PRACOVNÍ SKUPINA PODLE ČLÁNKU 29

16/EN
WP 242 rev. 01

Vodítka k právu na přenositelnost údajů

Schváleno dne 13. prosince 2016

Revize schválena 5. dubna 2017

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytlo Generální ředitelství Spravedlnost a spotřebitelé Evropské Komise, B-1049 Brusel, Belgie, kancelář č. MO59 05/35.

Internetové stránky: http://ec.europa.eu/justice/data-protection/index_cs.htm

OBSAH

Shrnutí

Článek 20 Obecného nařízení o ochraně osobních údajů nově zavádí právo na přenositelnost údajů, které má úzkou vazbu k právu na přístup, avšak liší se od něho v mnoha aspektech. Subjekty údajů jsou oprávněny získat osobní údaje, které poskytly správci ve strukturovaném, běžně používaném a strojově čitelném formátu a předat je jinému správci. Toto nové právo má posílit postavení subjektu údajů a dát mu větší kontrolu nad osobními údaji, které se ho týkají.

Jelikož umožní přímé předání osobních údajů od jednoho správce jinému, představuje právo na přenositelnost údajů významný nástroj, který podpoří volný pohyb osobních dat v EU a přispěje k soutěži mezi správci. Usnadní také přechod mezi různými poskytovateli služeb, čímž podpoří vývoj nových služeb v kontextu strategie jednotného digitálního trhu.

Toto stanovisko poskytuje návod jak vykládat a naplňovat právo na přenositelnost údajů zavedené Obecným nařízením o ochraně osobních údajů. Probírá právo na přenositelnost a jeho rozsah. Vyjasňuje podmínky, za kterých je toto nové právo uplatnitelné s přihlédnutím k právnímu základu pro zpracování dat (souhlas subjektu údajů nebo potřeba naplnit smlouvu) a ke skutečnosti, že toto právo je omezeno na osobní údaje poskytnuté subjektem údajů. Přináší rovněž konkrétní příklady a kritéria pro objasnění podmínek, za kterých toto právo může být využito. V tomto ohledu se Pracovní skupina podle článku 29 (WP29) domnívá, že právo na přenositelnost údajů se vztahuje na data vědomě a aktivně poskytnutá subjektem údajů a na data vytvořená prostřednictvím jeho činnosti. Toto nové právo nemůže být podkopáno a omezeno na osobní informace subjektem údajů přímo oznámené, například po internetu na elektronickém formuláři.

Správci by měli začít vyvíjet prostředky k uspokojování žádostí o přenos dat, jako jsou nástroje pro stahování souborů a rozhraní pro programování aplikací. Měli by zaručit předávání osobních údajů ve strukturovaném, běžně používaném a strojově čitelném formátu a měli by být pobízeni k zajištění vzájemné použitelnosti (interoperability) datového formátu použitého při vyřízení žádosti o přenos údajů.

Tento dokument má také správcům pomoci jasně porozumět svým povinnostem a doporučit příklady osvědčené praxe a nástroje podporující soulad s právem na přenositelnost údajů. A nakonec, toto stanovisko doporučuje, aby zainteresované strany z dotčených odvětví a obchodní asociace spolupracovaly na tvorbě vzájemně použitelných standardů a formátů a dostály tak požadavkům práva na přenositelnost údajů.

I. Úvod

Článek 20 Obecného nařízení o ochraně osobních údajů (dále jen „Obecné nařízení“) zavádí jako novinku právo na přenositelnost údajů. Subjekty údajů dostávají právo získat osobní údaje, které poskytly správci ve strukturovaném, běžně používaném a strojově čitelném formátu a předat tyto údaje bez překážek jinému správci. Toto právo, které je uplatnitelné za jistých podmínek, podporuje uživatelský výběr a kontrolu a posiluje postavení uživatele.

Jednotlivci uplatňující právo na přístup podle směrnice 95/46/ES byli omezováni formátem, který správce zvolil pro poskytnutí vyžádané informace. **Nové právo na přenositelnost údajů má posílit postavení subjektů údajů ve vztahu k vlastním osobním datům, jelikož jim usnadní přesouvání, kopírování nebo přenášení osobních údajů z jednoho IT prostředí do druhého** (ať už do svých vlastních systémů nebo do systémů důvěryhodných třetích stran či nových správců).

Toto právo představuje rovněž příležitost vyrovnat vztah mezi subjekty údajů a správci stvrzením osobních práv jednotlivců a jejich kontroly nad osobními údaji, které se jich týkají[1].

Byť právo na přenositelnost osobních údajů může také posílit soutěž mezi službami (usnadněním přechodu mezi nimi), Obecné nařízení reguluje osobní údaje a nikoliv soutěž. Konkrétně článek 20 neomezuje data podléhající přenositelnosti pouze na taková, která jsou nezbytná nebo užitečná pro přechod mezi službami[2].

I když je přenositelnost údajů novým právem, existují už jiné typy přenositelnosti nebo se o nich diskutuje v jiných oblastech legislativy (například v souvislosti s ukončením smlouvy, roamingem v komunikačních službách nebo přeshraničním přístupem ke službám [3]). Kombinované uplatnění různých typů přenositelnosti může vyvolat synergické efekty a dokonce přinést výhody jednotlivcům, byť s analogiemi by mělo být zacházeno opatrně.

Toto stanovisko poskytuje správcům vodítko jak upravit své zvyklosti, postupy a politiky a objasňuje význam přenositelnosti údajů, aby subjekty údajů byly schopny účinně využít nového práva.

II. Jaké jsou hlavní prvky přenositelnosti údajů?

Obecné nařízení definuje právo na přenositelnost údajů v článku 20, odst. 1 následovně:

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**

Přenositelnost údajů je v první řadě **právo subjektu údajů získat určitý podsoubor osobních údajů**, jež se ho týkají, zpracovaných správcem a uchovávat je pro další osobní použití. Uložena mohou tato data být na soukromém zařízení nebo v soukromém cloudu, aniž by nutně musela být předána jinému správci.

V tomto ohledu přenositelnost údajů doplňuje právo na přístup. Jedna zvláštnost přenositelnosti údajů spočívá ve skutečnosti, že nabízí subjektům údajů snadný způsob, jak samy mohou spravovat a znovu využívat osobní údaje. Tyto údaje mají být ve *„ve strukturovaném, běžně používaném a strojově čitelném formátu“*. Například může mít subjekt údajů zájem získat svůj aktuální playlist (historii poslouchaných skladeb) z hudebního přenosu přes internet, aby zjistil, kolikrát si pustil určitou skladbu nebo se podíval, jakou hudbu si chce koupit nebo poslouchat na jiné platformě. Může také chtít získat přehled kontaktů ze své webmailové aplikace, například kvůli sestavení seznamu svatebních hostů nebo získání informace o nákupech přes různé věrnostní karty, či posouzení své uhlíkové stopy[4].

---

[1] Prvořadým cílem přenositelnosti údajů je zlepšit kontrolu, kterou jednotlivci nad svými osobními údaji mají a zajistit, aby hráli aktivní úlohu v datovém prostředí.

