Pokyny 01/2022 k právům subjektů údajů – právo na přístup

Verze 2.0

Přijaté dne 28. března 2023

Přijato

Historie verzí

Verze 1.0	18. ledna 2022	Přijetí pokynů k veřejné konzultaci
Verze 2.0	28. března 2023	Přijetí pokynů po veřejné konzultaci

SHRNUTÍ

Právo subjektů údajů na přístup k údajům je zakotveno v článku 8 Listiny základních práv EU. Je součástí evropského právního rámce pro ochranu osobních údajů již od počátku a nyní je dále rozpracováno prostřednictvím konkrétnějších a přesnějších pravidel v článku 15 Obecného nařízení o ochraně osobních údajů (GDPR).

Účel a celková struktura práva na přístup

Účelem práva na přístup obecně je poskytnout fyzickým osobám dostatečné, transparentní a snadno dostupné informace o zpracování jejich osobních údajů tak, aby byly informovány o jejich zpracování a mohly se přesvědčit o jejich přesnosti a oprávněnosti jejich zpracování. To fyzickým osobám umožní – není to však podmínkou – snadněji uplatňovat další práva, jako je právo na výmaz nebo právo na opravu.

Právo na přístup podle práva na ochranu osobních údajů je třeba odlišit od podobných práv s jinými cíli, například práva na přístup k veřejným dokumentům, jehož účelem je zajistit transparentnost rozhodovacího procesu veřejných orgánů a řádnou správní praxi.

Subjekt údajů však nemusí žádost o přístup odůvodňovat a není úkolem správce, aby analyzoval, zda žádost skutečně pomůže subjektu údajů ověřit zákonnost příslušného zpracování nebo uplatnit jiná práva. Správce bude muset žádost vyřídit, pokud není zřejmé, že byla podána podle jiných pravidel než podle pravidel ochrany osobních údajů.

Právo na přístup zahrnuje tři různé složky:

- potvrzení, zda jsou nebo nejsou zpracovávány údaje o osobě,
- přístup k těmto osobním údajům a
- přístup k informacím o zpracování, jako je účel, kategorie údajů a příjemci, doba trvání zpracování, práva subjektů údajů a vhodné záruky v případě předávání do třetích zemí.

Obecné úvahy o posouzení žádosti subjektu údajů

Při analýze obsahu žádosti musí správce posoudit, zda se žádost týká osobních údajů fyzické osoby, která žádost podává, zda žádost spadá do působnosti článku 15 a zda existují jiná, konkrétnější ustanovení, která upravují přístup v určitém odvětví. Musí také posoudit, zda se žádost týká všech údajů zpracovávaných o subjektu údajů, nebo pouze jejich části.

Na formát žádosti nejsou kladeny žádné zvláštní požadavky. Správce by měl poskytnout vhodné a uživatelsky přívětivé komunikační kanály, které může subjekt údajů snadno používat. Subjekt údajů však nemusí tyto konkrétní kanály využít a místo toho může zaslat žádost oficiálnímu kontaktnímu místu správce. Správce není povinen reagovat na žádosti zaslané na zcela náhodné nebo zjevně nesprávné adresy.

Pokud správce není schopen identifikovat údaje, které se vztahují k subjektu údajů, informuje ho o tom a může odmítnout žádosti vyhovět, pokud subjekt údajů neposkytne další informace, které umožňují identifikaci. Pokud má však správce pochybnosti o tom, zda je subjekt údajů tím, za koho se vydává, může požádat o poskytnutí dodatečných informací za účelem potvrzení totožnosti subjektu údajů. Žádost o dodatečné informace musí být přiměřená druhu zpracovaných údajů, újmě, která by mohla vzniknout, atd., aby se zabránilo shromažďování neúměrného množství dat.

Rozsah působnosti práva na přístup

Rozsah působnosti práva na přístup je dán rozsahem pojmu osobní údaj, jak je definován v čl. 4 bodě 1 GDPR. Kromě základních osobních údajů, jako je jméno, adresa, telefonní číslo atd., může do této definice spadat široká škála údajů, jako jsou lékařské nálezy, historie nákupů, ukazatele úvěruschopnosti, záznamy o aktivitách, činnosti vyhledávání atd. Osobní údaje, na něž byla uplatněna pseudonymizace, jsou na rozdíl od anonymizovaných údajů stále osobními údaji. Právo na přístup se vztahuje na osobní údaje týkající se osoby, která žádost podává. To by nemělo být vykládáno příliš restriktivně a mohou sem patřit i údaje, které se mohou týkat jiných osob, například historie komunikace zahrnující příchozí a odchozí zprávy.

Kromě poskytnutí přístupu k osobním údajům musí správce poskytnout i další informace o zpracování a o právech subjektů údajů. Tyto informace mohou vycházet z toho, co je již shromážděno v záznamech správce o činnostech zpracování (článek 30 GDPR) a v oznámení o ochraně osobních údajů (články 13 a 14 GDPR). Tyto obecné informace však může být nutné aktualizovat k okamžiku podání žádosti nebo je přizpůsobit tak, aby zohledňovaly operace zpracování prováděné v souvislosti s konkrétní osobou, která žádost podává.

Jak poskytnout přístup

Způsoby poskytnutí přístupu se mohou lišit v závislosti na množství údajů a složitosti prováděného zpracování. Pokud není výslovně uvedeno jinak, měla by být žádost považována za žádost týkající se *všech* osobních údajů subjektu údajů a správce může subjekt údajů požádat o upřesnění žádosti, pokud zpracovává velké množství údajů.

Správce bude muset vyhledávat osobní údaje ve všech informačních systémech a jiných než počítačových evidencích na základě vyhledávacích kritérií, která odrážejí způsob, jakým jsou informace strukturovány, například jméno a číslo zákazníka. Sdělování údajů a dalších informací o zpracování musí probíhat stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků. Přesnější požadavky v tomto ohledu závisí na okolnostech zpracování údajů, jakož i na schopnosti subjektu údajů porozumět sdělení a pochopit je (například s ohledem na to, že subjektem údajů je dítě nebo osoba se zvláštními potřebami). Pokud údaje sestávají z kódů nebo jiných „nezpracovaných údajů“, může být nutné je vysvětlit, aby dávaly subjektu údajů smysl.

Hlavním způsobem poskytnutí přístupu je předat subjektu údajů kopii jeho údajů, ale lze předpokládat i jiné způsoby (například ústní informace a přístup na místě), pokud o to subjekt údajů požádá. Údaje lze zaslat e-mailem, pokud jsou uplatněny všechny nezbytné záruky, například s ohledem na povahu údajů, nebo jinými způsoby, například pomocí samoobslužného nástroje.

V některých případech, kdy existuje velké množství údajů a pro subjekt údajů by bylo obtížné pochopit informace, pokud by mu byly poskytnuty všechny najednou – zejména v online kontextu–-, může být nejvhodnějším opatřením vícevrstvý přístup. Poskytnutí informací v různých vrstvách může subjektu údajů usnadnit pochopení údajů. Správce musí být schopen prokázat, že vícevrstvý přístup má pro subjekt údajů přínos, a pokud se subjekt údajů pro něj rozhodne, měly by být všechny vrstvy poskytnuty současně.

Kopie údajů a doplňující informace by měly být poskytnuty v trvalé formě, například v písemné podobě, přičemž by se mohlo jednat o elektronickou formu, která se běžně používá, aby si je subjekt údajů mohl snadno stáhnout. Údaje mohou být uvedeny v přepisu nebo v souhrnné podobě, pokud jsou zahrnuty všechny informace a pokud se tím nezmění ani není nijak dotčen jejich obsah.

Žádost musí být vyřízena co nejdříve, v každém případě do jednoho měsíce od obdržení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce. O důvodu zpoždění pak musí být subjekt údajů informován. Správce musí co nejdříve zavést nezbytná opatření k vyřízení žádostí a přizpůsobit tato opatření okolnostem zpracování. Pokud jsou údaje uchovávány pouze po velmi krátkou dobu, musí existovat opatření, která zaručí, že žádost o přístup může být vyřízena, aniž by byly údaje během vyřizování žádosti vymazány. Pokud se zpracovává velké množství údajů, musí správce zavést postupy a mechanismy, které jsou přizpůsobeny složitosti zpracování.

Posouzení žádosti by mělo odrážet situaci v okamžiku, kdy správce žádost obdržel. Musí být poskytnuty i údaje, které mohou být nesprávné nebo byly zpracovávány protiprávně. Údaje, které již byly vymazány, například v souladu s pravidly pro uchovávání údajů, a správce je již tedy nemá k dispozici, nelze poskytnout.

Meze a omezení

GDPR umožňuje určitá omezení práva na přístup. Žádné další výjimky ani odchylky neexistují. Právo na přístup je bez jakékoli obecné výhrady k přiměřenosti, pokud jde o úsilí, které musí správce vynaložit, aby vyhověl žádosti subjektu údajů.

Podle čl. 15 odst. 4 nesmějí být právem získat kopii nepříznivě dotčena práva a svobody jiných osob. Evropský sbor pro ochranu údajů (EDPB) je toho názoru, že tato práva musí být zohledněna nejen při umožnění přístupu poskytnutím kopie, ale také v případě, že je přístup k údajům poskytnut jinými prostředky (například přístup na místě). Ustanovení čl. 15 odst. 4 se však nevztahuje na dodatečné informace o zpracování uvedené v čl. 15 odst. 1 písm. a) až h). Správce musí být schopen prokázat, že v konkrétní situaci by byla nepříznivě dotčena práva nebo svobody jiných osob. Použití čl. 15 odst. 4 by nemělo vést k úplnému zamítnutí žádosti subjektu údajů; vedlo by pouze k vynechání nebo znemožnění čitelnosti těch částí, které mohou mít negativní dopad na práva a svobody ostatních.

Ustanovení čl. 12 odst. 5 GDPR umožňuje správcům odmítnout vyhovět žádostem, které jsou zjevně nedůvodné nebo nepřiměřené, nebo za takové žádosti uložit přiměřený poplatek. Tyto pojmy je třeba vykládat úzce. Vzhledem k tomu, že existuje jen velmi málo nezbytných podmínek týkajících se žádostí o přístup, je rozsah posouzení žádosti jako zjevně nedůvodné poměrně omezený. Nepřiměřené žádosti závisí na zvláštnosti odvětví, ve kterém správce působí. Čím častěji dochází ke změnám ve správcově databázi, tím častěji může subjekt údajů žádat o přístup, aniž by to bylo nepřiměřené. Správce se může rozhodnout, že místo odmítnutí přístupu bude subjektu údajů účtovat poplatek. To by bylo relevantní pouze v případě nepřiměřeného počtu žádostí, aby se pokryly administrativní náklady, které takové žádosti mohou způsobit. Správce musí být schopen prokázat zjevnou nedůvodnost nebo nepřiměřenost žádosti.

Omezení práva na přístup mohou existovat i ve vnitrostátním právu členských států podle článku 23 GDPR a výjimek v něm uvedených. Správci, kteří hodlají taková omezení použít, musí pečlivě zkontrolovat požadavky vnitrostátních předpisů a vzít na vědomí případné zvláštní podmínky. Tyto podmínky mohou spočívat v tom, že právo na přístup je jen dočasně odloženo nebo že se omezení vztahuje pouze na určité kategorie údajů.

Obsah

Evropský sbor pro ochranu osobních údajů

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

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

s ohledem na články 12 a 22 svého jednacího řádu,

vzhledem k tomu, že přípravné práce na těchto pokynech zahrnovaly shromažďování podnětů od zúčastněných stran, a to jak písemně, tak na specializované akci pro zúčastněné strany o právech subjektů údajů, s cílem identifikovat výzvy a výkladové problémy, kterým čelí při uplatňování příslušných ustanovení GDPR,

PŘIJAL TYTO POKYNY:

1 ÚVOD – OBECNÉ PŘIPOMÍNKY

1. V dnešní společnosti jsou osobní údaje zpracovávány veřejnými i soukromými subjekty, při mnoha činnostech, pro širokou škálu účelů a mnoha různými způsoby. Fyzické osoby mohou být často v nevýhodném postavení, pokud jde o porozumění tomu, jak jsou jejich osobní údaje zpracovávány, včetně technologie použité v konkrétním případě, ať už soukromým nebo veřejným subjektem. Za účelem ochrany osobních údajů fyzických osob v těchto situacích vytvořilo GDPR soudržný a pevný právní rámec, který je obecně použitelný pro různé typy zpracování, včetně zvláštních ustanovení týkajících se práv subjektů údajů.

2. Právo na přístup k osobním údajům je jedním z práv subjektů údajů stanovených v kapitole III GDPR vedle dalších práv, jako je například právo na opravu a výmaz, právo na omezení zpracování, právo na přenositelnost, právo vznést námitku nebo právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování[2]. Právo subjektu údajů na přístup je zakotveno jak v Listině základních práv EU (dále jen „Listina“)[3], tak v článku 15 GDPR, kde je přesně formulováno jako právo na přístup k osobním údajům a dalším souvisejícím informacím.

3. Podle GDPR se právo na přístup skládá ze tří prvků, tj. potvrzení, zda se osobní údaje zpracovávají, přístupu k nim a informací o samotném zpracování. Subjekt údajů může rovněž získat kopii zpracovávaných osobních údajů, přičemž tato možnost není dalším právem subjektu údajů, ale způsobem poskytnutí přístupu k údajům. Právo na přístup lze tedy chápat jednak jako možnost subjektu údajů požádat správce o informaci, zda jsou zpracovávány osobní údaje o jeho osobě, jednak

[1] Odkazy na „členské státy“ v celém tomto dokumentu je třeba chápat jako odkazy na „členské státy EHP“.
[2] Články 15 až 22 GDPR.
[3] Podle čl. 8 odst. 1 Listiny základních práv Evropské unie má každý právo na ochranu osobních údajů, které se ho týkají. Podle čl. 8 odst. 2 druhé věty má každý právo na přístup k údajům, které o něm byly shromážděny, a právo na jejich opravu.

jako možnost přístupu k těmto údajům a jejich ověření. Správce je povinen poskytnout subjektu údajů na jeho žádost informace spadající do působnosti čl. 15 odst. 1 a 2 GDPR.

4. Výkon práva na přístup se uskutečňuje jak v rámci práva na ochranu údajů v souladu s cíli práva na ochranu údajů, tak konkrétně v rámci „*základních práv a svobod fyzických osob, a zejména jejich práva na ochranu osobních údajů*“, jak uvádí čl. 1 odst. 2 GDPR. Právo na přístup je důležitým prvkem celého systému ochrany údajů.

5. Praktickým cílem práva na přístup je umožnit fyzickým osobám kontrolu nad jejich vlastními osobními údaji[4]. Aby bylo možné tento cíl účinně realizovat v praxi, snaží se GDPR usnadnit tento výkon řadou záruk, které subjektu údajů umožní toto právo uplatňovat snadno, bez zbytečných omezení, v přiměřených odstupech a bez přílišných průtahů nebo nákladů. To vše by mělo vést k účinnějšímu prosazování práva subjektu údajů na přístup v digitálním věku, jehož součástí je v širším smyslu také právo subjektu údajů podat stížnost u dozorového úřadu a právo na účinnou soudní ochranu[5].

6. Pokud jde o vývoj práva na přístup jako součásti právního rámce ochrany údajů, je třeba zdůraznit, že je prvkem evropského systému ochrany údajů již od jeho začátku. Ve srovnání se směrnicí 95/46/ES byl standard práv subjektů údajů stanovený v GDPR zpřesněn a posílen; to platí i pro právo na přístup. Vzhledem k tomu, že způsoby uplatňování práva na přístup jsou nyní v GDPR vymezeny přesněji, je toto právo více přínosné i z hlediska právní jistoty, a to jak pro subjekt údajů, tak pro správce. Kromě toho konkrétní znění článku 15 a přesná lhůta pro poskytnutí údajů podle čl. 12 odst. 3 GDPR ukládá správci povinnost být připraven na dotazy subjektů údajů vypracováním postupů pro vyřizování žádostí.

7. Právo na přístup by nemělo být vnímáno izolovaně, neboť je úzce propojeno s dalšími ustanoveními GDPR, zejména se zásadami ochrany údajů včetně zásady korektnosti a zákonnosti zpracování, povinnosti správce zajistit transparentnost a s dalšími právy subjektů údajů stanovenými v kapitole III GDPR.

8. V rámci práv subjektů údajů je rovněž důležité zdůraznit význam článku 12 GDPR, který stanoví požadavky na vhodná opatření přijatá správcem při poskytování informací uvedených v článcích 13 a 14 GDPR a sdělení uvedených v článcích 15 až 22 a článku 34 GDPR; tyto požadavky obecně stanoví formu, způsob a lhůtu pro reakce subjektu údajů, a zejména pro veškeré informace určené dítěti.

9. EDPB považuje za nezbytné poskytnout přesnější pokyny k tomu, jak má být právo na přístup prováděno v různých situacích. Cílem těchto pokynů je analyzovat různé aspekty práva na přístup. Následující oddíl má zejména podat obecný přehled a vysvětlení obsahu samotného článku 15, zatímco následující oddíly poskytují hlubší analýzu nejčastějších praktických otázek a problémů při provádění práva na přístup.

[4] Viz 7., 68., 75. a 85. bod odůvodnění GDPR.
[5] Viz kapitola VIII články 77, 78 a 79 GDPR.

2 ÚČEL PRÁVA NA PŘÍSTUP, STRUKTURA ČLÁNKU 15 GDPR A OBECNÉ ZÁSADY

2.1 Účel práva na přístup

10. Právo na přístup je tudíž navrženo tak, aby fyzickým osobám umožnilo kontrolu nad osobními údaji, které se jich týkají, neboť jim umožňuje, *„aby byly o jejich zpracování informovány a mohly si ověřit jeho zákonnost“*[6]. Konkrétněji je účelem práva na přístup umožnit subjektům údajů pochopit, jak jsou jejich osobní údaje zpracovávány, jakož i důsledky takového zpracování, a ověřit si přesnost zpracovávaných údajů, aniž by musely svůj záměr zdůvodňovat. Jinými slovy, účelem práva na přístup je poskytnout fyzickým osobám dostatečné, transparentní a snadno přístupné informace o zpracování údajů, a to bez ohledu na použité technologie, a umožnit jim ověřit si různé aspekty konkrétní činnosti zpracování podle GDPR (např. zákonnost, přesnost).

11. Výklad GDPR uvedený v těchto pokynech vychází z dosavadní judikatury Soudního dvora EU (dále jen „SDEU“). S ohledem na význam práva na přístup lze očekávat, že související judikatura dozná v budoucnu značného vývoje.

12. V souladu s rozhodnutími Soudního dvora EU[7] slouží právo na přístup k údajům k zajištění ochrany práva subjektů údajů na soukromí a ochranu údajů, pokud jde o zpracování údajů, které se jich týkají[8], a může usnadnit výkon jejich práv vyplývajících například z článků 16 až 19, 21 až 22 a 82 GDPR. Výkon práva na přístup je však právem jednotlivce a není podmíněn výkonem těchto jiných práv a výkon ostatních práv nezávisí na výkonu práva na přístup.

13. Vzhledem k širokému cíli práva na přístup není vhodné, aby byl cíl práva na přístup správcem analyzován jako předpoklad pro výkon práva na přístup v rámci jeho posuzování žádostí o přístup. Správci by tedy neměli posuzovat, „proč“ subjekt údajů žádá o přístup, ale pouze „co“ subjekt údajů žádá (viz oddíl 3 o analýze žádosti) a zda mají v držení osobní údaje týkající se této osoby (viz oddíl 4). Správce by proto například neměl odmítnout přístup na základě podezření, že by požadované údaje mohl subjekt údajů použít ke své obraně u soudu v případě výpovědi nebo obchodního sporu se správcem[9]. Pokud jde o meze a omezení práva na přístup, viz oddíl 6.

Příklad 1: Zaměstnavatel propustil zaměstnance. O týden později se tato fyzická osoba rozhodne shromáždit důkazy pro podání žaloby na neoprávněné propuštění proti tomuto bývalému zaměstnavateli. S ohledem na to se fyzická osoba obrátí na bývalého zaměstnavatele s písemnou žádostí o přístup ke všem osobním údajům, které se jí jako subjektu údajů týkají a které bývalý zaměstnavatel jako správce zpracovává.

Správce nesmí posuzovat záměr subjektu údajů a subjekt údajů nemusí správci sdělit důvod své žádosti. Pokud tedy žádost splňuje všechny ostatní požadavky (viz oddíl 3), správce musí žádosti

[6] 63. bod odůvodnění GDPR.
[7] SDEU, C-434/16, Nowak, a spojené věci C-141/12 a C-372/12, YS a další.
[8] SDEU, C-434/16, Nowak, bod 56.
[9] Otázky související s tímto tématem jsou předmětem sporu, který v současné době projednává Soudní dvůr EU (věc C-307/22).

vyhovět, ledaže se žádost ukáže jako zjevně nedůvodná nebo nepřiměřená ve smyslu čl. 12 odst. 5 GDPR (viz oddíl 6.3), což je správce povinen prokázat.

Odchylka: Subjekt údajů uplatňuje právo na přístup k osobním údajům, které se ho týkají, v průběhu soudního řízení. Vnitrostátní právo členského státu, které upravuje pracovněprávní vztah mezi správcem a subjektem údajů, však obsahuje určitá ustanovení, která omezují rozsah informací, jež mají být poskytnuty stranám probíhajícího nebo případného budoucího soudního řízení nebo mezi těmito stranami vyměněny a které se vztahují na žalobu na neoprávněné propuštění, již podal subjekt údajů. V této souvislosti a za předpokladu, že tyto vnitrostátní předpisy splňují požadavky článku 23 GDPR[10], subjekt údajů nemá právo obdržet od správce více informací, než stanoví vnitrostátní právní předpisy členského státu upravující výměnu informací mezi stranami právních sporů.

14. Ačkoli je cíl práva na přístup široký, Soudní dvůr EU rovněž ukázal hranice působnosti práva ochrany údajů a práva na přístup. Soudní dvůr například konstatoval, že cíl práva na přístup zaručeného právem EU v oblasti ochrany údajů je třeba odlišovat od cíle práva na přístup k veřejným dokumentům stanoveného právními předpisy EU a vnitrostátními právními předpisy, přičemž cílem druhého z těchto práv je „co největší možná transparentnost rozhodovacího procesu veřejných orgánů a podpora řádné správní praxe“[11], což je cíl, který právní předpisy v oblasti ochrany údajů nesledují. Soudní dvůr EU dospěl k závěru, že právo na přístup k osobním údajům platí bez ohledu na to, zda se uplatňuje jiný druh práva na přístup s jiným cílem, například v rámci přezkumného řízení.

2.2 Struktura článku 15 GDPR

15. Aby bylo možné odpovědět na žádost o přístup a zajistit, že žádný z jejích aspektů nebude opomenut, je třeba nejprve pochopit strukturu článku 15 a jednotlivé prvky práva na přístup, které jsou v tomto článku stanoveny.

16. Článek 15 lze rozdělit na osm různých prvků uvedených v následující tabulce:

1.	Potvrzení, zda správce zpracovává osobní údaje týkající se žádající osoby, či nikoli	Čl. 15 odst. 1 první polovina věty
2.	Přístup k osobním údajům týkajícím se žádající osoby	Čl. 15 odst. 1 druhá polovina věty (první část)
3.	Přístup k následujícím informacím o zpracování: a) účely zpracování; b) kategorie osobních údajů; c) příjemci nebo kategorie příjemců údajů; d) plánovaná doba trvání zpracování nebo kritéria pro její určení; e) existence práva na opravu, výmaz, omezení zpracování a vznesení námitky proti zpracování; f) právo podat stížnost u dozorového úřadu; g) veškeré dostupné informace o zdroji údajů, pokud nejsou získány od subjektu údajů; h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, a další informace s ním související.	Čl. 15 odst. 1 druhá polovina věty (druhá část)

[10] Pokyny EDPB 10/2020 týkající se omezení podle článku 23 GDPR, verze k veřejné konzultaci, 18. prosince 2020.

[11] SDEU, spojené věci C-141/12 a C-372/12, YS a další, bod 47.

4.	Informace o zárukách podle článku 46 v případě předávání osobních údajů do třetí země nebo mezinárodní organizaci	Čl. 15 odst. 2
5.	Povinnost správce poskytnout kopii zpracovávaných osobních údajů	Čl. 15 odst. 3 první věta
6.	Účtování přiměřeného poplatku správcem na základě administrativních nákladů za další kopie na žádost subjektu údajů	Čl. 15 odst. 3 druhá věta
7.	Poskytování informací v elektronické formě	Čl. 15 odst. 3 třetí věta
8.	Zohlednění práv a svobod jiných osob	Čl. 15 odst. 4

Zatímco všechny prvky uvedené v čl. 15 odst. 1 a 2 společně definují obsah práva na přístup, čl. 15 odst. 3 se kromě obecných požadavků stanovených v čl. 12 GDPR zabývá způsoby poskytování přístupu. Čl. 15 odst. 4 doplňuje meze a omezení, které čl. 12 odst. 5 GDPR stanoví pro všechna práva subjektů údajů, se zvláštním zaměřením na práva a svobody jiných osob v souvislosti s přístupem.

2.2.1 Vymezení obsahu práva na přístup

17. Ustanovení čl. 15 odst. 1 a 2 zahrnují tyto tři aspekty: zaprvé potvrzení, zda jsou osobní údaje žádající osoby zpracovávány, a pokud ano, zadruhé přístup k těmto údajům a zatřetí informace o zpracování. Lze je považovat za tři různé složky, které společně vytvářejí právo na přístup.

2.2.1.1 Potvrzení o tom, „zda“ jsou či nejsou osobní údaje zpracovávány

18. Při podání žádosti o přístup k osobním údajům je první věcí, kterou subjekty údajů potřebují vědět, to, zda správce zpracovává údaje, které se jich týkají, či nikoli. Tato informace proto představuje první složku práva na přístup podle čl. 15 odst. 1. Pokud správce osobní údaje týkající se subjektu údajů žádajícího o přístup nezpracovává, informace, kterou je třeba poskytnout, by se omezila na potvrzení, že nejsou zpracovávány žádné osobní údaje týkající se subjektu údajů. Pokud správce údaje týkající se žádající osoby zpracovává, musí jí tuto skutečnost potvrdit. Toto potvrzení může být sděleno samostatně, nebo může být součástí informací o zpracovávaných osobních údajích (viz níže).

2.2.1.2 Přístup ke zpracovávaným osobním údajům

19. Přístup k osobním údajům je druhou složkou práva na přístup podle čl. 15 odst. 1 a tvoří podstatu tohoto práva. Souvisí s pojmem osobních údajů, jak je definován v čl. 4 bodě 1 GDPR. Kromě základních osobních údajů, jako je jméno a adresa, může do této definice spadat neomezené množství údajů, pokud spadají do věcné působnosti GDPR, zejména s ohledem na způsob jejich zpracování (článek 2 GDPR). Přístupem k osobním údajům se tedy rozumí přístup k samotným osobním údajům, nikoli pouze jejich obecný popis nebo pouhý odkaz na kategorie osobních údajů, které správce zpracovává. Pokud neplatí žádné meze ani omezení[12], mají subjekty údajů právo na přístup ke všem zpracovávaným údajům, které se jich týkají, nebo k jejich částem v závislosti na rozsahu žádosti (viz oddíl 2.3.1). Povinnost poskytnout přístup k údajům nezávisí na druhu nebo zdroji těchto údajů. Platí v plném rozsahu i v případech, kdy údaje původně poskytla správci žádající osoba, neboť jeho cílem je informovat subjekt údajů o skutečném zpracování těchto údajů správcem. Rozsah osobních údajů podle článku 15 je podrobně vysvětlen v oddílech 4.1 a 4.2.

