu, a měli by se podpořit v tom, aby zajistili interoperabilitu formátu údajů poskytovaných při plnění žádosti o přenositelnost údajů.

Toto stanovisko správcům rovněž pomáhá jasně porozumět jejich příslušným povinnostem a doporučuje osvědčené postupy a nástroje, které podporují dodržování souladu s právem na přenositelnost údajů. A konečně, stanovisko doporučuje, aby zainteresované strany v odvětví a oborové asociace spolupracovaly na společném souboru interoperabilních norem a formátů na splnění požadavků práva na přenositelnost údajů.

I. Úvod

Článek 20 obecného nařízení o ochraně osobních údajů (obecné nařízení o ochraně osobních údajů) zavádí nové právo na přenositelnost údajů. Toto právo umožňuje subjektům údajů získat osobní údaje, které poskytli správci údajů, a to ve strukturovaném, běžně používaném a strojově čitelném formátu, a předat tyto údaje jinému správci údajů, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Toto právo, jehož uplatnění podléhá splnění

určitých podmínek, podporuje uživatelskou volbu a kontrolu a rovněž posílení pravomocí uživatelů.

Jednotlivci využívající své právo na přístup k údajům podle směrnice o ochraně údajů 95/46/ES byli omezeni formátem zvoleným správcem údajů při poskytování požadovaných informací. **Cílem nového práva na přenositelnost údajů je posílení pravomocí subjektů údajů, pokud jde o jejich vlastní osobní údaje, jelikož usnadňuje jejich schopnost své osobní údaje snadno přemísťovat, kopírovat nebo předávat z jednoho informačního prostředí do jiného** (ať už do svých vlastních systémů, systémů důvěryhodných třetích stran, nebo do systémů nových správců).

Přenositelnost údajů prostřednictvím potvrzení osobních práv jednotlivců a jejich kontroly nad osobními údaji, které se jich týkají, představuje rovněž příležitost na „vyvážení" vztahu mezi subjekty údajů a správci údajů[1].

I když právo na přenositelnost osobních údajů rovněž může zvýšit hospodářskou soutěž mezi službami (usnadněním změny služeb), obecné nařízení o ochraně osobních údajů upravuje osobní údaje, nikoliv hospodářskou soutěž. Zejména článek 20 neomezuje přenositelné údaje na údaje, které jsou nezbytné nebo užitečné pro změnu služeb[2].

Ačkoliv přenositelnost údajů je nové právo, jiné druhy přenositelnosti již existují nebo jsou projednávány v dalších oblastech práva (např. v kontextu ukončení smlouvy, roamingu v oblasti komunikačních služeb a přeshraničního přístupu ke službám[3]). Mezi různými druhy přenositelnosti se mohou objevit některé synergie a dokonce výhody pro jednotlivce, budou-li se poskytovat prostřednictvím kombinovaného přístupu, avšak k analogiím by se mělo přistupovat opatrně.

Toto stanovisko obsahuje pokyny pro správce údajů, aby mohli aktualizovat své postupy, procesy a politiky, a vysvětluje význam přenositelnosti údajů, aby mohly subjekty údajů své nové právo účinně využívat.

II. Jaké jsou hlavní prvky přenositelnosti údajů?

Obecné nařízení o ochraně osobních údajů definuje právo na přenositelnost údajů v čl. 20 odst. 1 takto:

> *Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil […]*

- Právo získat osobní údaje

[1] Hlavním cílem přenositelnosti údajů je zvýšit kontrolu jednotlivců nad jejich osobními údaji a zajistit, že hrají aktivní úlohu v datovém ekosystému.
[2] Toto právo například umožňuje bankám poskytovat dodatečné služby, pod kontrolou uživatele, za použití osobních údajů původně shromážděných jako součást služby dodávky energie.
[3] Viz program Evropské komise pro jednotný digitální trh: https://ec.europa.eu/digital-agenda/en/digital-single-market, zejména první pilíř politiky „Lepší online přístup k digitálnímu zboží a službám".

Zaprvé, přenositelnost údajů je **právo subjektu údajů získat část osobních údajů**, které se ho týkají, zpracovaných správcem údajů a uložit si tyto údaje pro další osobní použití. Uložištěm může být soukromé zařízení nebo soukromý cloud, aniž by nutně došlo k předání údajů jinému správci údajů.

Z tohoto hlediska přenositelnost údajů doplňuje právo na přístup. Specifičnost přenositelnosti údajů spočívá v tom, že subjektům údajů nabízí snadný způsob, jak mohou samy spravovat a opětovně používat osobní údaje. Tyto údaje by měly být získány „*ve strukturovaném, běžně používaném a strojově čitelném formátu*“. Subjekt údajů například může mít zájem o získání svého stávajícího seznamu přehrávaných skladem (nebo historie přehrávaných skladeb) od služby pro streamování hudby, aby zjistil, kolikrát poslouchal konkrétní skladby, nebo aby si ověřil, kterou hudbu si chce zakoupit nebo poslouchat na jiné platformě. Podobně může chtít získat svůj seznam kontaktů ze své e-mailové aplikace, například aby si vytvořil seznam svatebních hostí, nebo získat informace o nákupech za použití různých věrnostních karet, nebo posoudit svou uhlíkovou stopu[4].

- **Právo předat osobní údaje od jednoho správce jinému správci**

Zadruhé, čl. 20 odst. 1 poskytuje subjektům údajů **právo předat osobní údaje od jednoho správce jinému správci**, „aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil“. Údaje mohou být na žádost subjektu údajů předány přímo jedním správcem správci druhému, je-li to technicky proveditelné (čl. 20 odst. 2). Ustanovení 68. bodu odůvodnění v této souvislosti podporuje správce údajů v rozvíjení interoperabilních formátů umožňujících přenositelnost údajů[5], aniž by zakládal povinnost správců údajů zavést nebo zachovávat technicky kompatibilní systémy[6]. Obecné nařízení o ochraně osobních údajů však správcům údajů zakazuje vytvářet překážky předávání.

Tento prvek přenositelnosti údajů subjektům údajů v podstatě poskytuje možnost nejen získat a opětovně použít údaje, které poskytly, ale také je předat jinému poskytovateli služeb (buď ve stejném podnikatelském odvětví, nebo v jiném odvětví). Očekává se, že kromě zlepšení postavení spotřebitelů tím, že se zabrání tomu, aby byli odkázáni na určitého dodavatele, podpoří právo na přenositelnost příležitosti pro inovace a výměnu údajů mezi správci údajů bezpečným a zabezpečeným způsobem pod kontrolou subjektu údajů[7]. Přenositelností údajů se může podpořit kontrolovaná a omezená výměna osobních údajů ze strany uživatelů mezi organizacemi, čímž se obohatí služby a zkušenosti spotřebitelů[8]. Přenositelnost údajů může usnadnit předání a opětovné použití osobních údajů týkajících se uživatelů mezi různými službami, o které mají zájem.

---

[4] V těchto případech může zpracování údajů poskytnutých subjektem údajů spadat buď do oblasti činnosti v domácnosti, kdy je veškeré zpracování prováděno pod výhradní kontrolou subjektu údajů, nebo může být jménem subjektu údajů prováděno jinou stranou. V takovém případě by měla být jiná strana považována za správce údajů, i když výhradně pro účely ukládání osobních údajů, a musí dodržovat zásady a povinnosti stanovené v obecném nařízení o ochraně osobních údajů.

[5] Viz také oddíl V.

[6] V důsledku toho je třeba věnovat zvláštní pozornost formátu předávaných údajů, aby bylo zaručeno, že subjekt údajů nebo jiný správce údajů může údaje s malým úsilím opakovaně použít. Viz také oddíl V.