[2] Toto právo může například bankám umožnit poskytnutí doplňkových služeb, pod kontrolou uživatele, využitím osobních údajů původně shromážděných v rámci energetické služby.

[3] Viz agenda Evropské komise pro jednotný digitální trh: http://ec.europa.eu/digital-agenda/en/digital-single-market, především první politický pilíř „Lepší přístup k výrobkům a službám online“.

[4] Zpracování dat prováděné subjektem údajů může v těchto případech spadat buď do kategorie činnosti v domácnosti, pokud veškeré zpracování je prováděno pod kontrolou pouze subjektu údajů, nebo může být vykonáno jinou stranou, ve prospěch subjektu údajů. V posledně jmenovaném případě by jiná strana měla být považována za správce, byť jen pro pouhý účel uchování osobních údajů a jako taková musí vyhovět zásadám a povinnostem stanoveným v Obecném nařízení.

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

Článek 20, odst. 1 dále vybavuje subjekty údajů **právem přenést osobní údaje od jednoho správce jinému správci** „aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil“. Data mohou také být přenesena přímo od jednoho správce druhému na žádost subjektu údajů a je-li to technicky proveditelné (Článek 20, odst. 2). V tomto ohledu recitál 68 vyzývá k podpoře správců při vývoji interoperabilních formátů umožňujících přenositelnost údajů[5], aniž by ovšem zakládalo povinnost správců zavést nebo zachovávat technicky kompatibilní systémy zpracování[6]. Obecné nařízení však správcům zakazuje klást přenosům překážky.

Tento prvek přenositelnosti údajů v podstatě dává subjektům údajů možnost data nejenom získat a znovu použít, ale také je předat jinému poskytovateli služeb (ve stejném oboru podnikání nebo v jiném). Kromě posílení pozice spotřebitelů zamezením efektu zaháčkování u jednoho poskytovatele (lock-in), je počítáno s přínosem ve smyslu příležitostí pro inovace a sdílení osobních údajů mezi správci chráněným a zabezpečeným způsobem pod kontrolou subjektem údajů[7]. Přenositelnost údajů může podpořit kontrolované a ohraničené sdílení (ze strany uživatelů) osobních údajů mezi organizacemi a obohatit tak služby a zákaznické zážitky[8]. Přenositelnost údajů může napomoci přenosu a opětovnému použití osobních údajů uživatelů mezi různými službami, o které mají zájem.

- **Správcovství**

Přenositelnost údajů zaručuje právo získat osobní údaje a zpracovávat je podle přání subjektu údajů[9].

Správci reagující na žádost o přenos údajů za podmínek stanovených v článku 20, nejsou odpovědni za zpracování vykonávané subjektem údajů nebo jinou společností, která osobní údaje získala. Jednají jménem subjektu údajů i v případech, kdy osobní údaje jsou přímo přenášeny jinému správci. V tomto ohledu není správce odpovědný za to, že přijímající správce bude v souladu s právními předpisy pro ochranu osobních údajů, neboť odesílající správce není tím, kdo vybírá příjemce. Současně by měl správce zavést opatření zaručující, že bude jednat skutečně v zájmu subjektu údajů. Může například zavést postupy zajišťující, že bude přenášen přesně ten druh dat, jaký si subjekt údajů přeje. To lze splnit získáním potvrzení od subjektu údajů buď před přenosem, nebo ještě dříve, v okamžiku kdy je získán původní souhlas se zpracováním nebo je naplněna smlouva.

Správci reagující na žádost o přenos údajů nemají žádnou konkrétní povinnost kontrolovat a ověřovat kvalitu dat před jejich přenosem. Data by ovšem měla už být přesná a aktualizovaná, podle zásad uvedených v Obecném nařízení v článku 5, odst. 1. Přenositelnost údajů neukládá správci povinnost uchovávat osobní údaje déle, než je nezbytné nebo stanovené konkrétní lhůtou[10]. Důležité je si uvědomit, že nevzniká žádný

[5] Viz také kapitola V.

[6] Zvláštní pozornost je tedy potřeba věnovat formátu přenášených dat, aby bylo zajištěno, že data budou opětovně použitelná, bez velkého úsilí, subjektem údajů nebo dalším správcem. Viz také kapitola V.

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

[8] Takzvané kvantifikované já a internet věcí jsou fenomény ukazující výhody (a rizika) spojování osobních údajů z různých oblastí lidského života, jako je sledování fitness aktivity a kalorického příjmu, což poskytuje úplnější obraz života jednotlivce v jednom jediném souboru.

[9] Právo na přenositelnost údajů není omezeno na osobní údaje, které jsou užitečné nebo důležité pro podobné služby poskytované konkurenty správce.

[10] V případě výše uvedeném platí, že neuchovává-li správce záznam o uživatelem přehrávaných písních, nemohou tyto osobní údaje být zahrnuty do žádosti o přenos.

dodatečný požadavek uchovávat data po dobu delší, než jinak uplatňované lhůty, jen kvůli případné budoucí žádosti o přenos údajů.

Jsou-li požadované osobní údaje zpracovány zpracovatelem, musí smlouva uzavřená v souladu s článkem 28 Obecného nařízení obsahovat povinnost být „správci nápomocen prostřednictvím vhodných technických a organizačních opatření, (…) reagovat na žádosti o výkon práv subjektu údajů“. Správce by tedy měl ve spolupráci se svými zpracovateli zavést konkrétní postupy pro vyřizování žádostí o přenos dat. V případě společného správcovství by smlouva měla jasně rozdělit mezi jednotlivé správce povinnosti související s žádostmi o přenos dat.

Zároveň platí, že je v odpovědnosti přijímajícího správce[11] zajistit, aby předané osobní údaje byly relevantní a nebyly nepřiměřené vzhledem k novému zpracování. Například v případě žádosti týkající se webmailové služby, kdy právo na přenositelnost údajů je využito subjektem údajů k získání emailů a jejich odeslání na zabezpečenou platformu pro archivaci, nepotřebuje nový správce zpracovávat kontaktní údaje adresátů dotyčného subjektu údajů. Není-li tato informace důležitá s ohledem k účelu nového zpracování, neměla by být uchována a zpracována. Přijímající správci každopádně nejsou povinni akceptovat a zpracovat osobní údaje předané na základě žádosti podle práva na přenositelnost. Obdobně, když subjekt údajů požádá o předání informací o svých bankovních transakcích společnosti pomáhající mu s peněžní správou, nemusí nový (přijímající) správce přijmout všechny údaje nebo uchovávat veškeré podrobnosti o bankovních převodech, pokud byly označeny pro účely nové služby. Jinými slovy, akceptovaná a uchovaná by měla být pouze ta data, která jsou nezbytná a vztahují se ke službě poskytované přijímajícím správcem.

