

Usmernenia



Usmernenia 01/2022 k právam dotknutých osôb – Právo na prístup

Verzia 2.0

Prijaté 28. marca 2023

Postupnosť verzií

Verzia 1.0	18. januára 2022	Prijatie usmernení na účely verejnej konzultácie
Verzia 2.0	28. marca 2023	Prijatie usmernení po verejnej konzultácii

ZHRNUTIE

Právo dotknutých osôb na prístup je zakotvené v článku 8 Charty základných práv Európskej únie. Je súčasťou európskeho právneho rámca v oblasti ochrany údajov od jeho vzniku a v súčasnosti ho ďalej rozvíjajú osobitnejšie a presnejšie pravidlá stanovené v článku 15 všeobecného nariadenia o ochrane údajov.

Cieľ a celková štruktúra práva na prístup

Celkovým cieľom práva na prístup je poskytovať jednotlivcom dostatočné, transparentné a jednoducho dostupné informácie o spracúvaní ich osobných údajov, aby si boli vedomí a mohli si overiť zákonnosť spracúvania a presnosť spracúvaných údajov. Jednotlivcom to uľahčí uplatňovanie iných práv, ako je napríklad právo na opravu alebo vymazanie, hoci nie je podmienkou pre ich uplatnenie.

Právo na prístup k údajom sa má podľa práva v oblasti ochrany údajov odlišovať od podobných práv, ktoré majú iné ciele, napríklad od práva na prístup k verejným dokumentom, ktorého účelom je zaručiť transparentnosť v rámci rozhodovacích postupov verejných orgánov a v rámci správnych úradných postupov.

Dotknutá osoba však nemusí uvádzať dôvody žiadosti o prístup a úlohou prevádzkovateľa nie je analyzovať, či žiadosť v skutočnosti pomôže dotknutej osobe overiť zákonnosť príslušného spracúvania alebo uplatniť iné práva. Prevádzkovateľ sa bude musieť žiadosťou zaoberať, pokiaľ nie je jasné, že žiadosť bola podaná podľa iných pravidiel, ako sú pravidlá o ochrane údajov.

Právo na prístup zahŕňa tri rôzne zložky:

- potvrdenie, či sa údaje o osobe spracúvajú alebo nie,
- prístup k týmto osobným údajom a
- prístup k informáciám o spracúvaní, ako je účel, kategórie údajov a príjemcovia, trvanie spracúvania, práva dotknutých osôb a primerané záruky v prípade prenosu údajov do tretích krajín.

Všeobecné úvahy o posúdení žiadosti dotknutej osoby

Prevádzkovateľ musí pri analyzovaní obsahu žiadosti posúdiť, či sa žiadosť týka osobných údajov jednotlivca, ktorý žiadosť podáva, či žiadosť patrí do rozsahu článku 15 a či existujú iné, osobitnejšie ustanovenia, ktorými sa upravuje prístup v určitom sektore. Takisto musí posúdiť, či sa žiadosť týka všetkých spracúvaných údajov o dotknutej osobe alebo len ich časti.

Neexistujú žiadne osobitné požiadavky na formát žiadosti. Prevádzkovateľ by mal poskytnúť vhodné a ľahko použiteľné komunikačné kanály, ktoré dotknutá osoba bude vedieť jednoducho používať. Od dotknutej osoby sa však nevyžaduje, aby používala tieto osobitné kanály, a namiesto toho môže žiadosť poslať na oficiálne kontaktné miesto prevádzkovateľa. Prevádzkovateľ nie je povinný konať vo veci žiadostí, ktoré sú poslané na úplne náhodné alebo zjavne nesprávne adresy.

Ak nie je prevádzkovateľ schopný identifikovať údaje týkajúce sa dotknutej osoby, informuje o tom danú dotknutú osobu a môže odmietnuť ich sprístupnenie, pokiaľ dotknutá osoba neposkytne dodatočné informácie, ktoré by identifikáciu umožnili. Okrem toho, ak má prevádzkovateľ pochybnosti o tom, či je dotknutá osoba tým, kým tvrdí, že je, môže si od nej vyžiadať dodatočné informácie s cieľom potvrdiť jej totožnosť. Žiadosť o dodatočné informácie musí byť primeraná druhu

spracúvaných údajov, škodám, ktoré by mohli vzniknúť atď., a to s cieľom vyhnúť sa neprimeranému zberu údajov.

Rozsah práva na prístup

Rozsah práva na prístup sa určuje rozsahom pojmu osobné údaje, ako sa vymedzuje v článku 4 bode 1 všeobecného nariadenia o ochrane údajov. Okrem základných osobných údajov, ako je meno, adresa, telefónne číslo atď., do rozsahu tohto vymedzenia môže patriť široký okruh údajov, ako sú lekárske zistenia, história nákupov, ukazovatele úverovej bonity, záznamy o činnostiach [activity logs], vyhľadávacie činnosti atď. Osobné údaje, ktoré boli pseudonymizované, sa stále považujú za osobné údaje na rozdiel od anonymizovaných údajov. Právo na prístup sa vzťahuje na osobné údaje týkajúce sa osoby, ktorá podáva žiadosť. Nemalo by sa to vykladať príliš reštriktívne, keďže toto právo sa môže týkať aj údajov, ktoré by mohli súvisieť aj s inými osobami, napríklad pokiaľ ide o históriu komunikácie prichádzajúcich a odchádzajúcich správ.

Prevádzkovateľ musí okrem udelenia prístupu k osobným údajom poskytnúť aj dodatočné informácie o ich spracúvaní a o právach dotknutých osôb. Takéto informácie môžu vychádzať z toho, čo už je zhromaždené v zázname prevádzkovateľa o spracovateľských činnostiach (článok 30 všeobecného nariadenia o ochrane údajov) a oznámení o ochrane osobných údajov [privacy notice] (články 13 a 14 všeobecného nariadenia o ochrane údajov). Môže sa však stať, že tieto všeobecné informácie sa budú musieť aktualizovať v čase prijatia žiadosti alebo sa budú musieť prispôbiť tak, aby odrážali spracovateľské operácie, ktoré sa vykonávajú v súvislosti s určitou osobou, ktorá podala žiadosť.

Ako poskytnúť prístup

Spôsoby, ako poskytnúť prístup sa môžu líšiť v závislosti od množstva údajov a zložitosti spracúvania, ktoré sa vykonáva. Pokiaľ sa výslovne neuvádza inak, žiadosť by sa mala chápať tak, že odkazuje na všetky osobné údaje týkajúce sa dotknutej osoby, pričom v prípade, že prevádzkovateľ spracúva veľké množstvo údajov, môže dotknutú osobu požiadať o spresnenie žiadosti.

Prevádzkovateľ bude musieť osobné údaje vyhľadávať vo všetkých IT systémoch a informačných systémoch nepatriacich do oblasti IT, a to na základe vyhľadávacieho kritéria, ktoré odzrkadľuje spôsob, v akom sú informácie štruktúrované, napríklad podľa mena a čísla zákazníka. Oznámenie o údajoch a iných informáciách týkajúcich sa ich spracúvania musí byť poskytnutá v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme a musí byť jasne a jednoducho formulovaná. Presnejšie požiadavky v tejto súvislosti závisia od okolností spracúvania údajov, ako aj od schopnosti dotknutej osoby uchopiť a pochopiť oznámenie (napríklad s ohľadom na skutočnosť, že dotknutá osoba je dieťa alebo osoba s osobitnými potrebami). Ak údaje pozostávajú z kódov alebo iných nespracovaných údajov [raw data], musia byť dotknutej osobe vysvetlené tak, aby jej dávali zmysel.

Hlavný spôsob poskytovania prístupu je poskytnúť dotknutej osobe kópiu jej údajov, pričom ak o to dotknutá osoba požiada môžu sa stanoviť aj iné spôsoby (ako sú ústne informácie a prístup na mieste). Údaje možno poslať prostredníctvom e-mailu za predpokladu, že sa uplatnili a zohľadnili všetky potrebné záruky, a to napríklad povaha údajov, alebo ich možno poslať inými spôsobmi, napríklad prostredníctvom samoobslužného nástroja [a self-service tool].

V niektorých prípadoch, keď ide o veľké množstvo údajov a pre dotknutú osobu by bolo náročné informácie pochopiť, ak by boli podané v jednom veľkom objeme, a to najmä v online kontexte, by najprimeranejším opatrením mohol byť viacúrovňový prístup [layered approach]. Poskytovanie informácií v rôznych úrovniach môže dotknutej osobe uľahčiť ich porozumenie. Prevádzkovateľ musí

byť schopný preukázať, že viacúrovňový prístup má pre dotknutú osobu pridanú hodnotu, a ak si to dotknutá osoba zvolí, mali by jej byť všetky úrovne poskytnuté naraz.

Kópia údajov a dodatočné informácie by sa mali poskytovať v trvalom formáte, ako je písaný text, ktorý by mohol byť v bežne používanom elektronickom formáte, aby si ho dotknutá osoba mohla jednoducho stiahnuť. Údaje môžu byť podané vo forme prepisu alebo súhrnu, pokiaľ bude obsahovať všetky informácie a neupraví alebo nezmení sa tým ich obsah.

Žiadosti sa musí vyhovieť čo najskôr a v každom prípade do jedného mesiaca od prijatia žiadosti. Uvedená lehota sa môže v prípade potreby predĺžiť o ďalšie dva mesiace, pričom sa zohľadní komplexnosť žiadosti a počet žiadostí. Dotknutá osoba musí byť následne informovaná o dôvodoch oneskorenia. Prevádzkovateľ musí vykonať potrebné opatrenia na spracovanie žiadostí čo najskôr a prispôbiť tieto opatrenia k okolnostiam spracúvania. Ak sa údaje uchovávajú len na veľmi krátke obdobie, musia byť zavedené opatrenia, ktorými sa zaručí, že žiadosti o prístup možno vyhovieť bez toho, aby boli údaje vymazané, kým sa žiadosť spracúva. Ak sa spracúva veľké množstvo údajov, prevádzkovateľ bude musieť zaviesť postupy a mechanizmy prispôbené zložitosti ich spracúvania.

Posúdenie žiadosti by malo odrážať situáciu vo chvíli, keď prevádzkovateľ žiadosť prijme. Poskytnúť sa budú musieť aj údaje, ktoré môžu byť nesprávne alebo ktoré boli spracúvané nezákonne. Údaje, ktoré už boli vymazané, napríklad v súlade s politikou uchovávanía, a z toho dôvodu ich už prevádzkovateľ nemá k dispozícii, nemôžu byť poskytnuté.

Limity a obmedzenia

Všeobecné nariadenie o ochrane údajov umožňuje určité obmedzenia práva na prístup. Ďalšie výnimky alebo odchýlky neexistujú. Právo na prístup je bez akejkoľvek všeobecnej výhrady k proporcionality, pokiaľ ide o úsilie, ktoré prevádzkovateľ musí vynaložiť na splnenie žiadosti dotknutej osoby.

Právo získať kópiu nesmie mať podľa článku 15 ods. 4 nepriaznivé dôsledky na práva a slobody iných. Podľa EDPB sa musia tieto práva zohľadniť nielen pri udeľovaní prístupu k údajom poskytnutím ich kópie, ale aj v prípade, že sa údaje poskytujú inými spôsobmi (napríklad prístupom na mieste). Článok 15 ods. 4 sa však neuplatňuje na dodatočné informácie o spracúvaní uvedené v článku 15 ods. 1 písm. a) až h). Prevádzkovateľ musí byť schopný preukázať, že práva alebo slobody iných by boli v konkrétnej situácii nepriaznivo ovplyvnené. Výsledkom uplatňovania článku 15 ods. 4 by nemalo byť celkové zamietnutie žiadosti dotknutej osoby, ale len vynechanie alebo znemožnenie čitateľnosti tých častí, ktoré by mohli nepriaznivo ovplyvniť práva a slobody iných.

Podľa článku 12 ods. 5 všeobecného nariadenia o ochrane údajov prevádzkovatelia môžu zamietnuť žiadosti, ktoré sú zjavne neopodstatnené alebo neprimerané, alebo požadovať primeraný poplatok za také žiadosti. Tieto pojmy sa musia vykladať reštriktívne. Keďže existuje len veľmi málo požiadaviek na žiadosti o prístup, rozsah, v rámci ktorého možno žiadosť považovať za zjavne neopodstatnenú, je pomerne obmedzený. Neprimerané žiadosti závisia od osobitostí sektoru, v ktorom prevádzkovateľ pôsobí. Čím častejšie sa v databáze prevádzkovateľa vyskytujú zmeny, tým častejšie môže byť dotknutej osobe umožnené žiadať o prístup bez toho, aby sa žiadosť považovala za neprimeranú. Namiesto toho, aby prevádzkovateľ prístup zamietol, sa môže rozhodnúť, že bude od dotknutej osoby žiadať poplatok. Toto by bolo relevantné len v prípade neprimeraných žiadostí s cieľom pokryť administratívne náklady, ktoré takéto žiadosti môžu spôsobiť. Prevádzkovateľ musí byť schopný preukázať zjavne neopodstatnenú alebo neprimeranú povahu žiadosti.

Obmedzenia práva na prístup môžu existovať aj vo vnútroštátnom práve členských štátov, ako sa uvádza v článku 23 všeobecného nariadenia o ochrane údajov a v ňom uvedených výnimkách.

Prevádzkovatelia, ktorí majú v pláne takéto obmedzenia uplatňovať, musia dôkladne skontrolovať požiadavky v rámci vnútroštátnych ustanovení a zohľadniť všetky osobitné podmienky, ktoré sa môžu uplatňovať. Takýmito podmienkami môže byť to, že právo na prístup je len dočasne odložené alebo že sa obmedzenie uplatňuje len na určité kategórie údajov.

Obsah

1	Úvod – všeobecné POznÁmky	9
2	Cieľ práva na prístup, štruktúra článku 15 všeobecného nariadenia o ochrane údajov a všeobecné zásady	11
2.1	Cieľ práva na prístup.....	11
2.2	Štruktúra článku 15 všeobecného nariadenia o ochrane údajov	12
2.2.1	Vymedzenie obsahu práva na prístup	13
2.2.1.1	Potvrdenie toho, či sa osobné údaje spracúvajú alebo nespracúvajú	13
2.2.1.2	Prístup k spracúvaným osobným údajom	13
2.2.1.3	Informácie o spracúvaní údajov a o právach dotknutých osôb.....	14
2.2.2	Ustanovenia o spôsoboch	14
2.2.2.1	Poskytnutie kópie	14
2.2.2.2	Poskytovanie ďalších kópií	15
2.2.2.3	Sprístupňovanie informácií v bežne dostupnej elektronickej podobe.....	16
2.2.3	Možné obmedzenie práva na prístup.....	16
2.3	Všeobecné zásady práva na prístup	17
2.3.1	Úplnosť informácií	17
2.3.2	Správnosť informácií.....	19
2.3.3	Referenčný časový bod posúdenia	19
2.3.4	Súlad s požiadavkami na bezpečnosť údajov	20
3	Všeobecné úvahy týkajúce sa posúdenia žiadostí o prístup	21
3.1	Úvod	21
3.1.1	Analýza obsahu žiadosti	22
3.1.2	Forma žiadosti	24
3.2	Identifikácia a autentifikácia	26
3.3	Posúdenie primeranosti týkajúce sa autentifikácie žiadateľa	28
3.4	Žiadosti podávané prostredníctvom tretích strán/splnomocnení	31
3.4.1	Uplatnenie práva na prístup v mene detí.....	32
3.4.2	Uplatňovanie práva na prístup prostredníctvom portálov/kanálov poskytovaných treťou stranou	32
4	Rozsah práva na prístup a osobné údaje a informácie, ktorých sa týka	33
4.1	Vymedzenie pojmu osobné údaje	33
4.2	Osobné údaje, ktorých sa týka právo na prístup.....	37
4.2.1	„Osobné údaje, ktoré sa týkajú dotknutej osoby“	37
4.2.2	Osobné údaje, ktoré „sa spracúvajú“	39
4.2.3	Rozsah novej žiadosti o prístup	39

4.3	Informácie o spracúvaní údajov a o právach dotknutých osôb	39
5	Ako môže prevádzkovateľ poskytnúť prístup?.....	43
5.1	Ako môže prevádzkovateľ získať požadované údaje?.....	44
5.2	Primerané opatrenia na zabezpečenie prístupu	44
5.2.1	Prijatie „primeraných opatrení“	44
5.2.2	Rôzne spôsoby poskytovania prístupu	46
5.2.3	Poskytnutie prístupu „v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho“	47
5.2.4	Veľké množstvo informácií si vyžaduje osobitné požiadavky týkajúce sa spôsobu poskytovania informácií	49
5.2.5	Formát	50
5.3	Načasovanie poskytnutia prístupu	53
6	Limity a obmedzenia práva na prístup	54
6.1	Všeobecné poznámky.....	54
6.2	Článok 15 ods. 4 všeobecného nariadenia o ochrane údajov.....	55
6.3	Článok 12 ods. 5 všeobecného nariadenia o ochrane údajov.....	58
6.3.1	Čo znamená zjavne neopodstatnená?	59
6.3.2	Čo znamená neprimeraná?	59
6.3.3	Dôsledky	62
6.4	Prípustné obmedzenia v práve Únie alebo členských štátov na základe článku 23 všeobecného nariadenia o ochrane údajov a výnimky	63
	Príloha – Vývojový diagram	64

Európsky výbor pre ochranu údajov

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o EHP, a najmä na prílohu XI a protokol 37 k tejto dohode, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018¹,

so zreteľom na články 12 a 22 svojho rokovacieho poriadku,

keďže prípravné práce na týchto usmerneniach zahŕňali zber príspevkov od zainteresovaných strán, písomne a aj v rámci tematického podujatia zainteresovaných strán o právach dotknutých osôb, s cieľom identifikovať výzvy a problémy s výkladom pri uplatňovaní príslušných ustanovení všeobecného nariadenia o ochrane údajov,

PRIJAL TIETO USMERNENIA

1 ÚVOD – VŠEOBECNÉ POZNÁMKY

1. V dnešnej spoločnosti spracúvajú osobné údaje verejné a súkromné subjekty v rámci mnohých činností, na široké spektrum účelov a mnohými rôznymi spôsobmi. Jednotlivci sa môžu často ocitnúť v nevýhodnej pozícii, pokiaľ ide o chápanie spôsobu spracúvania ich osobných údajov, ako aj o technológie používané v konkrétnych prípadoch, či už súkromným alebo verejným subjektom. S cieľom chrániť osobné údaje fyzických osôb v týchto situáciách sa v rámci všeobecného nariadenia o ochrane údajov vytvoril ucelený a spoľahlivý právny rámec vo všeobecnosti uplatniteľný s ohľadom na rôzne druhy spracúvania údajov, ako aj osobitné ustanovenia súvisiace s právami dotknutých osôb.
2. Právo na prístup k osobným údajom je jedným z práv dotknutých osôb stanovených v kapitole III všeobecného nariadenia o ochrane údajov, medzi ktoré patrí napríklad aj právo na opravu a vymazanie, právo na obmedzenie spracúvania, právo na prenosnosť údajov, právo namietať alebo právo nepodliehať automatizovanému individuálnemu rozhodovaniu vrátane profilovania². Právo dotknutej osoby na prístup je zakotvené v Charte základných práv Európskej únie (ďalej len „Charta“)³ a v článku 15 všeobecného nariadenia o ochrane údajov, v ktorom sa presnejšie vymedzuje ako právo na prístup k osobným údajom a k iným súvisiacim informáciám.
3. Podľa všeobecného nariadenia o ochrane údajov pozostáva právo na prístup z troch zložiek, t. j. z potvrdenia o tom, či sa spracúvajú osobné údaje, z prístupu k nim a z informácií o samotnom spracúvaní. Dotknutá osoba takisto môže získať kópiu spracúvaných osobných údajov, pričom táto možnosť nie je dodatočným právom dotknutej osoby, ale skôr spôsobom ako poskytovať prístup k údajom. Právo na prístup teda možno chápať ako možnosť dotknutej osoby, ako zistiť od

¹ Odkazy na „členské štáty“ v tomto dokumente by sa mali chápať ako odkazy na „členské štáty EHP“.