[7] Viz několik pokusných aplikací v Evropě, například MiData ve Spojeném království, MesInfos / SelfData organizace FING ve Francii.

[8] Odvětví zabývající se takzvaným *quantified self* a internetem věcí poukázaly na přínos (a rizika) propojení osobních údajů týkajících se různých aspektů života jedince, jako například fyzické kondice, činnosti a příjmu kalorií, z hlediska dodání úplnějšího obrazu života jedince v jediném souboru.

- **Kontrola**

Přenositelnost údajů zaručuje právo získávat osobní údaje a zpracovávat je podle vůle subjektu údajů[9].

Správci, kteří za podmínek stanovených v článku 20 odpovídají na žádosti o přenositelnost údajů, nejsou odpovědní za zpracování provedené subjektem nebo jinou společností, která osobní údaje obdržela. Jednají jménem subjektu údajů, a to včetně situací, kdy jsou osobní údaje předány přímo jinému správci. Vzhledem ke skutečnosti, že odesílající správce nevybírá, kdo bude příjemcem, není odesílající správce v této souvislosti odpovědný za to, zda přijímající správce dodržuje právo v oblasti ochrany údajů. Správci by měli současně stanovit záruky pro zajištění toho, že skutečně jednají jménem subjektu údajů. Mohou například zavést postupy, kterými se zajistí, že druh předávaných osobních údajů je skutečně tím druhem údajů, který chce subjekt údajů předat. To lze uskutečnit získáním potvrzení od subjektu údajů, buď před předáním, nebo dříve, při udělení původního souhlasu se zpracováním či při uzavření smlouvy.

Správci údajů odpovídající na žádost o přenositelnost údajů nemají žádnou zvláštní povinnost před předáním údajů zkontrolovat a ověřit jejich kvalitu. Samozřejmě, že údaje by v souladu se zásadami uvedenými v čl. 5 odst. 1 obecného nařízení o ochraně osobních údajů již měly být přesné a aktuální. Přenositelnost údajů navíc správci údajů neukládá povinnost uchovávat osobní údaje delší dobu, než je nezbytné, nebo delší dobu, než je stanovená doba uchování[10]. Důležité je, že neexistuje žádný dodatečný požadavek na uchovávání údajů delší dobu, než jsou jinak použitelné doby uchování, pouze pro účely případné budoucí žádosti o přenositelnost údajů.

Jsou-li požadované osobní údaje zpracovány správcem údajů, musí smlouva uzavřená v souladu s článkem 28 obecného nařízení o ochraně osobních údajů zahrnovat povinnost „být správci nápomocen prostřednictvím vhodných technických a organizačních opatření, (…) reagovat na žádosti o výkon práv subjektu údajů“. Za účelem odpovědí na žádosti o přenositelnost údajů by proto měl správce ve spolupráci se svými zpracovateli údajů zavést zvláštní postupy. V případě společné správy by měla smlouva každému správci údajů jasně přidělit, za co je v souvislosti se zpracováním žádostí o přenositelnost údajů odpovědný.

Přijímající správce[11] je kromě toho odpovědný za zajištění toho, že poskytnuté přenositelné údaje jsou s ohledem na nové zpracování údajů relevantní a nejsou nepřiměřené. Například v případě žádosti o přenositelnost údajů podané e-mailové službě, kdy subjekt údajů žádost použije pro získání e-mailů a jejich odeslání na zabezpečenou archivační platformu, nový správce nemusí zpracovávat kontaktní údaje osob, s nimiž si subjekt údajů koresponduje. Nejsou-li tyto informace s ohledem na účel nového zpracování relevantní, neměly by být uchovávány a zpracovávány. Přijímající správci údajů v každém případě nejsou povinni přijmout a zpracovat osobní údaje předané v návaznosti na žádost o přenositelnost údajů. Obdobně, pokud subjekt údajů požaduje předání údajů týkajících se jeho bankovních transakcí službě, která mu pomáhá při správě jeho rozpočtu, přijímající správce údajů nemusí

[9] Právo na přenositelnost údajů se nevztahuje pouze na osobní údaje, které jsou užitečné a relevantní pro podobné služby poskytované konkurenty správce údajů.

[10] Ve výše uvedeném příkladu, pokud správce údajů neuchovává záznam písní přehrávaných uživatelem, pak nemohou být tyto osobní údaje zahrnuty do žádosti o přenositelnost údajů.

[11] Tj. správce údajů, který v návaznosti na žádost o přenositelnost údajů, kterou subjekt údajů podal jinému správci, přijímá osobní údaje.

přijmout veškeré údaje, nebo uchovat veškeré údaje o transakcích, jakmile byly označeny pro účely nové služby. Jinými slovy, přijímat a uchovávat by se měly pouze ty údaje, které jsou nezbytné a relevantní pro služby poskytované přijímajícím správcem údajů.

„Přijímající "organizace se stane novým správcem údajů, pokud jde o tyto osobní údaje, a musí respektovat zásady uvedené v článku 5 obecného nařízení o ochraně osobních údajů. „Nový" přijímající správce údajů proto musí před jakoukoliv žádostí o předání přenositelných údajů v souladu s požadavky na transparentnost uvedenými v článku 14 jasně a přímo uvést účel nového zpracování[12]. Správce údajů by měl, stejně jako u jakéhokoliv jiného zpracování údajů, za které odpovídá, uplatňovat zásady uvedené v článku 5, jako např. zákonnost, korektnost a transparentnost, omezení účelu, minimalizaci údajů, přesnost, integritu a důvěrnost, omezení uložení a odpovědnost[13].

Správci údajů, kteří mají v držení osobní údaje, by ulehčit svým subjektům údajů výkon práva na přenositelnost údajů. Správci údajů se rovněž mohou rozhodnout od subjektu údajů údaje přijmout, ale nejsou povinni tak učinit.

- **Přenositelnost údajů vs. jiná práva subjektů údajů**

Fyzická osoba své právo na přenositelnost údajů uplatňuje, aniž by tím bylo dotčeno jakékoliv jiné právo (jako je tomu v případě jakýchkoliv jiných práv v obecném nařízení o ochraně osobních údajů). Subjekt údajů může pokračovat ve využívání služeb správce údajů a užívat jejich výhod i po operaci přenesení údajů. Přenositelnost údajů automaticky nevede k výmazu údajů[14] ze systémů správce údajů a neovlivňuje původní dobu uchování platnou pro údaje, které byly předány. Pokud správce údajů údaje stále zpracovává, může subjekt údajů uplatňovat svá práva.

Stejně tak, chce-li subjekt údajů uplatnit své právo na výmaz („právo být zapomenut" podle článku 17), nemůže být přenositelnost údajů správcem údajů použita jako způsob, jak takový výmaz zpozdit nebo odmítnout.

Zjistí-li subjekt údajů, že osobní údaje požadované podle práva na přenositelnost údajů jeho žádost plně neřeší, musí být jakákoliv další žádost o osobní údaje na základě práva na přístup plně vyhověno, v souladu s článkem 15 obecného nařízení o ochraně osobních údajů.

Kromě toho, pokud zvláštní evropský právní předpis nebo právní předpis členského státu v jiné oblasti rovněž stanoví určitou formu přenositelnosti dotčených údajů, musí být při splnění žádosti o přenositelnost údajů podle obecného nařízení o ochraně osobních údajů rovněž zohledněny podmínky stanovené v těchto konkrétních právních předpisech. Zaprvé, pokud ze žádosti podané subjektem údajů jasně vyplývá, že záměrem subjektu údajů není uplatňovat práva podle obecného nařízení o ochraně osobních údajů, ale uplatňovat práva pouze podle odvětvových právních předpisů, pak se ustanovení obecného nařízení o ochraně osobních

[12] Nový správce údajů by navíc neměl zpracovávat osobní údaje, které nejsou relevantní, a zpracování musí být omezeno na to, co je nezbytné pro nové účely, i když jsou osobní údaje součástí globálnějšího souboru údajů předaného prostřednictvím procesu přenositelnosti. Osobní údaje, které nejsou nezbytné pro dosažení účelu nového zpracování, by měly být co nejdříve vymazány.