Přijímající organizace se stává novým správcem získaných osobních údajů a musí dodržovat zásady uvedené v článku 5 Obecného nařízení. Nový, přijímající správce musí tedy jasně a přímo uvést účel nového zpracování ještě před podáním jakékoli žádosti o předání údajů podle práva na přenositelnost v souladu s požadavky transparentnosti vyložených v článku 14[12]. Stejně jako u jiných zpracování dat v odpovědnosti správce, musí tento uplatnit zásady stanovené v článku 5, jako je zákonnost, korektnost a transparentnost, účelové omezení, minimalizace údajů, přesnost, celistvost a důvěrnost, omezenost doby uložení a odpovědnost[13].

Správci držící osobní údaje by měli být připraveni usnadnit svým subjektům údajů uplatnění práva na přenositelnost údajů. Správci se také mohou rozhodnout přijmout data od subjektu údajů, ale není to jejich povinnost.

- **Přenositelnost údajů versus ostatní práva subjektu údajů**

Pokud jednotlivec uplatňuje právo na přenositelnost údajů, činí tak bez dopadu na jakékoli jiné právo (podobně jako v případě kterýchkoli jiných práv v Obecném nařízení). Subjekt údajů může nadále využívat služby správce a mít z nich prospěch i po uskutečnění operace datového přenosu. Přenositelnost údajů nespouští automaticky výmaz dat[14] ze systémů správce a nemá vliv na původní lhůtu pro uchování dat předaných podle

[11] Tj. toho, který obdrží osobní údaje na základě žádosti podle práva na přenositelnost, kterou subjekt údajů uplatnil vůči jinému správci

[12] Kromě toho by nový správce neměl zpracovávat osobní údaje, které nejsou relevantní, přičemž zpracování musí být omezeno jen na to, co je nezbytné pro nové účely a to tehdy, jsou-li osobní údaje součástí širší sady dat předávané v rámci procesu přenositelnosti. Osobní údaje, které nejsou nutné z hlediska účelu nového zpracování, by měly být co nejdříve vymazány.

[13] Data obdržená správcem na základě žádosti o přenos mohou být považována za „poskytnutá“ subjektem údajů a mohou být předána znovu v souladu s právem na přenositelnost údajů, v rozsahu takovém, aby byly splněny další podmínky uplatnitelné v rámci tohoto práva (např. právní základ pro zpracování,…).

[14] Jak uvedeno v článku 17 Obecného nařízení.

práva na přenositelnost. Subjekt údajů může svá práva uplatnit kdykoli po celou dobu, po kterou správce údaje zpracovává.

Stejně tak, chce-li subjekt údajů uplatnit právo na výmaz („právo být zapomenut“ podle článku 17), nemůže správce argumentovat právem na přenositelnost jako důvodem pro odložení nebo odmítnutí požadovaného výmazu.

Zjistí-li subjekt údajů, že data vyžádaná podle práva na přenositelnost neodpovídají plně žádosti, mělo by být plně vyhověno jakémukoli dalšímu požadavku na osobní údaje podle práva na přístup v souladu s článkem 15 Obecného nařízení.

Pokud nějaký právní předpis, evropský nebo členského státu, z jiné oblasti obsahuje nějakou formu přenositelnosti dotčených údajů, musí být podmínky stanovené těmito konkrétními předpisy také zohledněny při vyřizování žádosti o přenos dat podle Obecného nařízení. Pokud je ze žádosti podané subjektem údajů jasné, že jeho záměrem není uplatnit práva podle Obecného nařízení, nýbrž jen podle sektorové legislativy, pak ustanovení Obecného nařízení ohledně přenositelnosti údajů nebudou v případě této žádosti použita[15]. Na druhé straně, pokud je žádost zaměřena na přenositelnost podle Obecného nařízení, pak taková zvláštní legislativa nemá u žádného správce přednost před obecným uplatněním zásady přenositelnosti údajů, jak je stanovena v Obecném nařízení. Je nutné posoudit, případ od případu, jaký, pokud vůbec, může taková zvláštní legislativa mít vliv na právo na přenositelnost údajů.

III. Kdy je právo na přenositelnost uplatnitelné ?

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

Podle Obecného nařízení musí mít správce pro zpracování osobních údajů jasný právní základ.

V souladu s článkem 20, odst. 1, písm. a) Obecného nařízení **musí zpracování, aby se na ně vztahovalo právo na přenositelnost údajů, být založeno:**

- na souhlasu subjektu údajů (podle článku 6, odst. 1, písm. a) nebo podle článku 9, odst. 2, písm. a), jedná-li se o zvláštní kategorie osobních údajů), nebo
- na smlouvě jejíž smluvní stranou subjekt údajů je, podle článku 6, odst. 1, písm. b.

Jako další příklad údajů podléhajících přenositelnosti lze uvést tituly knih zakoupených jednotlivcem v internetovém knihkupectví nebo seznam písní poslouchaných přes internetovou hudební službu, neboť tyto informace jsou zpracovány na základě plnění smlouvy, jehož stranou je subjekt údajů.

Obecné nařízení neustanovuje obecné právo na přenositelnost pro případy, kde zpracování osobních údajů není založeno na souhlasu nebo smlouvě[16]. Například, finanční instituce nemusí vyhovět žádosti o přenos osobních údajů zpracovávaných v rámci jejich povinnosti

[15] Pokud například bude žádost subjektu údajů mířit konkrétně na poskytnutí přístupu k historii jeho bankovního účtu pro poskytovatele služeb informování o účtu za účelem uvedeným ve Směrnici o platebních službách na vnitřním trhu (PSD2), měl by podle ustanovení této směrnice být tento přístup umožněn.

[16] Viz recitál 68 a článek 20, odst. 3, Obecného nařízení. Článek 20, odst. 3 a recitál 68 stanoví, že přenositelnost údajů se nevztahuje na případy, kdy zpracování údajů je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen nebo pokud správce plní veřejné nebo právně stanovené povinnosti. V takových případech není správce povinen vyhovět požadavku přenositelnosti. Je však osvědčeným postupem ustavit procedury pro automatické vyřizování žádostí o přenos podle zásad stanovených pro přenositelnost údajů. Příkladem může být státní služba umožňující snadné stažení dříve podaných daňových přiznání. Přenositelnost údajů jako příklad osvědčené praxe u případů zpracování založených na nezbytnosti v legitimním zájmu a stávající dobrovolné modely jsou pojednány na stránkách 47 – 48 Stanoviska 6/2014 k pojmu o oprávněných zájmech (WP217) vypracovaného skupinou WP29.

prevence a odhalování případů praní špinavých peněz a dalších peněžních zločinů; stejně tak se přenositelnost údajů nevztahuje na pracovní kontakty zpracovávané v rámci obchodních vztahů v případech, kdy toto zpracování není opřeno ani o souhlas subjektu údajů, ani o smlouvu, kteréžto je smluvní stranou.

Jedná-li se o zaměstnanecká data, právo na přenositelnost údajů se typicky uplatní pouze, pokud je zpracování založeno na smlouvě, jejíž stranou subjekt údajů je. V této souvislosti se vyskytne řada případů, kdy souhlas nebude možné považovat za svobodně udělený vzhledem k nerovnovážnému postavení zaměstnavatele a zaměstnance [17]. Některá zpracování personalistických dat jsou opřena o právní důvod legitimního zájmu nebo jsou nezbytná pro splnění zvláštních, zákonem stanovených povinností, v oblasti zaměstnávání. V praxi se právo na přenositelnost v oblasti personalistiky bude nepochybně týkat mnoha jiných operací (jako třeba výplaty a náhrady, vnitřní nábor zaměstnanců), avšak v mnoha jiných situacích bude potřeba případ od případu ověřit, zda jsou splněny všechny podmínky týkající se práva na přenositelnost údajů.