² Články 15 až 22 všeobecného nariadenia o ochrane údajov.

³ Podľa článku 8 ods. 1 Charty základných práv Európskej únie má každý právo na ochranu osobných údajov, ktoré sa ho týkajú. Podľa článku 8 ods. 2 druhej vety má každý právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu.

prevádzkovateľa, či sa spracúvajú jej osobné údaje, a zároveň ako možnosť získať prístup k týmto údajom a overiť ich. Prevádzkovateľ poskytne dotknutej osobe na základe jej žiadosti informácie patriace do rozsahu článku 15 ods. 1 a 2 všeobecného nariadenia o ochrane údajov.

4. Uplatňovanie práva na prístup sa realizuje tak v rámci práva v oblasti ochrany údajov v súlade s cieľmi práva v oblasti ochrany údajov, ako aj konkrétnejšie v rámci „základných práv a slobôd fyzických osôb, najmä ich práva na ochranu osobných údajov“, ako sa stanovuje v článku 1 ods. 2 všeobecného nariadenia o ochrane údajov. Právo na prístup je dôležitým prvkom celého systému ochrany údajov.
5. Praktickým účelom práva na prístup je umožniť, aby mali fyzické osoby kontrolu nad vlastnými osobnými údajmi⁴. Aby sa tento cieľ mohol účinne realizovať aj v praxi, cieľom všeobecného nariadenia o ochrane údajov je uľahčiť jeho uplatňovanie viacerými zárukami, ktorými sa dotknutej osobe umožní uplatňovať toto právo jednoducho, bez zbytočných obmedzení, v primeraných intervaloch a bez prílišného zdržiavania alebo výdavkov. Toto všetko by malo viesť k účinnejšiemu presadzovaniu práva na prístup zo strany dotknutej osoby v digitálnom veku, ktorého súčasťou je v širšom zmysle aj právo dotknutej osoby na podanie sťažnosti dozornému orgánu a právo na účinnú súdnu ochranu⁵.
6. Pokiaľ ide o rozvoj práva na prístup ako súčasť právneho rámca v oblasti ochrany údajov, malo by sa zdôrazniť, že ide o prvok, ktorý je súčasťou európskeho systému ochrany údajov už od jeho začiatku. V porovnaní so smernicou 95/46/ES sa štandard pre práva dotknutej osoby stanovený vo všeobecnom nariadení o ochrane údajov upresnil a posilnil, čo platí aj v prípade práva na prístup. Keďže v súčasnosti sú spôsoby súvisiace s právom na prístup vo všeobecnom nariadení o ochrane údajov presnejšie určené, toto právo je zároveň pre dotknutú osobu a prevádzkovateľa informatívnejšie z hľadiska právnej istoty. Okrem toho konkrétne znenie článku 15 a presná lehota na poskytnutie údajov podľa článku 12 ods. 3 všeobecného nariadenia o ochrane údajov zaväzujú prevádzkovateľa, aby bol pripravený na požiadavky dotknutej osoby, a to tak, že vypracuje postupy pre vybavovanie žiadostí.
7. Právo na prístup by sa nemalo vnímať izolovane, keďže je úzko prepojené s inými ustanoveniami všeobecného nariadenia o ochrane údajov, najmä so zásadami ochrany údajov vrátane spravodlivosti a zákonnosti spracúvania, povinnosti prevádzkovateľa týkajúcej sa transparentnosti, a s inými právami dotknutej osoby stanovenými v kapitole III všeobecného nariadenia o ochrane údajov.
8. V rámci práv dotknutej osoby je takisto dôležité zdôrazniť význam článku 12 všeobecného nariadenia o ochrane údajov, ktorým sa stanovujú požiadavky na primerané opatrenia prijaté prevádzkovateľom pri poskytovaní informácií uvedených v článkoch 13 a 14 všeobecného nariadenia o ochrane údajov, ako aj oznámení uvedených v článkoch 15 až 22 a článku 34 všeobecného nariadenia o ochrane údajov. Týmito požiadavkami sa vo všeobecnosti špecifikuje forma, spôsob a lehota, pokiaľ ide o odpovede dotknutej osobe, a najmä pre akékoľvek informácie adresované dieťaťu.
9. EDPB považuje za potrebné poskytnúť presnejšie usmernenia o tom, ako uplatňovať právo na prístup v rôznych situáciách. Cieľom týchto usmernení je analýza rôznych aspektov práva na prístup. Preto je cieľom nasledujúceho oddielu poskytnúť všeobecný prehľad a vysvetlenie obsahu samotného článku 15, zatiaľ čo ďalšie oddiely poskytujú hlbšiu analýzu najčastejších praktických otázok a problémov týkajúcich sa uplatňovania práva na prístup.

⁴ Pozri odôvodnenia 7, 68, 75 a 85 všeobecného nariadenia o ochrane údajov.

⁵ Pozri kapitolu VIII, články 77, 78 a 79 všeobecného nariadenia o ochrane údajov.

2 CIEĽ PRÁVA NA PRÍSTUP, ŠTRUKTÚRA ČLÁNKU 15 VŠEOBECNÉHO NARIADENIA O OCHRANE ÚDAJOV A VŠEOBECNÉ ZÁSADY

2.1 Cieľ práva na prístup

10. Právo na prístup je teda navrhnuté tak, aby fyzické osoby mohli vykonávať kontrolu nad osobnými údajmi, ktoré sa ich týkajú, a umožnilo im, aby si „[boli vedomé] zákonnosti spracúvania a [mohli] si ju overiť“⁶. Konkrétnejšie je účelom práva na prístup umožniť dotknutým osobám pochopiť, ako sa ich osobné údaje spracúvajú, a aké sú následky takého spracúvania, ako aj overiť správnosť spracúvaných údajov bez toho, aby museli odôvodňovať svoj zámer. Inými slovami účelom práva na prístup je poskytnúť jednotlivcom dostatočné, transparentné a jednoducho dostupné informácie o spracúvaní údajov bez ohľadu na použité technológie a umožniť im overiť rôzne aspekty konkrétnej spracovateľskej činnosti podľa všeobecného nariadenia o ochrane údajov (napr. zákonnosť, správnosť).
11. Výklad všeobecného nariadenia o ochrane údajov poskytnutý v týchto usmerneniach vychádza z doteraz vydaných judikatúr Súdneho dvora Európskej Únie. Vzhľadom na význam práva na prístup možno očakávať, že v súvisiacej judikatúre nastane v budúcnosti významný vývoj.
12. Účelom práva na prístup v súlade s rozhodnutiami Súdneho dvora Európskej únie⁷ je zaručiť ochranu práva dotknutých osôb na súkromie a ochranu údajov, pokiaľ ide o spracúvanie údajov, ktoré sa ich týkajú⁸, a zároveň sa ním môže uľahčiť uplatňovanie ich práv vyplývajúcich napríklad z článkov 16 až 19, článkov 21 až 22 a článku 82 všeobecného nariadenia o ochrane údajov. Uplatňovanie práva na prístup je však právom jednotlivca a nie je podmienené uplatňovaním iných uvedených práv, pričom uplatňovanie iných práv nezávisí od uplatňovania práva na prístup.
13. Vzhľadom na všeobecný cieľ práva na prístup, nie je tento cieľ vhodný na to, aby ho prevádzkovateľ analyzoval ako podmienku pre uplatňovanie práva na prístup v rámci posudzovania žiadostí o prístup. Prevádzkovatelia by preto nemali posudzovať otázku, „prečo“ dotknutá osoba žiada o prístup, ale len otázku, „čo“ dotknutá osoba žiada (pozri oddiel 3 o analýze žiadosti), a to, či majú u seba osobné údaje týkajúce sa danej osoby (pozri oddiel 4). Preto by napríklad prevádzkovateľ nemal zamietnuť prístup na základe dôvodu alebo podozrenia, že požadované údaje by dotknutá osoba mohla použiť na svoju obhajobu pred súdom v prípade výpovede alebo obchodného sporu s prevádzkovateľom⁹. V súvislosti s limitmi a obmedzeniami práva na prístup pozri oddiel 6.

Príklad 1: Zamestnávateľ prepustil zamestnanca. O týždeň neskôr sa prepustená osoba rozhodne, že získa dôkazy na podanie žaloby proti svojmu bývalému zamestnávateľovi vo veci nespravodlivého prepustenia. S týmto úmyslom sa zamestnanec ako dotknutá osoba obráti na bývalého zamestnávateľa a požiada ho o prístup ku všetkým osobným údajom, ktoré sa ho týkajú. Túto žiadosť bývalý zamestnávateľ ako prevádzkovateľ spracuje.

Prevádzkovateľ nesmie posudzovať zámer dotknutej osoby a dotknutá osoba nemusí prevádzkovateľovi uvádzať dôvod svojej žiadosti. Z tohto dôvodu, ak žiadosť spĺňa všetky ostatné

⁶ Odôvodnenie 63 všeobecného nariadenia o ochrane údajov.

⁷ Rozsudky Súdneho dvora, Nowak, C-434/16, a YS a i., spojené veci C-141/12 a C-372/12.

⁸ Rozsudok Súdneho dvora, Nowak, C-434/16, bod 56.

⁹ Otázky súvisiace s touto témou sú predmetom veci, v ktorej v súčasnosti rozhoduje Súdny dvor Európskej únie (C-307/22).

požiadavky (pozri oddiel 3), prevádzkovateľ musí žiadosti vyhovieť, pokiaľ sa nepreukáže, že žiadosť je zjavne neopodstatnená alebo neprimeraná v súlade s článkom 12 ods. 5 všeobecného nariadenia o ochrane údajov (pozri oddiel 6.3), čo prevádzkovateľ musí preukázať.

Obmena: Dotknutá osoba počas súdneho konania uplatní právo na prístup k osobným údajom, ktoré sa jej týkajú. Vnútroštátne právne predpisy členského štátu, ktoré upravujú pracovnoprávny vzťah medzi prevádzkovateľom a dotknutou osobou, však zahŕňajú určité ustanovenia, ktorými sa obmedzuje rozsah informácií, ktoré možno poskytnúť alebo vymeniť medzi stranami prebiehajúceho alebo nadchádzajúceho súdneho konania, a ktoré sú uplatniteľné na žalobu vo veci nespravodlivého prepustenia podanú dotknutou osobou. V tomto kontexte a za predpokladu, že tieto vnútroštátne ustanovenia sú v súlade s požiadavkami stanovenými v článku 23 všeobecného nariadenia o ochrane údajov¹⁰, nie je dotknutá osoba oprávnená získať od prevádzkovateľa viac informácií, ako sa stanovuje vo vnútroštátnych právnych predpisoch členského štátu, ktorými sa upravuje výmena informácií medzi stranami súdnych sporov.

14. Hoci je cieľ práva na prístup všeobecný, Súdny dvor Európskej únie názorne predviedol aj obmedzenia rozsahu práva v oblasti ochrany údajov a práva na prístup. Súdny dvor Európskej únie napríklad zistil, že účel práva na prístup k údajom zaručený právom EÚ v oblasti ochrany údajov treba odlišovať od účelu práva na prístup k verejným listinám, ktorý sa stanovuje v právnych predpisoch EÚ a vnútroštátnych právnych predpisoch, ktorých cieľom je „zaručiť transparentnosť rozhodovacieho postupu verejných orgánov a podporovať dobrú administratívnu prax“¹¹, pričom toto nie je cieľom práva v oblasti ochrany údajov. Súdny dvor Európskej únie dospel k záveru, že právo na prístup k osobným údajom sa uplatňuje bez ohľadu na to, či sa uplatňuje iný druh práva na prístup s iným účelom, ako je to v kontexte postupu preskúmania.

2.2 Štruktúra článku 15 všeobecného nariadenia o ochrane údajov

15. S cieľom odpovedať na žiadosť o prístup a zabezpečiť, aby sa žiaden z jej aspektov nezanedbal, je potrebné porozumieť štruktúre článku 15 a hlavným zložkám práva na prístup stanoveným v tomto článku.
16. Článok 15 možno rozdeliť na osem rôznych prvkov, ako sa uvádza v tejto tabuľke:

1.	Potvrdenie toho, či prevádzkovateľ spracúva alebo nespracúva osobné údaje týkajúce sa žiadateľa	Článok 15 ods. 1 prvá polovica vety
2.	Prístup k osobným údajom týkajúcich sa žiadateľa	Článok 15 ods. 1 druhá polovica vety (prvá časť)
3.	Prístup k nasledujúcim informáciám o spracúvaní: a) účely spracúvania; b) kategórie osobných údajov; c) príjemcovia alebo kategórie príjemcov; d) predpokladané trvanie spracúvania alebo kritériá na určenie trvania;	Článok 15 ods. 1 druhá polovica vety (druhá časť)

¹⁰ Usmernenia EDPB 10/2020 k obmedzeniam podľa článku 23 všeobecného nariadenia o ochrane údajov, verzia na účely verejnej konzultácie, 18. decembra 2020.

¹¹ Rozsudok Súdného dvora, YS a i., spojené veci C-141/16 a C-372/12, bod 47.

	e) existencia práva na opravu osobných údajov, ich vymazanie, obmedzenie spracúvania a práva namietať proti spracúvaniu; f) právo podať sťažnosť dozornému orgánu; g) akékoľvek dostupné informácie o zdroji údajov, ak sa nezískali od dotknutej osoby; h) existencia automatizovaného rozhodovania vrátane profilovania a iných súvisiacich informácií.	
4.	Informácie o zárukách podľa článku 46, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii	Článok 15 ods. 2
5.	Povinnosť prevádzkovateľa poskytnúť kópiu osobných údajov, ktoré sa spracúvajú	Článok 15 ods. 3 prvá veta
6.	Požadovanie primeraného poplatku prevádzkovateľom zodpovedajúcemu administratívnym nákladom na akékoľvek ďalšie kópie vyžiadané dotknutou osobou	Článok 15 ods. 3 druhá veta
7.	Poskytovanie informácií v elektronickej podobe	Článok 15 ods. 3 tretia veta
8.	Zohľadnenie práv a slobôd iných	Článok 15 ods. 4

Zatiaľ čo sa prvkami článku 15 ods. 1 a 2 spoločne vymedzuje obsah práva na prístup, článok 15 ods. 3 sa okrem všeobecných požiadaviek stanovených v článku 12 všeobecného nariadenia o ochrane údajov zaoberá spôsobmi pri poskytovaní prístupu. V článku 15 ods. 4 sa dopĺňajú limity a obmedzenia, ktoré sa stanovujú v článku 12 ods. 5 všeobecného nariadenia o ochrane údajov pre všetky práva dotknutých osôb, s osobitným zameraním na práva a slobody iných v kontexte prístupu.

2.2.1 Vymedzenie obsahu práva na prístup

17. Článok 15 ods. 1 a 2 obsahuje tieto tri aspekty: prvým je potvrdenie, či sa osobné údaje žiadateľa spracúvajú, a ak áno, druhým aspektom je prístup k týmto údajom, a tretím sú informácie o danom spracúvaní. Tieto aspekty možno považovať za tri rôzne zložky, ktoré spoločne vytvárajú právo na prístup.

2.2.1.1 Potvrdenie toho, či sa osobné údaje spracúvajú alebo nespracúvajú

18. Pri podávaní žiadosti o prístup k osobným údajom musia dotknuté osoby v prvom rade vedieť, či prevádzkovateľ spracúva alebo nespracúva údaje, ktoré sa ich týkajú. Táto informácia preto predstavuje prvú zložku práva na prístup podľa článku 15 ods. 1. Ak prevádzkovateľ nespracúva osobné údaje týkajúce sa dotknutej osoby žiadajúcej o prístup, informácie, ktoré sa poskytnú, sa obmedzujú na potvrdenie toho, že sa nespracúvajú žiadne osobné údaje týkajúce sa dotknutej osoby. Ak prevádzkovateľ spracúva údaje týkajúce sa žiadateľa, prevádzkovateľ musí túto skutočnosť potvrdiť danej osobe. Toto potvrdenie môže byť oznámené samostatne alebo môže byť súčasťou informácií o spracúvaní osobných údajov (pozri ďalej).

2.2.1.2 Prístup k spracúvaným osobným údajom

19. Prístup k osobným údajom je druhou zložkou práva na prístup podľa článku 15 ods. 1 a predstavuje jadro tohto práva. Súvisí s pojmom osobné údaje, ako sa vymedzuje v článku 4 bode 1 všeobecného nariadenia o ochrane údajov. Okrem základných osobných údajov, ako je meno a adresa, môže do rozsahu tohto vymedzenia patriť neobmedzený okruh údajov, a to za predpokladu, že patria do vecnej pôsobnosti všeobecného nariadenia o ochrane údajov, najmä pokiaľ ide o spôsob, akým sú spracúvané

(článok 2 všeobecného nariadenia o ochrane údajov). Prístup k osobným údajom teda znamená prístup k skutočným osobným údajom ako takým, nie len všeobecný opis údajov, či len jednoduchý odkaz na kategórie osobných údajov spracúvaných prevádzkovateľom. Ak sa neuplatňujú žiadne limity či obmedzenia¹², dotknuté osoby sú oprávnené mať prístup ku všetkým spracúvaným údajom, ktoré sa ich týkajú, alebo k ich častiam, a to v závislosti od rozsahu žiadosti (pozri oddiel 2.3.1). Povinnosť poskytnúť prístup k údajom nezávisí od druhu ani zdroja daných údajov. Uplatňuje sa v plnom rozsahu aj v prípadoch, keď žiadateľ pôvodne poskytol prevádzkovateľovi údaje, lebo jeho účelom je dotknutú osobu informovať o skutočnom spracúvaní daných údajov prevádzkovateľom. Rozsah osobných údajov podľa článku 15 sa podrobne vysvetľuje v oddieloch 4.1 a 4.2.