[13] Jakmile správce údajů obdrží osobní údaje zaslané jako součást práva na přenositelnost údajů, mohou být tyto údaje považovány za „poskytnuté" subjektem údajů a opětovně předány podle práva na přenositelnost údajů, a to v rozsahu, v němž jsou splněny jiné podmínky vztahující se na toto právo (tj. právní základ zpracování atd.).

[14] Jak je uvedeno v článku 17 obecného nařízení o ochraně osobních údajů.

údajů týkající se přenositelnosti údajů na tuto žádost nepoužijí[15]. Pokud je však na straně druhé cílem žádosti přenositelnost podle obecného nařízení o ochraně osobních údajů, existence těchto zvláštních právních předpisů nemá přednost před uplatněním obecné zásady přenositelnosti údajů na každého správce údajů, jak stanoví obecné nařízení o ochraně osobních údajů. Namísto toho je třeba na základě konkrétních případů posoudit, jak mohou tyto zvláštní právní předpisy ovlivnit právo na přenositelnost údajů, pokud vůbec mohou ovlivnit.

III. Kdy se přenositelnost údajů uplatňuje?

- **Na které operace zpracování se vztahuje právo na přenositelnost údajů?**

Soulad s obecným nařízením o ochraně osobních údajů vyžaduje, aby správci údajů měli pro zpracování osobních údajů jasný právní základ.

V souladu s čl. 20 odst. 1 písm. a) obecného nařízení o ochraně osobních údajů musí být operace zpracování, **aby spadaly do oblasti působnosti přenositelnosti údajů**, založeny:

- buď na souhlasu subjektu údajů (podle čl. 6 odst. 1 písm. a), nebo v případě zvláštních kategorií osobních údajů podle čl. 9 odst. 2 písm. a)),

- nebo na smlouvě podle čl. 6 odst. 1 písm. b), jejíž je subjekt údajů stranou.

Příklady osobních údajů, které obecně spadají od oblasti působnosti přenositelnosti údajů, jsou například tituly knih zakoupených fyzickou osobou v internetovém knihkupectví, nebo písně poslouchané prostřednictvím služby pro streamování hudby, jelikož tyto údaje jsou zpracovány na základě plnění smlouvy, jejíž je subjekt údajů stranou.

Obecné nařízení o ochraně osobních údajů nestanoví obecné právo na přenositelnost údajů pro případy, kdy zpracování údajů není založeno na souhlasu nebo smlouvě[16]. Například finanční instituce nemají povinnost reagovat na žádost o přenositelnost údajů týkající se osobních údajů zpracovaných jako součást jejich povinností předcházet a odhalovat praní peněz a jiné finanční trestné činy; přenositelnost údajů stejně tak nepokrývá profesionální kontaktní údaje zpracované v rámci vztahu mezi podniky v případech, kdy zpracování není založeno ani na souhlasu subjektu údajů, ani na smlouvě, jejíž je subjekt údajů stranou.

[15] Například je-li konkrétním cílem žádosti subjektu údajů poskytnout přístup k historii transakcí na svém bankovním účtu poskytovateli služeb informování o účtu, a to pro účely uvedené v druhé směrnici o platebních službách, měl by být tento přístup udělen podle ustanovení této směrnice.

[16] Viz 68. bod odůvodnění a čl. 20 odst. 3 obecného nařízení o ochraně osobních údajů. V čl. 20 odst. 3 a 68. bodu odůvodnění se uvádí, že přenositelnost údajů se neuplatní, je-li zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce údajů pověřen, nebo vykonává-li správce údajů svou veřejnou moc, nebo je-li to nezbytné pro splnění právní povinnosti. Správci údajů proto v těchto případech nemají žádnou povinnost zajistit přenositelnost. Je však osvědčeným postupem vytvářet postupy pro automatické odpovídání na žádosti o přenositelnost podle zásad, kterými se řídí právo na přenositelnost údajů. Příkladem by byla vládní služba umožňující snadné stahování minulých podání daňového přiznání z příjmu fyzických osob. Přenositelnost údajů jakožto osvědčený postup v případě zpracování založeného na právním základě nutnosti oprávněného zájmu a stávající dobrovolné režimy viz strany 47 a 48 stanoviska pracovní skupiny WP29 6/2014 týkajícího se oprávněných zájmů (WP217).

V případě údajů zaměstnanců se právo na přenositelnost údajů typicky použije pouze tehdy, je-li zpracování založeno na smlouvě, jejíž je subjekt údajů stranou. Vzhledem k nerovnováze moci mezi zaměstnavatelem a zaměstnancem nebude v mnoha případech souhlas v této souvislosti považován za svobodný[17]. Některá zpracování týkající se lidských zdrojů jsou místo toho založena na právním základě oprávněného zájmu, nebo jsou nezbytná pro splnění zvláštních právních povinností v oblasti zaměstnanosti. V praxi se bude právo na přenositelnost údajů v kontextu lidských zdrojů nepochybně týkat některých operací zpracování (jako například platebních a kompenzačních služeb, vnitřních řízení pro obsazování pracovních míst), ale v mnoha jiných situacích bude na ověření, zda jsou splněny veškeré podmínky vztahující se na právo na přenositelnost údajů, potřeba individuální přístup.

A konečně, právo na přenositelnost údajů se použije pouze tehdy, je-li zpracování údajů „prováděno automatizovaně“, a proto se nevztahuje na většinu listinných spisů.

- **Které osobní údaje musí být zahrnuty?**

Aby údaje spadaly do působnosti práva na přenositelnost údajů, musí se podle čl. 20 odst. 1 jednat o:

- osobní údaje, které se týkají subjektu údajů a
- jež subjekt údajů *poskytl* správci údajů.

Ustanovení čl. 20 odst. 4 rovněž uvádí, že souladem s tímto právem nesmí být nepříznivě dotčena práva a svobody jiných osob.

<u>První podmínka: osobní údaje, které se týkají subjektu údajů</u>

Do oblasti působnosti žádosti o přenositelnost údajů spadají pouze osobní údaje. Všechny údaje, které jsou anonymní[18], nebo které se netýkají subjektu údajů, nespadají do působnosti tohoto práva. Do jeho působnosti však spadají pseudonymní údaje, které mohou být jasně spojeny se subjektem údajů (např. tím, že tento subjekt údajů poskytne příslušný identifikační informace, viz čl. 11 odst. 2).

V mnoha případech budou správci údajů zpracovávat informace obsahující osobní údaje několika subjektů údajů. Správci údajů by v těchto případech neměli přijímat příliš restriktivní výklad věty „osobní údaje, které se týkají subjektu údajů“. Například telefonní hovory, interpersonální přenos zpráv nebo záznamy VoIP mohou zahrnovat (v historii účtu uživatele) údaje o třetích stranách zapojených do příchozích a odchozích hovorů. Ačkoliv záznamy tedy budou obsahovat osobní údaje týkající se několika osob, uživatelé by měli být schopni tyto záznamy v návaznosti na žádost o přenositelnost údajů získat, jelikož tyto záznamy se (rovněž) týkají subjektu údajů. Jsou-li však tyto záznamy následně předány novému správci údajů, tento nový správce údajů by je neměl zpracovávat pro žádný účel, kterým by byla nepříznivě dotčena práva a svobody třetích stran (viz níže: třetí podmínka).

<u>Druhá podmínka: údaje poskytnuté subjektem údajů</u>

Druhá podmínka zužuje oblast působnosti práva na údaje „poskytnuté“ subjektem údajů.