Kromě toho, právo na přenositelnost údajů se vztahuje pouze na zpracování prováděná „automatizovanými prostředky" a netýká se tedy většiny papírových svazků.

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

Podle článku 20, odst. 1 musí data, aby spadala pod právo na přenositelnost:
- být údaji, které se týkají subjektu údajů
- být údaji, které subjekt údajů *poskytl* správci

Článek 20, odst. 4 dále stanoví, že splnění tohoto práva nemá mít negativní dopad do práv a svobod jiných osob.

<u>První podmínka: osobní údaje týkající se subjektu údajů</u>

Žádost podle práva na přenositelnost se může vztahovat jen na osobní údaje. Proto veškerá data, která jsou anonymní [18] nebo se netýkají subjektu údajů, nespadají pod právo na přenositelnost. Avšak na pseudonymní údaje, které mohou být jasně vztaženy k subjektu údajů (např. pokud subjekt údajů poskytne příslušný identifikátor, srovnej s článkem 11, odst. 2) se přenositelnost zcela jistě vztahuje.

V mnoha případech správci zpracovávají informace obsahující osobní údaje několika subjektů údajů. V takovém případě nemusí brát správci příliš restriktivně větu „osobní údaje týkající se subjektu údajů". Například záznamy telefonních hovorů, textování mezi osobami nebo hlasových služeb (VoIP) mohou obsahovat (ve výpisu volání) informace o třetích stranách účastnících se příchozích nebo odchozích hovorů. Ačkoliv záznamy v takovém případě budou obsahovat osobní údaje týkající se více osob, zákazník by je měl na základě žádosti podle páva přenositelnosti dostat, neboť tyto záznamy se (také) týkají subjektu údajů. Pokud však mají být tyto výpisy předány novému správci, neměl by je tento nový správce zpracovávat za žádným účelem, který by nepříznivě dopadl do práv a svobod třetích stran (viz níže: třetí podmínka).

<u>Druhá podmínka: data poskytnutá subjektem údajů</u>

Druhá podmínka zužuje rozsah dat poskytnutých subjektem údajů.

[17] Jak WP29 nastínila ve 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_en.pdf

Existuje mnoho příkladů dat, která jsou vědomě a aktivně poskytnuta subjektem údajů (např. emailová adresa, uživatelské jméno, věk) prostřednictvím online formuláře. Nicméně údaje „poskytnuté" subjektem údajů jsou rovněž výsledkem sledování jeho činnosti. WP29 se proto domnívá, že má-li toto nové právo být plnohodnotné, měl by výraz „poskytnutý" zahrnovat také osobní údaje získané sledováním činnosti uživatelů, jako jsou surová data zpracovávaná chytrými měřiči nebo jinými typy propojených předmětů[19], logy (záznamy) činností, historie navštívených webových stránek a vyhledávání na internetu.

Tato posledně jmenovaná kategorie nezahrnuje údaje vytvořené správcem (užitím vysledovaných nebo vstupních dat) jako je uživatelský profil sestavený na základě analýzy surových dat shromážděných z chytrého měření.

Pro určení, zda právo na přenositelnost je uplatnitelné, lze rozlišovat mezi různými kategoriemi dat v závislosti na jejich původu. Následující kategorie dat mohou být považovány za „poskytnuté subjektem údajů":

- **data aktivně a vědomě poskytnutá subjektem údajů** (např. emailová adresa, uživatelské jméno, věk atd.),
- **vysledovaná data poskytnutá subjektem údajů na základě využívání služby nebo zařízení**. Sem může patřit třeba vyhledávací historie, provozní a lokační údaje nebo také surová data jako tepová frekvence sbíraná pomocí nositelného zařízení.

Naproti tomu, dovozená nebo odvozená data jsou vytvářena správcem na základě údajů „poskytnutých subjektem údajů". Například výsledek zdravotního posudku uživatele nebo profilu vytvořeného v souvislosti s řízením rizika a finančních předpisů (např. přidělení úvěrového skóre nebo vyhovění předpisům proti praní špinavých peněz) nemůže sám o sobě být považován za „poskytnutá" subjektem údajů. I když taková data mohou být součástí profilu uchovávaného správcem a jsou dovozena nebo odvozena analýzou dat poskytnutých subjektem údajů (kupříkladu prostřednictvím jeho činnosti), nebudou tato data typicky brána jako „poskytnutá subjektem údajů" a tedy se na ně toto nové právo nebude vztahovat[20].

Obecně, vzhledem k záměru práva na přenositelnost, musí být výraz „poskytnutý subjektem údajů" vykládán široce s vyloučením pouze kategorií „dovozená data" a „odvozená data", které zahrnují osobní údaje vytvářené správcem (např. výsledky algoritmických postupů). Správce může tato dovozená data vyjmout, měl by však zahrnout všechny další osobní údaje poskytnuté subjektem údajů cestou technických prostředků daných k dispozici správcem.[21]

Slovo „poskytnutý" pokrývá tedy osobní údaje vztahující se k činnosti subjektu údajů nebo které jsou výsledkem sledování chování jednotlivce, nikoliv však následné analýzy tohoto chování. Naproti tomu, osobní údaje, které správce vytvořil v rámci zpracování, např. v procesu personalizace nebo doporučení podle kategorizace nebo profilování uživatele,

[19] Subjekt údajů, možností dostat data vyplývající ze sledování jeho činnosti, může také získat lepší přehled o správcem nabízeném výběru ohledně rozsahu sledovaných dat a ocitne se v lepší pozici při rozhodování, která data chce poskytnout pro získání podobné služby a získá lepší povědomí o míře respektu vůči jeho soukromí.

[20] Nicméně, subjekt údajů může i nadále využít svého práva „získat od správce 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" stejně jako má právo na informaci 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" podle článku 15 Obecného nařízení (který pojednává o právu na přístup).

[21] Patří sem veškerá data sesbíraná o subjektu údajů během činnosti, za jejímž účelem jsou data shromažďována, jako třeba transakční historie nebo přístupové logy. Data shromážděná cestou sledování a nahrávání (např. aplikace zaznamenávající srdeční tep nebo technologie sledující zvyklosti uživatele internetového vyhledávače) by také měla být považována za „jím poskytnutá", byť tato data nejsou vědomě nebo aktivně předávána.

jsou data odvozená nebo dovozená z údajů poskytnutých subjektem údajů a právo na přenositelnost se tak na ně nevztahuje.

Třetí podmínka: právo na přenositelnost nemá nepříznivě ovlivňovat práva a svobody ostatních

Ve vztahu k osobním datům týkajících se jiných subjektů údajů:
Třetí podmínka má zamezit získávání a přenosu informací zahrnujících osobní údaje jiných subjektů údajů (jež neposkytly souhlas) novému správci v situacích, kdy by tato data mohla být zpracována způsobem nepříznivě dopadajícím do práv a svobod jiných subjektů údajů (Obecné nařízení, článek 20, odst. 4)[22].