[12] Viz oddíl 6 těchto pokynů.

2.2.1.3 Informace o zpracování a o právech subjektu údajů

20. Třetí složkou práva na přístup jsou informace o zpracování a o právech subjektů údajů, které musí správce poskytnout podle čl. 15 odst. 1 písm. a) až h) a čl. 15 odst. 2. Tyto informace by mohly vycházet například z oznámení správce o ochraně osobních údajů[13] nebo ze záznamů správce o činnostech zpracování uvedených v článku 30 GDPR, může však být nutné je aktualizovat a přizpůsobit žádosti subjektu údajů. Obsah a míra upřesnění informací jsou dále rozvedeny v oddíle 4.3.

2.2.2 Ustanovení o způsobech

21. Ustanovení čl. 15 odst. 3 doplňuje požadavky na způsoby odpovědi na žádosti o přístup, jež stanoví článek 12 GDPR, o určitá upřesnění v souvislosti s žádostmi o přístup.

2.2.2.1 Poskytnutí kopie

22. Podle čl. 15 odst. 3 první věty GDPR musí správce bezplatně poskytnout kopii osobních údajů, kterých se zpracování týká. Kopie se proto týká pouze druhé složky práva na přístup („přístup ke zpracovávaným osobním údajům“, viz výše). Správce musí zajistit, aby první kopie byla bezplatná, a to i v případě, že považuje náklady na její zhotovení za vysoké (příklad: náklady na poskytnutí kopie záznamu telefonického rozhovoru).

23. Povinnost poskytnout kopii nelze chápat jako další právo subjektu údajů, ale jako způsob poskytnutí přístupu k údajům. Posiluje právo na přístup k údajům[14] a napomáhá výkladu tohoto práva, protože ukazuje, že přístup k údajům podle čl. 15 odst. 1 zahrnuje úplné informace o všech údajích a nelze jej chápat jako poskytnutí pouze souhrnu údajů. Povinnost poskytnout kopii přitom nemá za cíl rozšířit rozsah práva na přístup: vztahuje se (pouze) na kopii zpracovávaných osobních údajů, nikoli nutně na reprodukci originálních dokumentů (viz oddíl 5, bod 152). Obecněji řečeno, při poskytnutí kopie není třeba subjektu údajů poskytovat žádné další informace: rozsah informací, které mají být obsaženy v kopii, odpovídá rozsahu přístupu k údajům podle čl. 15 odst. 1 (druhá složka práva na přístup uvedená výše, viz bod 19), který zahrnuje všechny informace nezbytné k tomu, aby mohl subjekt údajů porozumět tomu, jak jsou jeho údaje zpracovávány, a ověřit zákonnost jejich zpracování[15].

24. Pokud je s ohledem na výše uvedené přístup k údajům ve smyslu čl. 15 odst. 1 zajištěn poskytnutím kopie, povinnost poskytnout kopii uvedená v čl. 15 odst. 3 je splněna. Povinnost poskytnout kopii sleduje cíle práva na přístup, aby byl subjekt údajů o zpracování údajů informován a mohl si ověřil jeho zákonnost (63. bod odůvodnění). K dosažení těchto cílů bude muset mít subjekt údajů tyto informace k dispozici ve většině případů nikoli pouze dočasně. Proto bude nutné, aby subjekt údajů získal přístup k informacím tím, že obdrží kopii osobních údajů.

25. S ohledem na výše uvedené je třeba pojem kopie vykládat v širokém smyslu, což zahrnuje různé druhy přístupu k osobním údajům, pokud je úplná (tj. zahrnuje všechny požadované osobní údaje) a subjekt údajů si ji může ponechat. Požadavek na poskytnutí kopie tedy znamená, že informace o osobních údajích týkajících se osoby, která žádost podává, jsou subjektu údajů poskytnuty způsobem, který umožňuje, aby si subjekt údajů mohl všechny informace ponechat a mohl se k nim vrátit.

---

[13] Informace k tomu viz pracovní skupina zřízená podle článku 29, Pokyny k transparentnosti podle nařízení 2016/679 – schválené Evropským sborem pro ochranu osobních údajů (dále jen „pokyny WP29 k transparentnosti – schválené EDPB“), WP260 rev.01, 11. dubna 2018.

[14] Ve směrnici o ochraně údajů 95/46/ES nebyla povinnost poskytnout kopii uvedena.

[15] Otázky související s tématem tohoto odstavce jsou předmětem sporu, který v současné době projednává Soudní dvůr EU (věc C-487/21).

26. I přes toto široké chápání kopie a s ohledem na to, že se jedná o hlavní způsob, jakým by měl být přístup poskytován, mohou být za určitých okolností vhodné i jiné způsoby. Další vysvětlení týkající se kopií a jiných způsobů poskytnutí přístupu je uvedeno v oddíle 5, zejména v oddílech 5.2.2 až 5.2.5.

2.2.2.2 Poskytnutí dalších kopií

27. Ustanovení čl. 15 odst. 3 druhé věty se týká situací, kdy subjekt údajů požádá správce o více než jednu kopii, například v případě, že první kopie byla ztracena nebo poškozena, nebo pokud chce subjekt údajů předat kopii jiné osobě nebo dozorovému úřadu. Na základě toho, že správce musí poskytnout na žádost subjektu údajů další kopie, čl. 15 odst. 3 stanoví, že za každou další vyžádanou kopii může správce účtovat přiměřený poplatek na základě administrativních nákladů (čl. 15 odst. 3 druhá věta).

28. Pokud subjekt údajů požádá o dodatečnou kopii po podání první žádosti, mohou vyvstat otázky, zda by to mělo být považováno za novou žádost, nebo zda subjekt údajů požaduje dodatečnou kopii údajů ve smyslu čl. 15 odst. 3 druhé věty, přičemž v takovém případě může být za dodatečnou kopii účtován poplatek. Odpověď na tyto otázky závisí pouze na obsahu žádosti: žádost by měla být vykládána jako žádost o dodatečnou kopii, pokud se z hlediska času a rozsahu týká stejného zpracování osobních údajů jako předchozí žádost. Pokud však subjekt údajů usiluje o získání informací o údajích zpracovávaných v jiném časovém okamžiku nebo týkajících se jiného souboru údajů, než o který původně požádal, uplatní se znovu právo získat bezplatnou kopii podle čl. 15 odst. 3. To platí i v případech, kdy subjekt údajů podal první žádost krátce předtím. Subjekt údajů může uplatnit své právo na přístup prostřednictvím následné žádosti a získat bezplatnou kopii, pokud není žádost považována za nepřiměřenou podle čl. 12 odst. 5, s možností případného uložení přiměřeného poplatku podle čl. 12 odst. 5 písm. a) (pokud jde o nepřiměřenost opakovaných žádostí, viz oddíl 6).

Příklad 2: Zákazník předloží obchodní společnosti žádost o přístup. Po uplynutí jednoho roku od odpovědi společnosti předloží tentýž zákazník stejné společnosti žádost o přístup podle článku 15. Tuto druhou žádost je třeba považovat za novou žádost bez ohledu na to, zda od předchozí žádosti došlo k novým obchodním transakcím nebo jiným kontaktům mezi stranami. Subjekt údajů má právo získat bezplatnou kopii údajů i v případě, že k žádné změně ve zpracování údajů společností nedošlo – o čemž nemusí být subjekt údajů vždy informován.

Odchylka 1: I když zákazník ve výše uvedených případech podá novou žádost například jen jeden týden po první žádosti, lze ji považovat za novou žádost podle čl. 15 odst. 1 a odst. 3 první věty, pokud ji nelze vykládat jako pouhé připomenutí první žádosti. Vzhledem ke krátkému odstupu a v závislosti na konkrétních okolnostech nové žádosti připadá v úvahu její nepřiměřenost podle čl. 12 odst. 5 (viz oddíl 6).

Odchylka 2: Žádost o „novou kopii“ informací, které již byly poskytnuty ve formě kopie v reakci na předchozí žádost, například v případě, že zákazník předešle obdrženou kopii ztratil, by měla být automaticky považována za žádost o dodatečnou kopii, protože se s ohledem na rozsah a dobu zpracování vztahuje k předchozí žádosti.

29. Pokud subjekt údajů opakuje první žádost o přístup z důvodu, že obdržená odpověď nebyla úplná nebo že nebyly uvedeny důvody odmítnutí, tuto žádost nelze považovat za novou žádost, neboť se jedná pouze o připomenutí první žádosti, jíž nebylo vyhověno.

30. Pokud jde o rozdělení nákladů v případech žádostí o dodatečnou kopii, čl. 15 odst. 3 stanoví, že správce může účtovat přiměřený poplatek na základě administrativních nákladů, které byly žádostí způsobeny. To znamená, že relevantním kritériem pro stanovení výše poplatku jsou administrativní náklady. Současně by měl být poplatek přiměřený s ohledem na význam práva na přístup jako základního práva

subjektu údajů. Správce by neměl na subjekt údajů přenášet režijní náklady nebo jiné obecné výdaje, ale měl by se zaměřit na konkrétní náklady, které vznikly poskytnutím dodatečné kopie. Při organizaci tohoto procesu by měl správce účinně využívat své lidské a materiální zdroje, aby udržel náklady na pořízení kopie na nízké úrovni, a to i v případě, že správce zapojí externí podporu.

31. V případě, že se správce rozhodne účtovat poplatek, měl by předem uvést, že poplatek bude účtován, a co nejpřesněji uvést výši nákladů, které hodlá subjektu údajů účtovat, aby měl subjekt údajů možnost se rozhodnout, zda na žádosti trvá, nebo ji stáhne.

2.2.2.3 Zpřístupnění informací v běžně používané elektronické formě

32. V případě, že subjekt údajů podává žádost v elektronické formě, poskytnou se informace, je-li to možné, v elektronické formě, pokud subjekt údajů nepožádá o jiný způsob (viz čl. 12 odst. 3 GDPR). Ustanovení čl. 15 odst. 3 třetí věty doplňuje tento požadavek v souvislosti se žádostmi o přístup tím, že správce je navíc povinen poskytnout odpověď v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob. Ustanovení čl. 15 odst. 3 předpokládá, že správci, kteří jsou schopni přijímat elektronické žádosti, budou moci poskytnout odpověď na žádost v běžně používané elektronické formě (podrobnosti viz oddíl 5.2.5). Toto ustanovení se týká všech informací, které je třeba poskytnout v souladu s čl. 15 odst. 1 a 2. Pokud tedy subjekt údajů podává žádost o přístup elektronickými prostředky, musí být všechny informace poskytnuty v běžně používaném elektronickém formátu. Otázky formátu jsou dále rozvedeny v oddíle 5. Správce by měl, jako vždy, zavést vhodná bezpečnostní opatření, zejména při nakládání se zvláštní kategorií osobních údajů (viz níže, oddíl 2.3.4).

2.2.3 Možné omezení práva na přístup

33. V souvislosti s právem na přístup čl. 15 odst. 4 předpokládá zvláštní omezení. Uvádí se v něm, že je třeba zvážit možné nepříznivé dopady na práva a svobody jiných osob. Otázky týkající se rozsahu a důsledků tohoto omezení, jakož i dalších mezí a omezení stanovených v čl. 12 odst. 5 GDPR nebo podle článku 23 GDPR, jsou vysvětleny v oddíle 6.

2.3 Obecné zásady práva na přístup

34. Pokud subjekt údajů požádá o přístup ke svým údajům, informace uvedené v článku 15 GDPR musí být vždy poskytnuty v plném rozsahu. Pokud tedy správce zpracovává údaje týkající se subjektu údajů, musí poskytnout všechny informace uvedené v čl. 15 odst. 1 a případně informace uvedené v čl. 15 odst. 2. Správce musí přijmout vhodná opatření, aby zajistil úplnost, správnost a aktuálnost informací, které co nejvíce odpovídají stavu zpracování údajů v době obdržení žádosti[16]. Pokud dva nebo více správců zpracovávají údaje společně, ujednání společných správců o jejich příslušných povinnostech, pokud jde o výkon práv subjektu údajů, a zejména pokud jde o odpovědi na žádosti o přístup, nemá vliv na práva subjektů údajů vůči správci, kterému adresují svou žádost[17].

[16] Pokyny týkající se vhodných opatření viz oddíl 5 body 123 až 129.
[17] Pokyny EDPB 07/2020 k pojmům správce a zpracovatele v GDPR, bod 162f. Zpracovatelé musí být správci nápomocni, tamtéž, bod 129.

2.3.1 Úplnost informací

35. Subjekty údajů mají právo na úplné zpřístupnění všech údajů, které se jich týkají, s níže uvedenými výjimkami (podrobnosti o rozsahu viz oddíl 4.2). Pokud subjekt údajů výslovně nepožádá o něco jiného, je žádost o výkon práva na přístup chápána obecně a zahrnuje všechny osobní údaje týkající se subjektu údajů[18]. Omezení přístupu k části informací lze zvážit v následujících případech:

a) Subjekt údajů výslovně omezil žádost na dílčí soubor. Aby se předešlo poskytování neúplných informací, může správce toto omezení žádosti subjektu údajů zohlednit pouze tehdy, pokud si může být jistý, že tento výklad odpovídá přání subjektu údajů (další podrobnosti viz oddíl 3.1.1, bod 51). Subjekt údajů v zásadě nemusí opakovat žádost o předání všech údajů, které je oprávněn získat.

b) V situacích, kdy správce zpracovává velké množství údajů týkajících se subjektu údajů, může mít pochybnosti, zda žádost o přístup, která je formulována velmi obecně, skutečně směřuje k získání podrobných informací o všech druzích zpracovávaných údajů nebo o všech odvětvích správcovy činnosti. Tyto pochybnosti mohou vzniknout zejména v situacích, kdy od počátku nebylo možné poskytnout subjektu údajů nástroje k upřesnění jeho žádosti nebo kdy subjekt údajů tyto nástroje nevyužil. Správce se pak potýká s problémem, jak poskytnout úplnou odpověď a zároveň zabránit tomu, aby byl subjekt údajů zahlcen informacemi, o které nemá zájem a které nemůže účinně zpracovat. V závislosti na okolnostech a technických možnostech mohou existovat způsoby, jak tento problém vyřešit, například poskytnutím samoobslužných nástrojů v online kontextu (viz oddíl 5 týkající se vícevrstvého přístupu). Pokud taková řešení nejsou použitelná, může správce, který zpracovává velké množství informací týkajících se subjektu údajů, před poskytnutím informací požádat subjekt údajů, aby konkrétně uvedl, kterých informací nebo činností zpracování se jeho žádost týká (viz 63. bod odůvodnění GDPR). Jako příklad lze uvést společnost s několika obory činnosti nebo orgán veřejné moci s různými územně správními jednotkami, pokud správce zjistil, že se v těchto útvarech zpracovává mnoho údajů týkajících se subjektu údajů. Správci, kteří shromažďují údaje o častých činnostech subjektu údajů po delší dobu, mohou navíc zpracovávat velké množství údajů.

Příklad 3: Orgán veřejné moci zpracovává údaje o subjektu údajů v řadě různých útvarů, a to v různých souvislostech. Správa a vedení spisů jsou částečně zpracovávány neautomatizovanými prostředky a většina údajů je uložena pouze v tištěné podobě. Pokud jde o obecné znění žádosti, orgán veřejné moci má pochybnosti o tom, zda si je subjekt údajů vědom rozsahu žádosti, zejména rozmanitosti operací zpracování, které by zahrnovala, množství informací a počtu stránek, které by subjekt údajů obdržel.

Příklad 4: Velká pojišťovna obdrží dopisem obecnou žádost o přístup od osoby, která je po mnoho let jejím zákazníkem. I když jsou lhůty pro výmaz plně dodržovány, společnost ve skutečnosti zpracovává velké množství údajů týkajících se zákazníka, neboť zpracování je stále nutné pro plnění smluvních povinností vyplývajících ze smluvního vztahu se zákazníkem (včetně například trvajících závazků, komunikace o sporných otázkách se zákazníkem a třetími stranami, ...) nebo pro splnění zákonných povinností (archivované údaje, které musí být uchovávány pro daňové účely, atd.). Pojišťovna může mít pochybnosti, zda žádost, která byla formulována velmi obecně, má skutečně zahrnovat všechny druhy těchto údajů. To může být problematické zejména v případě, že pojišťovna má k dispozici pouze poštovní adresu subjektu údajů, a musí proto veškeré informace zasílat v tištěné podobě. Stejné pochybnosti však mohou být relevantní i při poskytování informací jinými prostředky.

[18] Podrobnosti naleznete níže v oddíle 5.2.3 týkajícím se tématu vícevrstvého přístupu.

Pokud se v takových případech správce rozhodne požádat subjekt údajů o upřesnění žádosti, aby splnil svou povinnost usnadnit výkon práva na přístup (čl. 12 odst. 2 GDPR), správce současně poskytne smysluplné informace o svých operacích zpracování, které by se mohly týkat subjektu údajů, a to tak, že informuje o příslušných odvětvích své činnosti, databázích atd.

Příklad 5: V pracovněprávním vztahu není v případě obecně formulované žádosti o přístup samo o sobě jasné, že zaměstnanec si přeje získat všechny údaje o přihlášení uživatele, údaje o přístupu na pracoviště, údaje o úhradách v jídelně, údaje o výplatě mzdy atd. Žádost zaměstnavatele o upřesnění by mohla vést například k vyjasnění, že zájmem zaměstnance je pochopit nebo ověřit, komu bylo předáno jeho pracovní hodnocení. Bez žádosti o upřesnění by zaměstnanec obdržel velké množství informací, aniž by měl o většinu těchto údajů zájem. Zaměstnavatel by současně musel poskytnout informace o různých souvislostech zpracování, které by se mohly zaměstnance týkat, aby mohl zaměstnanec žádost rozumně upřesnit.

Je důležité zdůraznit, že cílem žádosti o upřesnění nesmí být omezení odpovědi na žádost o přístup a nesmí sloužit k utajení jakýchkoli informací o údajích nebo zpracování, které se týkají subjektu údajů. Pokud subjekt údajů, který byl požádán o upřesnění rozsahu své žádosti, potvrdí, že chce získat všechny osobní údaje, které se ho týkají, správce mu je samozřejmě musí poskytnout v plném rozsahu.

Správce by měl být v každém případě schopen prokázat, že způsob vyřízení žádosti směřuje k co možná nejširšímu uplatnění práva na přístup a že je v souladu s jeho povinností usnadnit výkon práv subjektů údajů (čl. 12 odst. 2 GDPR). S výhradou těchto zásad může správce před poskytnutím dalších údajů podle přání subjektu údajů vyčkat na odpověď subjektu údajů, pokud správce poskytl subjektu údajů jasný přehled všech operací zpracování, které by se mohly subjektu údajů týkat, zejména pak těch, které by subjekt údajů nemusel očekávat, pokud správce rovněž umožnil přístup ke všem údajům, o které subjekt údajů jasně usiloval, a pokud navíc tyto informace spojil s jasným uvedením způsobu, jak získat přístup ke zbývajícím částem zpracovávaných údajů.

c) Na právo na přístup se vztahují výjimky nebo omezení (viz níže v oddíle 6). V takových případech by měl správce pečlivě zkontrolovat, kterých částí informací se výjimka týká, a poskytnout všechny informace, které nejsou výjimkou vyloučeny. Výjimkou nemusí být například dotčeno potvrzení samotného zpracování osobních údajů (složka 1). V důsledku toho musí být poskytnuty informace o všech osobních údajích a všechny informace uvedené v čl. 15 odst. 1 a 2, kterých se výjimka nebo omezení netýká.

2.3.2 Správnost informací

36. Informace obsažené v kopii osobních údajů poskytnuté subjektu údajů musí obsahovat skutečné informace nebo osobní údaje, které jsou o subjektu údajů k dispozici. To zahrnuje povinnost informovat i o údajích, které jsou nepřesné, nebo o zpracování údajů, které není nebo již přestalo být zákonné. Subjekt údajů může například využít právo na přístup k údajům k tomu, aby odhalil zdroj nepřesných údajů, které kolují mezi různými správci. Pokud by správce opravil nepřesné údaje předtím, než o nich subjekt údajů informoval, subjekt údajů by byl o tuto možnost připraven. Totéž platí v případě protiprávního zpracování. Jedním z hlavních účelů práva na přístup je možnost dozvědět se o protiprávním zpracování údajů, které se subjektu údajů týká. Povinností informovat o nezměněném stavu zpracování není dotčena povinnost správce ukončit protiprávní zpracování nebo opravit nepřesné údaje. Otázky týkající se pořadí, v jakém mají být tyto povinnosti plněny, jsou zodpovězeny v následujícím textu.

2.3.3 Referenční časový bod posouzení

37. Posouzení zpracovávaných údajů musí co nejvěrněji odrážet situaci v okamžiku, kdy správce obdrží žádost, a odpověď by měla zahrnovat všechny údaje, které jsou v tomto okamžiku k dispozici. To znamená, že správce se musí bez zbytečného odkladu pokusit získat informace o všech činnostech zpracování údajů, které se subjektu údajů týkají. Správci tudíž nejsou povinni poskytovat osobní údaje, které v minulosti zpracovávali, ale které již nemají k dispozici[19]. Správce například mohl vymazat osobní údaje v souladu se svou politikou uchovávání údajů a/nebo zákonnými ustanoveními, a proto již nemusí být schopen požadované osobní údaje poskytnout. V této souvislosti je třeba připomenout, že doba, po kterou jsou údaje uchovávány, by měla být stanovena v souladu s čl. 5 odst. 1 písm. e) nařízení GDPR, neboť každé uchovávání údajů musí být objektivně odůvodnitelné.

38. Současně musí správce v předstihu provést nezbytná opatření, aby usnadnil výkon práva na přístup a aby tyto žádosti vyřídil co nejdříve (viz čl. 12 odst. 3) a předtím, než bude nutné údaje vymazat. Proto by v případě krátkých lhůt pro uchovávání měla být opatření přijatá k vyřízení žádosti přizpůsobena příslušné době uchovávání, aby se usnadnil výkon práva na přístup a zabránilo trvalé nemožnosti poskytnout přístup k údajům zpracovávaným v okamžiku podání žádosti[20]. V některých případech však nemusí být možné na žádost odpovědět před plánovaným výmazem údajů. Pokud například správce v rámci co nejrychlejší odpovědi na žádost získá osobní údaje, které měly být podle plánu vymazány následující den, může potřebovat určitý dodatečný čas na posouzení toho, zda je nutné provést úpravy za účelem ochrany svobod jiných osob předtím, než žadateli vydá kopii osobních údajů. Pokud byly údaje získány během plánované doby uchovávání, může správce tyto údaje nadále zpracovávat za účelem splnění své povinnosti odpovědět na žádost. Zpracování v těchto případech může být založeno na čl. 6 odst. 1 písm. c) ve spojení s článkem 15 GDPR a doba jeho trvání musí být v souladu s požadavky čl. 12 odst. 3 GDPR[21]. Použití tohoto právního základu je omezeno na zpracování údajů, které jsou považovány za nezbytné pro vyřízení konkrétní žádosti, a nelze je použít jako odůvodnění pro obecné prodloužení doby uchovávání.

39. Správce se dále nesmí úmyslně vyhnout povinnosti poskytnout požadované osobní údaje tím, že v reakci na žádost o přístup vymaže nebo změní osobní údaje (viz oddíl 2.3.2). Pokud správce v průběhu vyřizování žádosti o přístup zjistí, že jsou údaje nepřesné nebo že je zpracování protiprávní, musí před splněním svých dalších povinností posoudit stav zpracování a informovat o tom subjekt údajů. Aby se správce vyhnul nutnosti další komunikace v této věci a aby dodržel zásadu transparentnosti, měl by ve vlastním zájmu doplnit informace o následných opravách nebo výmazech.

Příklad 6: Správce při vyřizování odpovědi na žádosti o přístup zjistí, že žádost subjektu údajů o volné pracovní místo ve společnosti správce byla uložena déle než po dobu uchovávání. Správce v tomto případě nemůže nejprve provést výmaz a poté subjektu údajů odpovědět, že žádné údaje (týkající se

[19] V tomto ohledu viz další vysvětlení v oddíle 4 těchto pokynů, jakož i v rozsudku Soudního dvora EU ve věci C-553/07 ze dne 7. května 2009, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer týkajícím se práva na přístup k informacím o příjemcích údajů nebo kategoriích příjemců údajů ve vztahu k minulosti.

[20] V zájmu usnadnění rychlého jednání by bylo možné zvážit například zavedení samoobslužného nástroje, který by subjektu údajů umožnil snadný přístup k požadovaným osobním údajům, a systému oznámení, který by správce upozornil na žádost týkající se osobních údajů s krátkou dobou uchovávání, aby se usnadnila rychlá reakce.

[21] Tím není dotčeno následné zpracování údajů po přiměřenou dobu pro důkazní účely v souvislosti s vyřizováním žádosti o přístup.

uvedené žádosti) nezpracovává. Musí nejprve poskytnout přístup a poté data odstranit. Aby se předešlo následné žádosti o výmaz, bylo by vhodné doplnit informaci o provedení a čase výmazu.

Aby byla dodržena zásada transparentnosti, měli by správci informovat subjekt údajů o konkrétním okamžiku zpracování, kterého se odpověď správce týká. V některých případech, například v souvislosti s častými komunikačními činnostmi, může mezi tímto referenčním časovým bodem, v němž bylo zpracování vyhodnoceno, a odpovědí správce dojít k dalšímu zpracování nebo úpravám údajů. Pokud si je správce takových změn vědom, doporučuje se uvést informace o těchto změnách, jakož i informace o dodatečném zpracování, které je nezbytné k odpovědi na žádost.

2.3.4 Dodržování požadavků na zabezpečení dat

40. Vzhledem k tomu, že sdělování a zpřístupňování osobních údajů subjektu údajů je operací zpracování, je správce vždy povinen zavést vhodná technická a organizační opatření k zajištění úrovně zabezpečení odpovídající riziku zpracování (viz čl. 5 odst. 1 písm. f), články 24 a 32 GDPR). To platí nezávisle na způsobu, jakým je přístup poskytován. V případě jiného než elektronického přenosu údajů subjektu údajů může správce v závislosti na rizicích, která zpracování představuje, zvážit využití formy doporučeného dopisu nebo případně nabídnout, nikoli však uložit subjektu údajů, aby si soubor vyzvedl proti podpisu přímo v jedné z provozoven správce. Pokud jsou v souladu s čl. 12 odst. 1 a 3 informace poskytovány elektronickými prostředky, musí správce zvolit elektronické prostředky, které splňují požadavky na zabezpečení údajů. Správce musí při výběru způsobu předání elektronického souboru subjektu údajů zohlednit požadavky na zabezpečení údajů rovněž v případě poskytnutí kopie údajů v běžně používané elektronické podobě (viz čl. 15 odst. 3). To může zahrnovat použití šifrování, ochranu heslem atd. Aby se usnadnil přístup k zašifrovaným údajům, měl by správce rovněž zajistit, aby byly k dispozici vhodné informace, které subjektu údajů umožní přístup k dešifrovaným informacím. V případech, kdy by požadavky na bezpečnost údajů vyžadovaly šifrování elektronické pošty mezi koncovými body, ale správce by byl schopen zaslat pouze běžný e-mail, bude muset správce použít jiné prostředky, například zaslání zařízení USB subjektu údajů (doporučenou) zásilkou.