[17] Jak pracovní skupina WP29 uvedla ve svém stanovisku 8/2001 ze dne 13. září 2001 (WP48).
[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf

Existuje mnoho příkladů osobních údajů, které budou vědomě a aktivně „poskytnuty“ subjektem údajů, jako například údaje o účtu (např. poštovní adresa, uživatelské jméno, věk) sdělené prostřednictvím on-line formulářů. Údaje „poskytnuté “subjektem údajů nicméně rovněž vyplývají z pozorování jeho činnosti. V důsledku toho má pracovní skupina WP29 za to, že aby se toto nové právo uplatňovalo ve své úplnosti, měl by pojem „poskytnuté“ rovněž zahrnovat osobní údaje, které jsou vypozorované z činností uživatelů, jako např. primární údaje zpracované inteligentním měřičem nebo jinými druhy propojených předmětů[19], záznamy o činnosti, historie používání internetové stránky nebo činnosti vyhledávání.

Tato druhá kategorie údajů nezahrnuje údaje vytvořené správcem údajů (za použití vypozorovaných údajů nebo údajů poskytnutých přímo jako vstup), jako například uživatelský profil vytvořený analýzou shromážděných primárních údajů z inteligentních měřičů.

Rozlišovat lze mezi dvěma různými kategoriemi údajů, a to v závislosti na jejich původu, aby se určilo, zda údaje spadají do práva na přenositelnost údajů. Jako „poskytnuté subjektem údajů“ lze hodnotit tyto kategorie:

- **údaje aktivně a vědomě poskytnuté subjektem údajů** (například poštovní adresa, uživatelské jméno, věk atd.)
- **vypozorované údaje poskytnuté subjektem údajů na základě používání služby nebo zařízení.** Mezi tyto údaje může patřit například historie vyhledávání, údaje o provozu a lokalizační údaje osoby. Patřit se mohou rovněž další primární údaje, jako je puls sledovaný nositelným zařízením.

Oproti tomu vyvozené údaje a odvozené údaje vyváří správce údajů na základě údajů „poskytnutých subjektem údajů“. Například výsledek posouzení týkajícího se zdravotního stavu uživatele nebo profil vytvořený v souvislosti s řízením rizik a finančními nařízeními (např. za účelem přidělení úvěrového hodnocení nebo za účelem dodržení předpisů proti praní špinavých peněz) nemohou být samy o sobě považovány za „poskytnuté“ subjektem údajů. Ačkoliv tyto údaje mohou být součástí profilu uchovávaného správcem údajů a jsou vyvozeny nebo odvozeny z analýzy údajů poskytnutých subjektem údajů (například prostřednictvím jeho činnosti), tyto údaje zpravidla nebudou považovány za údaje „poskytnuté subjektem údajů“, a nebudou proto spadat do oblasti působnosti tohoto nového práva[20].

Obecně platí, že vzhledem k politickým cílům práva na přenositelnost údajů musí být pojem „poskytnuté subjektem údajů“ vykládán široce a měl by vylučovat „vyvozené údaje“ a „odvozené údaje“, které zahrnují osobní údaje vytvořené poskytovatelem služeb (například algoritmické výsledky). Správce údajů může tyto vyvozené údaje vyloučit, měl by však

[19] Tím, že bude subjekt údajů schopen získat údaje vyplývající z pozorování jeho činnosti, bude rovněž schopen získat lepší přehled o vykonávacích rozhodnutích správce údajů týkajících se rozsahu sledovaných údajů, a bude tak v lepším postavení, aby si mohl zvolit, které údaje je ochoten poskytnout na získání podobné služby, a dozví se, do jaké míry se dodržuje jeho právo na soukromí.

[20] Subjekt údajů však stále může podle článku 15 obecného nařízení o ochraně osobních údajů (který odkazuje na právo na přístup) využít své „právo získat od správce údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům“, jakož i k informacím o „skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů“.

zahrnout veškeré další osobní údaje poskytnuté subjektem údajů prostřednictvím technických prostředků poskytnutých správcem údajů [21].

Pojem „poskytnuté“ tedy zahrnuje osobní údaje, které souvisejí s činností subjektu údajů nebo které vyplývají z pozorování chování jednotlivce, ale nezahrnuje údaje vyplývající s následné analýzy tohoto chování. Naproti tomu veškeré osobní údaje, které byly vytvořeny správcem údajů jakožto součást zpracování údajů, např. personalizací nebo procesem doporučování či kategorizací nebo profilováním uživatelů, představují údaje, které jsou odvozeny nebo vyvozeny z osobních údajů poskytnutých subjektem údajů, a nevztahuje se na ně právo na přenositelnost údajů.

Třetí podmínka: právem na přenositelnost údajů nesmějí být nepříznivě dotčena práva a svobody jiných osob

Pokud jde o osobní údaje týkající se jiných subjektů údajů:

Cílem třetí podmínky je zamezit získávání a předávání údajů obsahujících osobní údaje jiných subjektů údajů (kteří k tomu neudělili souhlas) novému správci údajů v případech, kdy tyto údaje pravděpodobně budou zpracovány způsobem, kterým by byla nepříznivě dotčena práva a svobody jiných subjektů údajů (čl. 20 odst. 4 obecného nařízení o ochraně osobních údajů)[22].

Tento nežádoucí účinek by se mohl projevit například, pokud by předání údajů od jednoho správce údajů druhému mohlo třetím stranám zabránit v uplatnění jejich práv jakožto subjektů údajů podle obecného nařízení o ochraně osobních údajů (jako například práv na informace, na přístup atd.).

Subjekt údajů, který iniciuje předání svých osobních údajů správci údajů, buď novému správci údajů udělí souhlas se zpracováním, nebo s tímto správcem uzavře smlouvu. Jsou-li součástí souboru údajů osobní údaje třetích stran, je třeba pro zpracování určit jiný právní základ. Správce údajů například může sledovat oprávněný zájem podle čl. 6 odst. 1 písm. f), zejména je-li účelem správce údajů poskytnout subjektu údajů službu, která tomuto subjektu umožní zpracovávat osobní údaje v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti. Operace zpracování iniciované subjektem údajů v souvislosti s činností osobní povahy, které se týkají třetích stran a případně na ně mohou mít dopad, zůstávají odpovědností subjektu údajů v rozsahu, v jakém o takovémto zpracování žádným způsobem nerozhoduje správce údajů.

Například e-mailová služba může umožňovat vytváření adresáře kontaktů subjektu údajů a jeho přátel, příbuzných, rodinných členů a širšího okolí. Jelikož tyto údaje souvisejí s (a jsou vytvářeny) identifikovatelnou fyzickou osobou, která si přeje uplatnit své právo na

[21] To zahrnuje veškeré údaje týkající se subjektu údajů vypozorované během činností pro účel, za nímž jsou údaje shromažďovány, jako například historie transakcí nebo záznamy o přístupu. Za údaje „poskytnuté subjektem údajů“ by měly být považovány rovněž údaje shromážděné prostřednictvím sledování a zaznamenávání subjektu údajů (jako například aplikace zaznamenávající puls nebo technologie použitá pro sledování on-line chování), a to i tehdy, nejsou-li údaje aktivně nebo vědomě předávány.

[22] Ustanovení 68. bodu odůvodnění stanoví, že „ pokud se určitý soubor osobních údajů týká více než jednoho subjektu údajů, neměla by právem obdržet osobní údaje být dotčena práva a svobody jiných subjektů údajů podle tohoto nařízení“.

přenositelnost údajů, měli by správci údajů tomuto subjektu údajů předat celý adresář příchozích a odchozích e-mailů.