Takový nepříznivý dopad by mohl nastat třeba při přenosu dat od jednoho správce jinému podle práva na přenositelnost, pokud by to zabránilo třetím stranám uplatnit svá práva coby subjekty údajů podle Obecného nařízení (právo na informace, přístup, atd.).

Subjekt údajů, který spustí přenos dat jinému správci, buď udělí souhlas se zpracováním novému správci, nebo s ním vstoupí do smluvního vztahu. Pokud jsou v datovém souboru údaje třetích stran, je třeba dále zdůvodnit právoplatnost zpracování. Například, podle článku 6 odst. 1, písm. f oprávněným zájmem správce může být poskytování služby subjektu údajů, která tomuto subjektu umožní osobní údaje zpracovávat v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti. Zpracovatelské operace prováděné subjektem údajů v souvislosti s jeho osobní činností, která se týká třetích stran a může na ně mít dopad, zůstávají potud v jeho odpovědnosti, pokud o tomto zpracování žádným způsobem nerozhoduje správce.

Webmailová služba, například, může umožňovat sestavení seznamu kontaktů subjektu údajů, přátel, příbuzných, zkrátka osob z rodinného i širšího okruhu. Tato data se vztahují (a jsou vytvořena) identifikovatelným jednotlivcem, který si přeje uplatnit právo na přenositelnost, proto by správci měli subjektu údajů přenést celý adresář příchozích a odchozích e-mailů.

Obdobně bankovní účet subjektu údajů může obsahovat osobní údaje související s transakcemi nejenom držitele účtu, ale také informace o dalších jednotlivcích (pokud například převedli peníze na účet daného držitele). V této souvislosti je nepravděpodobné, že by práva a svobody těchto třetích stran byly nepříznivě ovlivněny předáním bankovní historie držiteli účtu na základě žádosti o přenos - budou-li data v obou jmenovaných případech použita ke stejnému účelu (např. jako kontaktní adresa používaná pouze subjektem údajů nebo jako přehled historie bankovního účtu subjektu údajů).

Naopak, práva a svobody by nebyly respektovány, pokud by je nový správce použil jako seznam kontaktů pro jiné účely, např. pokud by přijímající správce použil osobní údaje jiných jednotlivců obsažených v adresáři subjektu údajů pro účely marketingu.

Aby se předešlo nežádoucím dopadům na dotčené třetí strany, je zpracování takových osobních údajů jiným správcem povoleno pouze v rozsahu údajů, které jsou ve výhradním držení žádajícího uživatele a jsou spravovány jen pro čistě osobní nebo domácí potřeby. Přebírající „nový“ správce (kterému data mohou být předána na vyžádání uživatele) nesmí použít předaná data třetích stran pro vlastní účely, například k marketingu výrobků a služeb těmto dalším subjektům údajů – třetím stranám. Tyto informace by neměly být použity například pro rozšíření profilu subjektu údajů – třetí strany a pro vytváření obrazu jeho

[22] Recitál 68 říká, 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.“

společenského prostředí bez vědomí a souhlasu tohoto subjektu údajů[23]. Nelze je použít ani pro získání informací o těchto třetích stranách a vytváření konkrétních profilů, dokonce ani v případech, kdy jejich osobní údaje jsou už v držení správce. Jinak by takové zpracování mohlo být nezákonné nebo nečestné, zejména pokud dotčené třetí strany by nebyly informovány a neměly možnost uplatnit svá práva coby subjekty údajů.

Osvědčenou praxí pro správce (odesílající i přijímající) má také být zavádění nástrojů umožňujících subjektům údajů vybrat příslušné údaje dalších jednotlivců, pokud existují, které si přejí dostat, přenést nebo vyloučit. To bude další pomůckou omezující rizika pro třetí strany vyplývající z eventuálního přenosu jejich osobních údajů.

Správci by také měli zavést mechanismus souhlasu pro ostatní dotčené subjekty údajů k usnadnění přenosu dat v případech, kdy tyto strany jsou ochotny udělit souhlas, například když i oni si přejí přenést své údaje jinému správci. Taková situace může vzniknout kupříkladu u sociálních sítí, je však na správcích, zda se rozhodnou postupovat v duchu osvědčené praxe.

Ve vztahu k datům podléhajícím ochraně duševního vlastnictví a obchodního tajemství:
Práva a svobody jiných jsou zmíněny v článku 20, odst. 4. I když se nevztahují přímo na přenositelnost údajů, lze ho chápat jako zahrnující „obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení. Byť by tato práva měla být zvážena před vyřízením žádosti o přenos údajů, „*zohlednění těchto skutečností by ovšem nemělo vést k tomu, že by subjektu údajů bylo odepřeno poskytnutí všech informací*“. Dále by správce neměl odmítnout žádost o přenos údajů z důvodu porušení jiného smluvního práva (například nevyrovnaný dluh nebo obchodní spor se subjektem údajů).

Právo na přenositelnost údajů nedává jednotlivci právo zneužít informace způsobem, který by mohl být kvalifikován jako nečestná praktika nebo by zakládal porušení práv duševního vlastnictví.

Možné obchodní riziko ovšem nemůže samo o sobě sloužit jako záminka pro odmítnutí žádosti o přenos údajů, přičemž správci mohou předat subjektem údajů poskytnutá osobní data způsobem, který nezpůsobí únik informací chráněných obchodním tajemstvím nebo právy duševního vlastnictví.

IV. Jak obecná pravidla pro výkon práv subjektu údajů se vztahují na přenositelnost údajů?

- Jaké předchozí informace mají být subjektu údajů poskytnuty?

Aby bylo vyhověno novému právu na přenositelnost údajů, musí správci informovat subjekty údajů o jeho existenci. V případech, kdy předmětné osobní údaje jsou shromažďovány přímo od subjektu údajů, musí se tak stát „v okamžiku získání osobních údajů“. Pokud osobní data nebyla získána od subjektu údajů, musí správce poskytnout informaci jak požadováno v článcích 13, odst. 2, písm. b a 14, odst. 2, písm. c Obecného nařízení.

V případech, kdy „osobní údaje nebyly získány od subjektu údajů“, musí být podle článku 14, odst. 3 informace poskytnuta v přiměřené lhůtě po získání údajů, ale nejpozději do jednoho

[23] Služba sociálních sítí (social networking service) by neměla rozšiřovat profil svých členů použitím osobních údajů posílaných subjektem údajů v rámci práva na přenositelnost, aniž by respektovala zásadu transparentnosti a zajistila, že konkrétní zpracování bude mít náležitou právní oporu.

měsíce, v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů nebo při zpřístupnění osobních údajů třetím stranám[24].

Při poskytování požadovaných informací musí správci zajistit, aby právo na přenositelnost bylo vymezeno vůči dalším právům. Proto WP29 především doporučuje správcům, aby jasně vysvětlili rozdíl mezi druhy dat, které subjekt údajů může obdržet při využití práva na přístup nebo přenositelnost.