2.2.1.3 Informácie o spracúvaní údajov a o právach dotknutých osôb

20. Treťou zložkou práva na prístup sú informácie o spracúvaní údajov a o právach dotknutých osôb, ktoré musí prevádzkovateľ poskytnúť podľa článku 15 ods. 1 písm. a) až h) a článku 15 ods. 2. Tieto informácie by mohli vychádzať napríklad z oznámenia prevádzkovateľa o ochrane súkromia¹³ alebo zo záznamu prevádzkovateľa o spracovateľských činnostiach, ako sa uvádza v článku 30 všeobecného nariadenia o ochrane údajov, pričom však môže byť potrebná ich aktualizácia alebo prispôsobenie žiadosti dotknutej osoby. Obsahu a stupňu špecifikácie informácií sa ďalej venuje oddiel 4.3.

2.2.2 Ustanovenia o spôsoboch

21. Článkom 15 ods. 3 sa dopĺňajú požiadavky pre spôsoby odpovedania na žiadosti o prístup stanovené v článku 12 všeobecného nariadenia o ochrane údajov prostredníctvom špecifikácií v kontexte žiadostí o prístup.

2.2.2.1 Poskytnutie kópie

22. Podľa článku 15 ods. 3 prvej vety všeobecného nariadenia o ochrane údajov prevádzkovateľ poskytne bezplatnú kópiu osobných údajov, ktorých sa spracúvanie týka. Kópia teda odkazuje len na druhú zložku práva na prístup („prístup k spracúvaným osobným údajom“, pozri v predchádzajúcom texte). Prevádzkovateľ musí zabezpečiť, aby bola prvá kópia bezplatná, aj keď považuje náklady na rozmnožovanie za vysoké (napríklad: náklady na poskytnutie kópie nahrávky telefonického rozhovoru).
23. Povinnosť poskytnúť kópiu sa nemá považovať za dodatočné právo dotknutej osoby, ale ako spôsob poskytovania prístupu k údajom. Posilňuje sa tým právo na prístup k údajom¹⁴ a prispieva to k jeho správneému výkladu, keďže sa tým objasňuje, že prístup k údajom podľa článku 15 ods. 1 zahŕňa úplné informácie o všetkých údajoch a nemôže sa chápať len ako poskytnutie zhrnutia údajov. Zároveň však povinnosť poskytnúť kópiu nie je navrhnutá tak, aby sa ňou rozšíril rozsah práva na prístup: týka sa (len) kópie osobných údajov, ktoré sa spracúvajú, a nie nevyhnutne rozmnožovania originálnych dokumentov (pozri oddiel 5, bod 152). Vo všeobecnosti sa pri poskytovaní kópie dotknutej osobe nepodávajú dodatočné informácie: rozsah informácií, ktoré majú byť zahrnuté v kópii, je rozsah prístupu k údajom podľa článku 15 ods. 1 (druhá zložka práva na prístup, ako sa uvádza v texte, pozri

¹² Pozri oddiel 6 týchto usmernení.

¹³ Súvisiace informácie pozri v Usmerneniach pracovnej skupiny zriadenej podľa článku 29 k transparentnosti podľa nariadenia 2016/679, WP 260 rev.01, z 11. apríla 2018, schválené EDPB (ďalej len „usmernenia WP29 k transparentnosti – schválené EDPB“).

¹⁴ Povinnosť poskytnúť kópiu sa v smernici o ochrane údajov 95/46/ES neuvádzala.

bod 19), do ktorého patria všetky informácie potrebné na to, aby dotknutá osoba mohla porozumieť zákonnosti spracúvania a overiť ju¹⁵.

24. Vzhľadom na uvedené skutočnosti, ak sa prístup k údajom v zmysle článku 15 ods. 1 udelí poskytnutím kópie, je povinnosť poskytnúť kópiu uvedená v článku 15 ods. 3 splnená. Povinnosť poskytnúť kópiu slúži cieľom práva na prístup, ktorými je umožniť dotknutej osobe poznať zákonnosť spracúvania a overiť ju (odôvodnenie 63). Na splnenie týchto cieľov bude dotknutá osoba vo väčšine prípadov musieť vidieť informácie nie len dočasne. Z tohto dôvodu dotknutá osoba musí získať prístup k informáciám tým, že jej bude poskytnutá kópia osobných údajov.
25. Vzhľadom na uvedené skutočnosti sa pojem kópia musí vykladať v širšom zmysle, pričom zahŕňa rôzne druhy prístupu k osobným údajom, pokiaľ je úplná (t. j. obsahuje všetky požadované osobné údaje) a dotknutá osoba si ju môže ponechať. Požiadavka poskytnúť kópiu teda znamená, že informácie o osobných údajoch týkajúcich sa osoby, ktorá podáva žiadosť, sa dotknutej osobe poskytujú spôsobom umožňujúcim, aby si dotknutá osoba mohla všetky informácie ponechať a vrátiť sa k nim.
26. Aj napriek širšiemu chápaniu pojmu kópia a vzhľadom na to, že poskytnutie kópie predstavuje hlavný spôsob, ktorým sa prístup má poskytovať, za istých okolností by mohli byť vhodné aj iné spôsoby. Ďalšie vysvetlenia týkajúce sa kópií a iných spôsobov poskytovania prístupu sa uvádzajú v oddiele 5, najmä v oddieloch 5.2.2 až 5.2.5.

2.2.2.2 Poskytovanie ďalších kópií

27. Článok 15 ods. 3 druhá veta sa týka situácií, v ktorých dotknutá osoba žiada prevádzkovateľa o viac ako jednu kópiu, napríklad v prípade, že prvá kópia sa stratila alebo poškodila, alebo dotknutá osoba chce kópiu postúpiť inej osobe alebo dozornému orgánu. Keďže prevádzkovateľ musí dotknutej osobe na základe jej žiadosti poskytnúť ďalšie kópie, v článku 15 ods. 3 sa stanovuje, že prevádzkovateľ môže za každú ďalšiu požadovanú kópiu účtovať primeraný poplatok zodpovedajúci administratívnym nákladom (článok 15 ods. 3 druhá veta).
28. Ak dotknutá osoba požiada o dodatočnú kópiu po podaní prvej žiadosti, môžu vzniknúť otázky o tom, či by sa táto žiadosť mala považovať za novú, alebo či dotknutá osoba chce dodatočnú kópiu údajov v zmysle článku 15 ods. 3 druhej vety, pričom jej v takom prípade môže byť účtovaný poplatok za dodatočnú kópiu. Odpoveď na tieto otázky závisí len od obsahu žiadosti: žiadosť by sa mala vykladať ako požiadanie o dodatočnú kópiu, pokiaľ sa z hľadiska času a rozsahu týka rovnakého spracúvania osobných údajov ako predchádzajúca žiadosť. Ak je však cieľom dotknutej osoby získať informácie o spracúvaných údajoch v inom čase alebo súvisiacich s iným súborom údajov, ako sú pôvodne vyžiadané údaje, znova sa uplatňuje právo na získanie bezplatnej kópie podľa článku 15 ods. 3. Toto platí aj v prípadoch, keď dotknutá osoba podala prvú žiadosť krátko pred podaním ďalšej žiadosti. Dotknutá osoba si môže uplatniť právo na prístup prostredníctvom následnej žiadosti a získať bezplatnú kópiu, pokiaľ sa žiadosť podľa článku 12 ods. 5 nepovažuje za neprimeranú s možnosťou účtovania primeraného poplatku v súlade s článkom 12 ods. 5 písm. a) (viac o neprimeranej povahe opakujúcich sa žiadostí pozri oddiel 6).

Príklad 2: Zákazník požiada o prístup obchodnú spoločnosť. Jeden rok po odpovedi na žiadosť požiada ten istý zákazník tú istú spoločnosť o prístup podľa článku 15. Bez ohľadu na to, či od predchádzajúcej žiadosti prebehli nové obchodné transakcie alebo či medzi stranami vznikli nové kontakty, sa táto druhá žiadosť bude považovať za novú žiadosť. Aj v prípade, že nenastali žiadne zmeny v spracúvaní

¹⁵ Otázky súvisiace s témou tohto odseku sú predmetom veci, v ktorej v súčasnosti rozhoduje Súdny dvor Európskej únie (C-487/21).

údajov spoločnosťou, čo pre dotknutú osobu nemusí byť zrejmé, má dotknutá osoba právo na bezplatnú kópiu údajov.

Obmena 1: Ak aj zákazník vo vyššie uvedených prípadoch predloží novú žiadosť, napríklad len jeden týždeň po predložení prvej žiadosti, možno ju podľa článku 15 ods. 1 a článku 15 ods. 3 prvej vety považovať za novú žiadosť, pokiaľ sa to nebude vykladať len ako pripomienka prvej žiadosti. Vzhľadom na krátky interval a v závislosti od konkrétnych okolností novej žiadosti, podľa článku 12 ods. 5 je otázna jej neprimeranosť (pozri oddiel 6).

Obmena 2: Žiadosť o „novú kópiu“ informácií, ktoré už boli poskytnuté formou kópie ako odpovede na predchádzajúcu žiadosť, napríklad v prípade, že zákazník stratil predchádzajúcu kópiu, by sa mala, samozrejme, považovať za žiadosť o dodatočnú kópiu, keďže z hľadiska rozsahu a času spracúvania odkazuje na predchádzajúcu žiadosť.

29. Ak dotknutá osoba zopakuje prvú žiadosť o prístup na základe toho, že doručená odpoveď nebola úplná alebo že neboli uvedené dôvody jej zamietnutia, táto žiadosť sa nebude považovať za novú žiadosť, keďže je len pripomienkou prvej žiadosti, ktorej prevádzkovateľ nevyhovel.
30. Pokiaľ ide o náhradu nákladov v prípade žiadostí o dodatočnú kópiu, v článku 15 ods. 3 sa stanovuje, že prevádzkovateľ môže účtovať primeraný poplatok zodpovedajúci administratívnym nákladom, ktoré žiadosťou vznikli. To znamená, že administratívne náklady sú relevantným kritériom na určenie výšky poplatku. Zároveň by mal poplatok byť primeraný a mal by zohľadňovať význam práva na prístup ako základného práva dotknutej osoby. Prevádzkovateľ by nemal dotknutej osobe účtovať režijné náklady ani iné všeobecné výdavky, ale mal by sa zameriavať na osobitné náklady spojené s poskytnutím dodatočnej kópie. Prevádzkovateľ by mal do organizácie tohto procesu efektívne zapojiť svoje ľudské a materiálne zdroje, aby boli náklady na poskytnutie kópie nízke, a to aj v prípade, že prevádzkovateľ do procesu zapojí externú podporu.
31. V prípade, že sa prevádzkovateľ rozhodne účtovať poplatok, mal by vopred uviesť, že sa bude účtovať poplatok, a čo najpresnejšie aj výšku nákladov, ktorú plánuje dotknutej osobe účtovať, aby dotknutej osobe dal možnosť rozhodnúť, či žiadosť ponechá alebo ju stiahne.

2.2.2.3 Sprístupňovanie informácií v bežne dostupnej elektronickej podobe

32. Ak je žiadosť podaná elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob (pozri článok 12 ods. 3 všeobecného nariadenia o ochrane údajov). V článku 15 ods. 3 tretej vete sa dopĺňa táto požiadavka v kontexte žiadostí o prístup tým, že prevádzkovateľ je okrem toho povinný poskytnúť odpoveď v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob. V článku 15 ods. 3 sa predpokladá, že pre prevádzkovateľov, ktorí sú schopní prijímať elektronické žiadosti, bude možné poskytovať odpoveď na žiadosť v bežne používanej elektronickej podobe (podrobné informácie sa nachádzajú v oddiele 5.2.5). Toto ustanovenie sa týka všetkých informácií, ktoré je potrebné poskytnúť v súlade s článkom 15 ods. 1 a 2. Ak preto dotknutá osoba predloží žiadosť o prístup elektronicky, všetky informácie musia byť poskytnuté v bežne používanej elektronickej podobe. Otázky týkajúce sa formátu sa podrobnejšie rozoberajú v oddiele 5. Prevádzkovateľ by mal ako vždy zaviesť vhodné bezpečnostné opatrenia, najmä keď pracuje s osobitnou kategóriou osobných údajov (pozri ďalej v oddiele 2.3.4).

2.2.3 Možné obmedzenie práva na prístup

33. A napokon sa v kontexte práva na prístup v článku 15 ods. 4 stanovuje osobitné obmedzenie. V tomto ustanovení sa uvádza, že je potrebné zvážiť možné nepriaznivé dôsledky na práva a slobody iných.

Otázky týkajúce sa rozsahu a následkov tohto obmedzenia, ako aj dodatočné limity a obmedzenia stanovené v článku 12 ods. 5 všeobecného nariadenia o ochrane údajov alebo v článku 23 všeobecného nariadenia o ochrane údajov sú vysvetlené v oddiele 6.

2.3 Všeobecné zásady práva na prístup

34. Ak dotknuté osoby požiadajú o prístup k svojim údajom, v zásade sa informácie uvedené v článku 15 všeobecného nariadenia o ochrane údajov musia vždy poskytnúť v plnom rozsahu. Z toho vyplýva, že ak prevádzkovateľ spracúva údaje týkajúce sa dotknutej osoby, poskytne jej všetky informácie uvedené v článku 15 ods. 1 a prípadne informácie uvedené v článku 15 ods. 2. Prevádzkovateľ musí prijať primerané opatrenia, aby zaistil, že informácie sú úplné, správne a aktuálne a čo najviac zodpovedajú stavu spracúvania údajov v čase doručenia žiadosti¹⁶. Ak údaje spoločne spracúvajú dvaja alebo viacerí prevádzkovatelia, dohoda medzi spoločnými prevádzkovateľmi o ich príslušných záväzkoch v súvislosti s uplatňovaním práv dotknutej osoby, najmä pokiaľ ide o odpoveď na žiadosť o prístup, nemá vplyv na práva dotknutých osôb voči prevádzkovateľovi, ktorému adresovali svoju žiadosť¹⁷.

2.3.1 Úplnosť informácií

35. Dotknuté osoby majú právo, s výnimkami uvedenými ďalej, získať úplný prístup ku všetkým údajom, ktoré sa ich týkajú (podrobnosti o rozsahu sa nachádzajú v oddiele 4.2). Pokiaľ dotknutá osoba výslovne nežiada inak, žiadosť na uplatňovanie práva na prístup sa chápe všeobecne a vzťahuje sa na všetky osobné údaje týkajúce sa dotknutej osoby¹⁸. Obmedzenie prístupu k časti informácií možno zvážiť v týchto prípadoch:
- a) Dotknutá osoba výslovne zúžila žiadosť na podsúbor údajov. Prevádzkovateľ s cieľom zabrániť poskytnutiu neúplných informácií môže takéto obmedzenie žiadosti dotknutej osoby zvážiť, len ak si je istý, že tento výklad sa zhoduje so želaním dotknutej osoby (ďalšie podrobnosti sa nachádzajú v oddiele 3.1.1 bode 51). Dotknutá osoba v zásade nemusí opakovať svoju žiadosť na poskytnutie všetkých údajov, ktoré má dotknutá osoba právo získať.
- b) V situáciách, keď prevádzkovateľ spracúva veľké množstvo údajov týkajúcich sa dotknutej osoby, prevádzkovateľ môže mať pochybnosti, či je cieľom žiadosti o prístup, ktorá je vyjadrená veľmi všeobecne, skutočne získanie informácií všetkého druhu, ktoré sa spracúvajú, alebo získanie podrobných informácií o všetkých druhoch činností prevádzkovateľa. Takéto pochybnosti môžu vzniknúť najmä v situáciách, keď už od začiatku neexistovala možnosť poskytnúť dotknutej osobe nástroje na špecifikáciu jej žiadosti alebo keď dotknutá osoba tieto nástroje nevyužila. Prevádzkovateľ potom čelí problémom, ako poskytnúť odpoveď v plnom rozsahu a zároveň sa vyhnúť vytvoreniu nadbytku informácií pre dotknutú osobu, o ktoré dotknutá osoba nemá záujem a ani ich nemôže efektívne zvládnuť. Na riešenie tohto problému môžu v závislosti od okolností a technických možností existovať odpovede, ako napríklad poskytnutie samoobslužných nástrojov [a self-service tool] v online kontextoch (pozri oddiel 5 o viacúrovňovom prístupe). Ak takéto riešenia nie sú uplatniteľné, prevádzkovateľ, ktorý v súvislosti s dotknutou osobou spracúva veľké množstvo informácií, môže od dotknutej osoby požadovať, aby spresnila, ktorých informácií alebo spracovateľských činností sa žiadosť týka, a to skôr než sú jej také informácie doručené (pozri odôvodnenie 63 všeobecného nariadenia o ochrane údajov). Príkladom môže byť spoločnosť s viacerými oblasťami činností alebo

¹⁶ Usmernenie týkajúce sa primeraných opatrení sa nachádza v oddiele 5 bodoch 123 – 129.

¹⁷ Usmernenia EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov, bod 162f. Sprostredkovatelia musia pomáhať prevádzkovateľovi, tamže, bod 129.

¹⁸ Podrobnosti sa nachádzajú v oddiele 5.2.3 o otázke viacúrovňového prístupu.

orgán verejnej moci s rôznymi administratívnymi útvarmi, ak prevádzkovateľ zistil, že sa rôznymi odvetviami spracúvajú početné údaje súvisiace s dotknutou osobou. Okrem toho veľké množstvo údajov môžu spracúvať prevádzkovatelia, ktorí zbierajú údaje týkajúce sa častých činností dotknutej osoby počas dlhšieho obdobia.

Príklad 3: Orgán verejnej moci spracúva údaje o dotknutej osobe vo viacerých rôznych útvaroch týkajúcich sa rôznych kontextov. Správa a vedenie záznamov sa čiastočne spracúva neautomatizovanými prostriedkami a väčšina údajov sa uchováva len v papierových spisoch. Pokiaľ ide o všeobecné znenie žiadosti, orgán verejnej moci má pochybnosti, či si je dotknutá osoba vedomá rozsahu žiadosti, najmä rôznorodosti spracovateľských operácií, ktoré by zahŕňala, množstva informácií a počtu strán, ktoré by dotknutá osoba mala získať.