3 OBECNÉ ÚVAHY O POSUZOVÁNÍ ŽÁDOSTÍ O PŘÍSTUP

3.1 Úvod

41. Při přijímání žádostí o přístup k osobním údajům musí správce posuzovat každou žádost individuálně. Správce zohlední mimo jiné tyto otázky, které jsou dále rozpracovány v následujících odstavcích: zda se žádost týká osobních údajů spojených se žádající osobou a kdo je žádající osoba. Cílem tohoto oddílu je objasnit, jaké prvky žádosti o přístup by měl správce při posuzování zohlednit, a projednat možné scénáře takového posouzení i jeho důsledky. Při posuzování žádosti o přístup k osobním údajům musí správce podle čl. 12 odst. 2 GDPR rovněž vzít v úvahu povinnost usnadnit výkon práv subjektu údajů a zároveň dbát na náležité zabezpečení osobních údajů[22].

[22] Správce musí zajistit náležité zabezpečení osobních údajů v souladu se zásadou integrity a důvěrnosti (čl. 5 odst. 1 písm. f) GDPR) zavedením vhodných technických a organizačních opatření uvedených v článku 32 GDPR a upřesněnými v článku 24 nařízení GDPR. Správce musí být schopen prokázat, že zajišťuje odpovídající úroveň ochrany údajů v souladu se zásadou odpovědnosti (viz také: stanovisko č. 3/2010 pracovní skupiny zřízené podle článku 29 k zásadě odpovědnosti přijaté dne 13. července 2010, 00062/10/EN WP 173, a pokyny EDPB 07/2020 k pojmům správce a zpracovatele v GDPR).

42. Správci by proto měli být aktivně připraveni na vyřizování žádostí o přístup k osobním údajům. To znamená, že správce by měl být připraven žádost přijmout, řádně ji posoudit (toto posouzení je předmětem tohoto oddílu pokynů) a bez zbytečného odkladu poskytnout žádající osobě odpovídající odpověď. Způsob, jakým se správci připraví na výkon žádostí o přístup, by měl být odpovídající a přiměřený a měl by záviset na povaze, rozsahu, kontextu a účelu zpracování, jakož i na rizicích pro práva a svobody fyzických osob v souladu s článkem 24 GDPR. V závislosti na konkrétních okolnostech mohou být správci například povinni zavést vhodný postup, jehož provádění by mělo zaručit bezpečnost údajů, aniž by bránilo výkonu práv subjektu údajů.

3.1.1 Analýza obsahu žádosti

43. Tuto otázku lze konkrétněji posoudit položením následujících otázek.

a) Týká se žádost osobních údajů?

44. Podle GDPR musí rozsah žádosti zahrnovat pouze osobní údaje[23]. Žádost o informace týkající se jiných otázek, včetně obecných informací o správci, jeho obchodních modelech nebo jeho činnostech zpracování, které se netýkají osobních údajů, proto nelze považovat za žádost podanou podle článku 15 GDPR. Kromě toho se právo na přístup nevztahuje na žádost o informace o anonymních údajích nebo údajích, které se netýkají žádající osoby nebo osoby, jejímž jménem oprávněná osoba žádost podala. Tato otázka bude podrobněji analyzována v oddíle 4.

45. Na rozdíl od anonymních údajů (které nejsou osobními údaji) jsou pseudonymizované údaje, které lze přiřadit fyzické osobě pomocí dodatečných informací, osobními údaji[24]. Pseudonymizované údaje, které lze dát do souvislosti se subjektem údajů – např. pokud subjekt údajů poskytne příslušný identifikátor umožňující jeho identifikaci nebo pokud je správce schopen dát do souvislosti údaje s žádající osobou vlastními prostředky –, je tedy třeba považovat za údaje spadající do rozsahu žádosti[25].

b) Týká se žádost žádající osoby (nebo osoby, jejímž jménem oprávněná osoba žádost podává)?

46. Obecně platí, že žádost se může týkat pouze údajů osoby, která žádost podává. Přístup k údajům jiných osob lze požadovat pouze na základě příslušného povolení[26].

Příklad 7: Subjekt údajů X pracuje jako vedoucí oddělení ve společnosti, která poskytuje svým manažerům parkovací místa na firemním parkovišti. Ačkoli má subjekt údajů X stálé parkovací místo, stává se, že při jeho příjezdu do kanceláře na další směnu je toto místo často obsazeno jiným vozem. Vzhledem k tomu, že se jedná o opakovanou situaci, subjekt údajů požádá správce kamerového systému, který pokrývá dané parkoviště, o přístup k osobním údajům tohoto řidiče, aby mohl identifikovat řidiče, který neoprávněně obsazuje jeho parkovací místo. V takovém případě nebude žádost subjektu údajů X žádostí o přístup k jeho osobním údajům, protože se netýká údajů žádající osoby, ale údajů jiné osoby – a proto by neměla být považována za žádost podle článku 15 GDPR.

[23] Pokud se žádost netýká i neosobních údajů, které jsou neoddělitelně spojeny s osobními údaji subjektu údajů. Další vysvětlení viz bod 100.

[24] Viz 26. bod odůvodnění GDPR. Další vysvětlení pojmů anonymní údaje a pseudonymizované údaje lze nalézt ve stanovisku WP29 č. 4/2007 k pojmu osobní údaje, s. 18–21.

[25] Pracovní skupina zřízená podle článku 29, Pokyny k právu na přenositelnost údajů – schválené Evropským sborem pro ochranu údajů (dále jen „pokyny WP29 k právu na přenositelnost údajů – schválené EDPB“), WP242 rev.01, 5. dubna 2017, s. 9.

[26] Viz oddíl 3.4 („Žádosti podané prostřednictvím třetích stran / zástupců“).

c) Uplatní se jiná ustanovení než GDPR, která upravují přístup k určité kategorii údajů?

47. Subjekty údajů nemusí ve své žádosti uvádět právní základ. Pokud však subjekty údajů objasní, že se jejich žádost zakládá na odvětvových právních předpisech nebo vnitrostátních právních předpisech, které upravují konkrétní otázku přístupu k určitým kategoriím údajů, a nikoli na GDPR, správce takovou žádost případně posoudí v souladu s těmito odvětvovými nebo vnitrostátními předpisy. V závislosti na příslušných vnitrostátních právních předpisech mohou mít správci často povinnost poskytnout odděleně odpovědi, z nichž každá se zabývá konkrétními požadavky stanovenými v různých legislativních aktech. To nelze zaměňovat s vnitrostátními právními předpisy nebo právními předpisy EU, které stanoví omezení práva na přístup a které je třeba dodržovat při vyřizování žádostí o přístup.

48. Pokud má správce pochybnosti o tom, které právo chce subjekt údajů uplatnit, doporučuje se požádat subjekt údajů, který žádost podává, aby objasnil předmět žádosti. Tato korespondence se subjektem údajů nemá vliv na povinnost správce jednat bez zbytečného odkladu[27]. Pokud však správce v případě pochybností požádá subjekt údajů o další vysvětlení a neobdrží žádnou odpověď, měl by s ohledem na povinnost usnadnit výkon práva osoby na přístup interpretovat informace obsažené v první žádosti a jednat na tomto základě. V souladu se zásadou odpovědnosti může správce určit přiměřenou lhůtu, ve které může subjekt údajů poskytnout další vysvětlení. Při stanovení této lhůty by si měl správce ponechat dostatek času na to, aby mohl vyhovět žádosti po uplynutí lhůty, a proto by měl zvážit, kolik času je objektivně nezbytné k sestavení a poskytnutí požadovaných údajů poté, co subjekt údajů poskytne (nebo neposkytne) upřesnění.

49. Pokud žádost spadá do oblasti působnosti GDPR, existence těchto zvláštních právních předpisů nemůže vyloučit obecné uplatnění práva na přístup, jak je stanoveno v GDPR. Pokud to umožňuje článek 23 GDPR, mohou existovat omezení stanovená právem EU nebo vnitrostátním právem (viz oddíl 6.4).

d) Spadá žádost do oblasti působnosti článku 15?

50. Je třeba poznamenat, že GDPR nezavádí žádné formální požadavky pro osoby, které žádají o přístup k údajům. K podání žádosti o přístup stačí, aby žadatelé uvedli, že si přejí vědět, jaké osobní údaje, které se jich týkají, správce zpracovává. Správce proto nemůže odmítnout poskytnutí údajů s odkazem na nedostatečné uvedení právního základu žádosti, zejména na absenci konkrétního odkazu na právo na přístup nebo na GDPR.

K podání žádosti například stačí, aby žádající osoba uvedla, že:

- chce získat přístup k osobním údajům, které se jí týkají,
- uplatňuje své právo na přístup nebo
- chce vědět, jaké informace, které se jí týkají, správce zpracovává.

Je třeba mít na paměti, že žadatelé nemusí být obeznámeni se složitostmi GDPR a že je vhodné přistupovat mírněji k osobám, které uplatňují své právo na přístup, zejména pokud toto právo uplatňují nezletilé osoby. Jak je uvedeno výše, v případě jakýchkoli pochybností se doporučuje, aby správce požádal subjekt údajů, který žádost podává, o upřesnění předmětu žádosti.

e) Chtějí subjekty údajů získat přístup ke všem informacím, které se o nich zpracovávají, nebo jen k jejich části?

[27] Viz další pokyny týkající se časových lhůt v oddíle 5.3.

51. Správce musí posoudit, zda se žádosti žádajících osob týkají všech informací, které o nich zpracovává, nebo jen jejich části. Jakékoli omezení rozsahu žádosti na konkrétní ustanovení článku 15 GDPR ze strany subjektů údajů musí být jasné a jednoznačné. Pokud například subjekty údajů požadují doslovné „informace o údajích, které jsou v souvislosti s nimi zpracovávány“, měl by správce předpokládat, že subjekty údajů mají v úmyslu uplatnit své právo podle čl. 15 odst. 1 a 2 GDPR v plném rozsahu. Taková žádost by neměla být vykládána tak, že si subjekty údajů přejí obdržet pouze kategorie osobních údajů, které jsou zpracovávány, a vzdát se svého práva na obdržení informací uvedených v čl. 15 odst. 1 písm. a) až h). Jinak by tomu bylo například v případě, kdy by si subjekty údajů přály získat v souvislosti s údaji, které uvedou, přístup ke zdroji nebo původu osobních údajů nebo ke stanovené době jejich uchovávání. V takovém případě může správce omezit svou odpověď na konkrétní požadované informace.

3.1.2 Forma žádosti

52. Jak bylo již uvedeno, GDPR neukládá subjektům údajů žádné požadavky, pokud jde o formu žádosti o přístup k osobním údajům. Proto v zásadě neexistují žádné požadavky podle GDPR, které by subjekty údajů musely dodržovat při výběru komunikačního kanálu, jehož prostřednictvím vstupují do kontaktu se správcem.

53. EDPB vyzývá správce, aby v souladu s čl. 12 odst. 2 a článkem 25 GDPR poskytovali co nejvhodnější a uživatelsky nejpřívětivější komunikační kanály, jež subjektu údajů umožní podat účinnou žádost. Pokud však subjekt údajů podá žádost prostřednictvím komunikačního kanálu poskytnutého správcem[28], který se liší od kanálu, který je uváděn jako upřednostňovaný, je taková žádost obecně považována za účinnou a správce by měl takové žádosti odpovídajícím způsobem vyhovět (viz příklady níže). Správci by měli vynaložit veškeré přiměřené úsilí, aby zajistili, že výkon práv subjektu údajů bude usnadněn (například pokud subjekt údajů zašle žádost o přístup zaměstnanci, který je na dovolené, přiměřeným úsilím může být automatická zpráva informující subjekt údajů o alternativním komunikačním kanálu pro tuto žádost).

54. Je třeba poznamenat, že správce není povinen jednat na základě žádosti zaslané na náhodnou nebo nesprávnou e-mailovou (nebo poštovní) adresu, kterou správce sám neurčil, nebo na jakýkoli komunikační kanál, který zjevně není určen k přijímání žádostí týkajících se práv subjektu údajů, pokud správce poskytl vhodný komunikační kanál, který může subjekt údajů použít.

55. Správce rovněž není povinen reagovat na žádost zaslanou na e-mailovou adresu zaměstnance správce, který se nesmí podílet na vyřizování žádostí týkajících se práv subjektů údajů (např. řidiči, uklízečky apod.). Takové žádosti nelze považovat za účinné, pokud správce jasně poskytl subjektu údajů vhodný komunikační kanál. Pokud však subjekt údajů zašle žádost zaměstnanci správce, který mu byl přidělen jako jeho stálá kontaktní osoba (jako např. správce osobního účtu v bance nebo stálý konzultant u mobilního operátora), neměl by být takový kontakt považován za náhodný a správce by měl vynaložit veškeré přiměřené úsilí, aby takovou žádost vyřídil tak, aby mohla být přesměrována na kontaktní místo a zodpovězena ve lhůtách stanovených GDPR.

56. EDPB nicméně jako osvědčený postup doporučuje, aby správci zavedli vhodné mechanismy pro usnadnění výkonu práv subjektů údajů, včetně systémů automatických odpovědí, které informují o

[28] Může se jednat například o komunikační údaje správce uvedené v jeho sděleních adresovaných přímo subjektům údajů nebo o kontaktní údaje, které správce uvádí veřejně, například v zásadách ochrany osobních údajů správce nebo v jiných povinných právních sděleních správce (např. kontaktní údaje vlastníka nebo společnosti na internetových stránkách).

nepřítomnosti zaměstnanců a vhodném náhradním kontaktu, a pokud možno mechanismy pro zlepšení interní komunikace mezi zaměstnanci o žádostech obdržených těmi, kteří nemusejí být kompetentní k vyřizování takových žádostí.

Příklad 8: Správce X uvádí na svých internetových stránkách i v oznámení o ochraně osobních údajů dvě e-mailové adresy – obecnou e-mailovou adresu správce: CONTACT@X.COM a e-mailovou adresu kontaktního místa správce pro ochranu osobních údajů: QUERIES@X.COM. Kromě toho správce X na svých internetových stránkách uvádí, že pokud chtějí fyzické osoby předložit jakékoli dotazy nebo podat žádost týkající se zpracování osobních údajů, měly by se obrátit na kontaktní místo pro ochranu údajů prostřednictvím uvedené e-mailové adresy. Subjekt údajů však zašle žádost na obecnou e-mailovou adresu správce: CONTACT@X.COM.

V takovém případě by měl správce vynaložit veškeré přiměřené úsilí, aby se jeho útvary dozvěděly o žádosti podané prostřednictvím obecného e-mailu, mohly ji přesměrovat na kontaktní místo pro ochranu údajů a odpovědět na ni ve lhůtách stanovených GDPR. Správce navíc není oprávněn prodloužit lhůtu pro odpověď na žádost jen proto, že subjekt údajů zaslal žádost na obecnou e-mailovou adresu správce, a nikoli na e-mailovou adresu kontaktního místa správce pro ochranu osobních údajů.

Příklad 9: Společnost správce Y provozuje síť fitness klubů. Správce Y na svých internetových stránkách a v oznámení o ochraně osobních údajů pro klienty fitness klubu uvádí, že pro podání jakýchkoli dotazů nebo žádostí týkajících se zpracování osobních údajů by se fyzické osoby měly obrátit na správce prostřednictvím e-mailové adresy: QUERIES@Y.COM. Subjekt údajů nicméně zašle žádost na e-mailovou adresu, kterou nalezne v šatně, kde nalezl oznámení ve znění: „Pokud nejste spokojeni s čistotou místnosti, kontaktujte nás prosím na adrese: CLEANERS@Y.COM“, což je e-mailová adresa úklidového personálu zaměstnávaného společností Y. Úklidový personál se samozřejmě nepodílí na vyřizování záležitostí týkajících se výkonu práv subjektů údajů – zákazníků fitness klubu. Ačkoli byla e-mailová adresa k dispozici v prostorách fitness klubu, subjekt údajů nemohl oprávněně očekávat, že se jedná o vhodnou kontaktní adresu pro takové žádosti, neboť internetové stránky a oznámení o ochraně osobních údajů jasně informovaly o komunikačním kanálu, který má být použit pro uplatnění práv subjektů údajů.

57. V souladu s čl. 12 odst. 3 GDPR dnem přijetí žádosti správcem zpravidla začíná běžet jednoměsíční lhůta, do které má správce poskytnout informace o opatřeních přijatých na základě žádosti (další pokyny týkající se časových lhůt jsou uvedeny v oddíle 5.3). EDPB považuje za osvědčený postup, aby správci potvrdili přijetí žádostí písemně, například zasláním e-mailů (nebo případně informací poštou) žádajícím osobám, v nichž potvrdí, že jejich žádosti byly přijaty a že jednoměsíční lhůta běží ode dne X do dne Y.

3.2 Identifikace a autentizace

58. Aby byla zajištěna bezpečnost zpracování a minimalizováno riziko neoprávněného zveřejnění osobních údajů, musí být správce schopen zjistit, které údaje se týkají subjektu údajů (identifikace), a potvrdit totožnost této osoby (autentizace).

59. Lze připomenout, že v situacích, kdy účel, pro který jsou osobní údaje zpracovávány, nevyžaduje nebo již nevyžaduje identifikaci subjektu údajů, správce nemusí uchovávat identifikaci pouze pro účely dodržování práv subjektů údajů, a to i s ohledem na zásadu minimalizace údajů. Těmito situacemi se zabývá čl. 11 odst. 1 GDPR.

60. Ustanovení čl. 12 odst. 2 GDPR stanoví, že správce nesmí odmítnout vyhovět žádosti subjektu údajů za účelem výkonu jeho práv, ledaže zpracovává osobní údaje pro účel, který nevyžaduje identifikaci subjektu údajů, a doloží, že nemůže zjistit totožnost subjektu údajů. Za těchto okolností se však subjekt údajů může rozhodnout, že poskytne dodatečné informace umožňující jeho identifikaci (čl. 11 odst. 2 GDPR)[29].

61. Správce není povinen získávat tyto dodatečné informace pro zjištění totožnosti subjektu údajů výlučně k tomu, aby vyhověl žádosti subjektu údajů, také s ohledem na zásadu minimalizace údajů. Správce by však neměl odmítnout převzít tyto dodatečné informace poskytnuté subjektem údajů, aby podpořil výkon jeho práv (57. bod odůvodnění GDPR).

Příklad 10: X je správcem údajů zpracovávaných v souvislosti s kamerovým sledováním budovy. V souladu s čl. 11 odst. 1 GDPR není správce povinen identifikovat všechny osoby, které byly zaznamenány bezpečnostní kamerou v rámci monitorování (účel nevyžadující identifikaci). Správce obdrží žádost o přístup k osobním údajům od osoby, která tvrdí, že byla zaznamenána kamerovým systémem správce. Postup správce bude záviset na poskytnutých dodatečných informacích. Pokud žadatel uvede konkrétní den a čas, kdy kamery mohly danou událost zaznamenat, je pravděpodobné, že správce bude schopen tyto údaje poskytnout (čl. 11 odst. 2 GDPR). Pokud však správce není schopen subjekt údajů identifikovat (např. pokud si správce nemůže být jistý, že žádající osoba je skutečně subjektem údajů, nebo pokud se žádost týká např. dlouhého období zaznamenávání a správce není schopen zpracovávat tak velké množství údajů), může správce odmítnout přijmout opatření, pokud prokáže, že nemůže zjistit totožnost subjektu údajů (čl. 12 odst. 2 GDPR).

Příklad 11: Správce C zpracovává osobní údaje za účelem cílení behaviorální reklamy na uživatele jeho internetových stránek. Osobní údaje shromažďované pro účely behaviorální reklamy jsou obvykle shromažďovány pomocí souborů cookie a jsou spojeny s pseudonymními náhodnými identifikátory. Subjekt údajů pan X uplatní své právo na přístup u společnosti C prostřednictvím jejích internetových stránek. Společnost C je schopna přesně identifikovat pana X a zobrazit behaviorální reklamu pro subjekt údajů propojením koncového zařízení pana X s jejím reklamním profilem pomocí souborů cookie, které jsou umístěny v koncovém zařízení. Společnost C by pak také měla být schopna přesně identifikovat pana X, aby mu mohla poskytnout přístup k jeho osobním údajům, neboť lze nalézt souvislost mezi zpracovávanými údaji a subjektem údajů. Proto a s ohledem na zásady GDPR by výše uvedený příklad nespadal do působnosti článku 11 GDPR. Přesněji řečeno, ve výše uvedeném příkladu účely správce C vyžadují identifikaci subjektů údajů, zatímco článek 11 GDPR se zabývá situací zpracování, které nevyžaduje identifikaci, kdy správce není povinen zpracovávat dodatečné údaje ve smyslu čl. 11 odst. 1 GDPR výlučně k tomu, aby byl schopen GDPR dodržovat. V některých případech by proto neměly být za účelem výkonu práv subjektu údajů požadovány žádné dodatečné údaje.

Pokud se však pan X pokusí uplatnit své právo na přístup e-mailem nebo poštou, nebude mít správce C v této souvislosti jinou možnost než požádat pana X o poskytnutí „dodatečných informací“ (čl. 12 odst. 6 GDPR), aby mohl identifikovat reklamní profil spojený s panem X. V tomto případě bude dodatečnou informací identifikátor cookie uložený v koncovém zařízení pana X.

62. V případě prokázané nemožnosti zjistit totožnost subjektu údajů (článek 11 nařízení GDPR) musí správce subjekt údajů o této skutečnosti informovat, pokud je to možné, neboť správce musí na žádosti subjektu údajů reagovat bez zbytečného odkladu a uvést důvody, proč nehodlá těmto žádostem

[29] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 13.

vyhovět. Tyto informace je třeba poskytnout, pouze „pokud je to možné“, protože správce nemusí být schopen informovat subjekty údajů, pokud není možné je identifikovat.

63. Jak v případě, že zpracování nevyžaduje identifikaci, tak v případě, že identifikaci vyžaduje, může správce, pokud má důvodné pochybnosti o totožnosti fyzické osoby, která žádost podává, požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů (čl. 12 odst. 6 GDPR).

64. GDPR nestanoví žádné požadavky týkající se způsobu ověření subjektu údajů. Nicméně v článcích 11 a 12 GDPR jsou uvedeny podmínky pro výkon všech práv subjektu údajů, včetně práva na přístup k osobním údajům.

65. Je třeba mít na paměti, že správce zpravidla nemůže požadovat více osobních údajů, než je nezbytné pro toto ověření, a že použití těchto informací by mělo být přísně omezeno na splnění žádosti subjektu údajů.

66. Mezi subjekty údajů a správci již často existují postupy autentizace. Správci mohou tyto postupy autentizace používat za účelem zjištění totožnosti subjektů údajů, které žádají o své osobní údaje nebo uplatňují práva udělená podle GDPR[30]. V opačném případě by měli správci zavést postup autentizace, který to umožní[31].

67. V případech, kdy správce požaduje dodatečné informace nezbytné k potvrzení totožnosti subjektu údajů nebo mu tyto dodatečné informace subjekt údajů poskytne, správce musí pokaždé posoudit, jaké informace mu umožní potvrdit totožnost subjektu údajů, a případně položí žádající osobě dodatečné otázky nebo požádá subjekt údajů o předložení některých dodatečných identifikačních prvků, je-li to přiměřené (viz oddíl 3.3).

68. Aby mohl subjekt údajů poskytnout dodatečné informace potřebné ke zjištění jeho totožnosti nebo k identifikaci jeho údajů, měl by správce informovat subjekt údajů o povaze požadovaných dodatečných informací, které umožní identifikaci. Takových dodatečných informací by nemělo být více než informací původně potřebných k ověření totožnosti subjektu údajů. Obecně platí, že skutečnost, že správce může požadovat dodatečné informace k posouzení totožnosti subjektu údajů, nemůže vést k nepřiměřeným požadavkům a ke shromažďování osobních údajů, které nejsou relevantní nebo nezbytné k posílení souvislosti mezi fyzickou osobou a požadovanými osobními údaji[32].

69. V důsledku toho, jestliže jsou informace shromážděné online spojeny s pseudonymy nebo jinými jedinečnými identifikátory, může správce zavést vhodné postupy, které umožní žádající osobě podat žádost o přístup k údajům a získat údaje, které se jí týkají[33].

Příklad 12: Subjekt údajů paní X žádá o přístup ke svým údajům při hovoru s konzultantem na poradenské lince energetické společnosti, s níž uzavřela smlouvu. Konzultant, který má pochybnosti o totožnosti osoby, která žádost podává, vygeneruje v systému společnosti jednorázový jedinečný kód zaslaný na mobilní telefonní číslo uživatele, které uvedl při zřízení účtu, jako součást systému dvojího ověření, což by mělo být v tomto případě považováno za přiměřený postup.

[30] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 14.
[31] Viz další pokyny týkající se autentizace v oddíle 3.3.
[32] Tamtéž, s. 14.
[33] Tamtéž, s. 13–14.

3.3 Posouzení přiměřenosti, pokud jde o autentizaci žádající osoby

70. Jak je uvedeno výše, pokud má správce oprávněné důvody k pochybnosti o totožnosti žádající osoby, může si vyžádat dodatečné informace k potvrzení totožnosti subjektu údajů. Správce však musí zároveň zajistit, aby neshromažďoval více osobních údajů, než je nezbytné pro autentizaci žádající osoby. Správce proto provede posouzení přiměřenosti, které musí zohlednit typ zpracovávaných osobních údajů (např. zvláštní kategorie údajů či nikoli), povahu žádosti, kontext, v němž je žádost podávána, jakož i případnou újmu, která by mohla vzniknout v důsledku nevhodného zveřejnění. Při posuzování přiměřenosti je třeba mít na paměti, že je nutné se vyhnout nadměrnému shromažďování údajů a zároveň zajistit odpovídající úroveň zabezpečení zpracování.

71. Správce by měl zavést postup ověřování, aby si byl jistý totožností osob, které žádají o přístup ke svým údajům[34], a zajistit zabezpečení zpracování v celém procesu vyřizování žádostí o přístup v souladu s článkem 32 GDPR, včetně například bezpečného kanálu pro subjekty údajů pro poskytnutí dodatečných informací. Metoda použitá pro autentizaci by měla být relevantní, vhodná, přiměřená a měla by respektovat zásadu minimalizace údajů. Pokud správce ukládá opatření zaměřená na autentizaci subjektu údajů, která představují zátěž, musí to náležitě odůvodnit a zajistit soulad se všemi základními zásadami, včetně minimalizace údajů a povinnosti usnadnit subjektům údajů výkon jejich práv (čl. 12 odst. 2 GDPR).