Kromě toho WP29 doporučuje, aby správci vždy uváděli informaci o právu na přenositelnost ještě předtím, než subjekty údajů zruší jakýkoli případný účet. To uživatelům umožní získat před ukončením smlouvy přehled o svých osobních datech a snadno tyto údaje přenést do vlastních zařízení nebo jinému poskytovateli.

A konečně, WP29 doporučuje jako dobrou praxi „přijímajícím" správcům, aby subjektům údajů poskytli úplnou informaci o povaze osobních údajů nezbytných pro výkon svých služeb. Vedle posílení poctivosti zpracování to uživatelům umožní omezit rizika pro třetí strany a rovněž jakoukoli zbytečnou duplicitu osobních údajů v případech, kdy žádný další subjekt údajů není dotčen.

- **Jak správce může identifikovat subjekt údajů před vyřízením jeho žádosti?**

Obecné nařízení nestanoví žádné normativní požadavky ohledně ztotožnění subjektu údajů. Nicméně, Obecné nařízení v článku 12, odst. 2 uvádí, že správce nemá odmítnout žádost subjektu údajů za účelem výkonu jeho práv (včetně práva na přenositelnost údajů), ledaže zpracovává osobní údaje pro účely nevyžadující identifikaci subjektu údajů a může doložit, že není schopen totožnost subjektu údajů zjistit. V takových situacích ovšem může subjekt údajů, jak stanoveno v článku 11, odst. 2, poskytnout více informací, aby umožnil svoji identifikaci. Navíc, v článku 12, odst. 6 stojí, že pokud má správce důvodné pochybnosti o totožnosti subjektu údajů, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů. Poskytne-li subjekt údajů dodatečnou informaci umožňující jeho identifikaci, nesmí správce odmítnout danou žádostí se zabývat. Jsou-li informace nebo data shromážděná online spojena s pseudonymy nebo jedinečnými identifikátory, mohou správci zavést náležité postupy umožňující jednotlivci podat žádost na přenos údajů a získat data, která se ho týkají. Správci musí každopádně zavést postupy autentizace za účelem jasného zjištění totožnosti subjektu údajů požadujícího svá osobní data nebo vůbec uplatňujícího práva zaručená Obecným nařízením.

V mnoha případech už takové postupy existují. Často dochází k autentizaci subjektů údajů správcem již před uzavřením smlouvy nebo obdržením jejich souhlasu se zpracováním. Osobní údaje použité k registraci jednotlivce pro dané zpracování lze tedy následně použít pro ztotožnění subjektu údajů pro účely přenositelnosti[25].

V těchto případech může předchozí identifikace subjektu údajů vyžadovat ověření právní identity, přičemž takové ověření nemusí být relevantní pro posouzení vztahu mezi daty a dotyčným jednotlivcem, protože vazba na úřední nebo právní identitu neexistuje. Možnost správce, požadovat dodatečné informace k posouzení totožnosti dané osoby, zásadně nemůže vést k nepřiměřeným požadavkům a ke sběru osobních údajů, jež nejsou relevantní nebo nezbytná pro prohloubení vazby mezi jednotlivcem a požadovanými osobními údaji.

[24] Článek 12 vyžaduje, aby správce poskytnul „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."

[25] Pokud se zpracování dat týká například uživatelského účtu, může být poskytnutí uživatelského jména a hesla postačující k identifikaci subjektu údajů.

V mnoha případech už byly takové postupy autentizace ustaveny. Často například jsou používána uživatelská jména a hesla umožňující jednotlivcům přístup ke svým datům v emailových schránkách, účtech na sociálních sítích nebo účtech používaných pro různé další služby, z nichž některé se uživatelé rozhodli využívat, aniž by odhalili plné jméno nebo totožnost.

Pokud dělá problém objem dat požadovaných subjektem údajů přenést po internetu, je možné, aby správce namísto povolení prodloužit lhůtu k vyřízení žádosti na maximálně tři měsíce [26], zvážil alternativní prostředky k poskytnutí údajů, jako je kontinuální přenos (streaming) nebo uložení dat na CD, DVD nebo jiné fyzické nosiče nebo přenos osobních údajů přímo k jinému správci (viz Obecné nařízení, článek 20, odst. 2, pokud je to technicky proveditelné).

- **V jaké lhůtě musí být žádost o přenos vyřízena?**

Článek 12, odst. 3 požaduje, aby správce poskytnul subjektu údajů informaci „o přijatých opatřeních" „bez zbytečného odkladu" a v každém případě „do jednoho měsíce od obdržení žádosti". Tuto měsíční lhůtu lze prodloužit na maximálně tři měsíce u složitých případů za podmínky, že subjekt údajů byl do měsíce od podání původní žádosti informován o důvodech odkladu.

Správci provozující služby informační společnosti budou pravděpodobně lépe vybaveni, aby dokázali vyhovět žádostem ve velmi krátkém termínu. Pro naplnění očekávání uživatelů a s ohledem na osvědčené postupy by bylo dobré stanovit časový rámec, v němž typicky lze žádost o přenos údajů vyřídit a informovat o něm subjekty údajů.

Správci, kteří odmítnou žádosti o přenos vyhovět, musí podle článku 12, odst. 4 subjekt údajů informovat „o důvodech nepřijetí opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu", nejpozději do jednoho měsíce po obdržení žádosti.

Správci musí dodržet povinnost odpovědět ve stanovených lhůtách, byť by šlo o odmítnutí. Jinými slovy, správce nemůže zůstat nečinný, pokud je konfrontován se žádostí o přenos údajů.

- **V jakých případech lze žádost odmítnout nebo zpoplatnit?**

Podle článku 12 nesmí správci účtovat poplatek za poskytnutí osobních údajů, pokud správce neprokáže zjevnou neodůvodněnost nebo nadbytečnost žádostí, „zejména protože se opakují". U služeb informační společnosti specializovaných na automatizované zpracování osobních dat, může zavedení automatizovaných systémů, jako jsou rozhraní pro programování aplikací (API)[27] usnadnit komunikaci se subjektem údajů a tím snížit zátěž vyplývající z opakovaných žádostí. Případů, kdy správce bude schopen odůvodnit zamítnutí žádosti, by mělo být jen velmi málo a to i v případě násobných žádostí o přenos.

Kromě toho by celkové náklady na vyřízení žádosti o přenos údajů neměly hrát roli při posuzování, zda je žádost nadbytečná. Článek 12 Obecného nařízení se ve skutečnosti zabývá žádostmi podanými jedním subjektem údajů a nikoliv celkovým počtem žádostí, které správce obdrží. Ve výsledku tedy by celkové náklady na zavedení daného systému neměly být přeneseny na subjekty údajů, ani by neměly sloužit jako důvod k odmítnutí žádostí o přenos.

[26] Článek 12, odst. 3: „Správce poskytne […] informace o přijatých opatřeních".