Príklad 4: Veľká poisťovacia spoločnosť dostane listom všeobecnú žiadosť o prístup od osoby, ktorá bola roky jej zákazníkom. Hoci sa v plnej miere dodržiavajú lehoty na vymazanie údajov, spoločnosť v skutočnosti spracúva obrovské množstvo údajov týkajúcich sa zákazníka, keďže spracúvanie údajov je aj naďalej potrebné na plnenie zmluvných záväzkov vyplývajúcich zo zmluvného vzťahu so zákazníkom (napríklad vrátane pretrvávajúcich záväzkov, komunikácie o kontroverzných otázkach so zákazníkom a s tretím stranami...) alebo na plnenie právnych záväzkov (archivované údaje, ktoré sa musia uchovávať na daňové účely atď.). Poisťovacia spoločnosť môže mať pochybnosti, či je účelom žiadosti, ktorá mala veľmi všeobecné znenie, naozaj získať všetky druhy daných údajov. Toto môže byť problematické najmä, ak má poisťovacia spoločnosť len poštovú adresu dotknutej osoby, a preto musí všetky informácie posielat v papierovej podobe. Rovnaké pochybnosti však môžu byť relevantné aj pri poskytovaní informácií inými prostriedkami.

Ak sa v takých prípadoch prevádzkovateľ rozhodne požiadať dotknutú osobu o spresnenie žiadosti, aby mohol dodržať svoj záväzok uľahčiť uplatňovanie práva na prístup (článok 12 ods. 2 všeobecného nariadenia o ochrane údajov), prevádzkovateľ zároveň poskytne zmysluplné informácie o svojich spracovateľských operáciách, ktoré by sa mohli týkať dotknutej osoby, a to tak, že ju informuje o príslušných odvetviach svojich činností, databázach atď.

Príklad 5: V pracovnoprávnom vzťahu, sa môže vyskytnúť prípad, že je žiadosť o prístup formulovaná všeobecne, nie je *samo osebe* zjavné, že zamestnanec chce získať všetky prihlasovacie údaje používateľa, údaje o prístupe na pracovisko, údaje o úhradách v jedálni, údaje o platbách mzdy atď. Žiadosť o spresnenie zo strany zamestnávateľa by napríklad mohla viesť k objasneniu toho, či má zamestnanec záujem pochopiť a overiť si, komu boli poskytnuté posúdenia jeho výkonu. Bez žiadosti o spresnenie by zamestnanec získal veľké množstvo informácií bez toho, aby mal o väčšinu z nich záujem. Zamestnávateľ by zároveň musel poskytnúť informácie o rôznych kontextoch spracúvania, ktoré by sa mohli zamestnanca týkať, aby tak zamestnancovi umožnil rozumne spresniť žiadosť.

Je dôležité zdôrazniť, že cieľom žiadosti o spresnenie nie je obmedziť odpoveď na žiadosť o prístup a nemôže sa použiť na skrytie akýchkoľvek informácií o údajoch alebo o spracúvaní týkajúcich sa dotknutej osoby. Ak dotknutá osoba, ktorá bola požiadaná o spresnenie rozsahu svojej žiadosti, potvrdí, že má záujem o všetky osobné údaje, ktoré sa jej týkajú, prevádzkovateľ jej ich, samozrejme, musí v plnom rozsahu poskytnúť.

Prevádzkovateľ by mal byť v každom prípade vždy schopný preukázať, že spôsob spracovania žiadosti je zameraný na čo najširšie uplatnenie práva na prístup a že je v súlade so záväzkom uľahčiť uplatňovanie práv dotknutých osôb (článok 12 ods. 2 všeobecného nariadenia o ochrane údajov). Podľa týchto zásad prevádzkovateľ môže počkať na odpoveď dotknutej osoby, než jej poskytne dodatočné údaje podľa jej želania, ak prevádzkovateľ poskytne dotknutej osobe jasný prehľad

o všetkých spracovateľských operáciách, ktoré by sa mohli dotknutej osoby týkať, najmä vrátane tých, ktoré dotknutá osoba nemusela očakávať, ak prevádzkovateľ tiež poskytne prístup ku všetkým údajom, o ktoré mala dotknutá osoba jasný záujem, a ak sú tieto informácie kombinované s jasným uvedením toho, ako možno získať prístup k zvyšným častiam spracúvaných údajov.

- c) Na právo na prístup sa uplatňujú výnimky alebo obmedzenia (pozri ďalej v oddiele 6). V takýchto prípadoch by mal prevádzkovateľ dôkladne skontrolovať, ktorých častí informácií sa výnimka týka, a mal by poskytnúť všetky informácie, ktoré sa touto výnimkou nevylučujú. Napríklad potvrdenie o samotnom spracúvaní osobných údajov (zložka 1) nemôže byť dotknutá výnimkou. Výsledkom toho je, že informácie sa musia poskytovať o všetkých osobných údajoch a všetkých informáciách uvedených v článku 15 ods. 1 a 2, na ktoré sa nevzťahuje výnimka alebo obmedzenie.

2.3.2 Správnosť informácií

36. Informácie uvedené v kópii osobných údajov, ktorá sa poskytuje dotknutej osobe, musia zahŕňať aktuálne informácie alebo držané osobné údaje o dotknutej osobe. To zahŕňa povinnosť poskytnúť informácie o údajoch, ktoré sú nesprávne, alebo o spracúvaní údajov, ktoré nie sú alebo už nie sú zákonné. Dotknutá osoba môže napríklad použiť právo na prístup, aby zistila zdroj nesprávnych údajov, ktoré sa šíria medzi rôznymi prevádzkovateľmi. Ak prevádzkovateľ opravil nesprávne údaje predtým, než o tom informoval dotknutú osobu, dotknutá osoba by tým bola zbavená tejto možnosti. To isté platí aj v prípade nezákonného spracúvania. Možnosť vedieť o nezákonnom spracúvaní údajov týkajúcich sa dotknutej osoby predstavuje jeden z hlavných účelov existencie práva na prístup. Povinnosť informovať o nezmenenom stave spracúvania sa uplatňuje bez toho, aby bola dotknutá povinnosť prevádzkovateľa ukončiť nezákonné spracúvanie alebo opraviť nesprávne údaje. Otázky týkajúce sa poradia, v ktorom by dané povinnosti mali byť splnené, sú zodpovedané ďalej v texte.

2.3.3 Referenčný časový bod posúdenia

37. Posúdenie údajov, ktoré sa spracúvajú, musí čo najvernejšie odrážať situáciu, kedy prevádzkovateľ prijme žiadosť, pričom odpoveď bude zahŕňať všetky údaje dostupné v danom časovom okamihu. To znamená, že prevádzkovateľ sa bez zbytočného odkladu musí pokúsiť zistiť informácie o všetkých spracovateľských činnostiach súvisiacich s dotknutou osobou. Prevádzkovatelia však nemusia poskytnúť osobné údaje, ktoré spracúvali v minulosti, ktoré však už nemajú k dispozícii¹⁹. Prevádzkovateľ mohol napríklad vymazať osobné údaje v súlade so svojou politikou uchovávanía údajov a/alebo zákonnými ustanoveniami, a preto už nemusí byť schopný poskytnúť požadované osobné údaje. V tomto kontexte treba pripomenúť, že dĺžka času, keď sa údaje uchovávajú, by mala byť stanovená v súlade s článkom 5 ods. 1 písm. e) všeobecného nariadenia o ochrane údajov, keďže akékoľvek uchovávanie údajov musí byť objektívne odôvodnené.
38. Prevádzkovateľ zároveň vopred zavedie potrebné opatrenia s cieľom uľahčiť uplatňovanie práva na prístup a aby čo najskôr vybavoval takéto žiadosti (pozri článok 12 ods. 3), a to ešte skôr než sa tieto údaje budú musieť vymazať. Opatrenia prijaté s cieľom odpovedať na žiadosť by sa preto v prípade krátko obdobia uchovávanía mali upraviť na primerané obdobie uchovávanía s cieľom uľahčiť

¹⁹ V tomto zmysle pozri ďalšie objasnenia v oddiele 4 týchto usmernení, ako aj v rozsudku Súdneho dvora Európskej únie zo 7. mája 2009 vo veci C-553/07, College van burgemeester en wethouders van Rotterdam/pán E. E. Rijkeboer o práve na prístup k informáciám o príjemcoch alebo kategóriách príjemcov vzhľadom na minulosť.

uplatňovanie práva na prístup a vyhnúť sa trvalej nemožnosti poskytnúť prístup k údajom spracúvaným v čase podania žiadosti²⁰. V niektorých prípadoch však nemusí byť možné odpovedať na žiadosť pred plánovaným časom vymazania údajov. Napríklad, ak prevádzkovateľ v rámci čo najrýchlejšej odpovede na žiadosť uchová osobné údaje, ktoré sa podľa plánu majú vymazať nasledujúci deň, je možné, že prevádzkovateľ bude potrebovať dodatočný čas na zváženie toho, či je pred vydaním kópie osobných údajov žiadateľovi, potrebné vykonať nejaké úpravy s cieľom chrániť slobody iných. Ak sa údaje získali v rámci plánovaného obdobia uchovávaní, prevádzkovateľ môže pokračovať v spracúvaní daných údajov na účely plnenia svojej povinnosti odpovedať na žiadosť. Spracúvanie v takých prípadoch môže vychádzať z článku 6 ods. 1 písm. c) v kombinácii s článkom 15 všeobecného nariadenia o ochrane údajov a jeho trvanie musí byť v súlade s požiadavkami článku 12 ods. 3 všeobecného nariadenia o ochrane údajov²¹. Uplatňovanie tohto právneho základu sa vzťahuje len na spracúvanie údajov, ktoré boli identifikované ako potrebné na odpoveď na konkrétnu žiadosť a nepoužije sa ako odôvodnenie všeobecného predĺženia období uchovávaní.

39. Okrem toho, prevádzkovateľ sa nemôže zámerne vyhnúť povinnosti poskytnúť požadované osobné údaje ich vymazaním alebo pozmenením osobných údajov v rámci odpovede na žiadosť o prístup (pozri oddiel 2.3.2). Ak prevádzkovateľ pri spracovaní žiadosti o prístup odhalí nesprávne údaje alebo nezákonné spracúvanie, musí posúdiť stav spracúvania a musí o tom primerane informovať dotknutú osobu predtým ako si prevádzkovateľ splení svoje ostatných povinnosti. Vo svojom vlastnom záujme a s cieľom vyhnúť sa potrebe ďalšej komunikácie o tejto otázke, ako aj s cieľom dodržať zásadu transparentnosti, by mal prevádzkovateľ pridať informácie o následných opravách alebo vymazaní údajov.

Príklad 6: Pri odpovedaní na žiadosť o prístup si prevádzkovateľ uvedomí, že žiadosť dotknutej osoby o pracovnú pozíciu v spoločnosti prevádzkovateľa bola uložená aj po uplynutí obdobia uchovávaní. V tomto prípade prevádzkovateľ nemôže najprv vymazať údaje a potom dotknutej osobe odpovedať, že sa nespracúvajú žiadne údaje (týkajúce sa žiadosti). Najprv musí poskytnúť prístup a údaje môže vymazať až potom. S cieľom vyhnúť sa následnej žiadosti o vymazanie sa odporúča, aby prevádzkovateľ dodal informáciu o vymazaní údajov a jeho čase.

Prevádzkovatelia by s cieľom dodržať zásadu transparentnosti mali informovať dotknutú osobu o konkrétnom okamihu spracúvania, na ktorý sa vzťahuje odpoveď prevádzkovateľa. V niektorých prípadoch, napríklad v kontexte častých komunikačných činností, sa môže vyskytnúť dodatočné spracúvanie alebo úprava údajov, a to medzi referenčným časovým bodomsúčasnosti, v ktorom sa spracúvanie posúdilo, a odpoveďou prevádzkovateľa. Ak si je prevádzkovateľ vedomý takýchto zmien, odporúča sa, aby zahrnul informácie o daných zmenách, ako aj informácie o dodatočnom spracúvaní, ktoré je potrebné na odpoveď na žiadosť.

2.3.4 Súlad s požiadavkami na bezpečnosť údajov

40. Keďže komunikácia s dotknutou osobou a sprístupňovanie osobných údajov dotknutej osobe je spracovateľská operácia, prevádzkovateľ je vždy povinný realizovať vhodné technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti zodpovedajúcej riziku spracúvania [pozri článok 5

²⁰ S cieľom uľahčiť rýchlu reakciu by sa napríklad mohlo zvážiť zavedenie samoobslužného nástroja, ktorý by dotknutej osobe umožnil jednoducho získať prístup k požadovaným osobným údajom, ako aj oznamovací systém, ktorý by prevádzkovateľa upozornil na žiadosti súvisiace s osobnými údajmi s krátkymi obdobiami uchovávaní.

²¹ Týmto nie je dotknuté následné spracúvanie údajov na účely dokazovania súvisiaceho s vybavovaním žiadosti o prístup na primerané časové obdobie.

ods. 1 písm. f) a články 24 a 32 všeobecného nariadenia o ochrane údajov]. Toto sa uplatňuje nezávisle od spôsobu, ktorým sa prístup poskytuje. V prípade poskytnutia údajov dotknutej osobe inými ako elektronickými prostriedkami a v závislosti od rizík, ktoré spracúvanie údajov sprevádza, prevádzkovateľ môže zväziť použitie doporučenej pošty alebo prípadne môže dotknutej osobe ponúknuť, ale nie jej uložiť ako povinnosť, vyzdvihnutie súboru na podpis priamo v jednej z prevádzkárni prevádzkovateľa. Ak sa informácie poskytujú elektronickými prostriedkami v súlade s článkom 12 ods. 1 a 3, prevádzkovateľ si vyberie taký elektronický prostriedok, ktorý je v súlade s požiadavkami na bezpečnosť údajov. Aj v prípade poskytovania kópie údajov v bežne používanej elektronickej podobe (pozri článok 15 ods. 3), prevádzkovateľ pri výbere spôsobu poskytnutia elektronického súboru dotknutej osobe zohľadní požiadavky na bezpečnosť údajov. To môže zahŕňať použitie šifrovania, ochranu heslom atď. S cieľom uľahčiť prístup k šifrovaným údajom by prevádzkovateľ mal takisto zabezpečiť, aby boli sprístupnené vhodné informácie, aby dotknutá osoba mohla mať prístup k dešifrovaným informáciám. V prípadoch, keď by si požiadavky na bezpečnosť údajov vyžadovali šifrovanie e-mailov medzi koncovými bodmi [end-to-end encryption], ale prevádzkovateľ dokáže poslať len bežný e-mail, prevádzkovateľ bude musieť použiť iné prostriedky, ako je napríklad poslanie USB kľúča (doporučeným) listom dotknutej osobe.

3 VŠEOBECNÉ ÚVAHY TÝKAJÚCE SA POSÚDENIA ŽIADOSTÍ O PRÍSTUP

3.1 Úvod

41. Prevádzkovateľ musí každú prijatú žiadosť o prístup k osobným údajom posudzovať samostatne. Prevádzkovateľ, okrem iného, zohľadní otázky, ktoré sú uvedené ďalej v nasledujúcich odsekoch: či sa žiadosť týka osobných údajov súvisiacich so žiadateľom a kto je žiadateľom. Cieľom tohto oddielu je objasniť, ktoré prvky žiadosti o prístup by mal prevádzkovateľ zohľadniť pri vykonávaní svojho posúdenia, ako aj diskusia o prípadných scenároch pre takéto posúdenie a jeho následkoch. Prevádzkovateľ pri posudzovaní žiadosti o prístup k osobným údajom podľa článku 12 ods. 2 všeobecného nariadenia o ochrane údajov takisto zohľadní povinnosť uľahčiť uplatňovanie práv dotknutej osoby, pričom musí dbať na primeranú bezpečnosť osobných údajov²².
42. Z tohto dôvodu by prevádzkovatelia mali byť proaktívne pripravení spracúvať žiadosti o prístup k osobným údajom. Znamená to, že prevádzkovateľ by mal byť pripravený prijať žiadosť, riadne ju posúdiť (toto posúdenie je predmetom tohto oddielu usmernení) a žiadateľovi poskytnúť primeranú odpoveď bez zbytočného odkladu. Spôsob, akým sa prevádzkovatelia pripravujú na riešenie žiadostí o prístup, by mal byť vhodný a primeraný, a mal by závisieť od povahy, rozsahu, kontextu a účelov spracúvania, ako aj od rizík pre práva a slobody fyzických osôb, v súlade s článkom 24 všeobecného nariadenia o ochrane údajov. V závislosti od konkrétnych okolností sa od prevádzkovateľov môže

²² Prevádzkovateľ zabezpečí primeranú bezpečnosť osobných údajov v súlade so zásadou integrity a dôvernosti [článok 5 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov] vykonaním primeraných technických a organizačných opatrení, ako sa uvádza v článku 32 všeobecného nariadenia o ochrane údajov a rozvádza v článku 24 všeobecného nariadenia o ochrane údajov. Prevádzkovateľ musí byť schopný preukázať, že zabezpečuje primeranú úroveň ochrany údajov, v súlade so zásadou zodpovednosti (pozri aj: stanovisko pracovnej skupiny zriadenej podľa článku 29 č. 3/2010 k zásade zodpovednosti prijaté 13. júla 2010, 00062/10/EN WP 173 a usmernenia EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov).

napríklad vyžadovať zavedenie vhodného postupu, ktorého vykonávaním by sa mala zaistiť bezpečnosť údajov bez toho, aby sa obmedzovalo uplatňovanie práv dotknutej osoby.

3.1.1 Analýza obsahu žiadosti

43. Túto otázku možno riešiť konkrétnejšie kladením nasledovných otázok.

a) Týka sa žiadosť osobných údajov?

44. Podľa všeobecného nariadenia o ochrane údajov sa rozsah žiadosti týka len osobných údajov²³. Preto sa akákoľvek žiadosť o informácie o iných otázkach vrátane všeobecných informácií o prevádzkovateli, jeho obchodných modeloch alebo spracovateľských činnostiach, ktoré sa netýkajú osobných údajov, nepovažujú za žiadosť podanú podľa článku 15 všeobecného nariadenia o ochrane údajov. Okrem toho žiadosť o informácie o anonymných údajoch alebo údajoch, ktoré sa netýkajú žiadateľa alebo osoby, v mene ktorej oprávnená osoba žiadosť podala, nebude patriť do rozsahu práva na prístup. Táto otázka sa bude podrobnejšie analyzovať v oddiele 4.