Obdobně, bankovní účet subjektu údajů může obsahovat osobní údaje týkající se transakcí nejen držitele účtu, ale také jiných fyzických osob (např. pokud držiteli účtu převedli peníze). Je nepravděpodobné, že by předáním informací o bankovním účtu držiteli účtu poté, co byla podána žádost o přenositelnost, byla nepříznivě dotčena práva a svobody těchto třetích stran – za předpokladu, že údaje jsou v obou případech použity pro stejný účel (tj. kontaktní adresa použitá pouze subjektem údajů nebo historie transakcí na bankovním účtu subjektu údajů).

Naopak k porušení práv a svobod třetích stran dojde, pokud nový správce údajů použije osobní údaje pro jiné účely, např. pokud přijímající správce údajů použije osobní údaje jiných fyzických osob v adresáři kontaktů subjektu údajů pro marketingové účely.

Aby se zabránilo nežádoucímu účinku na zúčastněné třetí strany, je proto zpracování takovýchto osobních údajů jiným správcem povoleno pouze v míře, v jaké zůstávají údaje pod výlučnou kontrolou žádajícího uživatele a jsou spravovány pro potřeby týkající se výhradně osobní potřeby či domácnosti. Přijímající „nový“ správce údajů (jemuž byly údaje předány na žádost uživatele) nesmí předané údaje třetích stran používat pro své vlastní účely, např. těmto subjektům údajů jiné třetí strany navrhovat marketingové produkty a služby. Tyto informace například nemohou být použity k obohacení profilu subjektu údajů třetí strany a k přestavbě jeho sociálního prostředí bez jeho vědomí nebo souhlasu[23]. Nemohou být použity ani k získávání informací o této třetí straně a k vytváření zvláštních profilů, a to ni tehdy, jsou-li osobní údaje těchto třetích stran již v držení správce údajů. Jinak je pravděpodobné, že takovéto zpracování bude protiprávní či nepřiměřené, zejména nejsou-li dotčené třetí strany informovány a nemohou-li uplatnit svá práva jakožto subjekty údajů.

Kromě toho je osvědčeným postupem pro všechny správce údajů („odesílající“ i „přijímající“ strany) zavádět nástroje, které subjektům údajů umožní vybrat si relevantní údaje, které si přejí získat a předat a případně vyloučit údaje jiných fyzických osob. Tento postup ještě víc pomůže snížit rizika pro třetí strany, jejichž osobní údaje mohou být převedeny.

Správci údajů by navíc měli zavést mechanismus udělování souhlasu pro jiné zúčastněné subjekty údajů, aby se usnadnilo předávání údajů v případech, kdy jsou tyto strany ochotny souhlas udělit, např. pokud své údaje rovněž chtějí přesunout k jinému správci údajů. K této situaci může dojít například u sociálních sítí, je však na správcích údajů, aby se rozhodli, kterým osvědčeným postupem se budou řídit.

Pokud jde o údaje, na které se vztahuje duševní vlastnictví nebo obchodní tajemství:
Práva a svobody jiných osob jsou uvedeny v čl. 20 odst. 4. Ačkoliv přímo nesouvisejí s přenositelností, lze je chápat jako zahrnující „obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení“. Avšak i když by tato práva měla být před odpovědí na žádost o přenositelnost údajů zohledněna, „zohlednění těchto skutečností by nemělo vést k tomu, že by subjektu údajů bylo odepřeno poskytnutí všech informací“. Správce údajů by dále žádost o přenositelnost údajů neměl zamítnout na základě porušení jiného smluvního práva (například nesplaceného dluhu nebo obchodního sporu se subjektem údajů).

[23] Služby sociální sítě by neměly obohacovat profil svých členů za použití osobních údajů předaných subjektem údajů jako součást jeho práva na přenositelnost údajů, aniž by respektovaly zásadu transparentnosti a aniž by se také ujistily, že toto konkrétní zpracování se opírá o odpovídající právní základ.

Právo na přenositelnost údajů není právem fyzických osob na zneužívání informací způsobem, který by mohl být kvalifikován jako nekalá praktika, nebo který by mohl představovat porušení práv duševního vlastnictví.

Možné obchodní riziko však samo o sobě nemůže sloužit jako základ pro odmítnutí odpovědět na žádost o přenositelnost a správci údajů mohou osobní údaje poskytnuté subjekty údajů předávat způsobem, kterým neunikají informace, na které se vztahují obchodní tajemství nebo práva duševního vlastnictví.

IV. Jak se na přenositelnost údajů vztahují obecná pravidla, kterými se řídí uplatňování práv subjektu údajů?

- **Jaké předběžné informace by měly být poskytnuty subjektu údajů?**

Za účelem zajištění souladu s novým právem na přenositelnost údajů musí správci údajů informovat subjekty údajů o existenci nového práva na přenositelnost. Pokud se dotčené osobní údaje získávají přímo od subjektu údajů, musí o tomto právě správce informovat „při získávání osobních údajů“. Pokud nebyly osobní údaje získány od subjektu údajů, musí správce poskytnout informace, jak požaduje čl. 13 odst. 2 písm. b) a čl. 14 odst. 2 písm. c).

„Pokud nebyly osobní údaje získány od subjektu údajů“, vyžaduje čl. 14 odst. 3, aby byly informace poskytnuty v přiměřené lhůtě nepřesahující jeden měsíc od získání údajů, v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, nebo ke zpřístupnění třetím stranám[24].

Při poskytování požadovaných informací musí správci zajistit, že budou právo na přenositelnost údajů odlišovat od jiných práv. Pracovní skupina WP29 proto zejména doporučuje, aby správci jasně vysvětlili rozdíl mezi druhy údajů, které může subjekt údajů získat na základě práva subjektu na přístup a na základě práva na přenositelnost údajů.

Pracovní skupina kromě toho doporučuje, aby správci informaci o právu na přenositelnost údajů vždy zahrnuli předtím, než subjekty údajů uzavřou jakýkoliv účet, který mohou mít. To uživatelům umožní před ukončením smlouvy posoudit své osobní údaje a snadno je převést do svého zařízení nebo k jinému poskytovateli.

A konečně, pracovní skupina WP29 jakožto osvědčený postup pro „přijímající“ správce údajů doporučuje, aby byly subjektům údajů poskytnuty úplné informace o povaze osobních údajů, které jsou podstatné pro poskytování jejich služeb. Kromě podpory spravedlivého zpracování se tím uživatelům umožní snížit rizika pro třetí strany a rovněž omezit jakoukoliv další zbytečnou duplicitu osobních údajů, a to i tehdy, kdy do věci nejsou zapojené žádné další subjekty údajů.

- **Jak může správce údajů identifikovat subjekt údajů před tím, než odpoví na jeho žádost?**

Obecné nařízení o ochraně osobních údajů neobsahuje žádné normativní požadavky týkající způsobu ověření subjektu údajů. Ustanovení čl. 12 odst. 2 obecného nařízení o ochraně

[24] Článek 12 stanoví, že správci údajů poskytnou „veškerá sdělení […] stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, zejména pokud se jedná o informace určené konkrétně dítěti“.

osobních údajů nicméně uvádí, že správce údajů neodmítne vyhovět žádosti subjektu údajů za účelem výkonu jeho práv (včetně práva na přenositelnost údajů), ledaže zpracovává osobní údaje pro účel, který nevyžaduje identifikaci subjektu údajů, a může doložit, že není schopen identifikovat subjektu údajů. Podle čl. 11 odst. 2 však může subjekt údajů za těchto okolností poskytnout více informací umožňujících jeho identifikaci. Kromě toho čl. 12 odst. 6 stanoví, že pokud má správce údajů důvodné pochybnosti o totožnosti subjektu údajů, může požádat o další informace pro potvrzení totožnosti subjektu údajů. Poskytne-li subjekt údajů dodatečné informace umožňující jeho identifikaci, správce údajů neodmítne vyhovět jeho žádosti. Jsou-li informace a údaje shromážděné on-line spojeny s pseudonymy nebo jedinečnými identifikátory, mohou správci údajů zavést vhodné postupy umožňující fyzickým osobám podat žádost o přenositelnost údajů a získat údaje, které se jich týkají. Správci údajů musejí v každém případě zavést postup ověřování, kterým se spolehlivě prokáže totožnost subjektu údajů, jenž požaduje své osobní údaje, nebo jenž z obecnějšího hlediska uplatňuje práva přiznaná obecným nařízením o ochraně osobních údajů.