[27] Rozhraní pro programování aplikací (Application Programming Interface – API) jsou rozhraní aplikací nebo webových služeb dávaných správci k dispozici, aby se jiné systémy nebo aplikace mohly propojit a pracovat s jejich systémy.

V. Jak mají být přenositelné údaje poskytnuty?

- Jaké prostředky by měl správce očekávaně zavést pro poskytnutí dat?

Článek 20, odst. 1 Obecného nařízení stanoví, že subjekt údajů má právo předat data jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.

Toto bránění lze charakterizovat jako jakékoli právní, technické nebo finanční překážky ze strany správce za účelem vyhnutí se nebo přibrzdění přístupu, přenosu nebo opětovného použití dat subjektem údajů nebo dalším správcem. Takovou překážkou může například být: poplatek požadovaný za dodání dat, nedostatečná interoperabilita nebo přístup k datovému formátu nebo API nebo poskytnutý formát, nadměrný časový odklad nebo složitost vytáhnout celý datový soubor, záměrné rozostření datového souboru, požadavek specifické a nepřiměřené nebo nadbytečné standardizace nebo akreditace[28].

Článek 20, odst. 2 ukládá správcům také povinnosti ohledně předání přenositelných údajů přímo druhým správcům „je-li to technicky proveditelné“.

Technická proveditelnost předání od správce správci, za dohledu subjektu údajů, by měla být posuzována případ od případu. Recitál 68 více vymezuje hranice pojmu „technicky proveditelné“ konstatováním, že toto právo „by nemělo zakládat povinnost správců zavést nebo zachovávat technicky kompatibilní způsoby zpracování“.

Očekává se, že správci budou osobní údaje přenášet v interoperabilním formátu, ačkoli by to nemělo na jiné správce klást povinnost tyto formáty podporovat. Přímé předání od jednoho správce jinému by se tedy mělo uskutečnit, pokud je komunikace mezi dvěma systémy možná, zabezpečeným způsobem [29] a pokud systém na příjmu je technicky způsobilý příchozí data přijmout. Pokud technické překážky nedovolují přímé předání, musí správce tyto překážky vysvětlit subjektům údajů, neboť jeho rozhodnutí by se jinak svým účinkem podobalo odmítnutí přijmout opatření na žádost subjektu údajů (článek 12, odst. 4).

V technickém ohledu by správci měli prozkoumat a posoudit dvě různé a nezpoplatněné cesty k zajištění dostupnosti přenositelných dat pro subjekty údajů nebo jiným správcům:

- přímý přenos celého souboru přenositelných dat (nebo několik výňatků částí celkového souboru dat);
- automatický nástroj umožňující vybrat relevantní údaje.

Druhý způsob bude asi upřednostňován správci v případech týkajících se složitých a rozsáhlých souborů dat, neboť dovoluje vyjmout jakoukoli část datového souboru podstatnou pro subjekt údajů v souvislosti s jeho žádostí, může pomoci minimalizovat riziko a případně umožnit použití mechanismů datové synchronizace[30] (např. v rámci pravidelné komunikace mezi správci). Může to být lepší způsob zajištění souladu „novým“ správcem představující příklad dobré praxe při snižování rizika na straně správce původního.

Tyto dva různé a pokud možno bezplatné způsoby poskytnutí relevantních přenositelných údajů by mohly být uplatněny zpřístupněním dat prostřednictvím různých způsobů jako

[28] Některé oprávněné obtíže nastat mohou, týkající se třeba práv a svobod jiných, jak zmíněno v článku 20, odst. 4 nebo ve vztahu k bezpečnosti systémů správce. Je v odpovědnosti správce odůvodnit, proč jsou takové překážky oprávněné a proč nepředstavují zábranu ve smyslu článku 20, odst. 1.

[29] Použitím autentizované komunikace s nezbytnou hloubkou šifrování dat.

[30] Synchronizační mechanismus může napomoci splnit obecnou povinnost podle článku 5 Obecného nařízení, který stanoví, že „osobní údaje musí být přesné a v případě potřeby aktualizované“.

například zabezpečené textování, SFTP server, zabezpečený WebAPI nebo WebPortal. Subjektům údajů by mělo být umožněno využít úložiště osobních údajů, systému správy osobních informací[31] nebo jiných druhů důvěryhodných třetích stran k držení a uchovávání osobních dat a udělit správcům souhlas s přístupem k osobním údajům a jejich zpracování podle požadavku.

- **Jaký je očekávaný datový formát?**

Obecné nařízení klade požadavky na správce, aby poskytovali osobní údaje požadované jednotlivcem ve formátu podporujícím jejich opětovné použití. Konkrétně článek 20, odst. 1 Obecného nařízení stanoví, že osobní údaje musí být poskytnuty „ve strukturovaném, běžně používaném a strojově čitelném formátu". Recitál 68 dále objasňuje, že tento formát by měl být interoperabilní, což je termín definovaný v EU takto[32]:

> *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 datových formátů poskytovaných správcem. V tomto smyslu představují pojmy „strukturovaný, běžně používaný a strojově čitelný" prostředky, přičemž interoperabilita je žádoucím výsledkem.

Recitál 21 směrnice 2013/37/EU[33,34] definuje pojem „strojově čitelný" takto:

> *„strojově čitelným formátem" se rozumí 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 možných druhů dat, které správci mohou zpracovávat, nestanoví Obecné nařízení žádná konkrétní doporučení ohledně formátu pro poskytování osobních údajů. Typ nejvhodnějšího formátu se bude lišit podle odvětví a odpovídající formáty už možná existují, přičemž by vždy měly být zvoleny tak, aby naplnily účel čitelnosti a umožňovaly subjektu údajů vysoký stupeň přenositelnosti dat. Formáty podléhající nákladným licencím nebudou považovány za odpovídající.

Recitál 68 objasňuje, že *„právo subjektu údajů předat nebo obdržet osobní údaje, které se ho týkají, by nemělo zakládat povinnost správců zavést nebo zachovávat technicky kompatibilní*

---

[31] Informace o systémech pro správu osobních informací viz například Stanovisko 9/2016 Evropského inspektora ochrany údajů dostupné na: https://edps.europa.eu/sites/edp/files/publication/17-01-11_pims_ex_summ_cs_0.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, 03.10.2009, str. 20.

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

[34] Slovník EU (http://eur-lex.europa.eu/eli-register/glossary.html) poskytuje bližší vysvětlení jaká jsou očekávání ohledně konceptů uvedených v těchto vodítkách, jako jsou pojmy *stojově čitelný, interoperabilita, otevřený formát, standardní, metadata*.

způsoby zpracování“. **Přenositelnost tedy směřuje k vytváření interoperabilních, a nikoliv kompatibilních systémů**[35].

Počítá se s tím, že osobní údaje budou poskytovány ve formátech s vysokým stupněm abstrakce vůči formátu internímu nebo vlastnickému. Přenositelnost údajů jako taková představuje další rovinu zpracování dat správcem, kdy je potřeba vybrat data ze základu a odfiltrovat osobní údaje nespadající pod přenositelnost, jako jsou data odvozená nebo data týkající se bezpečnosti systémů. V tomto smyslu jsou správci vyzváni předem určit data ve svých systémech, na která se vztahuje přenositelnost údajů. Takové dodatečné zpracování bude považováno za doplňkové k hlavnímu zpracování, neboť nebude správcem prováděno pro dosažení nově definovaného účelu.