45. Na rozdiel od anonymných údajov (ktoré nie sú osobnými údajmi), pseudonymizované údaje, ktoré by mohli byť priradené fyzickej osobe použitím dodatočných informácií, sú osobné údaje²⁴. Preto sa pseudonymizované údaje, ktoré možno spojiť s dotknutou osobou, napríklad, keď dotknutá osoba poskytne príslušný identifikátor umožňujúci jej identifikáciu, alebo keď je prevádzkovateľ schopný vlastnými prostriedkami prepojiť údaje so žiadateľom, budú považovať za údaje, ktoré patria do rozsahu žiadosti²⁵.

b) Týka sa žiadosť žiadateľa (alebo osoby, v menej ktorej oprávnená osoba podáva žiadosť)?

46. Vo všeobecnosti platí, že žiadosť sa môže týkať len údajov osoby, ktorá žiadosť podáva. Prístup k údajom iných osôb môže byť vyžiadaný len na základe primeraného oprávnenia²⁶.

Príklad 7: Dotknutá osoba X pracuje na pozícii vedúceho oddelenia pre spoločnosť, ktorá poskytuje parkovacie miesta pre svojich manažérov na parkovisku spoločnosti. Hoci má dotknutá osoba X stále parkovacie miesto, keď príde do kancelárie na svoju druhú zmenu, toto miesto je častokrát už obsadené iným vozidlom. Keďže sa táto situácia opakuje, dotknutá osoba s cieľom identifikovať vodiča, ktorý neoprávnenne obsadzuje jej miesto, požiada prevádzkovateľa systému videomonitorovania, ktorý sníma parkovisko spoločnosti, o prístup k osobným údajom tohto vodiča. V tomto prípade žiadosť dotknutej osoby X nebude žiadosťou o prístup k jej osobným údajom, keďže sa žiadosť netýka údajov žiadateľa, ale údajov inej osoby, a preto sa nebude považovať za žiadosť podľa článku 15 všeobecného nariadenia o ochrane údajov.

c) Uplatňujú sa iné ustanovenia ako všeobecné nariadenie o ochrane údajov, ktorými sa upravuje prístup k určitej kategórii údajov?

47. Dotknuté osoby nie sú povinné vo svojej žiadosti uviesť právny základ. Ak však dotknuté osoby objasnia, že ich žiadosť sa zakladá na odvetvových právnych predpisoch alebo na vnútroštátnych

²³ Pokiaľ sa žiadosť netýka aj iných ako osobných údajov, ktoré sú neoddeliteľne spojené s osobnými údajmi dotknutej osoby. Ďalšie objasnenia sa nachádzajú v bode 100.

²⁴ Pozri odôvodnenie 26 všeobecného nariadenia o ochrane údajov. Ďalšie objasnenia pojmov anonymné údaje a pseudonymizované údaje sa nachádzajú v stanovisku 4/2007 WP29 k pojmu osobné údaje, s. 18 – 21.

²⁵ Pracovná skupina zriadená podľa článku 29, WP 242 rev.01, 5. apríla 2017, Usmernenia k právu na prenosnosť údajov – schválené EDPB (ďalej len „usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB“), s. 9.

²⁶ Pozri oddiel 3.4 („Žiadosti podávané prostredníctvom tretích strán/splnomocnených zástupcov“).

právnych predpisoch, ktorými sa upravuje konkrétna otázka prístupu k určitým kategóriám údajov, a nie na všeobecnom nariadení o ochrane údajov, takúto žiadosť prevádzkovateľ preskúma podľa potreby v súlade s týmito odvetvovými alebo vnútroštátnymi predpismi. Často, a to v závislosti od príslušných vnútroštátnych právnych predpisov, sa od prevádzkovateľov môže vyžadovať, aby poskytli samostatné odpovede, pričom každá sa zaoberá špecifickými požiadavkami stanovenými v rôznych legislatívnych aktoch. Nemalo by sa to zamieňať s vnútroštátnymi právnymi predpismi alebo právnymi predpismi EÚ, ktorými sa stanovujú obmedzenia týkajúce sa práva na prístup, ktoré treba dodržiavať pri poskytovaní odpovedí na žiadosti o prístup.

48. Ak má prevádzkovateľ pochybnosti o tom, ktoré právo chce dotknutá osoba uplatniť, odporúča sa, aby požiadal dotknutú osobu, ktorá podáva žiadosť, o vysvetlenie predmetu žiadosti. Takéto korešpondovanie s dotknutou osobou nemá vplyv na povinnosť prevádzkovateľa konať bez zbytočného odkladu²⁷. Napriek tomu v prípade pochybností, ak prevádzkovateľ požiada dotknutú osobu o ďalšie vysvetlenie a nedostane žiadnu odpoveď, so zreteľom na povinnosť uľahčiť dotknutej osobe uplatnenie práva na prístup k informáciám by prevádzkovateľ mal spraviť výklad informácií uvedených v prvej žiadosti a konať na základe tohto výkladu. V súlade so zásadou zodpovednosti môže prevádzkovateľ určiť primeraný časový rámec, počas ktorého môže dotknutá osoba poskytnúť ďalšie vysvetlenie. Pri určovaní takéhoto časového rámca by si mal prevádzkovateľ ponechať dostatok času na splnenie žiadosti po jeho uplynutí, a preto zvážiť, koľko času objektívne treba na zhromaždenie a poskytnutie požadovaných údajov po tom, čo dotknutá osoba poskytla (alebo neposkytla) upresnenie.
49. Ak žiadosť patrí do rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov, existencia takýchto špecifických právnych predpisov nemá prednosť pred všeobecným uplatňovaním práva na prístup, ako je stanovené vo všeobecnom nariadení o ochrane údajov. Môžu existovať obmedzenia stanovené v práve EÚ alebo vnútroštátnom práve, ak to umožňuje článok 23 všeobecného nariadenia o ochrane údajov (pozri oddiel 6.4).

d) Patrí žiadosť do rozsahu pôsobnosti článku 15?

50. Treba poukázať na to, že všeobecným nariadením o ochrane údajov sa nezavádzajú žiadne formálne požiadavky na osoby, ktoré žiadajú o prístup k údajom. Na podanie žiadosti o prístup stačí, aby žiadatelia uviedli, že chcú vedieť, aké osobné údaje, ktoré sa ich týkajú, prevádzkovateľ spracúva. Prevádzkovateľ preto nemôže odmietnuť poskytnúť údaje s odvolaním sa na chýbajúce označenie právneho základu žiadosti, najmä na chýbajúci konkrétny odkaz na právo na prístup alebo na všeobecné nariadenie o ochrane údajov.

Na podanie žiadosti by napríklad stačilo, aby žiadateľ uviedol, že:

- chce získať prístup k osobným údajom, ktoré sa ho týkajú,
- uplatňuje svoje právo na prístup, alebo
- chce poznať informácie, ktoré sa ho týkajú a ktoré prevádzkovateľ spracúva.

Treba pripomenúť, že žiadatelia nemusia poznať zložitosť všeobecného nariadenia o ochrane údajov a že sa odporúča byť zhovievavý k osobám, ktoré uplatňujú svoje právo na prístup, najmä keď ho uplatňujú maloletí. Ako už bolo uvedené, v prípade akýchkoľvek pochybností sa odporúča, aby prevádzkovateľ požiadal dotknutú osobu, ktorá podáva žiadosť, o spresnenie predmetu žiadosti.

²⁷ Pozri ďalšie usmernenie o určovaní času v oddiele 5.3.

e) Chcú dotknuté osoby získať prístup k všetkým informáciám alebo ich častiam, ktoré sa o nich spracúvajú?

51. Okrem toho musí prevádzkovateľ posúdiť, či sa žiadosti podané žiadateľmi týkajú všetkých informácií, ktoré sa o nich spracúvajú, alebo ich častí. Akékoľvek obmedzenie rozsahu žiadosti na konkrétne ustanovenie článku 15 všeobecného nariadenia o ochrane údajov, vykonané dotknutými osobami, musí byť jasné a jednoznačné. Ak napríklad dotknuté osoby požadujú doslovne „informácie o údajoch, ktoré sa vo vzťahu k nim spracúvajú“, prevádzkovateľ by mal predpokladať, že dotknuté osoby majú v úmysle uplatniť svoje úplné právo podľa článku 15 ods. 1 – 2 všeobecného nariadenia o ochrane údajov. Takáto žiadosť by sa nemala vykladať tak, že dotknuté osoby chcú dostať iba kategórie osobných údajov, ktoré sa spracúvajú a vzdať sa svojho práva na informácie uvedené v článku 15 ods. 1 písm. a) až h). Iné by to bolo napríklad vtedy, ak dotknuté osoby chcú, a to s ohľadom na údaje, ktoré špecifikovali, získať prístup k zdroju alebo pôvodu osobných údajov alebo k stanovenému obdobiu uchovávanía. V takomto prípade môže prevádzkovateľ obmedziť svoju odpoveď na konkrétne požadované informácie.

3.1.2 Forma žiadosti

52. Ako už bolo uvedené, vo všeobecnom nariadení o ochrane údajov sa dotknutým osobám neukladajú žiadne požiadavky týkajúce sa formy žiadosti o prístup k osobným údajom. Podľa všeobecného nariadenia o ochrane údajov teda v zásade neexistujú žiadne požiadavky, ktoré musia dotknuté osoby dodržať pri výbere komunikačného kanála, prostredníctvom ktorého vstupujú do styku s prevádzkovateľom.
53. EDPB vyzýva prevádzkovateľov, aby poskytovali najvhodnejšie a používateľsky najpriateľnejšie komunikačné kanály v súlade s článkom 12 ods. 2 a článkom 25 všeobecného nariadenia o ochrane údajov, aby dotknuté osoby mohli podať platnú žiadosť. Ak však dotknutá osoba podá žiadosť prostredníctvom komunikačného kanála poskytnutého prevádzkovateľom²⁸, ktorý je odlišný od kanála označeného ako vhodnejší, takáto žiadosť sa vo všeobecnosti považuje za platnú a prevádzkovateľ by mal s takouto žiadosťou podľa toho zaobchádzať (pozri príklady ďalej). Prevádzkovatelia by mali vynaložiť všetko primerané úsilie na to, aby uľahčili uplatňovanie práv dotknutej osoby (napríklad keď dotknutá osoba pošle žiadosť o prístup zamestnancovi, ktorý je na dovolenke, za primerané úsilie v prípade tejto žiadosti sa môže považovať automatická správa, ktorou sa dotknutá osoba informuje o alternatívnej komunikácii).
54. Treba upozorniť na to, že prevádzkovateľ nemusí konať na základe žiadosti zaslanej na náhodnú alebo nesprávnu e-mailovú (alebo poštovú) adresu, ktorú prevádzkovateľ priamo neposkytol, alebo na akýkoľvek komunikačný kanál, ktorý jednoznačne nie je určený na prijímanie žiadostí týkajúcich sa práv dotknutej osoby, ak prevádzkovateľ poskytol vhodný komunikačný kanál, ktorý môže dotknutá osoba použiť.
55. Prevádzkovateľ takisto nemusí konať na základe žiadosti zaslanej na e-mailovú adresu zamestnanca prevádzkovateľa, ktorý sa nemusí podieľať na vybavovaní žiadostí týkajúcich sa práv dotknutých osôb (napríklad vodiči, upratovací personál atď.). Takéto žiadosti sa nepovažujú za platné, ak prevádzkovateľ jednoznačne poskytol dotknutej osobe vhodný komunikačný kanál. Ak však dotknutá osoba pošle

²⁸ Môže to zahŕňať napríklad komunikačné údaje prevádzkovateľa poskytnuté v jeho oznámeniach adresovaných priamo dotknutým osobám alebo kontaktné údaje, ktoré prevádzkovateľ poskytuje verejne, ako napríklad v prevádzkovateľovej politike ochrany osobných údajov alebo v iných povinných právnych oznámeniach prevádzkovateľa (napr. kontaktné informácie týkajúce sa vlastníka alebo podnikania na webovom sídle).

žiadosť zamestnancovi prevádzkovateľa, ktorý jej bol pridelený ako jej riadna kontaktná osoba (ako je napríklad správca osobného účtu v banke alebo stály poradca prevádzkovateľa mobilných telefónnych služieb), takýto kontakt by sa nemal považovať za náhodný a prevádzkovateľ by mal vynaložiť všetko primerané úsilie s cieľom vybaviť túto žiadosť, aby sa mohla presmerovať na kontaktné miesto a vyriešiť v lehotách, ktoré sú stanovené vo všeobecnom nariadení o ochrane údajov.

56. EDPB napriek tomu odporúča, a to ako osvedčený postup, aby prevádzkovatelia zaviedli vhodné mechanizmy na uľahčenie uplatňovania práv dotknutých osôb vrátane systémov automatických odpovedačov [autoresponder systems] na informovanie o neprítomnosti zamestnancov a vhodnom náhradnom kontakte, a ak je to možné, mechanizmy na zlepšenie internej komunikácie medzi zamestnancami týkajúcej sa žiadostí, ktoré dostali zamestnanci, ktorí nemusia byť oprávnení na vybavovanie takýchto žiadostí.

Príklad 8: Prevádzkovateľ X uvádza, a to na svojom webovom sídle, ako aj v oznámení o ochrane osobných údajov, dve e-mailové adresy – všeobecnú e-mailovú adresu prevádzkovateľa: KONTAKT@X.COM a e-mailovú adresu kontaktného miesta prevádzkovateľa pre ochranu údajov: OTAZKY@X.COM. Prevádzkovateľ X okrem toho na svojom webovom sídle uvádza, že s cieľom predložiť akékoľvek otázky alebo podať žiadosť v súvislosti so spracúvaním osobných údajov by sa fyzické osoby mali obrátiť na kontaktné miesto pre ochranu údajov prostredníctvom poskytnutej e-mailovej adresy. Dotknutá osoba však pošle žiadosť na všeobecnú e-mailovú adresu prevádzkovateľa: KONTAKT@X.COM.

V tomto prípade by mal prevádzkovateľ vynaložiť všetko primerané úsilie na to, aby svoje útvary oboznámil so žiadosťou, ktorá bola podaná prostredníctvom všeobecného e-mailu, aby sa mohla presmerovať na kontaktné miesto pre ochranu údajov a vyriešiť v lehotách, ktoré sú stanovené vo všeobecnom nariadení o ochrane údajov. Prevádzkovateľ navyše nie je oprávnený predĺžiť lehotu na odpoveď na žiadosť len preto, že dotknutá osoba poslala žiadosť na všeobecnú e-mailovú adresu prevádzkovateľa, nie na e-mailovú adresu kontaktného miesta prevádzkovateľa pre ochranu údajov.

Príklad 9: Prevádzkovateľ Y prevádzkuje sieť fitness klubov. Prevádzkovateľ Y na svojom webovom sídle a v oznámení o ochrane osobných údajov pre zákazníkov fitness klubu uvádza, že v prípade poslania akýchkoľvek otázok alebo žiadostí v súvislosti so spracúvaním osobných údajov by sa fyzické osoby mali obrátiť na prevádzkovateľa prostredníctvom e-mailovej adresy: OTAZKY@Y.COM. Dotknutá osoba napriek tomu pošle žiadosť na e-mailovú adresu, ktorú našla v šatni, kde našla oznam „V prípade nespokojnosti s čistotou v miestnosti, nás kontaktujte na adrese: UPRAOVANIE@Y.COM“, čo je e-mailová adresa upratovacieho personálu zamestnávaného prevádzkovateľom Y. Upratovací personál zjavne nie je zapojený do vybavovania záležitostí týkajúcich sa uplatňovania práv dotknutých osôb – zákazníkov fitness klubu. Hoci bola e-mailová adresa k dispozícii v priestoroch fitness klubu, dotknutá osoba nemohla odôvodnene očakávať, že ide o vhodnú kontaktnú adresu pre takéto žiadosti, keďže na webovom sídle a v oznámení o ochrane osobných údajov bol jednoznačne uvedený komunikačný kanál, ktorý sa má používať na uplatňovanie práv dotknutých osôb.

57. Dátumom prijatia žiadosti prevádzkovateľom sa spravidla spúšťa mesačná lehota na poskytnutie informácií o opatreniach prijatých na základe žiadosti, a to v súlade s článkom 12 ods. 3 všeobecného nariadenia o ochrane údajov (ďalšie usmernenie o meraní času je uvedené v oddiele 5.3). EDPB považuje za osvedčený postup ten, keď prevádzkovatelia potvrdia prijatie žiadostí písomne, napríklad poslaním e-mailov (alebo prípadne poslaním informácií poštou) žiadateľom, ktorými sa potvrdzuje, že ich žiadosti boli prijaté a že lehota jedného mesiaca trvá odo dňa X do dňa Y.

3.2 Identifikácia a autentifikácia

58. V záujme zaistenia bezpečnosti spracúvania a minimalizácie rizika neoprávneného sprístupnenia osobných údajov musí byť prevádzkovateľ schopný zistiť, ktoré údaje sa týkajú dotknutej osoby (identifikácia), a potvrdiť totožnosť tejto osoby (autentifikácia).
59. Treba pripomenúť, že v situáciách, v ktorých sa na účel, na ktorý sa osobné údaje spracúvajú, nevyžaduje alebo prestala vyžadovať identifikácia dotknutej osoby, prevádzkovateľ nemusí uchovávať identifikáciu výlučne na účely dodržiavania práv dotknutých osôb, a to aj vzhľadom na zásadu minimalizácie údajov. Tieto situácie sa riešia v článku 11 ods. 1 všeobecného nariadenia o ochrane údajov.
60. V článku 12 ods. 2 všeobecného nariadenia o ochrane údajov sa uvádza, že prevádzkovateľ nesmie odmietnuť konať na základe žiadosti dotknutej osoby o uplatnenie jej práv, pokiaľ prevádzkovateľ nespracúva osobné údaje na účel, ktorý si nevyžaduje identifikáciu dotknutej osoby, a pokiaľ nepreukáže, že dotknutú osobu nie je schopný identifikovať. Za takýchto okolností sa však dotknutá osoba môže rozhodnúť poskytnúť dodatočné informácie, ktoré túto identifikáciu umožňujú (článok 11 ods. 2 všeobecného nariadenia o ochrane údajov)²⁹.
61. Prevádzkovateľ nie je povinný získavať takéto dodatočné informácie s cieľom identifikovať dotknutú osobu výlučne na účely toho, aby vyhovel žiadosti dotknutej osoby, a to aj vzhľadom na zásadu minimalizácie údajov. Nemal by však odmietnuť prijať takéto dodatočné informácie, ktoré mu poskytne dotknutá osoba na podporu uplatnenia svojich práv (odôvodnenie 57 všeobecného nariadenia o ochrane údajov).