Tyto postupy často již existují. Subjekty údajů jsou správcem údajů často ověřovány již před uzavřením smlouvy nebo před získáním jejich souhlasu se zpracováním. V důsledku toho mohou být osobní údaje použité pro zaregistrování fyzické osoby, které se týká zpracování, rovněž použity jako důkaz pro ověření subjektu údajů pro účely přenositelnosti[25].

I když v těchto případech se při identifikaci subjektu údajů dopředu může vyžadovat žádost o jeho zákonné totožnosti, takové ověření nemusí být pro posouzení souvislosti mezi údaji a dotčenou fyzickou osobou důležité, jelikož toto propojení nesouvisí s úřední nebo zákonnou totožnosti. V podstatě schopnost správce údajů vyžádat si dodatečné informace pro posouzení totožnosti osoby nemůže vést k nadměrným požadavkům a ke shromažďování osobních údajů, které nejsou relevantní ani nezbytné na posílení propojení mezi fyzickou osobou a požadovanými osobními údaji.

V mnoha případech už takové postupy ověřování existují. Například k tomu, aby byl fyzickým osobám umožněn přístup k údajům v jejich e-mailových účtech, účtech na sociálních sítích a účtech používaných pro různé jiné služby, jsou často používány uživatelská jména a hesla, z nichž některá si uživatelé volí, aniž by odhalili své celé jméno a totožnost.

Pokud je předání údajů požadovaných subjektem údajů prostřednictvím internetu kvůli jejich velkosti komplikované, může se stát, že místo případného prodloužení lhůty pro splnění žádosti v maximální délce tří měsíců[26] bude muset správce údajů rovněž zvážit alternativní způsoby poskytnutí údajů, jako například streamování nebo uložení na CD, DVD či jiné fyzické nosiče, nebo aby umožnil přímé předání osobních údajů jinému správci údajů (podle čl. 20 odst. 2 obecného nařízení o ochraně osobních údajů, je-li to technicky proveditelné).

- **Jaká je lhůta stanovená pro odpověď na žádost o přenositelnost?**

Ustanovení čl. 12 odst. 3 stanoví, že správce údajů poskytne subjektu údajů „informace o přijatých opatřeních, a to bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti“. U složitých případů je možné tuto jednoměsíční lhůtu prodloužit

[25] Například pokud je zpracování spojeno s uživatelským účtem, může k identifikaci subjektu údajů stačit poskytnutí příslušného přihlašovacího jména a hesla.
[26] Ustanovení čl. 12 odst. 3: „Správce poskytne subjektu údajů na žádost informace o přijatých opatřeních.“

maximálně na tři měsíce, a to za předpokladu, že subjekt údajů byl o důvodech tohoto odkladu informován do jednoho měsíce od původní žádosti.

Správci působící v oblasti služeb informační společnosti budou pravděpodobně lépe vybaveni na splnění žádostí ve velmi krátké lhůtě. Osvědčeným postupem na splnění očekávání uživatelů je definovat časový rámec, v němž může být na žádost o přenositelnost údajů zpravidla odpovězeno, a sdělit tuto informaci subjektům údajů.

Správci údajů, kteří odmítnou odpovědět na žádost o přenositelnost, musí podle čl. 12 odst. 4 subjekty údajů informovat „o důvodech nepřijetí opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu“, a to nejpozději do jednoho měsíce od přijetí žádosti.

Správci údajů musí dodržovat povinnost odpovědět ve stanovených lhůtách, i když se odpověď týká odmítnutí. Jinými slovy, je-li správce údajů požádán o odpověď na žádost o přenositelnost údajů, musí se vyjádřit.

- **V jakých případech může být žádost o přenositelnost údajů zamítnuta nebo kdy za ní může být účtován poplatek?**

Článek 12 správcům údajů zakazuje účtovat poplatek za poskytnutí osobních údajů, ledaže může správce doložit, že žádosti jsou zjevně nedůvodné nebo nepřiměřené, „zejména pro jejich opakující se povahu“. V případě služeb informační společnosti specializujících se na automatizované zpracování osobních údajů může zavádění automatizovaných systémů jako například rozhraní pro programování aplikací (API)[27] usnadnit výměny se subjektem údajů, a tím snížit případnou zátěž plynoucí z opakovaných žádostí. Proto by mělo existovat pouze velmi málo případů, kdy by byl správce údajů schopen odůvodnit odmítnutí dodat požadované informace, dokonce i pokud jde o vícenásobné žádosti o přenositelnost údajů.

Kromě toho při stanovování nepřiměřenosti žádosti by neměly být zohledňovány celkové náklady na procesy vytvořené za účelem odpovědi na žádosti o přenositelnost údajů. Článek 12 obecného nařízení o ochraně osobních údajů se ve skutečnosti zaměřuje na žádosti podané jedním subjektem údajů, nikoliv na celkový počet žádostí obdržených správcem údajů. V důsledku toho by celkové náklady na zavádění systému neměly být účtovány subjektům údajů, ani používány k odůvodnění odmítnutí odpovědět na žádosti o přenositelnost.

V. Jak se musí přenositelné údaje poskytovat?

- **Které očekávané prostředky by měli správci údajů zavést pro poskytování údajů?**

Ustanovení čl. 20 odst. 1 obecného nařízení o ochraně osobních údajů stanoví, že subjekty údajů mají právo předat údaje jinému správci údajů, aniž by tomu správce údajů, kterému byly osobní údaje poskytnuty, bránil.

Takové bránění lze charakterizovat jako jakékoliv právní, technické nebo finanční překážky kladené správcem za účelem vyhnutí se předání nebo opětovného použití subjektem údajů

[27] Aplikačním programovým rozhraním (API) se rozumí rozhraní aplikací nebo internetových služeb, které správci údajů zpřístupnili tak, aby se jiné systémy nebo aplikace mohly spojit s jejich systémy a pracovat s nimi.

nebo jiným správcem údajů, nebo tyto činnosti zdržet. Tímto bráněním mohou být například: poplatky za dodání údajů, nedostatečná interoperabilita nebo přístup k formátu údajů, k rozhraní pro programování aplikací (API), nebo k poskytnutému formátu, nepřiměřený odklad nebo složitost při získávání úplného souboru údajů, záměrné zastírání souboru údajů, nebo konkrétní a zbytečné nebo nepřiměřené požadavky týkající se odvětvové normalizace nebo akreditace[28].

Ustanovení čl. 20 odst. 2 správcům údajů rovněž ukládá povinnost předávat přenositelné údaje jiným správcům přímo, „je-li to technicky proveditelné“.

Technická proveditelnost předání ze strany správce údajů jinému správci údajů pod kontrolou subjektu údajů by měla být posouzena individuálně. Ustanovení 68. bod odůvodnění dále objasňuje limity toho, co je „technicky proveditelné“ a uvádí, že „by to nemělo zakládat povinnost správců údajů zavést nebo zachovávat technicky kompatibilní systémy zpracování“.