72. V online kontextu může mechanismus autentizace zahrnovat stejné pověřovací údaje, které subjekt údajů používá pro přihlášení k online službám poskytovaným správcem (57. bod odůvodnění GDPR)[35].

73. V praxi postupy autentizace často již existují a správci nemusejí zavádět další záruky, aby zabránili neoprávněnému přístupu ke službám. S cílem umožnit fyzickým osobám přístup k údajům obsaženým v jejich účtech (jako je e-mailový účet, účet na sociálních sítích nebo v internetových obchodech) správci nejčastěji požadují přihlášení prostřednictvím uživatelského jména a hesla uživatele, což by v těchto případech mělo pro autentizaci subjektu údajů postačovat[36]. Autentizace subjektů údajů je kromě toho správcem často prováděna před uzavřením smlouvy nebo získáním jejich souhlasu se zpracováním, a osobní údaje použité k registraci fyzické osoby, které se zpracování týká, proto mohou být použity také jako důkaz pro autentizaci subjektu údajů pro účely přístupu[37]. Proto je nepřiměřené požadovat kopii dokladu totožnosti v případě, že subjekt údajů, který žádost podává, je již správcem autentizován.

74. Je třeba zdůraznit, že použití kopie dokladu totožnosti jako součásti procesu autentizace představuje riziko pro zabezpečení osobních údajů a může vést k neoprávněnému nebo protiprávnímu zpracování, a proto by mělo být považováno za nepatřičné, pokud to není nezbytné, vhodné a v souladu s vnitrostátním právem. V takových případech by správci měli mít zavedeny systémy, které zajišťují úroveň zabezpečení vhodnou ke zmírnění vyšších rizik pro práva a svobody subjektu údajů, který takové údaje obdrží. Je také důležité poznamenat, že autentizace pomocí průkazu totožnosti nemusí

[34] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 14.
[35] Viz další pokyny týkají se metod autentizace v pokynech EDPB 01/2021 o příkladech týkajících se oznamování porušení zabezpečení osobních údajů, přijatých dne 14. ledna 2021, s. 30–31, a v pokynech EDPB 02/2021 o virtuálních hlasových asistentech, verze 2.0, přijatých dne 7. července 2021, oddíl 3.7.
[36] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 14.
[37] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 14.

být v internetovém prostředí přínosná (např. při použití pseudonymů), pokud dotyčná osoba nemůže poskytnout žádné další důkazy, např. další charakteristiky odpovídající uživatelskému účtu.

75. Vzhledem k tomu, že řada organizací (např. hotely, banky, půjčovny automobilů) požaduje kopie průkazů totožnosti svých klientů, nemělo by to být obecně považováno za vhodný způsob autentizace. Správce může případně zavést rychlé a účinné bezpečnostní opatření k identifikaci subjektu údajů na základě dříve provedené autentizace, např. prostřednictvím e-mailu nebo textové zprávy obsahující potvrzovací odkazy, bezpečnostní otázky nebo potvrzovací kódy[38].

76. Informace v průkazu totožnosti, které nejsou nezbytné pro potvrzení totožnosti subjektu údajů, jako je přístupové a pořadové číslo, státní příslušnost, výška, barva očí, fotografie a strojově čitelná zóna, může subjekt údajů v závislosti na posouzení každého jednotlivého případu před předložením správci údajů upravit nebo skrýt, s výjimkou případů, kdy vnitrostátní právní předpisy vyžadují úplnou nezakrytou kopii průkazu totožnosti (viz bod 78 níže). Obecně platí, že k ověření totožnosti správci postačí datum vydání nebo datum ukončení platnosti, vydávající orgán a celé jméno odpovídající online účtu, a to vždy za předpokladu, že je zajištěna pravost kopie a vztah k žadateli. Další informace, jako je datum narození subjektu údajů, mohou být vyžadovány pouze v případě, že přetrvává riziko záměny identity, pokud je správce schopen porovnat tyto informace s informacemi, které již zpracovává.

77. Aby byla dodržena zásada minimalizace údajů, měl by správce informovat subjekt údajů o tom, které informace nejsou potřebné, a o možnosti tyto části dokladu totožnosti upravit nebo skrýt. V takovém případě, jestliže subjekt údajů neví, jak takové informace upravit, nebo je upravit není schopen, je osvědčeným postupem, aby tyto informace upravil správce po obdržení dokumentu, pokud tak správce může učinit s ohledem na prostředky, které má za daných okolností k dispozici.

Příklad 13: Uživatelka, paní Y, si v internetovém obchodě vytvořila účet chráněný heslem a uvedla svůj e-mail a/nebo uživatelské jméno. Majitelka účtu následně požádá správce o informaci, zda zpracovává její osobní údaje, a pokud ano, požádá o přístup k nim v rozsahu uvedeném v článku 15. Správce si vyžádá průkaz totožnosti osoby, která žádost podává, aby potvrdil její totožnost. Postup správce je v tomto případě nepřiměřený a vede ke zbytečnému shromažďování údajů.

Aby však správce mohl potvrdit totožnost žádající osoby a zároveň zabránil zbytečnému shromažďování údajů, mohl by po ní požadovat autentizaci prostřednictvím přihlášení k účtu nebo jí položit (nevtíravé) bezpečnostní otázky, jejichž odpověď by měl znát pouze subjekt údajů, nebo použít vícefaktorovou autentizaci, která byla nastavena při registraci účtu subjektu údajů, nebo použít jiné existující komunikační prostředky, o nichž je známo, že patří subjektu údajů, jako je e-mailová adresa nebo telefonní číslo, pro účely zaslání přístupového hesla.

Příklad 14: Klient banky, pan Y, si chce vzít spotřebitelský úvěr. Za tímto účelem se pan Y dostaví na pobočku banky, aby získal informace, včetně informací o tom, které jeho osobní údaje jsou nezbytné pro posouzení jeho úvěruschopnosti. K ověření totožnosti subjektu údajů si konzultant vyžádá notářsky ověřené potvrzení o jeho totožnosti, aby mu mohl požadované informace poskytnout.

[38] Viz také nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Správce by neměl požadovat notářsky ověřené potvrzení totožnosti, pokud to není nezbytné, vhodné a v souladu s vnitrostátním právem (například pokud osoba dočasně nevlastní žádný doklad totožnosti a vnitrostátní právo pro provedení právního úkonu vyžaduje prokázání totožnosti subjektu údajů). Takový postup vystavuje žádající osoby dalším nákladům a představuje pro subjekty údajů nadměrnou zátěž, která brání výkonu jejich práva na přístup.

78. Aniž jsou dotčeny výše uvedené obecné zásady, může být za určitých okolností autentizace na základě průkazu totožnosti odůvodněným a přiměřeným opatřením, zejména pro subjekty, které zpracovávají zvláštní kategorie osobních údajů nebo provádějí zpracování údajů, které může představovat riziko pro subjekt údajů (např. lékařské nebo zdravotní informace). Současně je však třeba mít na paměti, že některé vnitrostátní předpisy stanoví omezení zpracování údajů obsažených ve veřejných listinách, včetně dokladů potvrzujících totožnost osoby (také na základě článku 87 GDPR). Omezení zpracování údajů z těchto dokumentů se mohou týkat zejména skenování nebo kopírování průkazů totožnosti nebo zpracování úředních osobních identifikačních čísel[39].

79. S ohledem na výše uvedené musí správce v případě, že je požadován průkaz totožnosti (a je to v souladu s vnitrostátním právem a odůvodněné a přiměřené podle GDPR), zavést záruky, jež zabrání protiprávnímu zpracování průkazu totožnosti. Bez ohledu na platné vnitrostátní předpisy týkající se ověření totožnosti to může zahrnovat zdržení se pořizování kopie nebo vymazání kopie průkazu totožnosti bezprostředně po úspěšném ověření totožnosti subjektu údajů. Je tomu tak proto, že další uchovávání kopie průkazu totožnosti by pravděpodobně znamenalo porušení zásad účelového omezení a omezení uložení (čl. 5 odst. 1 písm. b) a e) GDPR) a rovněž vnitrostátních právních předpisů týkajících se zpracování národního identifikačního čísla (článek 87 GDPR). EDPB doporučuje jako osvědčený postup, aby správce po kontrole průkazu totožnosti uvedl poznámku například „Průkaz totožnosti byl zkontrolován“, aby se předešlo zbytečnému kopírování nebo uchovávání kopií průkazů totožnosti.

3.4 Žádosti podané prostřednictvím třetích stran / zástupců

80. Ačkoli právo na přístup k údajům obecně vykonávají subjekty údajů, kterým toto právo náleží, je možné, aby žádost jménem subjektu údajů podala třetí strana. To se může vztahovat mimo jiné na jednání prostřednictvím zástupce nebo zákonných zástupců jménem nezletilých osob, jakož i jednání prostřednictvím jiných subjektů prostřednictvím online portálů. Za určitých okolností může být, pokud je to vhodné a přiměřené (viz oddíl 3.3 výše), vyžadováno ověření totožnosti osoby oprávněné vykonávat právo na přístup, jakož i oprávnění jednat jménem subjektu údajů[40]. Je třeba připomenout, že zpřístupnění osobních údajů někomu, kdo k nim nemá právo na přístup, může znamenat porušení zabezpečení osobních údajů[41].

81. Přitom je třeba zohlednit vnitrostátní právní předpisy upravující právní zastoupení (např. plné moci), které mohou stanovit zvláštní požadavky na prokázání oprávnění podat žádost jménem subjektu údajů, neboť GDPR tuto otázku neupravuje. V souladu se zásadou odpovědnosti, jakož i s ostatními zásadami ochrany údajů, musí být správci schopni prokázat existenci příslušného oprávnění podat žádost jménem subjektu údajů a obdržet požadované informace, s výjimkou případů, kdy se vnitrostátní právo

[39] Některé členské státy v tomto ohledu zavedly ve svých vnitrostátních předpisech takové omezení, které například stanoví, že pořizování kopií průkazů totožnosti je zákonné pouze tehdy, pokud vyplývá přímo z ustanovení právního předpisu.
[40] Pokud jde o lhůty pro uplatnění práva na přístup v případě, že správce potřebuje získat dodatečné informace, viz bod 157.
[41] Čl. 4 bod 12 GDPR.

liší (např. vnitrostátní právo obsahuje zvláštní pravidla týkající se důvěryhodnosti advokátů), v důsledku čehož je úkolem správce, aby ověřil totožnost zástupce (např. v případě advokátů ověřit zápis u advokátní komory). Proto se doporučuje shromáždit v tomto ohledu odpovídající dokumentaci, pokud jde o dříve uvedená obecná pravidla týkající se potvrzení totožnosti fyzické osoby, která podává žádost, a jestliže má správce důvodné pochybnosti o totožnosti osoby jednající jménem subjektu údajů, musí si vyžádat dodatečné informace pro potvrzení totožnosti této osoby.

82. Dalším příkladem přístupu třetí strany odlišné od subjektu údajů je výkon práva na přístup k osobním údajům zesnulých osob, avšak 27. bod odůvodnění upřesňuje, že na osobní údaje zesnulých osob se GDPR nevztahuje. Tuto otázku proto řeší vnitrostátní právo a členské státy mohou stanovit pravidla pro zpracování osobních údajů zesnulých osob. Je však třeba mít na paměti, že údaje se mohou mimoto týkat i žijících třetích osob, např. v souvislosti s požadovaným přístupem ke korespondenci zesnulé osoby. Důvěrnost těchto údajů musí být stále chráněna.

3.4.1 Výkon práva na přístup jménem dětí

83. Děti zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů[42]. Veškeré informace a sdělení určené dětem v případech, kdy jsou zpracovávány jejich osobní údaje, by měly být podávány za použití jasných a srozumitelných jazykových prostředků, aby jim děti snadno porozuměly[43].

84. Děti jsou svéprávnými subjekty údajů, a proto i jim náleží právo na přístup. V závislosti na vyspělosti a schopnostech dítěte může být zapotřebí, aby jeho jménem jednala třetí osoba, např. nositel rodičovské zodpovědnosti.

85. Hlavním hlediskem při všech rozhodnutích týkajících se výkonu práva na přístup v souvislosti s dětmi by měl být nejlepší zájem dítěte, zejména pokud je právo na přístup vykonáváno jménem dítěte, například nositelem rodičovské zodpovědnosti.

86. Vzhledem ke zvláštní ochraně osobních údajů dětí, již poskytuje GDPR, musí správce přijmout vhodná opatření, aby zabránil jakémukoli zpřístupnění osobních údajů nezletilých osob neoprávněné osobě (v tomto ohledu viz také oddíl 3.4 výše).

87. A konečně, právo nositele rodičovské zodpovědnosti jednat jménem dítěte by nemělo být zaměňováno s případy mimo oblast práva na ochranu údajů, kdy vnitrostátní právní předpisy mohou stanovit právo nositele rodičovské zodpovědnosti žádat o informace týkající se dítěte (např. ohledně prospěchu dítěte ve škole) a tyto informace dostávat.

3.4.2 Uplatnění práva na přístup prostřednictvím portálů / kanálů poskytovaných třetí stranou

88. Existují společnosti, které poskytují služby umožňující subjektům údajů podávat žádosti o přístup prostřednictvím portálu. Subjekt údajů se přihlásí a získá přístup na portál, prostřednictvím kterého

[42] 38. bod odůvodnění GDPR. Jak je uvedeno v pracovním programu sboru EDPB, jeho záměrem je poskytnout pokyny k údajům týkajícím se dětí. Očekává se, že takový dokument poskytne více pokynů ohledně podmínek, za kterých mohou děti vykonávat své vlastní právo na přístup a nositel rodičovské zodpovědnosti může vykonávat právo na přístup jménem dítěte.
[43] 58. bod odůvodnění GDPR. Pokyny EDPB 05/2020 k souhlasu podle nařízení 2016/679, oddíl 7.

může podat například žádost o přístup, žádat o opravu nebo výmaz údajů u různých správců. Při používání portálů poskytovaných třetí stranou vznikají různé otázky.

89. Prvním problémem, který musí správci za těchto okolností řešit, je zajistit, aby třetí strana jednala jménem subjektu údajů oprávněně, protože je třeba zajistit, aby údaje nebyly zpřístupněny neoprávněným osobám.

90. Správce, který obdrží žádost podanou prostřednictvím takového portálu, musí navíc tuto žádost vyřídit bez výjimky včas[44]. Správce však nemá povinnost poskytnout údaje podle článku 15 nařízení GDPR přímo portálu, pokud správce například zjistí, že bezpečnostní opatření jsou nedostatečná, nebo pokud by bylo považováno za vhodné použít jiný způsob zpřístupnění údajů subjektu údajů. Za těchto okolností, pokud má správce zavedeny jiné postupy pro účinné a zabezpečené vyřizování žádostí o přístup, může požadované informace poskytnout prostřednictvím těchto postupů.

4 ROZSAH PRÁVA NA PŘÍSTUP A OSOBNÍ ÚDAJE A INFORMACE, KTERÝCH SE TÝKÁ

91. Cílem tohoto oddílu je objasnit definici osobních údajů (4.1) a obecně vyjasnit rozsah informací, na které se právo na přístup vztahuje (4.2 a 4.3). Za zmínku stojí, že rozsah pojmu osobní údaje, a tedy rozlišení mezi osobními údaji a jinými údaji, je nedílnou součástí posouzení, které správce provádí za účelem určení rozsahu údajů, k nimž je subjekt údajů oprávněn získat přístup[45].

92. Úvodem je třeba připomenout, že právo na přístup lze uplatnit pouze v souvislosti se zpracováním osobních údajů, které spadá do věcné a územní působnosti GDPR. Na osobní údaje, které nejsou zpracovávány za použití automatizovaných postupů nebo které nejsou obsaženy v evidenci nebo do ní nemají být zařazeny podle čl. 2 odst. 1 GDPR nebo které jsou zpracovávány fyzickou osobou v průběhu výlučně osobních nebo domácích činností podle čl. 2 odst. 2 GDPR, se proto právo na přístup nevztahuje.

4.1 Definice osobních údajů

93. Ustanovení čl. 15 odst. 1 a 3 GDPR odkazuje na „*osobní údaje*“, resp. „*zpracovávané osobní údaje*“. Rozsah práva na přístup je proto v první řadě určen rozsahem pojmu osobní údaje, který je definován v čl. 4 bodě 1 GDPR[46]. Pojem osobní údaje byl již předmětem několika dokumentů pracovní skupiny

[44] Pokud jde o lhůty pro uplatnění práva na přístup v případě, že správce potřebuje získat dodatečné informace, viz bod 157.

[45] V souladu se zásadou záměrné ochrany soukromí je taková analýza součástí posouzení vhodných opatření a záruk na ochranu zásad ochrany údajů a práv subjektů údajů, které se provádí „*jak v době určení prostředků pro zpracování, tak v době zpracování samotného*“, přičemž jedním z měřítek může být např. zkrácení doby odezvy při uplatnění práv subjektů údajů. Pro další vysvětlení viz pokyny EDPB 4/2019 k záměrné a standardní ochraně osobních údajů podle článku 25.

[46] Podle čl. 4 bodu 1 se „osobními údaji“ rozumí „veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“.

zřízené podle článku 29[47] [48] a byl vykládán Soudním dvorem EU, a to i v souvislosti s právem na přístup podle článku 12 směrnice 95/46/ES.

94. Pracovní skupina zřízená podle článku 29 měla za to, že definice osobních údajů ve směrnici 95/46/ES *„odráží záměr evropského zákonodárce pojímat „osobní údaje" velmi široce*"[49]. Podle GDPR se definice stále vztahuje na *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě*". Kromě základních osobních údajů, jako je jméno a adresa, telefonní číslo atd., může do této definice spadat neomezené množství údajů, včetně lékařských nálezů, historie nákupů, ukazatelů úvěruschopnosti, obsahu komunikace atd. Vzhledem k širokému rozsahu definice osobních údajů by restriktivní posouzení této definice správcem vedlo k chybné klasifikaci osobních údajů[50] a v konečném důsledku k porušení práva na přístup.

95. Ve spojených věcech C-141/12 a C-372/12[51] Soudní dvůr EU rozhodl, že právo na přístup se vztahuje na osobní údaje obsažené v protokolech, konkrétně na *„jméno, datum narození, státní příslušnost, pohlaví, etnický původ, náboženství a jazyk žadatele"* a *„případně údaje uvedené v právním rozboru, který je v protokolu obsažen*", nikoli však na právní rozbor jako takový[52]. Právní rozbor v této souvislosti nebyl sám o sobě předmětem kontroly jeho přesnosti ze strany subjektu údajů ani jeho opravy. Poskytnutí přístupu k právnímu rozboru navíc neplní účel zaručení soukromí, ale přístupu ke správním dokumentům.

96. Ve věci Nowak[53] provedl Soudní dvůr EU širší analýzu a konstatoval, že písemné odpovědi uvedené zkoušeným v rámci odborné zkoušky a veškeré korekturní poznámky zkoušejícího týkající se těchto odpovědí představují osobní údaje, které se týkají zkoušeného. Přesněji řečeno, tyto subjektivní informace jsou osobními údaji *„ve formě názoru nebo hodnocení pod podmínkou, že jsou „o" dotčené osobě*"[54], na rozdíl od zkušebních otázek, které se za osobní údaje nepovažují[55]. Posouzení souvislostí by tedy mělo vyjasnit účinek nebo důsledek, který může mít informace na fyzickou osobu, a tím i rozsah práva na přístup.

Příklad 15: Fyzická osoba má pracovní pohovor u společnosti. V této souvislosti uchazeč o zaměstnání předkládá životopis a motivační dopis. Během pohovoru si personalista dělá poznámky do počítače, a dokumentuje tak průběh pohovoru. Poté uchazeč o zaměstnání jako subjekt údajů požádá o přístup k osobním údajům, které se ho týkají a které společnost jako správce shromáždila v průběhu náborového řízení.

Správce je povinen poskytnout subjektu údajů osobní údaje, které aktivně sdělil ve svém životopise a motivačním dopise. Kromě toho musí správce poskytnout subjektu údajů shrnutí pohovoru, včetně

[47] Pracovní skupina pro ochranu údajů zřízená podle článku 29 je nezávislá evropská pracovní skupina, která se zabývala otázkami ochrany soukromí a osobních údajů do 25. května 2018 (začátek platnosti GDPR), předchůdce Evropského sboru pro ochranu osobních údajů (EDBP).
[48] Např. pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení (EU) 2016/679, WP251 rev.01, s. 19; pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 9.
[49] Pracovní skupina zřízená podle článku 29, stanovisko č. 4/2007 k pojmu osobní údaje, s. 4.
[50] Jako informace, které se netýkají identifikované nebo identifikovatelné osoby.
[51] SDEU, spojené věci C-141/12 a C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel v. M a S, 17. července 2014.
[52] SDEU, spojené věci C-141/12 a C-372/12, YS a další, body 38 a 48.
[53] SDEU, C-434/16, Peter Nowak v. Data Protection Commissioner, 20. prosince 2017.
[54] Soudní dvůr EU, C 434/16, Nowak, body 34–35.
[55] SDEU, C-434/16, Nowak, bod 58.

subjektivních poznámek k chování subjektu údajů, které personalista zapsal během pracovního pohovoru, s výhradou výjimek podle vnitrostátního práva a v souladu s článkem 23 GDPR.

97. S ohledem na konkrétní okolnosti případu tak při posuzování konkrétní žádosti o přístup musí správci poskytnout mimo jiné tyto typy údajů, aniž je dotčen čl. 15 odst. 4 GDPR:

- zvláštní kategorie osobních údajů podle článku 9 GDPR,
- osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle článku 10 GDPR,
- údaje, které subjekt údajů vědomě a aktivně poskytl (např. údaje o účtu poskytnuté prostřednictvím formulářů, odpovědi na dotazník)[56],
- pozorované údaje nebo nezpracované údaje poskytnuté subjektem údajů na základě používání služby nebo zařízení (např. údaje zpracovávané propojenými objekty, historie transakcí, záznamy o činnosti, jako jsou záznamy o přístupu, historie používání internetových stránek, vyhledávací činnosti, údaje o poloze, klikání, jedinečné aspekty chování osoby, jako je rukopis, stisky tlačítek, zvláštní způsob chůze nebo mluvy)[57],
- údaje odvozené z jiných údajů, nikoli přímo poskytnuté subjektem údajů (např. úvěrový poměr, klasifikace založená na společných atributech subjektů údajů, země pobytu odvozená z poštovního směrovacího čísla)[58],
- údaje odvozené z jiných údajů, nikoli přímo poskytnuté subjektem údajů (např. za účelem přidělení úvěrového skóre nebo dodržení pravidel proti praní peněz, výsledky algoritmů, výsledky posouzení zdravotního stavu nebo personalizace či doporučování)[59],
- pseudonymizované údaje oproti anonymizovaným údajům (viz také oddíl 3 těchto pokynů).

Příklad 16: Prvky, které byly použity k rozhodnutí např. o povýšení, zvýšení platu nebo novém pracovním zařazení zaměstnance (např. roční pracovní hodnocení, žádosti o odbornou přípravu, disciplinární řízení, pořadí, kariérní potenciál), jsou osobními údaji týkajícími se daného zaměstnance. K těmto prvkům má tedy subjekt údajů přístup na svou žádost a za dodržení čl. 15 odst. 4 GDPR v případě, že se osobní údaje kupříkladu týkají i jiné fyzické osoby (např. totožnost nebo prvky odhalující totožnost jiného zaměstnance, jehož vyjádření o pracovní výkonnosti je zahrnuta do ročního pracovního hodnocení, mohou podléhat omezením podle čl. 15 odst. 4 GDPR, a je tedy možné, že je nelze sdělit subjektu údajů v zájmu ochrany práv a svobod uvedeného zaměstnance). Mohou však platit vnitrostátní pracovněprávní předpisy, například pokud jde o přístup zaměstnanců k osobním spisům, nebo jiné vnitrostátní předpisy, např. předpisy týkající se služebního tajemství. Za všech okolností musí taková omezení výkonu práva na přístup subjektu údajů (nebo jiných práv) stanovená ve vnitrostátním právu respektovat podmínky článku 23 GDPR (viz oddíl 6.4).

98. Z výše uvedeného neúplného seznamu osobních údajů, jež mohou být subjektu údajů v souvislosti s žádostí o přístup poskytnuty, lze vyvodit určité závěry Z výše uvedeného je zřejmé, že správce nesmí při poskytování přístupu k osobním údajům rozlišovat mezi údaji v tištěné podobě a údaji

[56] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 9.
[57] Stanovisko WP29 č. 4/2007 k pojmu osobní údaje, s. 8.
[58] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 10–11.
[59] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 10–11; pracovní skupina zřízená podle článku 29, Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení (EU) 2016/679 – schválené Evropským sborem pro ochranu osobních údajů (dále jen „pokyny WP29 k automatizovanému individuálnímu rozhodování a profilování – schválené EDPB“), WP 251 rev.01, 6. února 2018, s. 9–10.

v elektronické podobě, pokud spadají do oblasti působnosti GDPR. Jinými slovy, osobní údaje, které jsou obsaženy v tištěné podobě v evidenci nebo do ní mají být zařazeny, podléhají právu na přístup stejným způsobem jako osobní údaje uložené v paměti počítače například prostřednictvím binárního kódu nebo videonahrávky.

99. Kromě toho právo na přístup, stejně jako většina práv subjektů údajů, zahrnuje jak vydedukované, tak odvozené údaje, včetně osobních údajů vytvořených poskytovatelem služeb, zatímco právo na přenositelnost údajů zahrnuje pouze údaje poskytnuté subjektem údajů[60]. Proto by v případě žádosti o přístup a na rozdíl od žádosti o přenositelnost údajů měly být subjektu údajů poskytnuty nejen osobní údaje poskytnuté správci za účelem provedení následné analýzy nebo posouzení těchto údajů, ale také výsledek takové následné analýzy nebo posouzení.

100. Je také důležité připomenout, že existují informace, jako jsou anonymní údaje[61], což jsou údaje, které se přímo ani nepřímo nevztahují k identifikovatelné osobě, a které jsou tudíž z oblasti působnosti GDPR vyloučeny. Například umístění serveru, na kterém se zpracovávají osobní údaje subjektu údajů, není osobním údajem. Toto rozlišení může být náročné a správci si mohou klást otázku, jak stanovit jasnou hranici mezi osobními a neosobními údaji, zejména v případě smíšených souborů údajů. V takovém případě může být užitečné rozlišovat mezi smíšenými soubory údajů, v nichž jsou osobní a neosobní údaje neoddělitelně propojeny, a těmi, v nichž tomu tak není. Osobní a neosobní údaje mohou být neoddělitelně propojeny ve smíšených souborech údajů a spadají plně do rozsahu působnosti práva na přístup subjektu údajů, kterého se osobní údaje týkají[62]. V jiných případech nemusí být osobní a neosobní údaje ve smíšených souborech údajů neoddělitelně propojeny, takže je subjektu údajů umožněn přístup pouze k osobním údajům v souboru. Společnost bude například muset poskytnout subjektu údajů jednotlivá hlášení o incidentech v oblasti IT, která vyvolal, ale nikoliv databázi znalostí společnosti o problémech v oblasti IT. Bezpečnostní opatření, která správce zavedl, však obecně nelze chápat jako osobní údaje, a pokud nejsou neoddělitelně spojena s osobními údaji, a právo na přístup se na ně tudíž nevztahuje.