Príklad 10: X je prevádzkovateľ údajov spracúvaných v súvislosti s monitorovaním budovy kamerovým systémom. V súlade s článkom 11 ods. 1 všeobecného nariadenia o ochrane údajov prevádzkovateľ nie je povinný identifikovať všetky osoby, ktoré boli zaznamenané bezpečnostnou kamerou v rámci monitorovania (účel nevyžadujúci identifikáciu). Prevádzkovateľ dostane žiadosť o prístup k osobným údajom od osoby, ktorá tvrdí, že bola zaznamenaná monitorovaním kamerovým systémom prevádzkovateľa. Konanie prevádzkovateľa bude závisieť od poskytnutých dodatočných informácií. Ak žiadateľ uvedie konkrétny deň a čas, keď kamery mohli zaznamenať predmetnú udalosť, je pravdepodobné, že prevádzkovateľ bude môcť takéto údaje poskytnúť (článok 11 ods. 2 všeobecného nariadenia o ochrane údajov). Ak však prevádzkovateľ nemá možnosť identifikovať dotknutú osobu (napr. ak si prevádzkovateľ nemôže byť istý, že žiadateľ je skutočne dotknutou osobou, alebo ak sa žiadosť týka napr. dlhého obdobia záznamov a prevádzkovateľ nevie spracovať také veľké množstvo údajov), môže prevádzkovateľ odmietnuť konať, ak preukáže, že nie je schopný identifikovať dotknutú osobu (článok 12 ods. 2 všeobecného nariadenia o ochrane údajov).

Príklad 11: Prevádzkovateľ C spracúva osobné údaje na účely adresovania behaviorálnej reklamy používateľom svojho webu. Osobné údaje zbierané na účely behaviorálnej reklamy sa zvyčajne získavajú prostredníctvom súborov cookie a spájajú sa so pseudonymnými náhodnými identifikátormi. Dotknutá osoba, pán X, uplatňuje svoje právo na prístup voči prevádzkovateľovi C prostredníctvom webového sídla tohto prevádzkovateľa. C vie presne identifikovať pána X, aby zobrazil behaviorálnu reklamu dotknutej osoby tým, že pripojí koncové zariadenie pána X k jeho reklamnému profilu so súbormi cookie uloženými v koncovom zariadení. C by tak mal byť takisto schopný presne identifikovať pána X, aby mu poskytol prístup k jeho osobným údajom, keďže možno nájsť prepojenie medzi

²⁹ Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 13.

spracúvanými údajmi a dotknutou osobou. Z tohto dôvodu a s prihliadnutím na zásady všeobecného nariadenia o ochrane údajov by uvedený príklad nepatril do rozsahu pôsobnosti článku 11 všeobecného nariadenia o ochrane údajov. Presnejšie, v uvedenom prípade, si účely prevádzkovateľa C vyžadujú identifikáciu dotknutých osôb, zatiaľ čo v článku 11 všeobecného nariadenia o ochrane údajov sa rieši situácia spracúvania, ktorá si nevyžaduje identifikáciu, pri ktorej prevádzkovateľ nie je povinný spracúvať dodatočné údaje v zmysle článku 11 ods. 1 všeobecného nariadenia o ochrane údajov výhradne na účely dosiahnutia súladu so všeobecným nariadením o ochrane údajov. Následkom toho, by sa preto v niektorých prípadoch na uplatnenie práv dotknutej osoby, nemali požadovať žiadne dodatočné údaje.

Ak sa však pán X pokúsi uplatniť svoje právo na prístup e-mailom alebo bežnou poštou, potom v tejto súvislosti nebude mať prevádzkovateľ C inú možnosť, ako požiadať pána X o poskytnutie „dodatočných informácií“ (článok 12 ods. 6 všeobecného nariadenia o ochrane údajov), aby bol schopný identifikovať reklamný profil spojený s pánom X. V tomto prípade bude dodatočnou informáciou identifikátor súboru cookie uložený v koncovom zariadení pána X.

62. Ak prevádzkovateľ môže preukázať, že dotknutú osobu nie je schopný identifikovať (článok 11 všeobecného nariadenia o ochrane údajov), musí o tom primerane informovať dotknutú osobu, ak je to možné, keďže prevádzkovateľ musí na žiadosti od dotknutej osoby bez zbytočného odkladu odpovedať, pričom uvedie dôvody, keď nemá v úmysle vyhovieť takýmto žiadostiam. Tieto informácie treba poskytnúť iba „ak je to možné“, pretože prevádzkovateľ nemusí byť schopný informovať dotknuté osoby, ak ich identifikácia nie je možná.
63. V prípade, že spracúvanie nevyžaduje identifikáciu, ako aj v prípade, že ju vyžaduje, ak má prevádzkovateľ oprávnené pochybnosti v súvislosti s totožnosťou fyzickej osoby, ktorá žiadosť podáva, prevádzkovateľ môže požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby (článok 12 ods. 6 všeobecného nariadenia o ochrane údajov).
64. Všeobecným nariadením o ochrane údajov sa neukladajú žiadne požiadavky na spôsob autentifikácie dotknutej osoby. V článkoch 11 a 12 všeobecného nariadenia o ochrane údajov sa však uvádzajú podmienky na uplatnenie všetkých práv dotknutej osoby vrátane práva na prístup k osobným údajom.
65. Malo by sa pamätať na to, že prevádzkovateľ spravidla nemôže požadovať viac osobných údajov, ako je potrebné na umožnenie tejto autentifikácie, a že použitie takýchto informácií by sa malo prísne obmedziť na splnenie žiadosti dotknutých osôb.
66. Medzi dotknutými osobami a prevádzkovateľmi už často existujú postupy autentifikácie. Prevádzkovatelia môžu použiť tieto postupy autentifikácie na zistenie totožnosti dotknutých osôb, ktoré žiadajú o svoje osobné údaje alebo uplatňujú práva, ktoré sa im priznávajú všeobecným nariadením o ochrane údajov³⁰. V opačnom prípade by mali prevádzkovatelia zaviesť postup autentifikácie, aby tak robili³¹.
67. V prípadoch, keď prevádzkovateľ požaduje dodatočné informácie potrebné na potvrdenie totožnosti dotknutej osoby, alebo mu ich dotknutá osoba poskytne, prevádzkovateľ zakaždým posúdi, ktoré informácie mu umožnia potvrdiť totožnosť dotknutej osoby a prípadne položí žiadateľovi doplňujúce otázky, alebo ak je to vhodné, požiada dotknutú osobu o predloženie niektorých ďalších identifikačných prvkov (pozri oddiel 3.3).

³⁰ Usmernenia WP 29 k právu na prenosnosť údajov – schválené EDPB, s. 14.

³¹ Ďalšie usmernenie týkajúce sa autentifikácie sa nachádza v oddiele 3.3.

68. S cieľom umožniť dotknutej osobe poskytnúť dodatočné informácie potrebné na identifikáciu svojich údajov by mal prevádzkovateľ informovať dotknutú osobu o povahe dodatočných informácií potrebných na umožnenie identifikácie. Takýchto dodatočných informácií by nemalo byť viac ako informácií pôvodne potrebných na autentifikáciu dotknutej osoby. Vo všeobecnosti skutočnosť, že prevádzkovateľ môže požadovať dodatočné informácie na posúdenie totožnosti dotknutej osoby, nemôže viesť k neprimeraným požiadavkám a k zberu osobných údajov, ktoré nie sú relevantné alebo potrebné na posilnenie prepojenia medzi fyzickou osobou a požadovanými osobnými údajmi³².
69. V dôsledku toho, keď sú informácie zbierané online spojené s pseudonymami alebo inými jedinečnými identifikátormi, prevádzkovateľ môže zaviesť vhodné postupy umožňujúce žiadateľovi podať žiadosť o prístup k údajom a získať údaje, ktoré sa ho týkajú³³.

Príklad 12: Dotknutá osoba, pani X, žiada o prístup k svojim údajom tak, že hovorí s konzultantom telefonicky pomoci elektrárenskej spoločnosti, s ktorou má uzatvorenú zmluvu. Konzultant, ktorý má pochybnosti o totožnosti osoby, ktorá žiadosť podáva, vygeneruje v systéme spoločnosti jednorazový jedinečný kód a pošle ho na mobilné telefónne číslo používateľky, ktoré bolo poskytnuté pri založení účtu, v rámci systému dvojitého overenia, ktorého použitie by sa malo v tomto prípade považovať za primerané.

3.3 Posúdenie primeranosti týkajúce sa autentifikácie žiadateľa

70. Ako sa uvádza v predchádzajúcom texte, ak má prevádzkovateľ opodstatnené dôvody na to, aby pochyboval o totožnosti žiadateľa, môže požiadať o dodatočné informácie na potvrdenie totožnosti dotknutej osoby. Prevádzkovateľ však musí zároveň zabezpečiť, aby nezbiehal viac osobných údajov, ako je potrebné na umožnenie autentifikácie žiadateľa. Prevádzkovateľ preto vykoná posúdenie proporcionality, v ktorom musí zohľadniť druh osobných údajov, ktoré sa spracúvajú (napr. osobitné kategórie údajov alebo nie), charakter žiadosti, kontext, v ktorom sa žiadosť podáva, ako aj akúkoľvek škodu, ktorá by mohla vyplývať z nesprávneho poskytnutia. Pri posudzovaní primeranostiby sa malo pamätať na to, že sa treba vyhnúť nadmernému zberu údajov a zároveň sa musí zabezpečiť primeraná úroveň bezpečnosti spracúvania.
71. Prevádzkovateľ by mal zaviesť postup autentifikácie, aby sa presvedčil o totožnosti osôb, ktoré žiadajú o prístup k svojim údajom³⁴, a zaistiť bezpečnosť spracúvania počas celého postupu vybavovania žiadostí o prístup v súlade s článkom 32 všeobecného nariadenia o ochrane údajov, napríklad vrátane zabezpečeného kanála pre dotknuté osoby na poskytovanie dodatočných informácií. Metóda použitá na autentifikáciu by mala byť relevantná, vhodná, primeraná a mala by sa riadiť zásadou minimalizácie údajov. Ak prevádzkovateľ ukladá opatrenia zamerané na autentifikáciu dotknutej osoby, ktoré pôsobia nepriaznivo, musí to primerane odôvodniť a zabezpečiť súlad so všetkými základnými zásadami vrátane minimalizácie údajov a povinnosti uľahčiť uplatňovanie práv dotknutých osôb (článok 12 ods. 2 všeobecného nariadenia o ochrane údajov).

³² Tamže, s. 14.

³³ Tamže, s. 13 – 14.

³⁴ Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 14.

72. V online kontexte môže mechanizmus autentifikácie zahŕňať rovnaké prihlasovacie údaje, ktoré dotknutá osoba použila na prihlásenie do online služby ponúkanej prevádzkovateľom (odôvodnenie 57 všeobecného nariadenia o ochrane údajov)³⁵.
73. V praxi často existujú postupy autentifikácie a prevádzkovatelia nemusia zavádzať ďalšie bezpečnostné záruky, aby zabránili neoprávnenému prístupu k službám. S cieľom umožniť jednotlivcom prístup k údajom nachádzajúcim sa v ich účtoch (ako je e-mailový účet, účet na sociálnych sieťach alebo v online obchodoch) budú prevádzkovatelia s najväčšou pravdepodobnosťou požadovať prihlásenie prostredníctvom prihlasovacieho mena a hesla používateľa, ktoré by v takýchto prípadoch mali stačiť na autentifikáciu dotknutej osoby³⁶. Prevádzkovatelia okrem toho už často overujú dotknuté osoby pred uzavretím zmluvy alebo získaním ich súhlasu so spracúvaním a v dôsledku toho sa môžu osobné údaje použité na registráciu fyzickej osoby, ktorej sa spracúvanie týka, použiť aj ako dôkaz na autentifikáciu dotknutej osoby na účely prístupu³⁷. Takže je neprimerané požadovať kópiu dokladu totožnosti v prípade, že dotknutú osobu, ktorá podáva žiadosť, už prevádzkovateľ overil.
74. Treba zdôrazniť, že použitie kópie dokladu totožnosti v rámci postupu autentifikácie predstavuje riziko pre bezpečnosť osobných údajov a môže viesť k neoprávnenému alebo nezákonnému spracúvaniu, a ako také by sa malo považovať za nevhodné, pokiaľ nie je potrebné, vhodné a v súlade s vnútroštátnym právom. V takýchto prípadoch by prevádzkovatelia mali mať zavedené systémy, ktorými sa zaisťuje primeraná úroveň zabezpečenia na zmiernenie vyšších rizík pre práva a slobody dotknutej osoby na získanie takýchto údajov. Je takisto dôležité upozorniť na to, že autentifikácia pomocou preukazu totožnosti nemusí nevyhnutne pomôcť v online kontexte (napr. pri použití pseudonymov), ak dotknutá osoba nemôže poskytnúť žiadny iný dôkaz, napr. ďalšie charakteristiky zodpovedajúce používateľskému kontu.
75. Vzhľadom na skutočnosť, že mnohé organizácie (napr. hotely, banky, požičovne automobilov) požadujú kópie preukazu totožnosti svojich klientov, vo všeobecnosti by sa to nemalo považovať za vhodný spôsob autentifikácie. Prevádzkovateľ môže zaviesť aj rýchle a účinné bezpečnostné opatrenie na identifikáciu dotknutej osoby na základe autentifikácie, ktorú vykonal predtým, napr. prostredníctvom e-mailu alebo textovej správy obsahujúcej odkazy na potvrdenie, bezpečnostné otázky alebo potvrdzovacie kódy³⁸.
76. Informácie z preukazu totožnosti, ktoré nie sú potrebné na potvrdenie totožnosti dotknutej osoby, ako sú prístupové a sériové číslo, štátna príslušnosť, výška, farba očí, fotografia a strojovo čitateľná zóna, a to v závislosti od individuálneho posúdenia, sa môžu upraviť alebo skryť pred jeho predložením prevádzkovateľovi, okrem prípadov, keď vnútroštátne právne predpisy vyžadujú úplnú, nezmenenú kópiu preukazu totožnosti (pozri bod 78 ďalej). Vo všeobecnosti platí, že dátum vydania alebo dátum uplynutia platnosti, vydávajúci orgán a celé meno zhodné s online účtom postačujú prevádzkovateľovi na overenie totožnosti, a to vždy za predpokladu, že je zabezpečená pravosť kópie a vzťah k žiadateľovi. Ďalšie informácie, ako je dátum narodenia dotknutej osoby sa môžu požadovať len

³⁵ Pozri ďalšie usmernenie týkajúce sa metód autentifikácie v Usmerneniach EDPB 1/2021 k príkladom týkajúcim sa oznámenia porušenia ochrany osobných údajov, prijatých 14. januára 2021, s. 30 – 31 a v usmerneniach EDPB 02/2021 o virtuálnych hlasových asistentoch, verzia 2.0, prijatých 7. júla 2021, oddiel 3.7.

³⁶ Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 14.

³⁷ Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 14.

³⁸ Pozri aj nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES, ktorým sa zavádzajú rôzne služby, ktoré umožňujú bezpečnú identifikáciu na diaľku.

v prípade, ak pretrváva riziko zámieny osôb, ak ich prevádzkovateľ vie porovnať s informáciami, ktoré už spracúva.

77. V záujme dodržania zásady minimalizácie údajov by mal prevádzkovateľ informovať dotknutú osobu o informáciách, ktoré nie sú potrebné a o možnosti upraviť alebo skryť uvedené časti preukazu totožnosti. V takom prípade, ak dotknutá osoba nevie ako alebo nie je schopná tieto informácie upraviť, je osvedčenou praxou, aby ich prevádzkovateľ upravil pri prijatí dokumentu, ak je to pre prevádzkovateľa možné, pričom sa prihliada na prostriedky, ktoré má prevádzkovateľ za daných okolností k dispozícii.

Príklad 13: Používateľka, pani Y, si v internetovom obchode vytvorila účet chránený heslom, pričom poskytla svoj e-mail a/alebo používateľské meno. Potom majiteľka účtu požiada prevádzkovateľa o informáciu, či spracúva jej osobné údaje, a ak áno, požiada o prístup k nim v rozsahu uvedenom v článku 15. Prevádzkovateľ požiada o preukaz totožnosti žiadateľa, aby potvrdil jej totožnosť. Postup prevádzkovateľa je v tomto prípade neprimeraný a vedie k zbytočnému zberu údajov.

S cieľom potvrdiť totožnosť žiadateľky a zároveň predísť zbytočnému zberu údajov by však prevádzkovateľ mohol od nej požadovať autentifikáciu prihlásením sa do účtu, alebo jej položiť (nie dotieravé) bezpečnostné otázky, na ktoré by mala vedieť odpovedať iba dotknutá osoba, alebo použiť viacfaktorovú autentifikáciu, ktorá sa nastavila, keď si dotknutá osoba zaregistrovala svoj účet, alebo použiť iné existujúce komunikačné prostriedky, o ktorých je známe, že patria dotknutej osobe, ako je e-mailová adresa alebo telefónne číslo, na poslanie prístupového hesla.

Príklad 14: Klient banky, pán Y, má v úmysle získať spotrebiteľský úver. Na tento účel ide pán Y do pobočky banky, aby získal informácie vrátane svojich osobných údajov, ktoré sú potrebné na posúdenie jeho úverovej bonity. Na overenie totožnosti dotknutej osoby požiada konzultant o notársky overené potvrdenie jej totožnosti, aby jej mohol poskytnúť požadované informácie.

Prevádzkovateľ by nemal požadovať notársky overené potvrdenie totožnosti, pokiaľ to nie je potrebné, vhodné a v súlade s vnútroštátnym právom (napríklad ak osoba dočasne nemá žiadny doklad totožnosti a na vykonanie právneho úkonu sa podľa vnútroštátneho práva vyžaduje doklad totožnosti dotknutej osoby). Takáto prax vystavuje žiadateľov ďalším nákladom a nadmerne zaťažuje dotknuté osoby, čo bráni uplatneniu ich práva na prístup.

78. Bez toho, aby boli dotknuté uvedené všeobecné zásady, za určitých okolností môže byť autentifikácia na základe preukazu totožnosti odôvodneným a primeraným opatrením, najmä v prípade subjektov, ktoré spracúvajú osobitné kategórie osobných údajov, alebo vykonávajú spracúvanie údajov, ktoré môže predstavovať riziko pre dotknutú osobu (napr. lekárske alebo zdravotné informácie). Zároveň však treba mať na pamäti, že niektoré vnútroštátne ustanovenia stanovujú obmedzenia spracúvania údajov obsiahnutých vo verejných listinách vrátane dokladov potvrdzujúcich totožnosť osoby (aj na základe článku 87 všeobecného nariadenia o ochrane údajov). Obmedzenia týkajúce sa spracúvania údajov z týchto preukazov sa môžu týkať najmä skenovania alebo kopírovania preukazov totožnosti alebo spracúvania národných osobných identifikačných čísel³⁹.

³⁹ Niekoľko členských štátov v tejto súvislosti zaviedlo takéto obmedzenie do svojich vnútroštátnych ustanovení, pričom napríklad uviedlo, že vyhotovovanie kópií preukazov totožnosti je zákonné len vtedy, ak priamo vyplýva z ustanovení právneho aktu.