Očekává se, že správci osobní údaje předají v interoperabilním formátu, ačkoliv tím jiným správcům údajů nevzniká povinnost tyto formáty podporovat. K přímému předání jedním správcem údajů druhému může tudíž dojít, je-li možná komunikace mezi dvěma systémy, zabezpečeným způsobem[29], a je-li přijímající systém technicky schopen přijmout příchozí údaje. Pokud přímému předání brání technické překážky, správce údajů tyto překážky subjektům údajů vysvětlí, jelikož jinak bude mít jeho rozhodnutí podobný účinek jako odmítnutí přijmout opatření, o něž subjekt údajů požádal (čl. 12 odst. 4).

Na technické úrovni by správci údajů měli prozkoumat a posoudit dva odlišné a vzájemně se doplňující způsoby, jak přenositelné údaje zpřístupnit subjektům údajů nebo jiným správcům údajů:

- přímé předání celkového souboru přenositelných údajů (nebo několika částí globálního souboru údajů),
- automatizovaný nástroj umožňující získávání relevantních údajů.

Druhý způsob mohou správci údajů upřednostňovat v případech zahrnujících složité a velké soubory údajů, jelikož umožňuje získání jakékoliv části souboru údajů, která je pro subjekt údajů v souvislosti s jeho žádostí relevantní, může pomoci minimalizovat rizika a případně umožňuje používání mechanismů pro synchronizaci údajů[30] (např. v souvislosti s pravidelnou komunikací mezi správci údajů). Pro „nového“ správce údajů se může jednat o lepší způsob, jak zajistit dodržování souladu, a může to představovat osvědčený postup při snižování rizik v oblasti ochrany soukromí na straně původního správce údajů.

Tyto dva odlišné a případně vzájemně se doplňující způsoby poskytování relevantních přenositelných údajů mohou být provedeny tím, že se údaje zpřístupní prostřednictvím

[28] Mohou vzniknout i některé legitimní překážky, jako například překážky související s právy a svobodami jiných osob uvedenými v čl. 20 odst. 4, nebo překážky související s bezpečnostní vlastních systémů správců. Je odpovědností správce údajů odůvodnit, proč jsou takové překážky legitimní, a proč nepředstavují bránění ve smyslu čl. 20 odst. 1.

[29] Prostřednictvím ověřené komunikace s nezbytnou úrovní šifrování údajů.

[30] Mechanismus pro synchronizaci může pomoci při plnění obecných povinností podle povinnosti článku 5 obecného nařízení o ochraně osobních údajů, který stanoví, že „osobní údaje musí být (…) přesné a v případě potřeby aktualizované“.

různých prostředků, jako jsou například bezpečný přenos zpráv, server SFTP, zabezpečené rozhraní WebAPI nebo zabezpečený internetový portál. Subjektům údajů by mělo být umožněno, aby k uchovávání a ukládání osobních údajů a k udělení povolení správcům údajů týkajícího se přístupu k osobním údajům a jejich požadovaného zpracování využívali osobní úložiště dat, systémy pro správu osobních údajů[31], nebo jiné druhy důvěryhodných třetích stran.

- **Jaký je očekávaný formát údajů?**

Obecné nařízení o ochraně osobních údajů ukládá správcům údajů povinnost poskytnout osobní údaje požadované fyzickou osobou ve formátu, který podporuje opakované použití. Konkrétně čl. 20 odst. 1 obecného nařízení o ochraně osobních údajů uvádí, že osobní údaje musí být poskytnuty „ve strukturovaném, běžně používaném a strojově čitelném formátu". Ustanovení 68. bodu odůvodnění dále objasňuje, že tento formát by měl být interoperabilní, což je pojem, který je v EU definován[32] jako:

> *schopnost interakce různých nesourodých organizací, která přispívá k dosažení vzájemně prospěšných a dohodnutých společných cílů a zahrnuje sdílení informací a znalostí mezi organizacemi pomocí podnikových procesů, které tyto organizace podporují, na základě výměny údajů mezi jejich systémy IKT.*

Pojmy „strukturovaný", „běžně používaný" a „strojově čitelný" představují soubor minimálních požadavků, které by měly usnadnit interoperabilitu formátu údajů poskytnutých správcem údajů. Tímto způsobem jsou pojmy „strukturovaný, běžně používaný strojově čitelný" specifikacemi prostředků, kdežto interoperabilita představuje žádoucí výsledek.

Ustanovení 21. bod odůvodnění směrnice 2013/37/EU[33,34] definuje „strojově čitelný" jako:

> *formát souboru s takovou strukturou, která umožňuje softwarovým aplikacím v něm snadno nalézt, rozpoznat a získat z něj konkrétní údaje, včetně jednotlivých uvedených fakt a jejich vnitřní struktury. Za strojově čitelné údaje se považují údaje zakódované v souborech strukturovaných ve strojově čitelném formátu. Strojově čitelné formáty mohou být otevřené nebo chráněné vlastnickým právem; mohou být formálně normalizované, či nikoli. Dokumenty ve formě souboru, který toto automatické zpracování omezuje, jelikož údaje z nich nelze získat snadno či vůbec, by za dokumenty ve strojově čitelném formátu být považovány neměly. Členské státy by měly ve vhodných případech podporovat používání otevřených, strojově čitelných formátů.*

Vzhledem k široké škále případných druhů údajů, které mohou být správcem údajů zpracovávány, obecné nařízení o ochraně osobních údajů nestanoví konkrétní doporučení týkající se formátu, v němž mají být údaje poskytovány. Nejvhodnější formát se bude napříč

---

[31] Systémy pro správu osobních údajů (PIMS) viz například stanovisko evropského inspektora ochrany údajů 9/2016 dostupné na https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

[32] Článek 2 rozhodnutí Evropského parlamentu a Rady č. 922/2009/ES ze dne 16. září 2009 o řešeních interoperability pro evropské orgány veřejné správy (ISA) Úř. věst. L 260, 3.10.2009, s. 20.

[33] Kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru.

[34] Glosář EU (http://eur-lex.europa.eu/eli-register/glossary.html) obsahuje podrobnější objasnění očekávání souvisejících s pojmy použitými v těchto pokynech, jako například *strojově čitelný*, *interoperabilita*, *otevřený formát*, *norma* nebo *metadata*.

odvětvími lišit a odpovídající formáty již mohou existovat a měly by vždy být zvoleny tak, aby dosáhly účelu být interoperabilní a aby subjektu údajů umožňovaly vysoký stupeň přenositelnosti. Formáty, které podléhají nákladným omezením v oblasti udělování licencí, nejsou považovány za vhodný přístup.

V 68. bodu odůvodnění se objasňuje, že *„Právo subjektu údajů předat nebo obdržet osobní údaje, které se ho týkají, by nemělo zakládat povinnost správců zavést nebo zachovávat technicky kompatibilní systémy zpracování.“* **Cílem přenositelnosti je tedy vytvořit interoperabilní systémy, nikoliv kompatibilní systémy**[35].

Očekává se, že osobní údaje budou poskytnuty ve formátech, které mají vysokou úroveň abstrakce od jakéhokoliv interního formátu nebo formátu chráněného vlastnickým právem. Přenositelnost údajů jako taková předpokládá dodatečnou úroveň zpracování údajů správci údajů, aby získali údaje z platformy a vyfiltrovali osobní údaje mimo oblast působnosti přenositelnosti, jako např. vyvozené údaje nebo údaje související s bezpečností systémů. Správci údajů jsou tímto způsobem vybízeni k tomu, aby předem identifikovali údaje, které v jejich vlastních systémech spadají do oblasti působnosti přenositelnosti. Toto dodatečné zpracování údajů bude považováno za doplňkové k hlavnímu zpracování údajů, jelikož není prováděno s cílem dosáhnout nového účelu definovaného správcem údajů.