101. Před uzavřením tohoto oddílu EDPB v této souvislosti připomíná, že ochrana fyzických osob v souvislosti se zpracováním osobních údajů zahrnuje všechny výše uvedené typy osobních údajů a že restriktivní výklad definice je v rozporu s ustanoveními GDPR a v konečném důsledku porušuje článek 8 Listiny základních práv. Uplatnění odlišného režimu pro výkon práva ve vztahu k některým typům osobních údajů, které GDPR nepředpokládá, lze zavést výlučně zákonem, a to v souladu s článkem 23 GDPR (jak je dále vysvětleno v oddíle 6.4). Správci tedy nemohou omezit výkon práva na přístup nepatřičným omezením rozsahu osobních údajů.

4.2 Osobní údaje, kterých se právo na přístup týká

102. Podle čl. 15 odst. 1 GDPR „*subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, <u>které se ho týkají, jsou či nejsou zpracovávány</u>, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím*“ (zvýraznění doplněno).

[60] Jak již bylo uvedeno v pokynech WP29 k právu na přenositelnost údajů – schválených EDPB, s. 10, a zopakováno v pokynech WP29 k automatizovanému individuálnímu rozhodování a profilování – schválených EDPB, s. 17.

[61] Další vysvětlení pojmu anonymizace lze nalézt ve stanovisku pracovní skupiny zřízené podle článku 29 č. 05/2014 k technikám anonymizace, WP216, 10. dubna 2014, s. 5–19.

[62] Sdělení Komise Evropskému parlamentu a Radě, Pokyny k nařízení o rámci pro volný tok neosobních údajů v Evropské unii, 29.5.2019, COM(2019) 250 final.

103. Z čl. 15 odst. 1 GDPR vyplývá několik prvků. Odstavec výslovně odkazuje na „*osobní údaje, které se ho týkají*“(4.2.1), které správcem „*jsou či nejsou zpracovávány*“ (4.2.2):

4.2.1 „osobní údaje, které se ho týkají“

104. Právo na přístup může být uplatněno výhradně ve vztahu k osobním údajům týkajícím se subjektu údajů, který o přístup žádá, případně oprávněnou osobou nebo zástupcem (viz oddíl 3.4). Existují také situace, kdy údaje nemají souvislost s osobou uplatňující právo na přístup, ale s jinou osobou. Subjekt údajů má však právo pouze na osobní údaje, které se týkají jeho samotného, s vyloučením údajů, které se týkají výlučně někoho jiného[63].

105. Klasifikace údajů jako osobních údajů týkajících se subjektu údajů však nezávisí na skutečnosti, že se tyto osobní údaje týkají i někoho jiného[64]. Je tedy možné, že se osobní údaje týkají více osob najednou. To automaticky neznamená, že by měl být umožněn přístup k osobním údajům, které se týkají i někoho jiného, neboť správce musí dodržovat čl. 15 odst. 4 GDPR.

106. Slova „*osobní údaje, které se ho týkají*“ by správci neměli vykládat „*příliš restriktivně*“, jak uvedla již pracovní skupina zřízená podle článku 29 v souvislosti s právem na přenositelnost údajů[65]. Pokud jde o právo na přístup, má EDPB za to, že například na záznamy telefonických rozhovorů (a jejich přepis) mezi subjektem údajů, který žádá o přístup, a správcem se může vztahovat právo na přístup za předpokladu, že se jedná o osobní údaje[66]. Za předpokladu, že se uplatní GDPR a že se na zpracování nevztahuje výjimka pro domácí činnosti podle čl. 2 odst. 2 písm. c) GDPR, v případě, že subjekt údajů použije získaný záznam, který obsahuje osobní údaje partnera v rozhovoru, pro jiné účely, například zveřejnění záznamu, stane se subjekt údajů správcem pro toto zpracování osobních údajů týkajících se druhé osoby, jejíž hlas byl zaznamenán. Ačkoli to správce nezbavuje povinností v oblasti ochrany údajů při řádné analýze toho, zda lze poskytnout přístup k úplnému záznamu, doporučuje se, aby správce informoval subjekt údajů, že se v takovém případě může stát správcem. Tím není dotčeno další posouzení podle čl. 15 odst. 4 GDPR, které je podrobně popsáno v oddíle 6. Stejně tak se právo na přístup může vztahovat na sdělení, které subjekty údajů zaslaly jiným osobám ve formě interpersonálních sdělení a vymazaly je ze svého zařízení, přičemž poskytovatel služeb je má i nadále k dispozici.

107. Na druhou stranu existují situace, kdy se správci může zdát, že souvislost mezi údaji a několika fyzickými osobami je nejasná, například při krádeži identity. V případě krádeže identity jedná osoba podvodně jménem jiné osoby. V této souvislosti je důležité připomenout, že oběti by měly být

---

[63] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 9: „*Žádost o přenositelnost údajů se vztahuje pouze na osobní údaje. Z tohoto důvodu nebudou zahrnuty žádné údaje, které jsou anonymní nebo které se subjektu údajů netýkají. Do oblasti působnosti však spadají pseudonymní údaje, které lze jednoznačně spojit se subjektem údajů (např. poskytnutím příslušného identifikátoru, viz čl. 11 odst. 2).*“

[64] SDEU, rozsudek ve věci C-434/16 Peter Nowak v. Data Protection Commissioner, 2017, bod 44.

[65] Pokyny WP29 k právu na přenositelnost údajů – schválené EDPB, s. 9: „*V mnoha případech správci zpracovávají informace, které obsahují osobní údaje několika subjektů údajů. V takovém případě by správci neměli větu „osobní údaje týkající se subjektu údajů“ vykládat příliš restriktivně. Například záznamy telefonních hovorů, interpersonálních sdělení nebo VoIP mohou obsahovat (v historii účtu účastníka) údaje o třetích stranách, které se účastní příchozích a odchozích hovorů. Ačkoli tedy záznamy budou obsahovat osobní údaje týkající se více osob, měli by mít účastníci možnost, aby jim tyto záznamy byly v odpověď na žádost o přenositelnost údajů poskytnuty, protože se záznamy týkají (také) subjektu údajů. Pokud jsou však tyto záznamy následně předány novému správci, neměl by je tento nový správce zpracovávat za žádným účelem, který by měl nepříznivý vliv na práva a svobody třetích osob (viz níže: třetí podmínka)*.“

[66] Viz příklad 34 v oddíle 6.2.

poskytnuty informace o všech osobních údajích, které správce uchovává v souvislosti s její totožností, včetně těch, které byly shromážděny na základě jednání podvodníka. Jinými slovy, i poté, co se správce dozvěděl o krádeži identity, představují osobní údaje, které jsou spojeny s identitou oběti nebo se jí týkají, osobní údaje subjektu údajů.

Příklad 17: Osoba podvodně používá identitu někoho jiného, aby mohla hrát poker online. Pachatel zaplatí online kasinu pomocí kreditní karty, kterou oběti ukradl. Když se oběť dozví o krádeži identity, požádá poskytovatele online kasina, aby jí poskytl přístup k jejím osobním údajům, konkrétně k online hrám, které pachatel hrál, a k informacím o kreditní kartě, kterou pachatel použil.

Mezi shromážděnými údaji a obětí existuje souvislost, protože byla použita její identita. Výše uvedené osobní údaje mají i po odhalení podvodu souvislost z důvodu jejich obsahu (kreditní karta oběti se jednoznačně týká oběti), účelu a účinku (informace o online hrách, které pachatel hrál, mohou být například použity k vystavení faktur oběti). Online kasino proto musí oběti poskytnout přístup k výše uvedeným osobním údajům.

108. V případě potřeby lze použít k uchovávání záznamů o přístupech k souboru a ke zpětnému sledování, které činnosti byly provedeny v souvislosti s přístupy k záznamu, například tisk, kopírování nebo mazání osobních údajů, interní záznamy o připojení. Tyto záznamy mohou obsahovat čas přihlášení, důvod přístupu k souboru a také informace identifikující osobu, která měla přístup. Otázky související s tímto tématem jsou předmětem sporu, který v současné době projednává Soudní dvůr EU (věc C-579/21). Zavedení záznamů o připojení, dohled nad nimi a jejich revize spadají do odpovědnosti správce a podléhají kontrole dozorových úřadů. Správce by tedy měl zajistit, aby osoby jednající pod jeho vedením, které mají přístup k osobním údajům, nezpracovávaly osobní údaje jinak než na základě správcových pokynů podle článku 29 GDPR. Pokud osoba přesto zpracovává osobní údaje pro jiné účely, než je plnění správcových pokynů, může se s ohledem na toto zpracování stát správcem a podléhat disciplinárnímu nebo trestnímu řízení nebo správním sankcím uloženým dozorovými úřady. EDPB upozorňuje, že součástí odpovědnosti zaměstnavatele podle článku 24 GDPR je využít vhodná opatření, a ti od vzdělávání po disciplinární řízení, aby bylo zajištěno, že zpracování je v souladu s GDPR a že nedochází k jeho porušování.

4.2.2 Osobní údaje, které „jsou zpracovávány“

109. Ustanovení čl. 15 odst. 1 GDPR se kromě toho vztahuje i na osobní údaje, které „jsou zpracovávány“. Referenční časový bod pro určení rozsahu osobních údajů, které spadají do žádosti o přístup, již byl popsán v oddíle 2.3.3. Toto znění však také naznačuje, že právo na přístup nerozlišuje mezi účely operací zpracování.

Příklad 18: Společnost zpracovávala osobní údaje týkající se subjektu údajů za účelem vyřízení jeho objednávky a zajištění dopravy na adresu bydliště subjektu údajů. Poté, co tyto původní účely, pro které byly osobní údaje shromážděny, pominou, uchovává správce některé osobní údaje pouze za účelem splnění svých právních povinností týkajících se vedení záznamů.

Subjekt údajů požádá o přístup k osobním údajům, které se ho týkají. Aby správce splnil svou povinnost podle čl. 15 odst. 1 GDPR, musí subjektu údajů poskytnout požadované osobní údaje, které jsou uloženy za účelem splnění zákonných povinností správce.

110. Archivované osobní údaje je třeba odlišovat od záložních údajů, jimiž jsou osobní údaje uložené pouze za účelem obnovení údajů v případě jejich ztráty. Je třeba zdůraznit, že s ohledem na zásady záměrné ochrany údajů a minimalizace údajů jsou záložní údaje v zásadě podobné údajům v reálném systému.

Pokud existují drobné rozdíly mezi osobními údaji v záložním a reálném produkčním systému, jsou zpravidla spojeny se shromažďováním dalších údajů od doby uložení poslední zálohy. Úbytek dat v reálném systému (např. vymazání po uplynutí doby uchovávání některých údajů nebo na základě žádosti o výmaz) bude v některých případech přepsán v záložních údajích až při následném zálohování. V případě, že je žádost o přístup podána v okamžiku, kdy je v záloze obsaženo více osobních údajů týkajících se subjektu údajů než v reálném systému nebo se jedná o jiné osobní údaje (což je patrné například z protokolu o výmazech v reálném produkčním systému, který byl zaveden v plném souladu se zásadou minimalizace údajů), musí být správce v souvislosti s touto situací transparentní a pokud je to technicky proveditelné, musí poskytnout přístup podle požadavků subjektu údajů, a to i k osobním údajům uloženým v záloze. S cílem být transparentní vůči subjektům údajů, které uplatňují své právo, může protokol o výmazech v reálném produkčním systému správci například umožnit zjistit, že jsou v záložním systému uloženy údaje, které již v reálném systému neexistují, neboť byly v nedávné době vymazány a v záložním systému ještě nebyly přepsány.

4.2.3 Rozsah nové žádosti o přístup

111. Zbývá dodat, že subjekty údajů mají právo na přístup ke všem zpracovávaným údajům, které se jich týkají, nebo k jejich částem, a to v závislosti na rozsahu žádosti (viz také oddíl 2.3.1 o úplnosti informací a oddíl 3.1.1 o analýze obsahu žádosti). V důsledku toho, jestliže správce již v minulosti vyhověl žádosti o přístup a za předpokladu, že žádost není nepřiměřená, správce nemůže zúžit rozsah této nové žádosti. To znamená, že v souvislosti s jakoukoli další žádostí téhož subjektu údajů o přístup by správce neměl subjekt údajů informovat jen o pouhých změnách zpracovávaných osobních údajů nebo o samotném zpracování od poslední žádosti, pokud s tím subjekt údajů výslovně nesouhlasí. V opačném případě by subjekty údajů byly povinny shromáždit své osobní údaje poskytnuté za účelem úplného souboru osobních údajů týkajících se jejich informací o zpracování a o právech subjektů údajů.

4.3 Informace o zpracování a o právech subjektu údajů

112. Kromě přístupu k osobním údajům jako takovým musí správce poskytnout informace o jejich zpracování a o právech subjektu údajů podle čl. 15 odst. 1 písm. a) až h) a čl. 15 odst. 2 GDPR. Většina informací o těchto konkrétních prvcích je již alespoň v obecné podobě shromážděna v záznamu správce o činnostech zpracování podle článku 30 GDPR a/nebo v jeho oznámení o ochraně osobních údajů vypracovaném v souladu s články 12 až 14 GDPR. Proto by mohlo být přínosné se nejprve opírat o „pokyny k transparentnosti podle nařízení 2016/679“ [67] pracovní skupiny zřízené podle článku 29, které se týkají obsahu informací, jež mají být poskytnuty podle článků 13 a 14 GDPR.

113. Ke splnění požadavků čl. 15 odst. 1 písm. a) až h) a čl. 15 odst. 2 mohou správci s opatrností používat textové moduly svého oznámení o ochraně osobních údajů, pokud se ujistí, že jsou aktuální a přesné s ohledem na žádost subjektu údajů. Před zahájením zpracování údajů nebo na jeho začátku často ještě nelze poskytnout některé informace, jako je identifikace konkrétních příjemců nebo konkrétní doba trvání zpracování údajů. Některé informace, jako například právo podat stížnost u dozorového úřadu (viz čl. 15 odst. 1 písm. f)), se nemění v závislosti na osobě, která podává žádost o přístup, a proto je lze sdělit obecně, jak je tomu i v oznámení oochraně osobních údajů. Další typy informací, jako jsou informace o příjemcích, o kategoriích a o zdroji údajů, se mohou lišit v závislosti na tom, kdo žádost podává a jaký je její rozsah. V souvislosti s žádostí o přístup podle článku 15 proto může být nutné

[67] Pracovní skupina zřízená podle článku 29, Pokyny k transparentnosti podle nařízení 2016/679 – schválené Evropským sborem pro ochranu osobních údajů (dále jen „pokyny WP29 k transparentnosti – schválené EDPB“), WP260 rev.01, 11. dubna 2018.

aktualizovat veškeré informace o zpracování, které má správce k dispozici, a přizpůsobit je operacím zpracování, které jsou skutečně prováděny, s ohledem na subjekt údajů, který žádost podává. Odkaz na znění zásad ochrany osobních údajů by tedy nepředstavoval dostatečný způsob, jakým by správce mohl poskytnout informace požadované v čl. 15 odst. 1 písm. a) až h) a odst. 2, ledaže by „přizpůsobené a aktualizované" informace byly stejné jako informace poskytnuté na začátku zpracování. Při vysvětlení, které informace se týkají žádající osoby, by správce mohl případně odkázat na určité činnosti (například „pokud jste využil/a tuto službu ...", „pokud jste zaplatil/a fakturou"), je-li subjektům údajů zřejmé, zda se jich to týká. V následujícím textu je vysvětlena požadovaná míra specifikace ve vztahu k jednotlivým typům informací.

114. Informace o účelech podle čl. 15 odst. 1 písm. a) musí být konkrétní, pokud jde o přesný účel (účely) v konkrétním případě žádajícího subjektu údajů. Nestačilo by vyjmenovat obecné účely správce, aniž by bylo objasněno, jaký účel či účely správce sleduje v aktuálním případě žádajícího subjektu údajů. Pokud je zpracování prováděno pro více účelů, musí správce objasnit, které údaje nebo které kategorie údajů jsou zpracovávány pro který účel (účely). Na rozdíl od čl. 13 odst. 1 písm. c) a čl. 14 odst. 1 písm. c) GDPR informace o zpracování uvedené v čl. 15 odst. 1 písm. a) neobsahují informace o právním základu zpracování. Jelikož však některá práva subjektů údajů závisí na použitelném právním základu, jsou tyto informace pro subjekty údajů důležité, aby si mohly ověřit zákonnost zpracování údajů a určit, která práva subjektu údajů lze v konkrétní situaci použít. Proto, aby se usnadnil výkon práv subjektů údajů v souladu s čl. 12 odst. 2 GDPR, se správci doporučuje, aby informoval subjekt údajů také o platném právním základu pro každou operaci zpracování nebo aby uvedl, kde lze tyto informace najít. Zásada transparentního zpracování v každém případě vyžaduje, aby informace o právních základech zpracování byly subjektu údajů zpřístupněny dostupným způsobem (např. v oznámení o ochraně osobních údajů).

115. Informace o kategoriích údajů (čl. 15 odst. 1 písm. b)) mohou být rovněž přizpůsobeny situaci subjektu údajů a kategorie, které se ukázaly být v případě žadatele nerelevantní, by měly být tudíž odstraněny.

> **Příklad 19:** V souvislosti s informacemi uvedenými v článcích 13 a 14 GDPR hotel uvádí, že zpracovává řadu kategorií údajů o zákaznících (identifikační údaje, kontaktní údaje, bankovní údaje a číslo kreditní karty atd.). Pokud je žádost o přístup podána na základě článku 15, musí být subjekt údajů, který žádost podává, kromě přístupu ke skutečným zpracovávaným údajům (složka 2) v souladu s čl. 15 odst. 1 písm. b) informován také o konkrétních kategoriích údajů, které jsou v daném případě zpracovávány (např. nezahrnutí bankovních údajů nebo údajů o kreditní kartě v případě, že platba byla provedena v hotovosti).

116. Informace o „příjemcích nebo kategoriích příjemců" (čl. 15 odst. 1 písm. c)) musí zaprvé zohledňovat definici příjemců uvedenou v čl. 4 bodě 9 GDPR. Definice příjemců je založena na zpřístupnění osobních údajů fyzické nebo právnické osobě, orgánu veřejné moci, agentuře nebo jinému subjektu[68]. Z čl. 4 bodu 9 GDPR vyplývá, že orgány veřejné moci jednající v rámci konkrétního šetření, na které se vztahují zvláštní vnitrostátní předpisy, se za příjemce nepovažují.

117. Pokud jde o otázku, zda si správce může vybrat mezi informacemi o příjemcích nebo o kategoriích příjemců, je třeba poznamenat, že „na rozdíl od článků 13 a 14 GDPR o ochraně osobních údajů, které

[68] Dále je třeba poznamenat, že v rámci téže společnosti mohou existovat různí správci ve smyslu čl. 4 bodu 7 GDPR. V této situaci je možné zpřístupnění údajů od jednoho příjemce druhému příjemci v rámci jedné společnosti.

stanoví povinnost správce (...), článek 15 obecného nařízení o ochraně osobních údajů stanoví skutečné právo na přístup ve prospěch subjektu údajů, takže subjekt údajů musí mít na výběr, zda chce získat informace pokud možno o konkrétních příjemcích, kterým byly nebo budou uvedené údaje zpřístupněny, nebo informace o kategoriích příjemců“[69]. Je rovněž třeba připomenout, že jak je uvedeno ve výše uvedených pokynech týkajících se transparentnosti[70], informace o příjemcích nebo kategoriích příjemců by již podle článku 13 a 14 GDPR měly být co nejkonkrétnější s ohledem na zásady transparentnosti a spravedlnosti. Podle článku 15, pokud se subjekt údajů nerozhodl jinak, je správce povinen uvést skutečné příjemce, ledaže není možné tyto příjemce určit nebo správce prokáže, že žádosti subjektu údajů o přístup jsou zjevně nedůvodné nebo nepřiměřené ve smyslu čl. 12 odst. 5 GDPR[71] [72]. EDPB v této souvislosti připomíná, že uchovávání informací týkajících se skutečných příjemců je nezbytné mimo jiné proto, aby bylo možné splnit povinnosti správce podle čl. 5 odst. 2 a článku 19 GDPR.

Příklad 20: Zaměstnavatel ve svém oznámení o ochraně osobních údajů uvádí informace o tom, které kategorie údajů jsou předávány „cestovním kancelářím“ nebo „hotelům“ v případě služebních cest v souladu s čl. 13 odst. 1 písm. e) a čl. 14 odst. 1 písm. e) GDPR. Pokud zaměstnanec požádá o přístup k osobním údajům po uskutečnění pracovních cest, měl by zaměstnavatel v takovém případě, pokud jde o příjemce osobních údajů podle čl. 15 odst. 1 písm. c), uvést ve své odpovědi cestovní kancelář(e) a hotel(y), které údaje obdržely. Zatímco zaměstnavatel ve svém oznámení o ochraně osobních údajů legitimně odkázal na kategorie příjemců podle článků 13 a 14, protože v této fázi ještě nebylo možné příjemce jmenovat, měl by, pokud se zaměstnanec při podání žádost o přístup nerozhodl jinak, poskytnout informace o konkrétních příjemcích (názvy cestovních kanceláří, hotelů atd.).

Pokud správce za dodržení výše uvedených podmínek může sdělit pouze kategorie příjemců, měly by být tyto informace co nejkonkrétnější, s uvedením druhu příjemce (tj. odkazem na jeho činnosti), oboru, odvětví, pododvětví a místa, kde se příjemce nachází[73].

118. Podle čl. 15 odst. 1 písm. d) musí být, je-li to možné, poskytnuta informace o plánované době, po kterou budou osobní údaje uloženy. Pokud to možné není, je třeba uvést kritéria použitá ke stanovení této doby. Informace poskytnuté správcem musí být dostatečně přesné, aby subjekt údajů věděl, jak dlouho budou údaje, které se ho týkají, nadále uchovávány. Pokud není možné určit dobu výmazu, uvede se doba trvání uložení a počátek tohoto období nebo aktivační událost (např. ukončení smlouvy, uplynutí záruční doby atd.). Pouhý odkaz, například na „výmaz po uplynutí zákonné doby uložení“, nestačí. Údaje týkající se doby uložení údajů se budou muset zaměřit na konkrétní údaje týkající se subjektu údajů. Pokud se na osobní údaje subjektu údajů vztahují různé lhůty pro výmaz (např. proto, že ne všechny údaje podléhají zákonné povinnosti uchovávání), uvedou se lhůty pro výmaz ve vztahu k příslušným operacím zpracování a kategoriím údajů.

119. Zatímco informace o právu podat stížnost u dozorového úřadu (čl. 15 odst. 1 písm. f)) není závislá na konkrétních okolnostech, práva subjektů údajů uvedená v čl. 15 odst. 1 písm. e) se liší v závislosti na právním základu zpracování. S ohledem na povinnost správce usnadnit výkon práv subjektu údajů

[69] SDEU, C-154/21 (Österreichische Post AG), bod 36.
[70] Pracovní skupina zřízená podle článku 29, Pokyny k transparentnosti podle nařízení 2016/679 – schválené Evropským sborem pro ochranu osobních údajů (dále jen „pokyny WP29 k transparentnosti – schválené EDPB“), WP260 rev.01, 11. dubna 2018, s. 37 (příloha).
[71] SDEU, C-154/21 (Österreichische Post AG).
[72] Samotná skutečnost, že údaje byly zpřístupněny velkému počtu příjemců, by sama o sobě neznamenala, že je žádost nepřiměřená, viz oddíl 6 bod 188.
[73] Pokyny WP29 k transparentnosti – schválené EDPB, s. 37 (příloha).

podle čl. 12 odst. 2 GDPR musí být reakce správce na tato práva individuálně přizpůsobena případu subjektu údajů a vztahovat se k příslušným operacím zpracování. Je třeba se vyhnout informacím o právech, která se na subjekt údajů v dané konkrétní situaci nevztahují.

120. Podle čl. 15 odst. 1 písm. g) musí být poskytnuty „veškeré dostupné informace“ o zdroji údajů, pokud osobní údaje nejsou získány od subjektu údajů. Míra dostupných informací se může v průběhu času měnit.

Příklad 21: Zásady ochrany osobních údajů jedné velké společnosti uvádějí:

„Posouzení bonity nám pomáhá předcházet problémům při platebních transakcích. Zaručuje ochranu naší společnosti před finančními riziky, která mohou ovlivnit i prodejní ceny ve střednědobém až dlouhodobém horizontu. Posouzení bonity je nutně prováděno, pokud se chystáme odeslat zboží, aniž bychom současně obdrželi příslušnou úhradu kupní ceny, například v případě nákupu na účet. Bez provedení posouzení bonity je možná pouze platba předem (okamžitý bankovní převod, online poskytovatel plateb, kreditní karta).

Pro účely posouzení bonity zašleme vaše jméno, adresu a datum narození například následujícím poskytovatelům služeb: 1) agentura pro finanční informace X, 2) poskytovatel obchodních informací Y, 3) komerční úvěrová referenční agentura Z.

Údaje jsou předávány výše uvedeným úvěrovým institucím pouze v rozsahu, který je zákonem povolen, a pouze pro účely analýzy vaší platební morálky v minulosti, jakož i pro posouzení rizika nesplácení na základě matematicko-statistických postupů s využitím údajů o adrese a pro ověření vaší adresy (kontrola doručení). V závislosti na výsledku posouzení bonity se může stát, že vám již nebudeme moci nabídnout individuální způsoby platby, například nákup na fakturu.“

Oznámení o ochraně osobních údajů tedy obsahuje obecné informace o možnosti získat informace od uvedených úřadů pro hospodářské informace v souladu s článku 13 a 14 GDPR. Pokud není předem jasné, které společnosti se budou na zpracování podílet, stačí v zásadách ochrany osobních údajů uvést jména způsobilých společností. V souvislosti s žádostí na základě článku 15 by pak kromě informace, že byly získány informace o úvěruschopnosti, bylo nutné (ex post) sdělit, o kterou z uvedených společností se konkrétně jednalo. V čl. 15 odst. 1 písm. g) je jasně uvedeno, že informace o zpracování údajů zahrnují „veškeré dostupné informace o zdroji osobních údajů“, pokud nejsou získány od subjektu údajů.

121. Ustanovení čl. 15 odst. 1 písm. h) stanoví, že každý subjekt údajů by měl mít právo obdržet mimo jiné smysluplné informace o existenci a použitém postupu automatizovaného rozhodování, včetně profilování, týkajícího se subjektu údajů a o významu a předpokládaných důsledcích, které by takové zpracování mohlo mít[74]. Je-li to možné, informace podle čl. 15 odst. 1 písm. h) musí být konkrétnější, pokud jde o důvody, které vedly ke konkrétním rozhodnutím týkajícím se subjektu údajů, který požádal o přístup.

122. Podle čl. 13 odst. 1 písm. f) a čl. 14 odst. 1 písm. f) GDPR musí být poskytnuty informace o zamýšleném předání údajů do třetí země nebo mezinárodní organizaci, včetně existence rozhodnutí Komise o odpovídající ochraně nebo vhodných záruk. V souvislosti s žádostí o přístup podle článku 15 ustanovení

[74] K tomu viz pokyny k transparentnosti podle nařízení 2016/679 (WP 260), bod 41, s odkazem na pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 (WP 251).