Pokud v daném odvětví nebo v určité souvislosti neexistují žádné běžně používané formáty, **měli by správci poskytnout osobní údaje v běžně užívaných otevřených formátech (např. XML, JSON, CSV,…) spolu s** upotřebitelnými **metadaty v reálně dosažitelné rozlišitelnosti**, při zachování vysoké úrovně neurčitosti. Vhodná metadata by měla být použita k přesnému popisu významu sdělované informace. Tato metadata by měla postačovat k umožnění funkčnosti a opětovného použití dat, ale ovšem, bez vyzrazení obchodních tajemství. Je proto nepravděpodobné, že poskytnutí PDF verzí emailové schránky bude dostatečně strukturované a popisné, aby byl jednotlivec schopen tato data snadným způsobem opětovně použít. Údaje z e-mailu musí být dodané ve formátu, který zachová veškerá metadata, aby bylo možné opakovaně tyto údaje použít. Při výběru formátu by měl správce zvážit, jak tento formát ovlivní nebo ztíží uplatnění práva na opakované použití dat. V případech, kdy správce je schopen subjektu údajů nabídnout výběr upřednostňovaného formátu, měl by poskytnout jasné vysvětlení ohledně důsledků konkrétního rozhodnutí. Avšak zpracování dodatečných metadat jen s domněnkou, že by mohla být potřebná nebo vyžadovaná pro vyřízení žádosti o přenositelnost, nezakládá legitimní účel zpracování.

WP29 silně vyzývá zainteresované strany v odvětví a obchodní asociace ke spolupráci při tvorbě obecně uznávaných standardů interoperability a formátů pro naplnění práva na přenositelnost údajů. Touto výzvou se zabývá i Evropský rámec interoperability (EIF). EIF vytvořil „rámec interoperability“, který byl odsouhlasen pro organizace, jež si přejí společně poskytovat veřejné služby. V hranicích své platnosti konkretizuje tento rámec sadu společných prvků, jako jsou slovník, koncepty, zásady, politiky, vodítka, doporučení, standardy, specifikace a praktiky[36].

- **Jak nakládat s velkým nebo složitým shromažďováním dat?**

Obecné nařízení nevysvětluje, jak se chovat v případě sběru velkého množství dat, komplexních datových struktur nebo jiných technických otázek, které mohou způsobit potíže správcům nebo subjektům údajů.

V každém případě je však naprosto důležité respektovat, že definice, schémata a struktury osobních dat, která by správcem mohla být předána, mají být pro jednotlivce zcela srozumitelné. Data například mohou být nejprve poskytnuta souhrnně za použití přehledů (dashboardů), umožňujících subjektu údajů přenést podmnožiny osobních údajů a nikoliv celý jejich výčet. Správce má poskytnout přehled „stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků“ (viz Obecné nařízení, článek 12, odst. 1), aby subjekt údajů vždy jasně věděl, jaká data

[35] ČSN ISO/IEC 2382-01 definuje interoperabilitu následovně: Schopnost komunikovat, provádět programy, nebo přenášet data mezi různými funkčními jednotkami způsobem, jaký požaduje uživatel s malými nebo žádnými znalostmi jedinečných charakteristik těchto jednotek.

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

stáhnout nebo předat druhému správci v souvislosti s daným účelem. Subjekt údajů by měl být sto využít softwarových aplikací ke snadnému určení, rozpoznání a zpracování konkrétních dat získaných z této informace.

Jak zmíněno výše, jedním z praktických způsobů, kterým správce může vyřídit žádost o přenesení údajů je nabídka náležitě zabezpečeného a doložitelného rozhraní pro programování aplikací (API). To by mohlo umožnit, aby jednotlivci byli schopni podávat žádosti prostřednictvím softwaru vlastního nebo třetích stran nebo zajistit souhlas, aby to za ně udělal někdo jiný (včetně druhého správce) jak je stanoveno v článku 20, odst. 2 Obecného nařízení. Poskytnutím přístupu přes externě dostupné API lze nabídnout sofistikovanější přístupový systém umožňující jednotlivcům podat následné žádosti o data, buď ve formě úplného stažení nebo jako funkci delta zohledňující pouze změny od posledního stažení, aniž by tyto požadavky byly pro správce obtěžující.

- **Jak mohou být přenášená data zabezpečena?**

Správci by obecně měli zajistit „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 („integrita a důvěrnost“) podle článku 5, odst. 1, písm. f Obecného nařízení.

V souvislosti s přenosem dat subjektu údajů se však může objevit několik bezpečnostních problémů:

Jak mohou správci zajistit, aby osobní údaje byly bezpečně doručeny správné osobě? Jelikož přenositelnost údajů znamená vyjmutí osobních dat z informačního systému správce, může jejich přenos být zdrojem možných rizik (zejména narušení ochrany během přenosu). Správce je odpovědný za veškerá bezpečnostní opatření pro zajištěný přenos osobních údajů (např. použitím šifrování end-to-end nebo šifrování dat) ke správnému příjemci (použitím silných autentizačních opatření), ale také za stálou ochranu osobních údajů, které zůstaly v jeho systémech, jakožto i za transparentní postupy zacházení s možnými porušeními bezpečnosti ochrany dat[37]. Správci by měli posoudit rizika konkrétně spojená s přenositelností údajů a přijmout odpovídající opatření pro zmírnění těchto rizik.

Tato riziko zmírňující opatření mohou být: použití doplňkové autentizační informace, jako je sdílené tajemství nebo jiný autentizační faktor typu jednorázového hesla, pokud už je potřeba subjekt údajů identifikovat; přerušení nebo zmrazení předávky při podezření, že účet byl prolomen; autentizace na základě mandátu, jakou je na tokenech založená autentizace, v případě přenosu od jednoho správce druhému.

Tato bezpečnostní opatření nesmí být obtěžující a nesmí bránit uživatelům ve výkonu jejich práv, např. účtováním vícenákladů.

Jak pomoci uživatelům při uchovávání jejich osobních údajů ve vlastních systémech? Po vyzvednutí osobních údajů z internetové služby vždy existuje riziko, že uživatelé je mohou uložit do systému méně zabezpečeného, než byl ten předchozí. Subjekt údajů požadující data je odpovědný za výběr správných opatření pro zajištění osobních údajů ve vlastním systému. Měl by však na to být upozorněn, aby podniknul kroky k ochraně obdržených informací. Správci také v rámci dobré praxe mohou subjektu údajů doporučit vhodný formát nebo formáty, šifrovací prostředky a další bezpečnostní opatření a být mu tak nápomocni při splnění jeho cíle.

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

V Bruselu dne 13. prosince 2016

Za pracovní skupinu
předsedkyně
Isabelle FALQUE-PIERROTIN

Posledně revidováno a schváleno 5. dubna 2017

Za pracovní skupinu
předsedkyně
Isabelle FALQUE-PIERROTIN