Pokud v daném odvětví nebo v dané souvislosti neexistují žádné běžně používané formáty, **měli by správci údajů osobní údaje poskytnout za použití běžně používaných otevřených formátů (např. XML, JSON, CSV atd.), spolu s užitečnými metadaty, v co nejlepší možné úrovni rozčlenění** a při zachování vysoké úrovně abstrakce. Vhodná metadata by měla být použita na přesný popis významu vyměňovaných informací. Tato metadata by měla stačit k tomu, aby umožnila fungování a opětovné použití údajů, ale samozřejmě aniž by vyzrazovala obchodní tajemství. Je proto nepravděpodobné, že poskytnou-li se fyzické osobě PDF verze příchozích e-mailů, budou dostatečně strukturované nebo deskriptivní na to, aby umožnily snadné opětovné použití údajů z došlé pošty. Aby bylo umožněno účinné opětovné použití údajů, měly by být tyto údaje z e-mailového účtu poskytnuty ve formátu, který zachovává veškerá metadata. Při volbě formátu údajů, v němž budou osobní údaje poskytnuty, by měl správce údajů zvážit, jak by tento formát ovlivnil právo fyzické osoby opětovně použít údaje nebo jak by mu bránil. V případech, kdy je správce údajů schopen subjektu údajů poskytnout možnost volby týkající se upřednostňovaného formátu osobních údajů, by mělo být rovněž poskytnuto jasné vysvětlení dopadu jeho volby. Zpracovávání dodatečných metadat výhradně na jediný účel, že mohou být potřebné nebo žádoucí pro odpověď na žádost o přenositelnost údajů, však nepředstavuje žádný oprávněný základ pro takové zpracování.

Pracovní skupina WP29 silně podporuje spolupráci mezi zúčastněnými stranami z odvětví a oborovými sdruženími, aby spolu vypracovaly společný soubor interoperabilních norem a formátů pro splnění požadavků práva na přenositelnost údajů. Touto výzvou se řešil rovněž v Evropském rámci interoperability (EIF), který vytvořil schválený přístup k interoperabilitě pro organizace, jež si přejí společně dodávat veřejné

[35] Norma ISO/IEC 2382-01 definuje interoperabilitu takto: „Schopnost komunikovat, provádět programy nebo předávat údaje mezi různými funkčními jednotkami způsobem, který od uživatele žádá pouze malou nebo žádnou znalost jedinečných vlastností těchto jednotek.“

služby. V tomto rámci se v rozsahu jeho uplatňování stanovuje soubor společných prvků, jako jsou terminologie, pojmy, zásady, pokyny, doporučení, normy, specifikace a postupy[36].

- **Jak přistupovat k velkým nebo komplexním souborům osobních údajů?**

Obecné nařízení o ochraně osobních údajů nevysvětluje, jak řešit problém, který představuje reagování v případech velkého shromažďování údajů, složité struktury údajů, nebo v případech, kdy vyvstanou jiné technické problémy, které mohou správcům údajů nebo subjektům údajů způsobit potíže.

Ve všech případech je však klíčové, aby byla fyzická osoba v pozici, jež jí umožní plně chápat definici, schéma a strukturu osobních údajů, které mohou být správcem údajů poskytnuty. Údaje například mohou být nejprve poskytnuty v souhrnné formě za použití přehledů umožňujících subjektu údajů převádět podskupiny osobních údajů namísto všech osobních údajů. Správce údajů by měl přehled poskytnout „stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků“ (viz čl. 12 odst. 1 obecného nařízení o ochraně osobních údajů) a tak, aby měl subjekt údajů vždy jasné informace o tom, jaké údaje si v souvislosti s daným účelem lze stáhnout nebo převést jinému správci údajů. Subjekty údajů by například měly být schopny použít softwarové aplikace pro snadnou identifikaci, rozpoznání a zpracování konkrétních údajů z těchto aplikací.

Jak bylo uvedeno výše, praktickým způsobem, kterým může správce údajů odpovědět na žádosti o přenositelnost údajů, může být nabízení odpovídajícím způsobem zabezpečených a zdokumentovaných rozhraní pro programování aplikací (API). To může fyzickým osobám umožnit podávat správci žádosti o jejich osobní údaje prostřednictvím svého vlastního programového vybavení nebo programového vybavení třetích stran, nebo jiným osobám (včetně jiného správce údajů) udělovat povolení, aby tak učinily jejich jménem, jak je uvedeno v čl. 20 odst. 2 obecného nařízení o ochraně osobních údajů. Udělením přístupu k údajům prostřednictvím rozhraní pro programování aplikací (API) přístupného zvnějšku bude rovněž možné nabídnout sofistikovanější systém přístupu, který fyzickým osobám umožní podávat další žádosti o údaje, a to buď v podobě stažení úplného souboru údajů, nebo v podobě funkce delta obsahující pouze změny od posledního stažení, bez toho, aby tyto dodatečné žádosti představovaly pro správce údajů zátěž.

- **Jak lze přenositelné údaje zabezpečit?**

Obecně by správci údajů měli podle čl. 5 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů zaručit „náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením“.

Předání osobních údajů subjektu údajů však může rovněž nastolit určité bezpečnostní otázky:

Jak mohou správci údajů zajistit, že byly osobní údaje bezpečně doručeny správné osobě?

Jelikož cílem přenositelnosti údajů je dostat osobní údaje ven z informačního systému správce údajů, předání se může stát v souvislosti s těmito údaji možným zdrojem rizika (zejména

[36] Zdroj: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

porušení ochrany údajů během předání). Správce údajů je odpovědný přijmout veškerá bezpečnostní opatření potřebná na to, aby zajistil nejen bezpečný přenos (za použití šifrování mezi koncovými body nebo šifrování údajů) na správné místo určení (za použití silných ověřovacích opatření), ale také nepřetržitou ochranu osobních údajů, které zůstaly v jeho systémech, jakož i transparentní postupy pro řešení případných porušení ochrany údajů[37]. Správci údajů by měli posoudit konkrétní rizika spojená s přenositelností údajů a přijmout náležitá opatření ke zmírnění rizik.

Tato opatření ke zmírnění rizik mohou zahrnovat: pokud je už nutné ověřit totožnost subjektu údajů, použití dodatečných ověřovacích informací, jako například sdíleného klíče nebo jiného faktoru ověřování, jako například jednorázového hesla; pozastavení nebo zmrazení předání, existuje-li podezření, že účet byl ohrožen; v případech přímého předání jedním správcem údajů druhému správci údajů by mělo být použito ověření na základě pověření, jako například tzv. ověřování pomocí tokenů.

Tato bezpečnostní opatření nesmí mít omezující charakter a nesmí uživatelům bránit v uplatňování jejich práv, např. zavedením dodatečných výdajů.

Jak uživatelům pomoci při zabezpečení uložiště osobních údajů v jejich vlastních systémech?

Tím, že uživatelé od on-line služby získají své osobní údaje, vzniká vždy riziko, že si je mohou uložit do systému, který je méně zabezpečený než systém poskytovaný službou. Za identifikaci správných opatření k zabezpečení osobních údajů ve vlastním systému je vždy odpovědný subjekt údajů požadující údaje. Měl by na to však být upozorněn, aby mohl přijmout opatření k ochraně informací, které získal. Jakožto příklad osvědčeného postupu mohou správci údajů rovněž doporučovat vhodné formáty, šifrovací nástroje a další bezpečnostní opatření, aby subjektu údajů pomohli dosáhnout tohoto cíle.

* * *

V Bruselu dne 13. prosince 2016

Za pracovní skupinu
Předsedkyně
Isabelle FALQUE-PIERROTIN

Naposledy revidováno a přijato dne 5. dubna 2017

Za pracovní skupinu
Předsedkyně
Isabelle FALQUE-PIERROTIN

[37] V souladu se směrnicí (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.