čl. 15 odst. 2 vyžaduje informace o vhodných zárukách podle článku 46 GDPR pouze v případech, kdy skutečně dochází k předání do třetí země nebo mezinárodní organizaci.

5 JAK MŮŽE SPRÁVCE ZAJISTIT PŘÍSTUP?

123. GDPR příliš nepředepisuje, jakým způsobem musí správce poskytnout přístup. V některých situacích může být uplatnění práva na přístup snadné a jednoduché, například když má malá organizace v držení jen omezené informace o subjektu údajů. V jiných situacích je právo na přístup složitější, protože zpracování údajů je komplexnější; a to s ohledem na počet subjektů údajů, kategorie zpracovávaných údajů a tok údajů v rámci různých organizací a mezi nimi. Vzhledem k rozdílům ve zpracování osobních údajů se může vhodný způsob poskytování přístupu lišit.

124. Cílem tohoto oddílu je poskytnout určité vodítko a praktické příklady různých způsobů, jak mohou správci vyhovět žádosti o přístup, i pokud jde o význam čl. 12 odst. 1 GDPR v souvislosti s právem na přístup. Tento oddíl rovněž poskytne určité vodítko k tomu, co se považuje za běžně používaný elektronický formulář, a také ke lhůtám pro poskytnutí přístupu podle čl. 12 odst. 3 GDPR.

5.1 Jak může správce získat požadované údaje?

125. Subjekty údajů by měly mít přístup ke všem informacím, které o nich správce zpracovává. To například znamená, že správce je povinen vyhledávat osobní údaje ve svých informačních systémech i v jiných než informačních evidencích. Při provádění takového vyhledávání by měl správce použít dostupné informace v organizaci, které se týkají subjektu údajů a které pravděpodobně povedou ke shodám v systémech v závislosti na tom, jak jsou informace strukturovány[75]. Pokud jsou například informace v souborech seřazeny podle jména nebo referenčního čísla, může být vyhledávání omezeno na tyto prvky. Pokud však struktura údajů závisí na jiných faktorech, jako jsou rodinné vztahy nebo profesní tituly nebo jakýkoli druh přímých či nepřímých identifikátorů (např. číslo zákazníka, uživatelské jméno nebo IP adresa), je třeba vyhledávání rozšířit tak, aby zahrnovalo i tyto údaje za předpokladu, že správce má k dispozici i tyto informace týkající se subjektu údajů nebo mu je subjekt údajů poskytl. Totéž platí, pokud záznamy týkající se třetích osob pravděpodobně obsahují osobní údaje týkající se subjektu údajů. Správce však nesmí od subjektu údajů vyžadovat více informací, než je nezbytné k identifikaci subjektu údajů. Pokud správce využívá pro své činnosti zpracování údajů zpracovatele, musí být vyhledávání přirozeně rozšířeno i na osobní údaje zpracovávané zpracovatelem.

126. V souladu s článkem 25 GDPR o záměrné a standardní ochraně údajů by správce (a případní zpracovatelé, které využívá) měl mít již také zavedeny funkce umožňující dodržování práv subjektu údajů. To v této souvislosti znamená, že by měly existovat vhodné způsoby, jak při vyřizování žádosti najít a získat informace o subjektu údajů. Je však třeba poznamenat, že nepřiměřený výklad v tomto ohledu by mohl vést k využití funkcí pro nalézání a získávání informací, které samy o sobě představují riziko pro soukromí subjektů údajů. Je proto důležité mít na paměti, že proces získávání údajů by měl být rovněž navržen způsobem šetrným k ochraně osobních údajů, aby neohrožoval soukromí jiných osob, například zaměstnanců správce.

5.2 Vhodná opatření pro zajištění přístupu

[75] Takové vyhledávání by samozřejmě mělo zahrnovat i informace, které jsou v držení zpracovatele, viz čl. 28 odst. 3 písm. e) GDPR.

5.2.1 Přijetí „vhodných opatření“

127. Článek 12 GDPR stanoví požadavky na poskytování přístupu, tj. na poskytnutí potvrzení, osobních údajů a doplňujících informací podle článku 15, a stanoví rovněž formu, způsob a lhůtu v souvislosti s právem na přístup. „Pokyny k transparentnosti podle nařízení 2016/679“[76] vypracované pracovní skupinou zřízenou podle článku 29 poskytují, pokud jde o článek 12, další pokyny, většinou v souvislosti s články 13 a 14 GDPR, ale i v souvislosti s článkem 15 a k transparentnosti obecně. To, co je stanoveno v těchto pokynech, lze tedy často použít také v souvislosti s poskytováním přístupu podle článku 15.

128. Ustanovení čl. 12 odst. 1 GDPR stanoví, že správce musí přijmout vhodná opatření, aby stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků poskytl subjektu veškerá sdělení podle článku 15 o zpracování. V čl. 12 odst. 2 se stanoví, že správce musí usnadnit výkon práva subjektu údajů na přístup. Přesnější požadavky v tomto ohledu bude nutné posuzovat případ od případu. Při rozhodování, která opatření jsou vhodná, musí správci zohlednit všechny relevantní okolnosti, mimo jiné množství zpracovávaných údajů, složitost jejich zpracování údajů a znalosti, které mají o svých subjektech údajů, například pokud většinu subjektů údajů tvoří děti, starší osoby nebo osoby se zdravotním postižením. V situacích, kdy je správce informován o zvláštních potřebách subjektu údajů, který žádost podává, například prostřednictvím dodatečných informací v podané žádosti, musí navíc správce tyto okolnosti zohlednit. Vhodná opatření se proto budou lišit.

129. Při posuzování je důležité mít na paměti, že pojem „vhodný“ by nikdy neměl být chápán jako způsob omezení rozsahu údajů, na které se právo na přístup vztahuje. Pojem „vhodný“ neznamená, že úsilí o poskytnutí informací lze odstupňovat například podle zájmu, který může mít subjekt údajů na získání osobních údajů, Posouzení by se místo toho mělo zaměřit na zvolení nejvhodnějšího způsobu poskytnutí všech informací, na něž se toto právo vztahuje, v závislosti na konkrétních okolnostech každého případu. Správce, který zpracovává velké množství údajů ve velkém měřítku, proto musí vynaložit velké úsilí, aby zajistil právo na přístup k údajům pro subjekty údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků

130. Je třeba se vyhnout tomu, aby byl subjekt údajů v reakci na žádost o přístup k údajům odkázán na různé zdroje. Jak již bylo uvedeno v pokynech WP29 k transparentnosti (v souvislosti s pojmem „poskytnout“ v článcích 13 a 14 GDPR), pojem „poskytnout“ znamená, že „*subjekt údajů nesmí být nucen aktivně hledat informace uvedené v těchto článcích mezi dalšími informacemi, například v podmínkách použití internetových stránek nebo aplikace*“[77]. Z tohoto důvodu a s ohledem na zásadu transparentnosti musí subjekty údajů získat od správce informace a osobní údaje požadované v čl. 15 odst. 1, 2 a 3 způsobem, který umožňuje úplný přístup k požadovaným informacím. Za zvláštních okolností by bylo sdílení informací v rámci správce nevhodné nebo dokonce protiprávní, například kvůli citlivé povaze informací (jako např. informace týkající se oznamování porušení předpisů). V těchto případech by bylo považováno za vhodné jako odpověď na žádost subjektu údajů o přístup rozdělit informace do několika odpovědí. Způsob zvolený správcem musí subjektu údajů skutečně poskytnout požadované údaje a informace, proto by nebylo vhodné odkazovat subjekt údajů pouze na kontrolu požadovaných údajů

[76] Pracovní skupina zřízená podle článku 29, Pokyny k transparentnosti podle nařízení 2016/679 – schválené Evropským sborem pro ochranu osobních údajů (dále jen „pokyny WP29 k transparentnosti – schválené EDPB“), WP260 rev.01, 11. dubna 2018.

[77] Pokyny WP29 k transparentnosti – schválené EDPB, bod 33.

uložených ve vlastním zařízení správce, včetně například kontroly historie kliknutí a IP adres v jeho mobilním telefonu.

131. V souladu se zásadou odpovědnosti musí správce svůj přístup zdokumentovat, aby byl schopen prokázat, jak jsou prostředky zvolené k poskytnutí nezbytných informací podle článku 15 za daných okolností vhodné.

5.2.2 Různé prostředky pro zajištění přístupu

132. Jak bylo již vysvětleno v oddíle 2.2.2 výše, při podání žádosti o přístup mají subjekty údajů právo obdržet kopii svých zpracovávaných údajů podle čl. 15 odst. 3 spolu s doplňujícími informacemi, což se považuje za hlavní způsob poskytnutí přístupu k osobním údajům.

133. Za určitých okolností by však mohlo být vhodné, aby správce poskytl přístup jiným způsobem než poskytnutím kopie. Takovými nestálými způsoby přístupu k údajům mohou být například: ústní informace, kontrola souborů, přístup na místě nebo vzdálený přístup bez možnosti stažení. Tyto způsoby mohou být vhodnými způsoby poskytnutí přístupu například v případech, kdy je to v zájmu subjektu údajů nebo pokud o to subjekt údajů požádá. Přístup na místě by mohl být jako počáteční opatření vhodný také v případě, že správce zpracovává velké množství nedigitalizovaných údajů, aby se subjekt údajů mohl seznámit s tím, jaké osobní údaje jsou zpracovávány, a mohl se informovaně rozhodnout, jaké osobní údaje si přeje obdržet prostřednictvím kopie. Nestálé způsoby přístupu mohou být dostatečné a vhodné v určitých situacích; mohou například uspokojit potřebu subjektů údajů ověřit si správnost údajů zpracovávaných správcem tím, že subjektům údajů umožní nahlédnout do původních údajů. Správce není povinen poskytnout informace jiným způsobem než poskytnutím kopie, měl by však posuzování takové žádosti zaujmout rozumný přístup. Poskytnutí přístupu jiným způsobem než poskytnutím kopie nevylučuje právo subjektů údajů obdržet rovněž kopii, ledaže se rozhodnou, že tuto kopii neobdrží.

134. Správce se může v závislosti na dané situaci rozhodnout, že kopii zpracovávaných údajů spolu s doplňujícími informacemi poskytne různými způsoby, např. e-mailem, fyzickou poštou nebo pomocí samoobslužného nástroje. Jestliže subjekt údajů podává žádost v elektronické formě a v případě, že subjekt údajů nepožádá o jiný způsob, poskytnou se informace v elektronické formě, která se běžně používá, jak se uvádí v čl. 15 odst. 3. Správce musí v každém případě zvážit vhodná technická a organizační opatření, včetně odpovídajícího šifrování při poskytování informací prostřednictvím e-mailu nebo online samoobslužných nástrojů.

135. V situaci, kdy správce zpracovává osobní údaje týkající se osoby, která podala žádost, pouze v malém rozsahu, mohou být a měly by být kopie osobních údajů a doplňující informací poskytnuty jednoduchým postupem.

Příklad 22: Místní knihkupectví vede záznamy o jménech a adresách svých zákazníků, kteří si objednali doručení do domu. Zákazník navštíví knihkupectví a požádá o přístup. V této situaci by stačilo vytisknout osobní údaje o zákazníkovi přímo z obchodního systému a zároveň poskytnout doplňující informace uvedené v čl. 15 odst. 1 a 2.

Příklad 23: Dárce charitativní organizace přispívající každý měsíc požádá e-mailem o přístup. Charitativní organizace uchovává informace o darech poskytnutých v posledních dvanácti měsících, jakož i jména a e-mailové adresy dárců. Správce by mohl poskytnout kopii osobních údajů a doplňující informace prostřednictvím odpovědi na e-mail za předpokladu, že budou uplatněny všechny nezbytné záruky, například s ohledem na povahu údajů.

136. Dokonce i správci, kteří zpracovávají velké množství údajů, se mohou rozhodnout využít při vyřizování žádostí o přístup manuální postupy. Pokud správce zpracovává údaje v několika různých odděleních, musí shromáždit osobní údaje z každého oddělení, aby mohl odpovědět na žádost subjektu údajů.

Příklad 24: Správce jmenuje administrativní sílu, aby se zabývala praktickými záležitostmi týkajícími se žádostí o přístup. Po obdržení žádosti zašle administrativní síla e-mailem dotaz různým oddělením organizace a požádá je o shromáždění osobních údajů, které se týkají subjektu údajů. Zástupci jednotlivých oddělení předají administrativní síle osobní údaje zpracovávané jejich oddělením. Administrativní síla poté všechny osobní údaje zašle subjektu údajů spolu s nezbytnými doplňujícími informacemi, například, a pokud je to vhodné, e-mailem.

137. Ačkoli manuální postupy při vyřizování žádostí o přístup lze považovat za vhodné, pro některé správce může být výhodné používat při vyřizování žádostí subjektů údajů automatizované postupy. Může tomu tak být například u správců, kteří přijímají velké množství požadavků. Jedním ze způsobů, jak poskytnout informace podle článků 15, je poskytnout subjektu údajů samoobslužné nástroje. To by mohlo usnadnit účinné a včasné vyřizování žádostí subjektů údajů o přístup a správci to rovněž umožní zahrnout ověřovací mechanismus do samoobslužného nástroje.

Příklad 25: Služba sociálních médií má zaveden automatizovaný proces vyřizování žádostí o přístup, který subjektu údajů umožňuje přístup k jeho osobním údajům z jeho uživatelského účtu. Pro získání osobních údajů mohou uživatelé sociálních médií po přihlášení ke svému uživatelskému účtu zvolit možnost „Stáhnout své osobní údaje“. Tato samoobslužná možnost umožňuje uživatelům stáhnout soubor obsahující jejich osobní údaje přímo z uživatelského účtu do vlastního počítače.

138. Používání samoobslužných nástrojů by nikdy nemělo omezovat rozsah obdržených osobních údajů. Pokud není možné poskytnout prostřednictvím samoobslužného nástroje všechny informace podle článku 15, je třeba zbývající informace poskytnout jiným způsobem. Správce může vyzvat subjekt údajů, aby použil samoobslužný nástroj, který správce pro vyřizování žádostí o přístup zavedl. Je však třeba poznamenat, že správce musí vyřizovat i žádosti o přístup, které nejsou zasílány prostřednictvím zavedeného komunikačního kanálu[78].

5.2.3 Poskytnutí přístupu stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků

139. Podle čl. 12 odst. 1 GDPR musí správce přijmout vhodná opatření, aby poskytl subjektu údajů přístup podle článku 15 stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků.

140. Požadavek, že poskytnutí údajů subjektu údajů musí být provedeno stručným a transparentním způsobem, znamená, že správci by měli předkládat informace účinně a stručně, aby jim subjekt údajů snadno porozuměl, zejména pokud se jedná o dítě. Správce musí při volbě prostředků pro poskytnutí přístupu podle článku 15 vzít v úvahu množství a složitost údajů.

Příklad 26: Poskytovatel sociálních médií zpracovává velké množství informací o subjektu údajů. Velkou část těchto osobních údajů tvoří informace obsažené na stovkách stran protokolových souborů, kde jsou zaznamenány aktivity subjektu údajů na internetových stránkách. Pokud subjekty údajů požádají o přístup ke svým osobním údajům, právo na přístup se ovšem vztahuje i na osobní údaje v těchto protokolových souborech. Právo na přístup by proto mohlo být formálně naplněno, pokud by

[78] Viz oddíl 3.1.2.

byly subjektu údajů poskytnuty tyto stovky stran protokolových souborů. Bez opatření přijatých k usnadnění porozumění informacím v protokolových souborech by však právo subjektu údajů na přístup nemuselo být v praxi naplněno, protože z protokolových souborů nelze snadno získat žádné poznatky, a proto nesplňují požadavek čl. 12 odst. 1 GDPR. Správce proto musí být opatrný a důkladný při výběru způsobu, jakým jsou informace a osobní údaje subjektu údajů předkládány.

141. Za okolností uvedených ve výše uvedeném příkladu by mohlo být vhodným opatřením pro splnění obou požadavků obsažených v článku 15 a v čl. 12 odst. 1 GDPR použití vícevrstvého přístupu podobného tomu, který je doporučován v pokynech k transparentnosti s ohledem na oznámení o ochraně osobních údajů[79]. Toto bude dále rozvedeno v oddíle 5.2.4 níže. Požadavek, aby informace byly „srozumitelné“, znamená, že by měly být pochopeny cílovou skupinou[80], přičemž je třeba mít na paměti veškeré zvláštní potřeby, které by subjekt údajů mohl mít a které jsou správci známy[81]. Vzhledem k tomu, že právo na přístup často umožňuje výkon dalších práv subjektu údajů, je zásadní, aby poskytované informace byly podány srozumitelně a jasně. Je tomu tak proto, že subjekty údajů budou moci zvážit, zda uplatní své právo například na opravu podle článku 16 GDPR, pouze tehdy, když vědí, jaké osobní údaje jsou zpracovávány, pro jaké účely atd. V důsledku toho může být nutné, aby správce poskytl subjektu údajů dodatečné informace, které poskytnuté údaje vysvětlí. Je třeba zdůraznit, že složitost zpracování údajů ukládá správci povinnost poskytnout prostředky, aby byly údaje podány srozumitelně, a nelze ji použít jako argument pro omezení přístupu ke všem údajům. Stejně tak nelze povinnost správce poskytnout údaje stručným způsobem použít jako argument pro omezení přístupu ke všem údajům.

Příklad 27: Internetové stránky elektronického obchodu shromažďují pro účely marketingu údaje o položkách prohlížených nebo zakoupených na jeho internetových stránkách. Část těchto údajů budou tvořit údaje v nezpracovaném formátu[82], které nebyly analyzovány a nemusí mít pro čtenáře přímý význam (kódy, historie aktivit atd.). Na tyto údaje týkající se činností subjektů údajů se rovněž vztahuje právo na přístup, a proto by měly být subjektu údajů poskytnuty v reakci na žádost o přístup. Při poskytování údajů v nezpracovaném formátu je důležité, aby správce přijal nezbytná opatření k zajištění toho, že subjekt údajů údajům rozumí, například poskytnutím vysvětlujícího dokumentu, který nezpracovaný formát převede do uživatelsky přívětivé podoby. V takovém dokumentu by také mohlo být vysvětleno, že zkratky a jiná zkratková slova, například „A“, znamenají, že nákup byl přerušen, a „B“ znamená, že nákup proběhl.

142. Prvek „snadno přístupný“ znamená, že informace podle článku 15 by měly být předkládány způsobem, který je pro subjekt údajů snadno přístupný. To se týká například rozvržení, vhodných nadpisů a členění na odstavce. Informace by měly být vždy poskytovány pomocí jednoduchých a jasných jazykových prostředků. Správce, který poskytuje službu v určité zemi, by měl rovněž poskytovat odpovědi v jazyce, kterému rozumí subjekty údajů v dané zemi. Doporučuje se rovněž používat standardizované ikony,

[79] Pokyny WP29 k transparentnosti – schválené EDPB, bod 35.

[80] Srozumitelnost úzce souvisí s požadavkem na používání jednoduchého a jasných jazykových prostředků (pokyny WP29 k transparentnosti – schválené EDPB, bod 9). To, co se uvádí v bodech 12 až 16 o jednoduchých a jasných jazykových prostředcích, pokud jde o informace uvedené v článcích 13 a 14 GDPR, platí rovněž i pro sdělení podle článku 15.

[81] Viz bod 128.

[82] Údaje v nezpracovaném formátu v příkladu je třeba chápat jako neanalyzovaná data podléhající zpracování, a nikoli jako nejnižší úroveň nezpracovaných dat, která mohou být pouze strojově čitelná (např. „bity“).

pokud to usnadňuje srozumitelnost a přístupnost informací. Jestliže se žádost o informace týká subjektů údajů se zrakovým postižením nebo jiných subjektů údajů, které mohou mít potíže s přístupem k informacím nebo s jejich pochopením, očekává se, že správce přijme opatření usnadňující porozumění poskytovaným informacím, včetně ústních informací, pokud je to přiměřené[83]. Správce by měl zejména dbát na to, aby svá práva mohly vykonávat starší osoby, děti, osoby se zrakovým postižením nebo osoby s kognitivním či jiným postižením, například aktivním poskytováním snadno přístupných prvků, které výkon těchto práv usnadní.

5.2.4 Velké množství informací klade zvláštní požadavky na způsob jejich poskytování

143. Bez ohledu na způsob, jakým se přístup poskytuje, může existovat napětí mezi množstvím informací, které musí správce subjektům údajů poskytnout, a požadavkem, aby byly stručné. Jedním ze způsobů, jak dosáhnout obojího, a příkladem vhodného opatření pro některé správce, jestliže je třeba poskytnoutvelké množství údajů, je použití vícevrstvého přístupu. Tento přístup může usnadnit porozumění údajům ze strany subjektů údajů. Je však třeba zdůraznit, že tento přístup lze použít pouze za určitých okolností a musí být prováděn způsobem, který neomezuje právo na přístup, jak je vysvětleno níže. Kromě toho by použití vícevrstvého přístupu nemělo pro subjekt údajů představovat další zátěž. Proto by bylo nejvhodnější, kdyby byl přístup poskytnut v internetovém prostředí. Vícevrstvý přístup je pouze jeden ze způsobů, jak prezentovat informace podle článku 15 způsobem, který je rovněž v souladu s požadavky čl. 12 odst. 1 GDPR, a neměl by být zaměňován s možností správců požadovat, aby subjekt údajů upřesnil informace nebo činnosti zpracování, kterých se žádost týká, jak je stanoveno v 63. bodě odůvodnění GDPR[84].

144. Vícevrstvý přístup v souvislosti s právem na přístup znamená, že správce může za určitých okolností poskytnout osobní údaje a doplňující informace požadované podle článku 15 v různých vrstvách. První vrstva by měla obsahovat informace o zpracování a právech subjektu údajů podle čl. 15 odst. 1 písm. a) až h) a odst. 2, jakož i první část zpracovávaných osobních údajů. Ve druhé vrstvě by mělo být poskytnuto více osobních údajů.

145. Při rozhodování o tom, jaké informace by měly být uvedeny v jednotlivých vrstvách, by měl správce zvážit, jaké informace by subjekt údajů obecně považoval za nejdůležitější. V souladu se zásadou spravedlnosti by první vrstva měla obsahovat také informace o zpracování, které má na subjekt údajů největší dopad[85]. Správci musí být schopni prokázat odpovědnost, pokud jde o, z jakých úvah ve výše uvedeném případě vycházeli.

Příklad 28: Správce analyzuje velké soubory dat a zařazuje zákazníky do různých segmentů v závislosti na jejich chování na internetu. V této situaci lze předpokládat, že informacemi, jejichž získání je pro subjekty údajů nejdůležitější, jsou informace o tom, do jakého segmentu byly zařazeny. Proto by tato informace měla být zahrnuta do první vrstvy. Osobními údaji, na které se vztahuje právo na přístup, jsou i údaje v nezpracovaném formátu[86], které ještě nebyly analyzovány ani dále zpracovány, například aktivita uživatele na internetových stránkách, avšak v některých případech by mohlo postačovat poskytnutí těchto informací v jiné vrstvě.

146. Aby mohlo být použití vícevrstvého přístupu považováno za vhodné opatření, je nutné, aby byl subjekt údajů na začátku informován o tom, že informace podle článku 15 jsou strukturovány do různých

[83] Viz pokyny WP29 k transparentnosti – schválené EDPB, bod 21.
[84] Viz také oddíl 2.3.1.
[85] Viz pokyny WP29 k transparentnosti – schválené EDPB, bod 36.
[86] Viz poznámka pod čarou č. 82.

vrstev, a aby mu byl poskytnut popis toho, jaké osobní údaje a informace budou v jednotlivých vrstvách obsaženy. Subjekt údajů se tak bude moci snáze rozhodnout, k jakým vrstvám chce mít přístup. Popis by měl objektivně odrážet všechny kategorie osobních údajů, které správce skutečně zpracovává. Musí být také jasné, jak může subjekt údajů získat přístup k jednotlivým vrstvám. Přístup k různým vrstvám nesmí být pro subjekt údajů spojen s nepřiměřeným úsilím a nesmí být podmíněn podáním nové žádosti subjektu údajů. To znamená, že subjekty údajů musí mít možnost si zvolit, zda chtějí mít přístup ke všem vrstvám najednou, nebo přístup k jedné či dvěma vrstvám, pokud jim to vyhovuje.

Příklad 29: Subjekt údajů podá žádost o přístup ke službě streamování videa. Žádost je podána s využitím možnosti, která je k dispozici při přihlášení subjektu údajů k jeho účtu. Subjektu údajů jsou nabídnuty dvě možnosti, které se na internetových stránkách zobrazí jako tlačítka. První možností je stažení části 1 osobních údajů a doplňujících informací. Obsahuje například historii posledních streamů, informace o účtu a informace o platbách. Druhou možností je stažení části 2 osobních údajů, která obsahuje technické protokoly o aktivitách subjektu údajů a historické informace o účtu. V tomto případě správce umožnil subjektům údajů uplatnit jejich právo způsobem, který pro ně nepředstavuje další zátěž.

Odchylka 1: V případě, kdy subjekt údajů zvolí pouze tlačítko pro stažení části 1 osobních údajů, je správce povinen poskytnout pouze část 1 údajů.

Odchylka 2: V případě, kdy subjekt údajů zvolí tlačítka pro část 1 i část 2 údajů, nemůže správce před sdělením části 2 údajů sdělit pouze část 1 údajů a požádat o nové potvrzení. Místo toho musí být subjektu údajů poskytnuty obě části údajů, jak vyplývá z podané žádosti.

147. Použití vícevrstvého přístupu nebude považováno za vhodné pro všechny správce nebo ve všech situacích. Měl by být použit pouze tehdy, pokud by pro subjekt údajů bylo obtížné pochopit informace, kdyby mu byly poskytnuty celé. Jinými slovy, správce musí být schopen prokázat, že použití vícevrstvého přístupu přináší subjektu údajů přidanou hodnotu, neboť mu pomáhá porozumět poskytovaným informacím. Vícevrstvý přístup by byl proto považován za vhodný pouze tehdy, pokud správce zpracovává o subjektu údajů, který podává žádost, velké množství osobních údajů, a pokud by pro subjekt údajů bylo zjevně obtížné pochopit nebo porozumět informacím, kdyby byly poskytnuty všechny najednou. Skutečnost, že poskytnutí informací podle článku 15 by od správce vyžadovalo velké úsilí a zdroje, není sama o sobě argumentem pro použití vícevrstvého přístupu.

5.2.5 Formát

148. Podle čl. 12 odst. 1 GDPR musí být informace podle článku 15 poskytnuty písemně nebo jinými prostředky, případně i v elektronické formě. Pokud jde o přístup ke zpracovávaným osobním údajům, ustanovení čl. 15 odst. 3 stanoví, že jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob. GDPR nespecifikuje, co je běžně používaná elektronická forma. Existuje tedy několik myslitelných formátů, které lze použít. To, co je považováno za běžně používanou elektronickou formu, se mění i v průběhu času.