79. Vzhľadom na uvedené musí prevádzkovateľ tam, kde sa požaduje preukaz totožnosti (a je to v súlade s vnútroštátnym právom, ako aj opodstatnené a primerané podľa všeobecného nariadenia o ochrane údajov), zaviesť záruky, aby zabránil nezákonnému spracúvaniu preukazu totožnosti. Bez ohľadu na akékoľvek platné vnútroštátne ustanovenia týkajúce sa autentifikácie preukazu totožnosti to môže zahŕňať zdržať sa kopírovania alebo vymazanie kópie preukazu totožnosti hneď po úspešnej autentifikácii totožnosti dotknutej osoby. Je to preto, že ďalšie uchovávanie kópie preukazu totožnosti pravdepodobne znamená porušenie zásad obmedzenia účelu a minimalizácie uchovávania [článok 5 ods. 1 písm. b) a e) všeobecného nariadenia o ochrane údajov] a okrem toho aj porušenie vnútroštátnych právnych predpisov o spracúvaní národného identifikačného čísla (článok 87 všeobecného nariadenia o ochrane údajov). EDPB ako osvedčený postup odporúča, aby prevádzkovateľ po kontrole preukazu totožnosti urobil poznámku napr. „Preukaz totožnosti bol skontrolovaný“, aby sa predišlo zbytočnému kopírovaniu alebo uchovávaniu kópií preukazov totožnosti.

3.4 Žiadosti podávané prostredníctvom tretích strán/splnomocnení

80. Hoci právo na prístup vo všeobecnosti vykonávajú dotknuté osoby, pokiaľ sa ich týka, je možné, aby v mene dotknutej osoby podala žiadosť tretia strana. Môže sa to okrem iného týkať konania prostredníctvom splnomocnenia alebo právnych zástupcov v mene maloletých osôb, ako aj konania prostredníctvom iných subjektov prostredníctvom online portálov. Za určitých okolností môže byť v náležitých a primeraných situáciách potrebné overiť totožnosť osoby oprávnenej na uplatnenie práva na prístup, ako aj oprávnenie konať v mene dotknutej osoby (pozri oddiel 3.3)⁴⁰. Treba pripomenúť, že sprístupnenie osobných údajov niekomu, kto na ne nemá oprávnenie, môže predstavovať porušenie ochrany osobných údajov [personal data breach]⁴¹.
81. Pritom by sa mali zohľadniť vnútroštátne zákony upravujúce právne zastupovanie (napr. splnomocnenia advokátov), ktorými sa môžu klásť osobitné požiadavky na preukázanie oprávnenia podať žiadosť v mene dotknutej osoby, keďže vo všeobecnom nariadení o ochrane údajov sa táto otázka neupravuje. V súlade so zásadou zodpovednosti, ako aj s inými zásadami v oblasti ochrany údajov musia byť prevádzkovatelia schopní preukázať existenciu príslušného oprávnenia podať žiadosť v mene dotknutej osoby a dostať požadované informácie, okrem prípadov, keď sa vnútroštátne právo líši (napr. vnútroštátne právo obsahuje osobitné pravidlá týkajúce sa dôveryhodnosti právnikov), pričom ponecháva na prevádzkovateľa, aby overil totožnosť splnomocnenca (napr. v prípade právnikov kontrolou ich registrácie v advokátskej komore). Preto sa v tejto súvislosti odporúča zhromaždiť príslušnú dokumentáciu v súvislosti s uvedenými všeobecnými pravidlami týkajúcimi sa potvrdenia totožnosti fyzickej osoby, ktorá podáva žiadosť, a ak má prevádzkovateľ dôvodné pochybnosti o totožnosti osoby konajúcej v mene dotknutej osoby, vyžiada si dodatočné informácie na potvrdenie totožnosti tejto osoby.
82. Zatiaľ čo uplatnenie práva na prístup k osobným údajom zosnulých osôb je ďalším príkladom prístupu tretej strany, ktorá nie je dotknutou osobou, v odôvodnení 27 sa uvádza, že všeobecné nariadenie o ochrane údajov sa nevzťahuje na osobné údaje zosnulých osôb. Vec sa preto rieši podľa vnútroštátneho práva a členské štáty môžu stanoviť pravidlá týkajúce sa spracúvania osobných údajov zosnulých osôb. Netreba však zabúdať na to, že údaje sa môžu okrem toho týkať aj žijúcich tretích osôb,

⁴⁰ Pokiaľ ide o lehoty na uplatnenie práva na prístup, keď prevádzkovateľ potrebuje získať ďalšie informácie, pozri bod 157.

⁴¹ Článok 4 bod 12 všeobecného nariadenia o ochrane údajov.

napr. v kontexte požadovaného prístupu ku korešpondencii zosnulej osoby. Dôvernosc takýchto údajov je stále potrebné chrániť.

3.4.1 Uplatnenie práva na prístup v mene detí

83. Osobitnú ochranu osobných údajov si zasluhujú deti, pretože si môžu byť v menšej miere vedomé rizík, dôsledkov a záruk týkajúcich sa ich práv v súvislosti so spracúvaním osobných údajov⁴². Všetky informácie a každá komunikácia s dieťaťom, pri ktorej sa spracúvajú osobné údaje dieťaťa, by mali byť formulované jasne a jednoducho, aby ich dieťa mohlo ľahko pochopiť⁴³.
84. Deti sú samy osebe dotknuté osoby, a tak právo na prístup patrí dieťaťu. Dieťa môže v závislosti od svojej vyspelosti a spôsobilosti potrebovať tretiu osobu, aby konala v jeho mene, napr. nositeľ rodičovských práv a povinností.
85. Pri všetkých rozhodnutiach prijatých vzhľadom na uplatnenie práva na prístup v súvislosti s deťmi by mali byť prvoradým hľadiskom najlepšie záujmy dieťaťa, najmä ak sa právo na prístup vykonáva v mene dieťaťa, napr. nositeľom rodičovských práv a povinností.
86. Z dôvodu osobitnej ochrany osobných údajov detí, ktorá je súčasťou všeobecného nariadenia o ochrane údajov, prijme prevádzkovateľ primerané opatrenia, aby zabránil akémukoľvek sprístupneniu osobných údajov maloletej osoby neoprávnenej osobe (v tejto súvislosti pozri aj oddiel 3.4 v predchádzajúcom texte).
87. Právo nositeľa rodičovských práv a povinností konať v mene dieťaťa by sa napokon nemalo zamieňať s prípadmi mimo práva v oblasti ochrany údajov, pri ktorých sa vo vnútroštátnych právnych predpisoch môže stanoviť právo nositeľa rodičovských práv a povinností žiadať a dostávať informácie o dieťati (napr. výsledky dieťaťa v škole).

3.4.2 Uplatňovanie práva na prístup prostredníctvom portálov/kanálov poskytovaných treťou stranou

88. Existujú spoločnosti, ktoré poskytujú služby, ktoré umožňujú dotknutým osobám podávať žiadosti o prístup prostredníctvom portálu. Dotknutá osoba sa prihlási a dostane prístup na portál, prostredníctvom ktorého môže napríklad podať rôznym prevádzkovateľom žiadosť o prístup, požiadať ich o opravu údajov alebo vymazanie údajov. Pri používaní portálov poskytovaných treťou stranou vznikajú rôzne problémy.
89. Prvým problémom, ktorý musia prevádzkovatelia riešiť, keď čelia týmto okolnostiam, je zabezpečiť, aby tretia strana konala v mene dotknutej osoby v súlade so zákonom, pretože treba zabezpečiť, aby sa žiadne údaje nesprístupnili neoprávneným stranám.
90. Prevádzkovateľ, ktorý dostane žiadosť podanú prostredníctvom takéhoto portálu, musí okrem toho vybaviť uvedenú žiadosť vždy včas⁴⁴. Prevádzkovateľ však nie je povinný poskytnúť údaje podľa

⁴² Odôvodnenie 38 všeobecného nariadenia o ochrane údajov. Ako sa uvádza v pracovnom programe EDPB, jeho zámerom je poskytnúť usmernenia týkajúce sa údajov detí. Očakáva sa, že takýto dokument poskytne viac usmernení o podmienkach, za ktorých môže dieťa uplatňovať svoje vlastné právo na prístup a nositeľ rodičovských práv a povinností môže právo na prístup uplatňovať v mene dieťaťa.

⁴³ Odôvodnenie 58 všeobecného nariadenia o ochrane údajov. Usmernenia EDPB 05/2020 k súhlasu podľa nariadenia 2016/679, oddiel 7.

⁴⁴ Pokiaľ ide o lehoty na uplatnenie práva na prístup, keď prevádzkovateľ potrebuje získať ďalšie informácie, pozri bod 157.

článku 15 všeobecného nariadenia o ochrane údajov priamo na portál, ak prevádzkovateľ napríklad zistí, že bezpečnostné opatrenia sú nedostatočné alebo že by bolo vhodnejšie použiť iný spôsob sprístupnenia údajov dotknutej osobe. Za takýchto okolností, keď má prevádzkovateľ zavedené iné postupy na vybavovanie žiadostí o prístup účinným a bezpečným spôsobom, môže prevádzkovateľ poskytnúť požadované informácie prostredníctvom týchto postupov.

4 ROZSAH PRÁVA NA PRÍSTUP A OSOBNÉ ÚDAJE A INFORMÁCIE, KTORÝCH SA TÝKA

91. Cieľom tohto oddielu je vysvetliť vymedzenie osobných údajov (oddiel 4.1) a objasniť rozsah informácií, na ktoré sa vo všeobecnosti vzťahuje právo na prístup (oddiely 4.2 a 4.3). Treba poznamenať, že rozsah pojmu osobné údaje, a teda aj rozlišovanie medzi osobnými údajmi a inými údajmi, je neoddeliteľnou súčasťou posúdenia, ktoré prevádzkovateľ vykonáva s cieľom určiť rozsah údajov, ku ktorým má dotknutá osoba právo získať prístup⁴⁵.
92. Na úvod treba pripomenúť, že právo na prístup je možné uplatniť len v súvislosti so spracúvaním osobných údajov, ktoré patria do vecnej a územnej pôsobnosti všeobecného nariadenia o ochrane údajov. Z tohto dôvodu sa osobné údaje, ktoré sa nespracúvajú automatizovanými prostriedkami, alebo ktoré netvoria súčasť informačného systému, alebo nie sú určené na to, aby tvorili súčasť informačného systému podľa článku 2 ods. 1 všeobecného nariadenia o ochrane údajov, alebo ktoré spracúva fyzická osoba v rámci výlučne osobnej alebo domácej činnosti podľa článku 2 ods. 2 všeobecného nariadenia o ochrane údajov, nevzťahuje právo na prístup.

4.1 Vymedzenie pojmu osobné údaje

93. Článok 15 ods. 1 a 3 všeobecného nariadenia o ochrane údajov sa týkajú „osobných údajov“ a „osobných údajov, ktoré sa spracúvajú“. Rozsah práva na prístup je preto v prvom rade určený rozsahom pojmu osobné údaje, ktorý je vymedzený v článku 4 bode 1 všeobecného nariadenia o ochrane údajov⁴⁶. Pojem osobné údaje bol už predmetom viacerých dokumentov⁴⁷ pracovnej skupiny zriadenej podľa článku 29⁴⁸ a jeho výklad podal Súdny dvor EÚ, a to aj v kontexte práva na prístup podľa článku 12 smernice 95/46/ES.

⁴⁵ V súlade so zásadou špecificky navrhutej ochrany údajov, je takáto analýza súčasťou posúdenia primeraných opatrení a záruk na ochranu zásad ochrany údajov a práv dotknutých osôb, ktoré sa vykonáva „v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania“, napr. skrátenie času odozvy, keď dotknuté osoby uplatňujú svoje práva, môže byť jednou z metrik. Ďalšie vysvetlenia sa nachádzajú v usmerneniach 4/2019 týkajúcich sa článku 25 Špecificky navrhnutá a štandardná ochrana údajov.

⁴⁶ Podľa článku 4 bodu 1 všeobecného nariadenia o ochrane údajov „osobné údaje“ sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.“

⁴⁷ Napríklad Usmernenia WP 251 rev01 k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, s. 19; Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 9.

⁴⁸ Pracovná skupina zriadená podľa článku 29 (WP29) je nezávislá európska pracovná skupina, ktorá sa do 25. mája 2018 (začatie uplatňovania všeobecného nariadenia o ochrane údajov) zaoberala otázkami súvisiacimi s ochranou súkromia a osobných údajov a ktorá je predchodcom Európskeho výboru pre ochranu údajov.

94. Pracovná skupina zriadená podľa článku 29 uviedla, že vo vymedzení pojmu osobné údaje v smernici 95/46/ES „sa odráža zámer európskeho zákonodarcu o širší pojem „osobných údajov““⁴⁹. Podľa všeobecného nariadenia o ochrane údajov sa vymedzenie stále vzťahuje na „akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby“. Okrem základných osobných údajov, ako je meno a adresa, telefónne číslo atď., môže do tohto vymedzenia patriť neobmedzený, široký okruh údajov, vrátane lekárskeho zistenia, histórie nákupov, ukazovateľov úverovej bonity, obsahu komunikácie atď. Vzhľadom na široký rozsah vymedzenia osobných údajov by obmedzujúce posúdenie tohto vymedzenia zo strany prevádzkovateľa viedlo k chybnému klasifikácii osobných údajov⁵⁰ a v konečnom dôsledku k porušeniu práva na prístup.
95. Súdny dvor Európskej únie v spojených veciach C-141/12 a C-372/12⁵¹ rozhodol, že právo na prístup sa vzťahuje na osobné údaje uvedené v zázpise, a to „meno, dátum narodenia, štátna príslušnosť, pohlavie, etnická príslušnosť, vierovyznanie a jazyk žiadateľa“ a „prípadne takéto údaje nachádzajúce sa v právnej analýze v nej obsiahnutej“, ale nie na samotnú právnu analýzu ako takú⁵². Právna analýza nebola v tejto súvislosti sama osebe predmetom kontroly jej správnosti dotknutou osobou ani predmetom opravy. Okrem toho poskytnutie prístupu k právnej analýze neplní účel zaručenia súkromia, ale prístupu k administratívnym dokumentom.
96. Súdny dvor Európskej únie vo veci Nowak⁵³ vykonal širšiu analýzu a zistil, že písomné odpovede uchádzača na odbornej skúške a prípadné poznámky skúšajúceho, ktoré sa vzťahujú k odpovediam, predstavujú osobné údaje týkajúce sa uchádzača na skúške. Presnejšie povedané, takéto subjektívne informácie sú osobnými údajmi „vo forme názoru alebo hodnotení pod podmienkou, že sa „týkajú“ dotknutej osoby“⁵⁴ na rozdiel od skúšobných otázok, ktoré sa nepovažujú za osobné údaje⁵⁵. Kontextovým posúdením by sa teda mal objasniť účinok alebo výsledok, ktorý informácia môže mať na fyzickú osobu, a teda aj na rozsah práva na prístup.

Príklad 15: Fyzická osoba má pracovný pohovor v spoločnosti. V tejto súvislosti uchádzač o zamestnanie odovzdá životopis a žiadosť o zamestnanie. Počas pohovoru si personalista robí poznámky do počítača, aby zdokumentoval pohovor. Potom uchádzač o zamestnanie ako dotknutá osoba požiada o prístup k osobným údajom, ktoré sa ho týkajú a ktoré podnik ako prevádzkovateľ zhromaždil v priebehu náborového procesu.

Prevádzkovateľ je povinný poskytnúť dotknutej osobe osobné údaje, ktoré mu aktívne oznámila vo svojom životopise a žiadosti o zamestnanie. Prevádzkovateľ musí okrem toho poskytnúť dotknutej osobe zhrnutie pohovoru vrátane subjektívnych poznámok k správaniu dotknutej osoby, ktoré personalista zaznamenal počas pracovného pohovoru, s výhradou akýchkoľvek výnimiek podľa vnútroštátneho práva a v súlade s článkom 23 všeobecného nariadenia o ochrane údajov.

⁴⁹ Stanovisko 4/2007 WP29 k pojmu osobné údaje, s. 4.

⁵⁰ Ako informácia, ktorá sa netýka identifikovanej alebo identifikovateľnej fyzickej osoby.

⁵¹ Rozsudok Súdneho dvora zo 17. júla 2014, YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S, spojené veci C-141/12 a C-372/12.

⁵² Rozsudok Súdneho dvora, YS a i., spojené veci C-141/12 a C-372/12, body 38 a 48.

⁵³ Rozsudok Súdneho dvora z 20. decembra 2017, Peter Nowak/Data Protection Commissioner, C-434/16.

⁵⁴ Rozsudok Súdneho dvora, Nowak, C-434/16, body 34 – 35.

⁵⁵ Rozsudok Súdneho dvora, Nowak, C-434/16, bod 58.

97. Takže, s ohľadom na konkrétne okolnosti prípadu, pri posudzovaní konkrétnej žiadosti o prístup majú prevádzkovatelia okrem iného poskytovať tieto druhy údajov bez toho, aby bol dotknutý článok 15 ods. 4 všeobecného nariadenia o ochrane údajov:

- osobitné kategórie osobných údajov podľa článku 9 všeobecného nariadenia o ochrane údajov,
- osobné údaje týkajúce sa uznania viny za trestné činy a priestupky podľa článku 10 všeobecného nariadenia o ochrane údajov,
- údaje vedome a aktívne poskytnuté dotknutou osobou (napr. údaje o konte predložené prostredníctvom formulárov, odpovede na dotazník)⁵⁶,
- pozorované údaje [observed data] alebo nespracované údaje [raw data] poskytnuté dotknutou osobou na základe využívania služby alebo zariadenia (napr. údaje spracúvané vzájomne prepojenými objektmi, história transakcií, záznamy o činnosti [activity logs], ako sú evidencia prístupov, história používania webového sídla, vyhľadávacie činnosti, údaje o polohe, klikanie, jedinečné aspekty správania osoby, ako je rukopis, stláčanie kláves, konkrétny spôsob chôdze alebo reči)⁵⁷,
- údaje odvodené [derived] z iných údajov, namiesto údajov, ktoré by priamo poskytla dotknutá osoba (napr. úverový pomer, klasifikácia na základe spoločných znakov dotknutých osôb, krajina bydliska odvodená z PSČ)⁵⁸,
- údaje vyvodené [inferred] z iných údajov, namiesto údajov, ktoré by priamo poskytla dotknutá osoba (napr. na účely pridelenia úverového hodnotenia alebo dodržania predpisov v oblasti boja proti praniu špinavých peňazí, algoritmické výsledky, výsledky posúdenia zdravotného stavu alebo proces personalizácie alebo odporúčaní)⁵⁹,
- pseudonymizované údaje na rozdiel od anonymizovaných údajov (pozri aj oddiel 3 týchto usmernení).