149. To, co lze považovat za běžně používanou elektronickou formu, by mělo být založeno na objektivním posouzení, a nikoli na tom, jaký formát správce používá při svých každodenních operacích. Aby mohl správce určit, jaký formát má být v dané situaci považován za běžně používaný, bude muset posoudit, zda v oblasti jeho působnosti nebo v daném kontextu existují specifické formáty, které se obecně používají. Pokud žádné takové formáty, které by byly obecně používány, neexistují, měly by se za běžně používané elektronické formáty obecně považovat otevřené formáty stanovené v mezinárodní normě,

například v normě ISO. EDPB však nevylučuje, že za běžně používané formáty ve smyslu čl. 15 odst. 3 lze považovat i jiné formáty. Při posuzování, zda je formát běžně používaným elektronickým formátem, považuje EDPB za důležité, jak snadno může jednotlivec získat přístup k informacím poskytovaným v daném formátu. V tomto ohledu je třeba uvést, jaké informace správce subjektu údajů poskytl o tom, jak získat přístup k souboru, který byl poskytnut v určitém formátu, například jaké programy nebo software lze použít, aby byl formát pro subjekt údajů přístupnější. Subjekt údajů by však neměl být povinen zakoupit software, aby získal přístup k informacím.

150. Při rozhodování o tom, v jakém formátu by měla být kopie osobních údajů a informací podle článku 15 poskytnuta, musí mít správce na paměti, že formát musí umožnit, aby informace byly prezentovány způsobem, který je srozumitelný a snadno přístupný. Důležité je, aby subjekt údajů obdržel informace ve zhmotněné trvalé formě (textové, elektronické). Vzhledem k tomu, že informace by měly mít trvalý charakter, je v zásadě vhodnější písemná, a to i elektronická forma, než jiné formy. Kopie osobních údajů může být případně uložena na elektronickém paměťovém zařízení, jako je CD nebo USB.

151. Je třeba poznamenat, že k tomu, aby správce mohl mít za to, že subjektům údajů byla poskytnuta kopie osobních údajů, nestačí, aby jim poskytl přístup k jejich osobním údajům. Aby byl požadavek na poskytnutí kopie osobních údajů splněn a v případě, že jsou údaje poskytovány elektronicky/digitálně, musí mít subjekty údajů možnost stáhnout si své údaje v běžně užívané elektronickém formátu.

152. Úkolem správce je rozhodnout o vhodné formě, v níž budou osobní údaje poskytnuty. Správce může, i když nemusí, poskytnout dokumenty obsahující osobní údaje o subjektech údajů, které podaly žádost, v jejich původní formě. Správce by například mohl v jednotlivých případech poskytnout přístup ke kopii nosiče jako takového, a to s ohledem na potřebu transparentnosti (například za účelem ověření přesnosti údajů, které má správce v držení, v případě žádosti o přístup ke zdravotnické dokumentaci nebo zvukovému záznamu, jehož přepis je sporný). Soudní dvůr EU však ve svém výkladu práva na přístup podle směrnice 95/46/ES uvedl, že „za účelem dodržení tohoto práva na přístup postačí, aby tento žadatel obdržel úplný přehled těchto údajů ve srozumitelné formě, tedy ve formě, která tomuto žadateli umožní seznámit se s uvedenými údaji a ověřit, že tyto údaje jsou přesné a že jsou zpracovány v souladu s touto směrnicí, aby případně mohl uplatnit svá práva, která mu přiznává *[uvedená směrnice]*“[87]. Na rozdíl od směrnice obsahuje GDPR výslovně povinnost poskytnout subjektu údajů kopii zpracovávaných osobních údajů. To však neznamená, že subjekt údajů má vždy právo získat kopii dokumentů obsahujících osobní údaje, ale nezměněnou kopii osobních údajů, které jsou v těchto dokumentech zpracovávány.[88] Taková kopie osobních údajů by mohla být poskytnuta prostřednictvím shrnutí obsahujícího všechny osobní údaje, na které se právo na přístup vztahuje, pokud toto shrnutí umožňuje, aby se subjekt údajů seznámil se těmito údaji a ověřil si zákonnost jejich zpracování. Mezi zněním GDPR a rozhodnutím Soudního dvora EU v této věci tedy není žádný rozpor. Slovo shrnutí v rozsudku by nemělo být vykládáno nesprávně v tom smyslu, že by shrnutí nezahrnovala všechny údaje, na které se vztahuje právo na přístup, ale jedná se pouze o způsob, jak všechny tyto údaje prezentovat, aniž by byl poskytnut přístup k podkladovým dokumentům, které osobní údaje obsahují. Vzhledem k tomu, že shrnutí musí obsahovat kopii osobních údajů, je třeba zdůraznit, že nesmí být provedeno způsobem, který by nějakým způsobem měnil nebo upravoval obsah informací.

Příklad 30: Subjekt údajů je u pojišťovny pojištěn již řadu let. Došlo k několika pojistným událostem. V každém z těchto případů proběhla mezi subjektem údajů a pojišťovnou písemná korespondence

[87] SDEU, spojené věci C-141/12 a C-372/12, YS a další, bod 60.

[88] Otázky související s tímto tématem jsou předmětem věcí, které v současné době projednává Soudní dvůr EU (C-487/21 a C-307/21).

prostřednictvím e-mailu. Vzhledem k tomu, že subjekt údajů musel poskytnout informace o konkrétních okolnostech každé pojistné události, obsahuje korespondence mnoho osobních informací o subjektu údajů (záliby, spolubydlící, denní zvyky atd.). V některých případech vznikly neshody ohledně povinnosti pojišťovny odškodnit subjekt údajů, což vyvolalo rozsáhlou komunikaci v obou směrech. Veškerá tato korespondence je v pojišťovně uložena. Subjekt údajů podá žádost o přístup. V této situaci nemusí správce nutně poskytnout e-maily v jejich původní podobě a odeslat je subjektu údajů. Místo toho by se správce mohl rozhodnout, že e-mailovou korespondenci obsahující osobní údaje subjektu údajů shrne v souboru, který subjektu údajů poskytne.

153. Bez ohledu na formu, v níž správce osobní údaje poskytuje, např. poskytnutím skutečných dokumentů obsahujících osobní údaje nebo shrnutí osobních údajů, musí tyto informace splňovat požadavky na transparentnost stanovené v článku 12 GDPR. V některých případech může být způsobem, jak těmto požadavkům vyhovět, vytvoření určitého shrnutí a/nebo výtahu údajů tak, aby byly informace snadno srozumitelné. V jiných případech je informace lépe pochopitelná, pokud je poskytnuta kopie skutečného dokumentu obsahujícího osobní údaje. O tom, která forma je nejvhodnější, proto musí být rozhodnuto v každém jednotlivém případě.

154. V této souvislosti je důležité připomenout, že mezi právem na získání přístupu podle článku 15 GDPR a právem na obdržení kopie správních dokumentů upraveným vnitrostátním právem existuje rozdíl, přičemž v posledně uvedeném případě se jedná o právo na obdržení kopie skutečného dokumentu. To neznamená, že právo na přístup podle článku 15 GDPR vylučuje možnost obdržet kopii dokumentu/média, na kterém jsou osobní údaje uvedeny.

155. V některých případech jsou požadavky na formát osobních údajů určovány samotnými osobními údaji. Pokud například osobní údaje představují informace psané vlastnoručně subjektem údajů, může být nutné poskytnout subjektu údajů fotokopii těchto ručně psaných informací, neboť tento rukopis je sám o sobě osobním údajem. Mohlo by tomu tak být zejména v případě, kdy je rukopis něčím, co je podstatné pro zpracování, např. při analýze písma. Totéž platí obecně pro zvukové záznamy, protože hlas subjektu údajů je sám o sobě osobním údajem. V některých případech však může být přístup umožněn například poskytnutím přepisu rozhovoru, pokud se na tom subjekt údajů a správce dohodnou.

156. Je třeba poznamenat, že ustanovení ohledně požadavků na formát se liší, pokud jde o právo na přístup a právo na přenositelnost údajů. Zatímco právo na přenositelnost údajů podle článku 20 GDPR vyžaduje, aby byly informace poskytnuty ve strojově čitelném formátu, právo na informace podle článku 15 to nevyžaduje. Formáty, které se nepovažují za vhodné pro vyhovění žádosti o přenositelnost údajů, například soubory ve formátu PDF, tudíž mohou být vhodné pro vyhovění žádosti o přístup.

5.3 Lhůty pro poskytnutí přístupu

157. Ustanovení čl. 12 odst. 3 GDPR vyžaduje, aby správce poskytl subjektu údajů informace o opatřeních přijatých v souvislosti s žádostí podle článku 15 bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Tuto lhůtu je možné s ohledem na složitost a počet žádostí prodloužit nanejvýš o dva měsíce za předpokladu, že subjekt údajů byl do jednoho měsíce od obdržení žádosti informován o důvodech takového odkladu. Tato povinnost informovat subjekt údajů o prodloužení a jeho důvodech by neměla být zaměňována s informacemi, které musí být poskytnuty bezodkladně a nejpozději do jednoho měsíce, pokud správce nepřijme na základě žádosti opatření, jak je podrobně uvedeno v čl. 12 odst. 4 GDPR.

158. Správce musí reagovat a v zásadě poskytnout informace podle článku 15 bez zbytečného odkladu, což znamená, že informace by měly být poskytnuty co nejdříve. To znamená, že pokud je možné poskytnout požadované informace v kratší lhůtě než jeden měsíc, správce by tak měl učinit. EDPB má rovněž za to, že lhůta pro odpověď na žádost musí být v některých situacích přizpůsobena době uložení, aby bylo možné přístup poskytnout[89].

159. Lhůta začíná běžet od okamžiku, kdy správce obdrží žádost podle článku 15, tj. když je žádost doručena správci některým z jeho oficiálních kanálů[90]. Není nutné, aby správce o žádosti skutečně věděl. Pokud však správce musí se subjektem údajů komunikovat z důvodu nejistoty ohledně totožnosti osoby, která žádost podala, může dojít k přerušení lhůty, dokud správce nezíská od subjektu údajů potřebné informace za předpokladu, že správce bez zbytečného odkladu o dodatečné informace požádal. Totéž platí pro případ, kdy správce požádal subjekt údajů o upřesnění operací zpracování, kterých se žádost týká, pokud jsou splněny podmínky stanovené v 63. bodě odůvodnění[91].

Příklad 31: Po obdržení žádosti správce okamžitě reaguje a vyžádá si informace, které potřebuje pro potvrzení totožnosti osoby, která žádost podala. Uvedená osoba odpoví až o několik dnů později a informace, které subjekt údajů zašle za účelem ověření identity, se nezdají být dostatečné, a správce je tak nucen požádat o vyjasnění. V této situaci dojde k přerušení lhůty, dokud správce nezíská dostatek informací pro ověření totožnosti subjektu údajů.

160. Lhůtu pro odpověď na žádost o přístup je třeba vypočítat v souladu s nařízením č. 1182/71[92].

Příklad 32: Organizace obdrží žádost 5. března. Lhůta začíná běžet od téhož dne. Organizace tak může žádosti vyhovět nejpozději do 5. dubna včetně.

Příklad 33: Pokud organizace obdrží žádost 31. srpna a vzhledem k tomu, že je následující měsíc kratší a odpovídající datum neexistuje, je datem pro odpověď nejpozději poslední den následujícího měsíce, tedy 30. září.

161. Pokud poslední den této lhůty připadne na víkend nebo svátek, má správce na odpověď čas do následujícího pracovního dne.

162. Za určitých okolností může správce v případě potřeby lhůtu pro odpověď na žádost o přístup prodloužit o další dva měsíce, a to s ohledem na složitost a počet žádostí. Je třeba zdůraznit, že tato možnost představuje výjimku z obecného pravidla a neměla by být nadužívána. Pokud jsou správci často nuceni lhůtu prodlužovat, může to svědčit o potřebě dále rozvíjet jejich obecné postupy pro vyřizování žádostí.

163. To, co představuje složitou žádost, se liší v závislosti na konkrétních okolnostech každého případu. Mezi faktory, které lze považovat za relevantní, patří například:

- množství údajů zpracovávaných správcem,
- jak jsou informace uloženy, zejména pokud je obtížné je vyhledat, například když jsou údaje zpracovávány různými útvary organizace,

[89] Viz oddíl 2.3.3.
[90] V některých členských státech existuje vnitrostátní právo, které určuje, kdy se zpráva považuje za přijatou, s ohledem na víkendy a státní svátky.
[91] Viz dále oddíl 2.3.1.
[92] Nařízení Rady (EHS, Euratom) č. 1182/71 ze dne 3. června 1971, kterým se určují pravidla pro lhůty, data a termíny.

- nutnost upravit informace, na které se vztahuje výjimka, například informace týkající se jiných subjektů údajů nebo informace, které představují obchodní tajemství, a
- to, že je zapotřebí s informacemi dále pracovat, aby byly srozumitelné.

164. Samotná skutečnost, že splnění žádosti by vyžadovalo velké úsilí, neznamená, že žádost je složitá. Stejně tak skutečnost, že velká společnost dostává velký počet žádostí, automaticky nevyvolává prodloužení lhůty. Pokud však správce dočasně obdrží velké množství žádostí, například v důsledku mimořádné publicity týkající se jeho činnosti, lze to považovat za legitimní důvod pro prodloužení doby reakce. Správce, zejména ten, který zpracovává velké množství údajů, by však měl mít zavedeny postupy a mechanismy, aby byl za běžných okolností schopen vyřizovat žádosti ve stanovené lhůtě.

6 MEZE A OMEZENÍ PRÁVA NA PŘÍSTUP

6.1 Obecné poznámky

165. Právo na přístup podléhá omezením, jež vyplývají z čl. 15 odst. 4 GDPR (práva a svobody jiných osob) a z čl. 12 odst. 5 GDPR (zjevně nedůvodné nebo nepřiměřené žádosti). Kromě toho může právo Unie nebo členského státu omezit právo na přístup v souladu s článkem 23 GDPR. Odchylky týkající se zpracování osobních údajů pro účely vědeckého či historického výzkumu nebo pro statistické účely či pro účely archivace ve veřejném zájmu mohou být založeny na čl. 89 odst. 2, respektive čl. 89 odst. 3 GDPR a odchylky týkající se zpracování prováděného pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu mohou být založeny na čl. 85 odst. 2 GDPR.

166. Je důležité poznamenat, že kromě výše uvedených mezí, odchylek a možných omezení GDPR nepovoluje žádné další výjimky ani odchylky od práva na přístup. To mimo jiné znamená, že právo na přístup je bez jakékoli obecné výhrady k přiměřenosti, pokud jde o úsilí, které musí správce vynaložit na splnění žádosti subjektu údajů podle článku 15 GDPR[93]. Kromě toho není dovoleno omezit právo na přístup ve smlouvě mezi správcem a subjektem údajů.

167. Podle 63. bodu odůvodnění je právo na přístup subjektům údajů přiznáno, aby byly informovány o jejich zpracování a mohly si ověřit jeho zákonnost. Právo na přístup mimo jiné umožňuje subjektu údajů dosáhnout v závislosti na okolnostech opravy, výmazu nebo blokování osobních údajů[94]. Subjekty údajů však nejsou povinny uvádět důvody a svou žádost zdůvodňovat. Pokud jsou splněny požadavky článku 15 GDPR, účely, pro které byla žádost podána, je třeba považovat za irelevantní[95].

6.2 Čl. 15 odst. 4 GDPR

168. Podle čl. 15 odst. 4 GDPR nesmí být právem získat kopii nepříznivě dotčena práva a svobody jiných osob. Vysvětlení tohoto omezení je podáno v páté a šesté větě 63. bodu odůvodnění. Tímto právem by neměla být nepříznivě dotčena práva ani svobody ostatních, například obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení. Zohlednění těchto skutečností by ovšem nemělo vést k tomu, že by subjektu údajů bylo odepřeno poskytnutí všech informací. Při výkladu čl. 15 odst. 4 GDPR je třeba postupovat zvlášť opatrně, aby

[93] Pokud správce zpracovává velké množství informací týkajících se subjektu údajů, jak je uvedeno v 63. bodě odůvodnění GDPR, může správce požádat subjekt údajů, aby konkrétně uvedl, kterých informací nebo činností zpracování se jeho žádost týká. Viz také oddíl 2.3.1.
[94] SDEU, spojené věci C-141/12 a C-372/12, YS a další.
[95] Tím nejsou dotčeny platné vnitrostátní právní předpisy, jež splňují požadavky článku 23 GDPR, viz kapitola 6.4.

nedošlo k neoprávněnému rozšíření omezení stanovených v článku 23 GDPR, která jsou přípustná pouze za přísných podmínek.

169. Ustanovení čl. 15 odst. 4 GDPR se vztahuje na právo získat kopii údajů, což je hlavní způsob umožnění přístupu ke zpracovávaným údajům (druhá složka práva na přístup). To platí – a je třeba zohlednit práva a svobody ostatních – i v případě, že přístup k osobním údajům je výjimečně umožněn jiným způsobem než prostřednictvím kopie, Například není odůvodněný rozdíl v tom, zda je obchodní tajemství dotčeno poskytnutím kopie, nebo umožněním přístupu subjektu údajů na místě. Ustanovení čl. 15 odst. 4 GDPR se nevztahuje na další informace o zpracování uvedené v čl. 15 odst. 1 písm. a) až h) GDPR.

170. Podle 63. bodu odůvodnění protichůdná práva a svobody zahrnují obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení. Tato výslovně uvedená práva a svobody je třeba považovat pouze za příklady, neboť v zásadě lze mít za to, že omezení podle čl. 15 odst. 4 GDPR může být uplatněno na jakékoli právo nebo svobodu založenou na právu Unie nebo členského státu[96]. Za dotčené právo ve smyslu čl. 15 odst. 4 GDPR lze tedy rovněž považovat právo na ochranu osobních údajů (článek 8 Listiny základních práv Evropské unie). Pokud jde o právo získat kopii, je právo na ochranu údajů jiných osob typickým příkladem, kdy je nutné toto omezení posoudit. Dále je třeba zohlednit právo na důvěrnost korespondence, například pokud jde o soukromou e-mailovou korespondenci v souvislosti se zaměstnáním[97]. Je důležité poznamenat, že ne každý zájem představuje „práva a svobody“ podle čl. 15 odst. 4 GDPR. Například ekonomické zájmy společnosti nezveřejňovat osobní údaje nedosahují hranice pro uplatnění výjimky podle čl. 15 odst. 4, pokud nejsou dotčena obchodní tajemství, duševní vlastnictví nebo jiná chráněná práva.

171. „Jinou osobou“ se rozumí jakákoli jiná osoba nebo subjekt kromě subjektu údajů, který uplatňuje své právo na přístup. Proto by se mohlo přihlížet k právům a svobodám správce nebo zpracovatele (například při zachování důvěrnosti obchodních tajemství a duševního vlastnictví). Kdyby zákonodárce EU chtěl vyloučit práva a svobody správců nebo zpracovatelů, použil by pojem „třetí strana“, který je definován v čl. 4 bodě 10 GDPR.

172. Obecná obava, že by vyhovění žádosti o přístup mohlo mít vliv na práva a svobody jiných osob, nestačí k tomu, aby bylo možné se odvolávat na čl. 15 odst. 4 GDPR. Správce musí být schopen prokázat, že v konkrétní situaci by skutečně byla dotčena práva nebo svobody jiných osob.

Příklad 34: O osobu, která je nyní dospělá, se v minulosti několik let staral úřad péče o mládež. Příslušné soubory mohou případně obsahovat citlivé informace o dalších osobách (rodičích, sociálních pracovnících, dalších nezletilých). Žádost o informace podanou subjektem údajů však obecně z tohoto důvodu nelze zamítnout s odkazem na čl. 15 odst. 4 GDPR. Naopak, úřad péče o mládež jako správce musí podrobně prozkoumat a prokázat práva a svobody jiných osob. V závislosti na dotčených zájmech a jejich relativní váze může být poskytnutí těchto konkrétních informací odmítnuto (např. úpravou jmen).

173. S ohledem na 4. bod odůvodnění GDPR a odůvodnění čl. 52 odst. 1 Listiny základních práv Evropské unie právo na ochranu osobních údajů není právem absolutním[98]. Proto musí být také výkon práva na přístup vyvážen s ostatními základními právy v souladu se zásadou proporcionality. Pokud posouzení

[96] Váha nebo priorita protichůdných práv a svobod není otázkou definice pojmů „práva a svobody“. Vyvážení těchto zájmů je však součástí druhého kroku posouzení, zda je čl. 15 odst. 4 použitelný. Viz bod 173 výše.
[97] Evropský soud pro lidská práva, Bărbulescu proti Rumunsku, č. 61496/08, bod 80, 5. září 2017.
[98] Viz například také SDEU, spojené věci C-92/09 a C-93/09, Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen [GC], 9. listopadu 2010, bod 48.

podle čl. 15 odst. 4 GDPR prokáže, že vyhovění žádosti má nepříznivé (negativní) účinky na práva a svobody jiných účastníků (krok 1), je třeba zvážit zájmy všech účastníků s přihlédnutím ke konkrétním okolnostem případu a zejména k pravděpodobnosti a závažnosti rizik, která jsou se sdělením údajů spojena. Správce by se měl pokusit o sladění protichůdných práv (krok 2), například zavedením vhodných opatření zmírňujících riziko pro práva a svobody jiných osob. Jak je zdůrazněno v 63. bodě odůvodnění, ochrana práv a svobod jiných osob na základě čl. 15 odst. 4 GDPR by neměla vést k tomu, že by subjektu údajů bylo odepřeno poskytnutí všech informací. To například znamená, že v případě, kdy platí omezení, musí být informace týkající se jiných osob v co největší míře učiněny nečitelnými, namísto aby bylo odepřeno poskytnutí kopie osobních údajů. Pokud však není možné nalézt řešení, jak sladit příslušná práva, musí správce v dalším krokurozhodnout, které z protichůdných práv a svobod má přednost (krok 3).

Příklad 35: Maloobchodník nabízí svým zákazníkům možnost objednat si výrobky prostřednictvím horké linky, kterou provozuje jeho zákaznický servis. Za účelem prokázání obchodních transakcí ukládá maloobchodník záznam hovoru v souladu s přísnými požadavky příslušných právních předpisů. Zákazník chce obdržet kopii rozhovoru, který vedl se zástupcem zákaznického servisu. V prvním kroku maloobchodník žádost analyzuje a zjistí, že záznam obsahuje osobní údaje, které se týkají i někoho jiného, konkrétně zástupce zákaznického servisu. Ve druhém kroku, aby bylo možné posoudit, zda by poskytnutím kopie byla dotčena práva a svobody jiných osob, musí maloobchodník vyvážit protichůdné zájmy, zejména s přihlédnutím k pravděpodobnosti a závažnosti možných rizik pro práva a svobody zástupce zákaznického servisu, která existují při sdělení záznamu zákazníkovi. Maloobchodník dojde k závěru, že osobní údaje týkající se zástupce zákaznického servisu jsou v záznamu velmi omezené, jedná se pouze o jeho hlas. Maloobchodník/správce shledá, že zástupce není snadno identifikovatelný. Obsah rozhovoru je navíc odborné povahy a subjektem údajů byl partner. Na základě výše uvedených okolností správce objektivně dospěje k závěru, že právem na přístup nejsou nepříznivě dotčena práva a svobody zástupce zákaznického servisu, a proto může správce poskytnout subjektu údajů celý záznam, včetně částí hlasového záznamu, které se týkají zástupce zákaznického servisu.

Příklad 36: Zákaznice obchodu se zdravotnickými potřebami požaduje přístup k výsledkům měření jejích nohou na základě článku 15 GDPR. Obchod se zdravotnickými potřebami změřil nohy subjektu údajů, aby mohl vyrobit individuální zdravotní kompresivní punčochy. V obchodě se zdravotnickými potřebami měli zřejmě bohaté zkušenosti a zavedli speciální techniku pro přesné měření. Po měření v obchodě se zdravotnickými potřebami chce zákaznice využít výsledky měření k nákupu levnějších punčoch jinde (objedná si je v internetovém obchodě). Obchod se zdravotnickými potřebami zčásti odepře přístup k údajům na základě čl. 15 odst. 4 GDPR s odůvodněním, že výsledky jsou vzhledem k jejich speciálním, přesným technikám měření chráněny jako obchodní tajemství. V takovém případě a za předpokladu, že je správce schopen prokázat, že:

- poskytnutí informací o výsledcích měření subjektu údajů není možné, aniž by bylo odhaleno, jakým způsobem byla měření provedena, a
- informace o tom, jak byla měření provedena, případně včetně přesného určení měřicích bodů, jsou obchodním tajemstvím,

může uplatnit čl. 15 odst. 4 GDPR.

Správce by přesto musel poskytnout co možná nejvíce informací o výsledcích měření, které by neodhalovaly jeho obchodní tajemství, a to i kdyby to znamenalo vyvinout snahu o revizi a úpravu výsledků.

Příklad 37: Hráč X je registrován jako uživatel herní platformy Y. Jednoho dne je hráč X upozorněn, že jeho online účet byl omezen. Protože se již nemůže přihlásit, požádá hráč X správce o přístup ke všem osobním údajům, které se ho týkají. Kromě toho hráč X vyžaduje přístup k důvodům omezení účtu. Platforma Y, správce online herní platformy, u níž byla žádost podána, informuje uživatele ve svých všeobecných podmínkách, které jsou k dispozici na jejích internetových stránkách, že jakýkoli druh podvádění (zejména pomocí softwaru třetích stran) bude mít za následek dočasný nebo trvalý zákaz přístupu na platformu. Platforma Y ve svých zásadách ochrany osobních údajů rovněž v souladu s požadavky stanovenými v článku 13 GDPR informuje uživatele o zpracování osobních údajů za účelem odhalování herních podvodů.

Po obdržení žádosti hráče X o přístup by měla platforma Y poskytnout hráči X kopii osobních údajů, které o něm zpracovává. Pokud jde o důvod omezení účtu, platforma Y by měla hráči X potvrdit, že se rozhodla omezit jeho přístup k online hrám kvůli používání jednoho nebo více herních podvodů, které porušují obecné podmínky užívání. Kromě informací poskytnutých o zpracování pro účely odhalování herních podvodů by měla platforma poskytnout hráči X přístup k informacím, které má uloženy o herních podvodech hráče X, jež vedly k omezení. Platforma Y by měla zejména poskytnout hráči X informace, které vedly k omezení účtu (např. přehled záznamů, datum a čas, kdy došlo k podvádění, zjištění softwaru třetí strany atd.), aby si subjekt údajů (tj. hráč X) mohl ověřit, že zpracování údajů bylo přesné.

Podle čl. 15 odst. 4 GDPR a 63. bodu odůvodnění GDPR není platforma Y povinna zveřejnit žádnou část technického fungování softwaru proti podvodům, a to i kdyby se tyto informace týkaly hráče X, pokud je lze považovat za obchodní tajemství. Nezbytné vyvážení zájmů podle čl. 15 odst. 4 GDPR povede k výsledku, že obchodní tajemství platformy Y brání zveřejnění těchto osobních údajů, protože znalost technického fungování softwaru proti podvodům by uživateli mohla rovněž umožnit obejít budoucí odhalování klamání nebo podvodů[99].

174. Pokud správci odmítnou zcela nebo zčásti vyhovět žádosti o právo na přístup podle čl. 15 odst. 4 GDPR, musí neprodleně, nejpozději však do jednoho měsíce, informovat subjekt údajů o důvodech (čl. 12 odst. 4 GDPR). Vysvětlení musí odkazovat na konkrétní okolnosti, aby subjekty údajů mohly posoudit, zda chtějí proti odmítnutí podat žalobu. Musí obsahovat informace o možnosti podat stížnost u dozorového úřadu (článek 77 GDPR) a o možnosti požádat o soudní ochranu (článek 79 GDPR).

6.3 Čl. 12 odst. 5 GDPR

175. Ustanovení čl. 12 odst. 5 GDPR umožňuje správcům zamítnout žádosti o právo na přístup, které jsou zjevně nedůvodné nebo nepřiměřené. Tyto pojmy je třeba vykládat úzce, neboť nesmí být narušeny zásady transparentnosti a práva subjektů údajů na bezplatnost.

[99] Rozsah informací poskytovaných fyzickým osobám bude do značné míry záviset na kontextu, a to s ohledem na povahu správce a povahu porušení podmínek poskytování služby. V některých případech může být možné, aby správce v odpovědi na žádost o přístup poskytl pouze základní informace, na které se vztahuje čl. 15 odst. 4.

176. Správci musí být schopni fyzické osobě prokázat, proč považují žádost za zjevně nedůvodnou nebo nepřiměřenou, a na požádání vysvětlit tyto důvody příslušnému dozorovému úřadu. Každá žádost by měla být posuzována jednotlivě v souvislostech, v jakých byla podána, aby bylo možné rozhodnout, zda je zjevně nedůvodná nebo nepřiměřená.

6.3.1 Co znamená zjevně nedůvodná?

177. Žádost o právo na přístup je zjevně nedůvodná, pokud při uplatnění objektivního přístupu nejsou splněny požadavky článku 15 GDPR. Jak bylo však vysvětleno zejména v oddíle 3 výše, pro žádosti o právo na přístup existuje jen velmi málo nezbytných podmínek. EDPB proto zdůrazňuje, že pokud jde o žádosti o právo na přístup, pro uplatnění alternativy „nedůvodnosti" podle čl. 12 odst. 5 nařízení GDPR existuje pouze velmi omezený prostor.

178. Dále je důležité připomenout, že před uplatněním tohoto omezení musí správci pečlivě analyzovat obsah a rozsah žádosti. Žádost by například neměla být považována za zjevně nedůvodnou, pokud se týká zpracování osobních údajů, na něž se GDPR nevztahuje (v tomto případě by žádost neměla být vůbec vyřizována jako žádost podle článku 15).

179. Další případy, v nichž je uplatnění čl. 12 odst. 5 GDPR sporné, jsou žádosti týkající se informací nebo činností zpracování, které zjevně a očividně nejsou předmětem činností zpracování daného správce.

> **Příklad 38:** Subjekt údajů se obrací na obecní úřad s žádostí týkající se údajů, které zpracovává státní orgán. Namísto argumentace, že žádost je zjevně nedůvodná, by bylo vhodnější a také snazší, aby dožádaný orgán potvrdil, že tyto údaje nezpracovává (první složka článku 15 GDPR: „zda" jsou zpracovávány osobní údaje)[100].

180. Správce by neměl předpokládat, že žádost je zjevně nedůvodná, protože subjekt údajů již dříve podal žádosti, které byly zjevně nedůvodné nebo nepřiměřené, nebo v případě, že žádost obsahuje neobjektivní nebo nevhodné formulace.

6.3.2 Co znamená nepřiměřená?

181. Pojem „nepřiměřená" není v GDPR definován. Na jedné straně formulace „zejména protože se opakují" v čl. 12 odst. 5 GDPR umožňuje vyvodit závěr, že hlavním scénářem pro použití této části v souvislosti s článkem 15 GDPR souvisí s množstvím žádostí subjektu údajů o uplatnění práva na přístup. Na druhou stranu z výše uvedené formulace vyplývá, že nejsou a priori vyloučeny jiné důvody, které by mohly způsobit nepřiměřenost.

182. Podle čl. 15 odst. 3 GDPR týkajícího se práva získat kopii subjekt údajů může samozřejmě podat správci více než jednu žádost[101]. V případě žádostí, které by potenciálně mohly být považovány za nepřiměřené, závisí posouzení „nepřiměřenosti" na analýze provedené správcem a na specifikách odvětví, v němž působí.

183. V případě následných žádostí je třeba posoudit, zda byla překročena hranice přiměřených odstupů (viz 63. bod odůvodnění), či nikoli. Správci musí pečlivě zohlednit konkrétní okolnosti každého případu.

184. Například v případě sociálních sítí se očekává, že ke změně souboru údajů dojde v kratších odstupech než v případě katastrů nemovitostí nebo centrálních registrů společností. V případě obchodních

[100] Jinou otázkou je, zda je orgán, kterému byla žádost o přístup adresována, oprávněn žádost předat příslušnému státnímu orgánu.
[101] Podle druhé věty čl. 15 odst. 3 může správce účtovat za další požadované kopie přiměřený poplatek.

partnerů je třeba zvážit četnost kontaktů se zákazníkem. V souladu s tím se liší i „přiměřené odstupy“, ve kterých mohou subjekty údajů opět uplatnit své právo na přístup. Čím častěji dochází ke změnám v databázi správce, tím častěji smí subjekty údajů žádat o přístup ke svým osobním údajům, aniž by to bylo nepřiměřené. Na druhé straně by druhá žádost téhož subjektu údajů mohla být za určitých okolností považována za opakovanou.

185. Při rozhodování o tom, zda uplynula přiměřená doba, by správci měli s ohledem na přiměřená očekávání subjektu údajů zvážit tyto skutečnosti:

- jak často se údaje mění – je nepravděpodobné, že by se informace mezi jednotlivými žádostmi změnily? Pokud soubor údajů zjevně nepodléhá jinému zpracování než uložení a subjekt údajů si je toho vědom, např. vzhledem k předchozí žádosti o právo na přístup, může to naznačovat nepřiměřenost žádosti,
- povaha údajů – může se jednat například o zvlášť citlivé údaje,
- účely zpracování – ty by mohly zahrnovat, zda je pravděpodobné, že zpracování způsobí žadateli újmu (poškození), bude-li zveřejněno,
- zda se následné žádosti týkají stejného typu informací nebo stejných činností zpracování, nebo jiných[102].

Příklad 39 (truhlář): Subjekt údajů podává **každé dva měsíce** žádost o přístup u truhláře, který pro něj vyrobil stůl. Truhlář na první žádost odpověděl v plném rozsahu. Při rozhodování o tom, zda uplynul přiměřený časový odstup, je třeba vzít v úvahu, že truhlář zpracovává a shromažďuje osobní údaje pouze příležitostně (první odrážka výše), nikoli v rámci své hlavní činnosti, a ještě méně pravděpodobné je, že truhlář často poskytuje služby témuž subjektu údajů. V daném případě totiž truhlář neposkytl subjektu údajů více než jednu službu, takže je nepravděpodobné, že by v souboru údajů týkajících se subjektu údajů došlo ke změnám. Zejména vzhledem k povaze a množství zpracovaných osobních údajů lze rizika spojená se zpracováním považovat za nízká (druhá odrážka výše), například účel zpracování (fakturační účely a plnění povinnosti vést záznamy) pravděpodobně nezpůsobí subjektu údajů újmu (třetí odrážka výše). Žádost se kromě toho týká stejných informací jako poslední žádost (čtvrtá odrážka výše). Takové žádosti mohou být v důsledku toho považovány za nepřiměřené z důvodu jejich opakování.

Příklad 40 (platforma sociálních médií): Platforma sociálních médií, jejíž hlavní činností je shromažďování a/nebo zpracování osobních údajů subjektu údajů, provádí rozsáhlé komplexní a nepřetržité činnosti zpracování. Subjekt údajů, který využívá služeb platformy, podává žádosti o přístup **každé tři měsíce**. V tomto případě jsou vysoce pravděpodobné časté změny osobních údajů týkajících se subjektu údajů (první odrážka výše), široká škála shromažďovaných údajů zahrnuje odvozené citlivé osobní údaje (druhá odrážka výše) zpracovávané za účelem zobrazení příslušného obsahu a členů sítě subjektu údajů (třetí odrážka). Žádosti o přístup podávané každé tři měsíce nelze za těchto okolností v zásadě považovat za nepřiměřené z důvodu opakování.

[102] Pokud se následná žádost týká stejného typu informací co do rozsahu A času, nejedná se o nepřiměřenost, ale o žádost o další kopii, viz oddíl 2.2.2.2.

Příklad 41 (úvěrové agentury): Stejně jako v případě sociálních sítí nelze vyloučit, že k úpravám příslušných údajů v držení úvěrových agentur bude docházet v mnohem kratších intervalech než v jiných oblastech (první odrážka výše). Vyplývá to z mnoha faktorů, které si subjekt údajů jako osoba zvenčí obvykle neuvědomuje vzhledem ke složitosti obchodního modelu. Odpověď na otázku, které typy údajů byly správcem shromážděny za účelem výpočtu bodového hodnocení a které jsou v současné době do výpočtu zahrnuty, proto může poskytnout pouze samotná úvěrová agentura. Kromě toho může mít zpracování údajů prostřednictvím úvěrových agentur a výsledné bodové hodnocení pro subjekt údajů dalekosáhlé důsledky, pokud jde o zamýšlené právní úkony, jako je uzavírání kupních, nájemních nebo leasingových smluv (třetí odrážka výše).

Není možné konkrétně určit časový odstup, při kterém by podání další žádosti o přístup mohlo být považováno za nepřiměřené podle čl. 12 odst. 5 druhé věty GDPR. Je nutné spíše celkově zvážit okolnosti konkrétního případu. Vzhledem k významu zpracování údajů pro realitu každodenního života subjektů údajů však lze předpokládat, že **jednoroční odstup** mezi bezplatně poskytnutými informacemi bude v každém případě příliš dlouhý na to, aby žádost mohla být považována za nepřiměřenou. Pokud je žádost podána ve velmi krátkém časovém odstupu, mělo by být rozhodující, zda má subjekt údajů důvod předpokládat, že se informace nebo zpracování od poslední žádosti změnily. Pokud například subjekt údajů provedl finanční transakci, například si vzal úvěr, měl by mít právo požádat o přístup k informacím o úvěru, i když taková žádost byla podána a zodpovězena krátce předtím.

186. Pokud je možné informace snadno poskytnout elektronickými prostředky nebo prostřednictvím vzdáleného přístupu do zabezpečeného systému, což znamená, že vyhovění takovým žádostem správce skutečně nezatěžuje, není pravděpodobné, že by následné žádosti mohly být považovány za nepřiměřené.

187. Jestliže se žádost překrývá s předchozí žádostí, lze překrývající se žádost obecně považovat za nepřiměřenou, pokud se týká zcela stejných informací nebo činností zpracování a pokud správce předchozí žádosti dosud nevyhověl, aniž by bylo dosaženo stavu „zbytečného odkladu“ (viz čl. 12 odst. 3 GDPR). V praxi by tak bylo možné obě žádosti zkombinovat.

188. Skutečnost, že poskytnutí informací nebo kopie subjektu údajů by vyžadovalo obrovské množství času a úsilí ze strany správce, nemůže samo o sobě učinit žádost nepřiměřenou[103]. Velký počet činností zpracování obvykle znamená větší úsilí při vyhovění žádostí o přístup. Jak je však uvedeno výše, za určitých okolností lze žádosti považovat za nepřiměřené i z jiných důvodů než proto, že se opakují. Podle názoru EDPB to zahrnuje zejména případy zneužití článku 15 GDPR, což znamená případy, kdy se subjekty údajů uchylují k nepřiměřenému využívání práva na přístup s jediným záměrem, a to správce poškodit nebo mu způsobit újmu.

189. V této souvislosti by žádost neměla být považována za nepřiměřenou na základě toho, že

- subjekt údajů neuvede žádné důvody pro podání žádosti nebo správce považuje žádost za bezpředmětnou,
- subjekt údajů používá nevhodné nebo neslušné výrazy,

[103] Žádný test přiměřenosti, viz bod 166 výše.

- subjekt údajů hodlá údaje použít k uplatnění dalších nároků vůči správci[104].

190. Na druhé straně může být žádost shledána nepřiměřenou, například pokud:

- fyzická osoba podá žádost, ale zároveň nabídne, že ji stáhne výměnou za určitou formu výhody od správce, nebo
- žádost je podložena zlým úmyslem a je použita k obtěžování správce nebo jeho zaměstnanců, a to výlučně za účelem způsobit narušení činnosti, například na základě skutečnosti, že:
  - fyzická osoba v samotné žádosti nebo v jiných sděleních výslovně uvedla, že má v úmyslu způsobit narušení a nic jiného, nebo
  - fyzická osoba systematicky zasílá správci různé žádosti v rámci kampaně, např. jednou týdně, se záměrem a účinkem způsobit narušení[105].

6.3.3 Důsledky

191. V případě zjevně nedůvodné nebo nepřiměřené žádosti o právo na přístup mohou správci podle čl. 12 odst. 5 GDPR buď účtovat přiměřený poplatek (s přihlédnutím k administrativním nákladům na poskytnutí informací nebo sdělení či provedení požadovaného úkonu), nebo odmítnout žádosti vyhovět.

192. EDPB poukazuje na to, že správci na jedné straně nejsou obecně povinni účtovat přiměřený poplatek předtím, než odmítnou žádosti vyhovět. Na druhé straně ani oni nemohou zcela svobodně zvolit mezi oběma alternativami. Ve skutečnosti musí správci přijmout adekvátní rozhodnutí v závislosti na konkrétních okolnostech případu. Zatímco v případě zjevně nedůvodných žádostí si lze jen stěží představit, že by účtování přiměřeného poplatku bylo vhodným opatřením, při nepřiměřených žádostech – v souladu se zásadou transparentnosti – bude často vhodnější účtovat poplatek jako náhradu administrativních nákladů, které opakované žádosti způsobují.

193. Správci musí být schopni prokázat zjevnou nedůvodnost nebo nepřiměřenost žádosti (čl. 12 odst. 5 třetí věta GDPR). Proto se doporučuje zajistit řádné zdokumentování základních skutečností. V souladu s čl. 12 odst. 4 GDPR platí, že pokud správci odmítnou zcela nebo částečně vyhovět žádosti o přístup, musí bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti informovat subjekt údajů

- o důvodech nevyhovění,
- o právu podat stížnost u dozorového úřadu,
- o možnosti požádat o soudní ochranu.

194. Před účtováním přiměřeného poplatku na základě čl. 12 odst. 5 GDPR by správci měli subjektům údajů oznámit, že tak hodlají učinit. Subjektům údajů musí být umožněno se rozhodnout, zda žádost stáhnou, aby se vyhnuly poplatkům.

---

[104] Tím nejsou dotčeny platné vnitrostátní právní předpisy, jež splňují požadavky článku 23 GDPR, viz kapitola 6.4.

[105] „Systematické zasílání v rámci kampaně“ znamená, že žádosti, které by mohly být snadno sloučeny do jedné, jsou subjektem údajů uměle rozděleny ne na několik, ale na mnoho jednotlivých částí se zjevným záměrem způsobit narušení.

195. Neoprávněné zamítnutí žádosti o uplatnění práva na přístup lze považovat za porušení práv subjektu údajů podle článků 12 až 22 GDPR, a proto může podléhat výkonu nápravných pravomocí příslušných dozorových úřadů, včetně správních pokut na základě čl. 83 odst. 5 písm. b) nařízení GDPR. Pokud se subjekty údajů domnívají, že došlo k porušení jejich práv, mají právo podat stížnost na základě článku 77 GDPR.

6.4 Možná omezení v právu Unie nebo členských států na základě článku 23 GDPR a odchylky

196. Rozsah povinností a práv stanovených v článku 15 GDPR může být omezen prostřednictvím legislativních opatření v právu Unie nebo členských států[106].

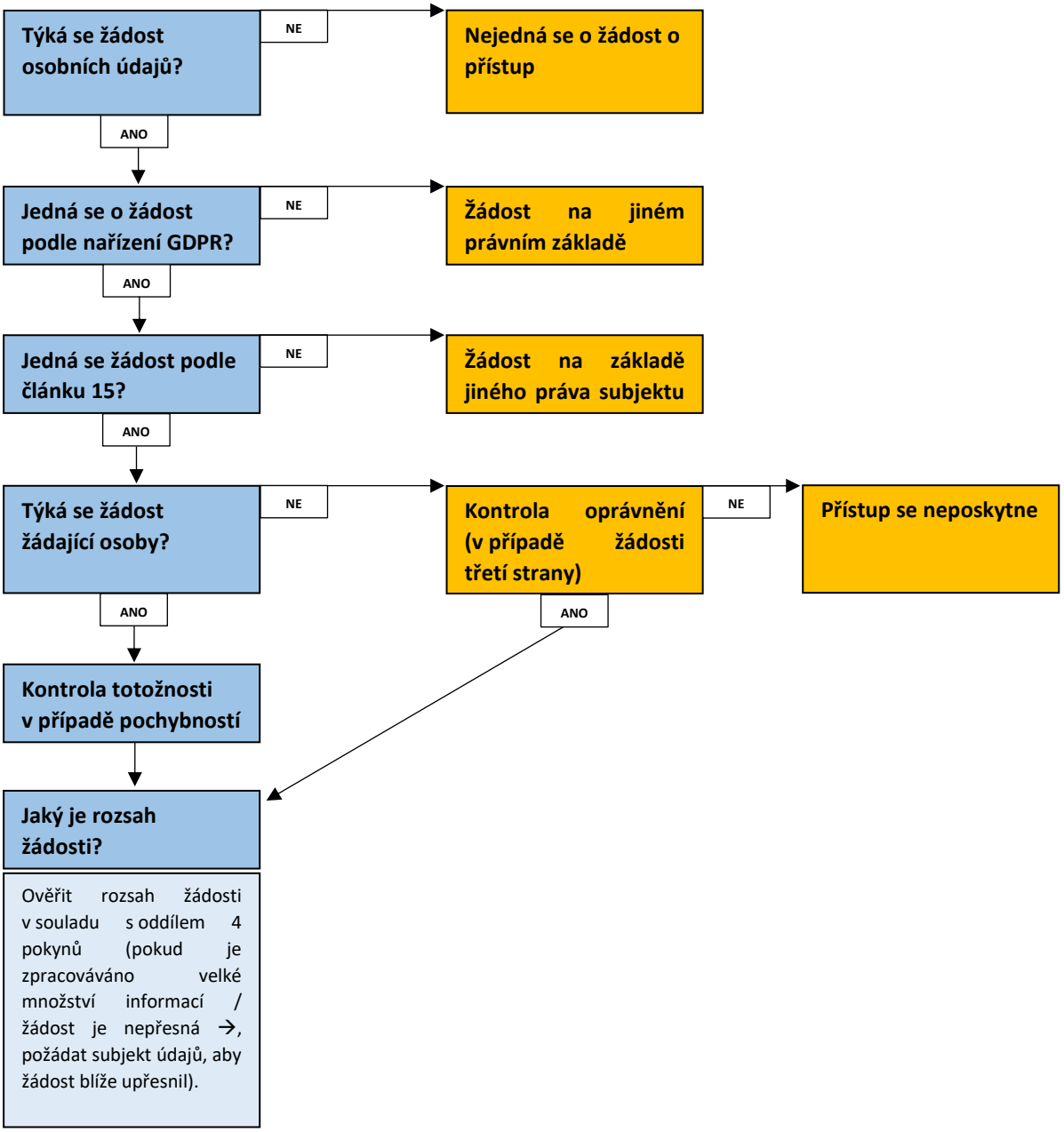
197. Správci, kteří hodlají uplatnit omezení založené na vnitrostátním právu, musí pečlivě zkontrolovat požadavky, jež stanoví ustanovení příslušných vnitrostátních právních předpisů. Kromě toho je důležité poznamenat, že omezení práva na přístup v právu členských států (nebo Unie), která jsou založena na článku 23 GDPR, musí striktně splňovat podmínky stanovené v tomto ustanovení. EDPB vydal pokyny 10/2020 k omezením podle článku 23 GDPR s dalšími vysvětleními k této problematice. Pokud jde o právo na přístup, EDPB připomíná, že správci by měli omezení zrušit, jakmile okolnosti, které je odůvodňují, pominou[107].

198. Legislativní opatření, která se týkají omezení podle článku 23 GDPR, mohou rovněž stanovit odložený výkon práva, částečný výkon práva nebo jeho omezení na určité kategorie údajů, nebo že právo lze vykonávat nepřímo prostřednictvím nezávislého dozorového úřadu[108].

[106] Viz například § 32 až 37 německého spolkového zákona o ochraně osobních údajů (BDSG), § 16 a 17 norského zákona o ochraně osobních údajů a kapitola 5 švédského zákona o ochraně osobních údajů.
[107] Bod 76 pokynů 10/2020 k omezením podle článku 23 GDPR, verze 2.0, přijatých dne 13. října 2021.
[108] Bod 12 pokynů 10/2020 k omezením podle článku 23 GDPR, verze 2.0, přijatých dne 13. října 2021. V § 34 odst. 3 německého spolkového zákona o ochraně osobních údajů se například uvádí, že pokud orgán veřejné moci neposkytne subjektu údajů informace vyhovující žádosti o uplatnění práva na přístup z důvodu určitých omezení, musí být tyto informace na žádost subjektu údajů poskytnuty spolkovému dozorovému úřadu, ledaže odpovědný spolkový dozorový úřad (nadřízený úřadu, u něhož byla žádost podána) v jednotlivém případě rozhodne, že by takový postup ohrozil bezpečnost spolkové republiky nebo spolkové země. Italský kodex ochrany osobních údajů umožňuje nepřímý přístup (prostřednictvím úřadu) v případě, že by se přístup mohl nepříznivě dotknout řady zájmů (např. zájmu na potírání praní peněz), viz článek 2-L italského kodexu ochrany osobních údajů.

PŘÍLOHA – VÝVOJOVÝ DIAGRAM

Krok 1: Jak žádost interpretovat a posoudit?



Krok 2: Jak odpovědět na žádost (1)?

Tři hlavní složky práva na přístup (struktura článku 15)		
Potvrzení, zda jsou či nejsou zpracovávány osobní údaje	Přístup k osobním údajům	Další informace o účelech, příjemcích atd. (čl. 15 odst. 1 písm. a) až h))

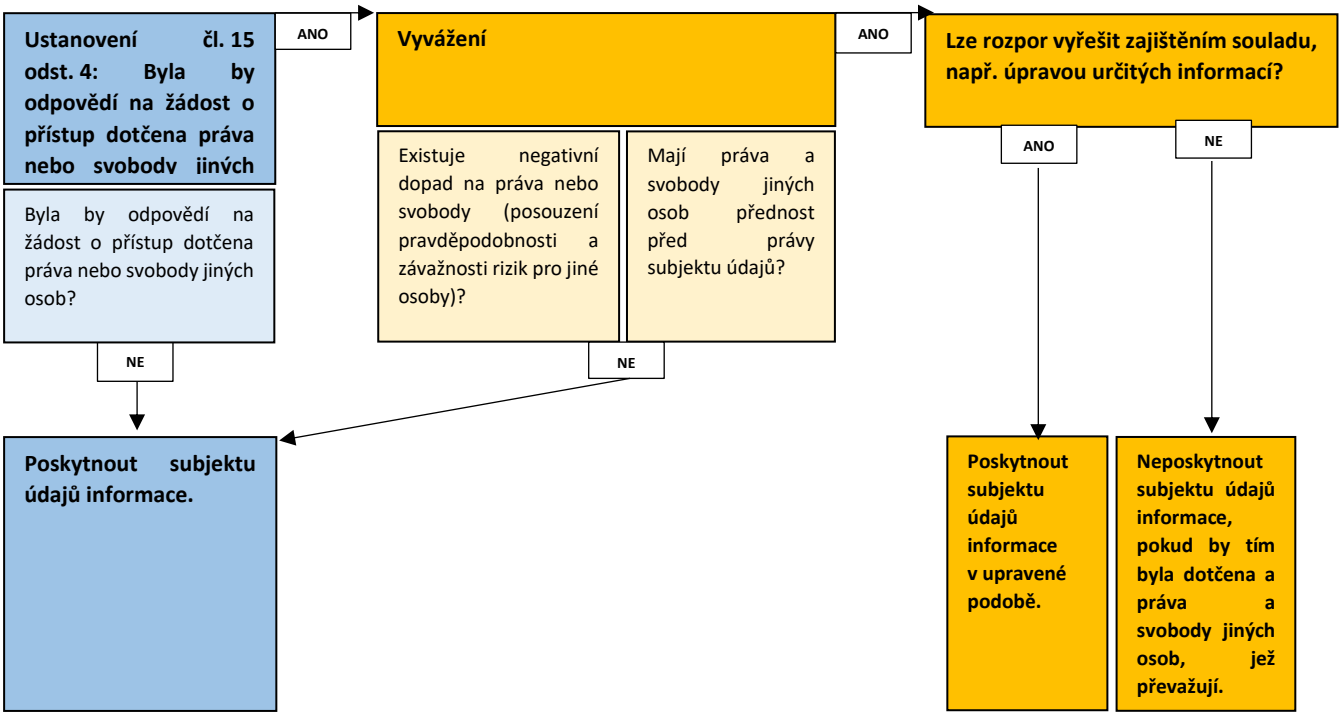
Krok 2: Jak odpovědět na žádost (2)?

Přijmout vhodná opatření			
Ustanovení čl. 12 odst. 1: stručný, transparentní, srozumitelný a snadno	Ustanovení čl. 12 odst. 2: usnadnit výkon práva na přístup		
Zvolit mezi různými prostředky	Poskytnout kopii, pokud není dohodnuto jinak (čl. 15 odst. 3)	V případě potřeby použít vícevrstvý přístup (nejvíce relevantní	Načasování – bez zbytečného odkladu, v každém případě do jednoho měsíce (ve výjimečných případech prodloužení o další dva měsíce) (čl. 12 odst. 3)

Krok 2: Jak odpovědět na žádost (3)?

Jak může správce získat všechny údaje o subjektu údajů?			
Definovat kritéria vyhledávání – na základě toho, co subjekt údajů poskytl, dalších informací, které má správce o subjektu údajů, a faktorů, na jejichž základě jsou údaje strukturovány (např. číslo zákazníka, IP adresy, profesní titul, rodinné vztahy atd.).	Určit všechny technické funkce, které mohou být pro získání údajů k dispozici.	Prohledat všechny příslušné informační systémy nebo jiné než počítačové evidence.	Shromáždit, extrahovat nebo jinak získat údaje, které se týkají subjektu údajů, způsobem, který plně odráží zpracování, tj. který zahrnuje všechny osobní údaje týkající se subjektu údajů, a který umožňuje, aby byl subjekt údajů o zpracování údajů informován a mohl si ověřit jeho zákonnost. Vyhledávání informací lze provádět v každém jednotlivém případě, nebo, je-li to relevantní, pomocí nástroje pro

Krok 3: Kontrola mezí a omezení (1)



Krok 3: Kontrola mezí a omezení (2)