Príklad 16: Prvky, ktoré sa použili na rozhodnutie napr. o povýšení zamestnanca, zvýšení odmeny alebo novom pracovnom zaradení (napr. výročné preskúmanie výkonnosti, žiadosti o odbornú prípravu, disciplinárne záznamy, hodnotenie, kariérny potenciál), sú osobné údaje týkajúce sa uvedeného zamestnanca. Takže dotknutá osoba má k týmto prvkom prístup na požiadanie a pri dodržaní článku 15 ods. 4 všeobecného nariadenia o ochrane údajov v prípade, že sa osobné údaje napríklad týkajú aj inej fyzickej osoby (napr. totožnosť alebo prvky odhaľujúce totožnosť iného zamestnanca, ktorého svedectvo o profesionálnom výkone je zahrnuté vo výročnom preskúmaní výkonnosti, môžu podliehať obmedzeniam podľa článku 15 ods. 4 všeobecného nariadenia o ochrane údajov, a preto je možné, že ich nebude možné oznámiť dotknutej osobe z dôvodu ochrany práv a slobôd uvedeného zamestnanca). Napriek tomu sa môžu uplatňovať ustanovenia vnútroštátneho pracovného práva, napríklad pokiaľ ide o prístup zamestnancov k osobným spisom alebo iné vnútroštátne ustanovenia, ako sú napríklad ustanovenia o služobnom tajomstve. Takéto obmedzenia uplatnenia práva na prístup dotknutej osoby (alebo iných práv) stanovené vo vnútroštátnom práve musia za každých okolností spĺňať podmienky článku 23 všeobecného nariadenia o ochrane údajov (pozri oddiel 6.4).

⁵⁶ Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 9.

⁵⁷ Stanovisko 4/2007 WP29 k pojmu osobné údaje, s. 8.

⁵⁸ Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 10 – 11.

⁵⁹ Usmernenia WP 29 k právu na prenosnosť údajov – schválené EDPB, s. 10 – 11; Pracovná skupina zriadená podľa článku 29, WP 251 rev.01, 6. februára 2018, Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679 – schválené Európskym výborom pre ochranu údajov (ďalej len „usmernenia WP29 k automatizovanému individuálnemu rozhodovaniu a profilovaniu – schválené EDPB“), s. 9 – 10.

98. Z uvedeného neúplného zoznamu osobných údajov, ktoré možno dotknutej osobe poskytnúť v rámci žiadosti o prístup, možno vyvodiť niekoľko úvah. Z uvedeného je zrejmé, že prevádzkovateľ nesmie pri poskytovaní prístupu k osobným údajom rozlišovať medzi údajmi, ktoré sa nachádzajú v papierových spisoch, a údajmi, ktoré sa uchovávajú elektronicky, pokiaľ patria do pôsobnosti všeobecného nariadenia o ochrane údajov. Inými slovami, na osobné údaje, ktoré sa nachádzajú v papierových spisoch ako súčasť informačného systému alebo ktoré sú určené na to, aby tvorili súčasť informačného systému, sa vzťahuje právo na prístup rovnakým spôsobom ako na osobné údaje uložené v pamäti počítača napríklad prostredníctvom binárneho kódu alebo videopásky.
99. Právo na prístup, ako väčšina práv dotknutej osoby, okrem toho zahŕňa vyodené, ako aj odvodené údaje vrátane osobných údajov vytvorených poskytovateľom služieb, zatiaľ čo právo na prenosnosť údajov zahŕňa iba údaje poskytnuté dotknutou osobou⁶⁰. Preto v prípade žiadosti o prístup a na rozdiel od žiadosti o prenosnosť údajov by sa dotknutej osobe mali poskytnúť nielen osobné údaje poskytnuté prevádzkovateľovi na účely následnej analýzy alebo posúdenia týchto údajov, ale aj výsledok každej takejto následnej analýzy alebo posúdenia.
100. Je takisto dôležité pripomenúť, že existujú informácie, ako sú anonymné údaje⁶¹, čo sú údaje, ktoré sa priamo ani nepriamo netýkajú identifikovateľnej osoby, a preto sú vylúčené z rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov. Osobným údajom nie je napríklad umiestnenie servera, na ktorom sa spracúvajú osobné údaje dotknutej osoby. Rozlišovanie môže byť náročné a prevádzkovatelia môžu uvažovať nad tým, ako urobiť jasnú hranicu medzi osobnými a inými ako osobnými údajmi, najmä v prípade zmiešaných dátových súborov. V takomto prípade môže byť užitočné rozlišovať medzi zmiešanými dátovými súborami, v ktorých sú osobné a iné ako osobné údaje neoddeliteľne spojené, a tými, v ktorých to tak nie je. Osobné a iné ako osobné údaje môžu byť neoddeliteľne spojené v zmiešaných dátových súboroch a v úplnosti patria do rozsahu práva na prístup dotknutej osoby, ktorej sa osobné údaje týkajú⁶². V ostatných prípadoch nemusia byť osobné a iné ako osobné údaje v zmiešaných dátových súboroch neoddeliteľne spojené, čím sa dotknutej osobe sprístupnia iba osobné údaje v súbore. Spoločnosť môže napríklad potrebovať poskytnúť dotknutej osobe jednotlivé správy o IT incidentoch, ktoré táto osoba vyvolala, ale nie vedomostnú databázu IT problémov spoločnosti. Aké bezpečnostné opatrenia prevádzkovateľ zaviedol, však vo všeobecnosti nemožno chápať ako osobné údaje, a to za predpokladu, že nie sú neoddeliteľne spojené s osobnými údajmi, a preto sa na ne nevzťahuje právo na prístup.
101. Na záver tohto oddielu EDPB v tejto súvislosti pripomína, že ochrana fyzických osôb pri spracúvaní osobných údajov zahŕňa všetky druhy osobných údajov uvedené v predchádzajúcom texte a že reštriktívny výklad ich vymedzenia je v rozpore s ustanoveniami všeobecného nariadenia o ochrane údajov a v konečnom dôsledku porušuje článok 8 Charty základných práv. Použitie odlišného režimu na uplatnenie práva vo vzťahu k niektorým druhom osobných údajov, s ktorým sa vo všeobecnom nariadení o ochrane údajov nepočíta, je možné zaviesť výlučne právnym predpisom, a to v súlade s článkom 23 všeobecného nariadenia o ochrane údajov (ako sa ďalej vysvetľuje v oddiele 6.4).

⁶⁰ Ako už bolo uvedené v usmerneniach WP 29 k právu na prenosnosť údajov – schválených EDPB, s. 10, a zopakované v usmerneniach WP29 k automatizovanému individuálnemu rozhodovaniu a profilovaniu – schválených EDPB, s. 17.

⁶¹ Ďalšie vysvetlenia týkajúce sa pojmu anonymizácia možno nájsť v stanovisku 5/2014 pracovnej skupiny zriadenej podľa článku 29 k technikám anonymizácie, WP 216, 10. apríla 2014, s. 5 – 19.

⁶² Oznámenie Komisie Európskemu parlamentu a Rade, Usmernenie k nariadeniu o rámci pre voľný tok iných ako osobných údajov v Európskej únii, 29.5.2019 [COM(2019) 250 final].

Prevádzkovatelia teda nemôžu obmedziť uplatnenie práva na prístup neprimeraným obmedzením rozsahu osobných údajov.

4.2 Osobné údaje, ktorých sa týka právo na prístup

102. Podľa článku 15 ods. 1 všeobecného nariadenia o ochrane údajov „dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie“ (zvýraznenie doplnené).
103. Z článku 15 ods. 1 všeobecného nariadenia o ochrane údajov vyplýva niekoľko prvkov. V uvedenom odseku sa výslovne spomínajú „osobné údaje, ktoré sa jej týkajú“ (oddiel 4.2.1), ktoré „sa spracúvajú“ (oddiel 4.2.2) zo strany prevádzkovateľa:

4.2.1 „Osobné údaje, ktoré sa týkajú dotknutej osoby“

104. Právo na prístup možno uplatniť výlučne vzhľadom na osobné údaje týkajúce sa dotknutej osoby, ktorá žiada o prístup, prípadne prostredníctvom oprávnenej osoby alebo splnomocnenca (pozri oddiel 3.4). Existujú aj situácie, keď údaje nesúvisia s osobou uplatňujúcou právo na prístup, ale s inou fyzickou osobou. Dotknutá osoba však má právo len na osobné údaje, ktoré sa týkajú jej samej, z čoho sú vylúčené údaje, ktoré sa týkajú výlučne niekoho iného⁶³.
105. Klasifikácia údajov ako osobných údajov týkajúcich sa dotknutej osoby však nezávisí od skutočnosti, že sa uvedené osobné údaje týkajú aj niekoho iného⁶⁴. Je teda možné, že osobné údaje sa súčasne týkajú viac ako jednej fyzickej osoby. To automaticky neznamená, že by sa mal udeliť prístup k osobným údajom, ktoré sa týkajú aj niekoho iného, keďže prevádzkovateľ musí dodržiavať článok 15 ods. 4 všeobecného nariadenia o ochrane údajov.
106. Slová „osobné údaje, ktoré sa jej týkajú“ by prevádzkovatelia nemali vykladať „príliš reštriktívne“, ako už uviedla pracovná skupina zriadená podľa článku 29 s ohľadom na právo na prenosnosť údajov⁶⁵. Pokiaľ ide o právo na prístup, EDPB sa domnieva, že napríklad nahrávky telefonických rozhovorov (a ich prepis) medzi dotknutou osobou, ktorá žiada o prístup, a prevádzkovateľom môžu patriť pod právo na prístup za predpokladu, že ide o osobné údaje⁶⁶. Za predpokladu, že sa uplatňuje všeobecné nariadenie

⁶³ Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 9: „Do rozsahu pôsobnosti žiadosti o uplatnenie práva na prenosnosť údajov patria iba osobné údaje. Všetky údaje, ktoré sú anonymné alebo ktoré sa netýkajú dotknutej osoby, teda do rozsahu pôsobnosti žiadosti nepatria. Do tohto rozsahu však patria pseudonymné údaje, ktoré možno jednoznačne dať do súvisu s dotknutou osobou (napr. keď táto osoba poskytne príslušné informácie umožňujúce jej identifikáciu, pozri článok 11 ods. 2).“

⁶⁴ Rozsudok Súdneho dvora z 20. decembra 2017, Peter Nowak/Data Protection Commissioner, C-434/16, bod 44.

⁶⁵ Usmernenia WP29 k právu na prenosnosť údajov – schválené EDPB, s. 9: „V mnohých prípadoch budú prevádzkovatelia spracúvať informácie, ktoré obsahujú osobné údaje niekoľkých dotknutých osôb. Ak takáto situácia nastane, prevádzkovatelia by nemali uplatňovať príliš reštriktívny výklad vety ‚osobné údaje, ktoré sa týkajú dotknutej osoby‘. Napríklad súčasťou záznamov o telefónnych hovoroch, správach medzi osobami alebo záznamov o internetovej telefónii môžu byť (v histórii účastníkovho konta) údaje o tretích stranách zapojených do prichádzajúcich a odchádzajúcich hovorov. Hoci záznamy budú tým pádom obsahovať osobné údaje týkajúce sa viacerých ľudí, účastníci by mali mať možnosť získať tieto záznamy v rámci odpovede na žiadosť o uplatnenie práva na prenosnosť údajov, pretože sa (tiež) týkajú dotknutej osoby. Ak však budú tieto záznamy následne prenesené novému prevádzkovateľovi, nový prevádzkovateľ by ich nemal spracúvať na akýkoľvek účel, ktorý by mal nepriaznivé dôsledky na práva a slobody tretích strán (pozri ďalej: tretia podmienka).“

⁶⁶ Pozri príklad 34 v oddiele 6.2.

o ochrane údajov a na spracúvanie sa nevzťahuje výnimka pre domáce činnosti podľa článku 2 ods. 2 písm. c) všeobecného nariadenia o ochrane údajov, ak dotknutá osoba použije získaný záznam, ktorý obsahuje osobné údaje účastníka konania, na iné účely, napríklad zverejnením záznamu, stane sa dotknutá osoba prevádzkovateľom pre toto spracúvanie osobných údajov týkajúcich sa druhej osoby, ktorej hlas sa zaznamenal. Hoci sa tým prevádzkovateľ neoslobodí od svojej povinnosti v oblasti ochrany údajov, pri náležitej analýze, či možno poskytnúť prístup k úplnému záznamu, sa prevádzkovateľovi odporúča, aby informoval dotknutú osobu o skutočnosti, že sa v takom prípade môže stať prevádzkovateľom. Tým nie je dotknuté ďalšie posudzovanie podľa článku 15 ods. 4 všeobecného nariadenia o ochrane údajov, ktoré je podrobne opísané v oddiele 6. V tom istom zmysle môžu pod právo na prístup patriť aj správy, ktoré dotknuté osoby poslali iným vo forme osobných správ a samy ich vymazali zo svojho zariadenia, a ktoré sú stále k dispozícii poskytovateľovi služieb.

107. Na druhej strane existujú situácie, v ktorých sa prepojenie medzi údajmi a niekoľkými fyzickými osobami môže prevádzkovateľovi zdať nejasné, ako napríklad v prípade krádeže totožnosti. V prípade krádeže totožnosti, jedna osoba podvodne koná v mene inej osoby. V tejto súvislosti je dôležité pripomenúť, že obeti by sa mali poskytnúť informácie o všetkých osobných údajoch, ktoré prevádzkovateľ uchováva v spojení s jej totožnosťou vrátane tých, ktoré sa zhromaždili na základe konania páchatela. Inými slovami, aj po tom, čo sa prevádzkovateľ dozvedel o krádeži totožnosti, osobné údaje, ktoré sú spojené s totožnosťou obete, alebo s ňou súvisia, sú osobnými údajmi dotknutej osoby.

Príklad 17: Fyzická osoba podvodne používa identitu niekoho iného, aby mohla hrať online poker. Páchatel platí online kasínu kreditnou kartou, ktorú ukradol obeti. Keď obeť zistí krádež totožnosti, požiadala poskytovateľa online kasína, aby jej poskytol prístup k jej osobným údajom, a konkrétnejšie, k odohraným online hrám a informáciám o kreditnej karte, ktorú páchatel použil.

Medzi zhromaždenými údajmi a obeťou existuje prepojenie, keďže sa použila totožnosť obete. Po zistení podvodu majú uvedené osobné údaje stále prepojenie z dôvodu svojho obsahu (kreditná karta obete je jednoznačne o obeti), účelu a účinku (informácie o online hrách, ktoré páchatel odohral, sa môžu napríklad použiť na vystavenie faktúr obeti). Online kasíno preto poskytne obeti prístup k uvedeným osobným údajom.

108. Ak je to vhodné, interné záznamy o pripojení [internal connection logs] možno použiť na uchovávanie záznamov o prístupoch k súboru a na spätné sledovanie aktivít vykonaných v súvislosti s prístupmi k záznamu, ako je tlač, kopírovanie alebo vymazanie osobných údajov. Tieto záznamy môžu obsahovať čas prihlásenia, dôvod prístupu k súboru, ako aj informácie identifikujúce osobu, ktorá mala prístup. Otázky súvisiace s touto témou sú predmetom vecí, v ktorej v súčasnosti rozhoduje Súdny dvor Európskej únie (C-579/21). Zavedenie a kontrola a revízia záznamov o pripojení patrí do zodpovednosti prevádzkovateľa a podlieha kontrole zo strany dozorných orgánov. Prevádzkovateľ by tak mal preveriť, že osoby konajúce na základe jeho oprávnenia, ktoré majú prístup k osobným údajom, nespracúvajú osobné údaje s výnimkou pokynov prevádzkovateľa podľa článku 29 všeobecného nariadenia o ochrane údajov. Ak daná osoba napriek tomu spracúva osobné údaje na iné účely, ako je plnenie pokynov prevádzkovateľa, môže sa stať prevádzkovateľom tohto spracúvania a podliehať disciplinárnemu alebo trestnému konaniu alebo správny sankciám zo strany dozorných orgánov. EDPB upozorňuje na to, že zamestnávateľ podľa článku 24 všeobecného nariadenia o ochrane údajov je zodpovedný za to, aby používal primerané opatrenia siahajúce od vzdelávania až po disciplinárne konania s cieľom zabezpečiť, že spracúvanie je v súlade so všeobecným nariadením o ochrane údajov a že nedochádza k žiadnemu porušovaniu.

4.2.2 Osobné údaje, ktoré „sa spracúvajú“

109. Článok 15 ods. 1 všeobecného nariadenia o ochrane údajov sa navyše vzťahuje na osobné údaje, ktoré „sa spracúvajú“. Referenčnému časovému bodu na určenie rozsahu osobných údajov, ktoré patria do žiadosti o prístup, sa venovala pozornosť v oddiele 2.3.3. Zo znenia však takisto vyplýva, že v práve na prístup sa nerozlišuje medzi účelmi spracovateľských operácií.

Príklad 18: Spoločnosť spracúvala osobné údaje týkajúce sa dotknutej osoby s cieľom spracovania objednávky a zabezpečenia dopravy na adresu bydliska dotknutej osoby. Po tom, čo tieto prvotné účely, na ktoré sa osobné údaje zhromaždili, už neexistujú, prevádzkovateľ uchováva niektoré z osobných údajov výlučne na splnenie svojich zákonných povinností týkajúcich sa vedenia evidencie.

Dotknutá osoba požiada o prístup k osobným údajom, ktoré sa jej týkajú. Na to, aby prevádzkovateľ splnil svoju povinnosť podľa článku 15 ods. 1 všeobecného nariadenia o ochrane údajov, musí dotknutej osobe poskytnúť požadované osobné údaje, ktoré sa uchovávajú, aby splnil svoje zákonné povinnosti.

110. Archivované osobné údaje treba odlišiť od zálohovaných údajov, ktoré sú osobnými údajmi uchovávanými výlučne na účely obnovy údajov v prípade straty údajov. Treba zdôrazniť, že vzhľadom na zásady špecificky navrhutej ochrany údajov a minimalizácie údajov sú zálohované údaje v podstate podobné údajom v živom systéme. Ak existujú malé rozdiely medzi osobnými údajmi v zálohe a v živom produkčnom systéme, tieto rozdiely sú vo všeobecnosti spojené so zhromažďovaním dodatočných údajov od posledného zálohovania. Zníženie množstva údajov v živom systéme (napr. vymazanie niektorých údajov po uplynutí obdobia uchovávania alebo po žiadosti o vymazanie) sa v niektorých prípadoch prepíše v zálohovaných údajoch iba v čase následného zálohovania. V prípade, že existuje žiadosť o prístup v momente, keď je zálohovaných viac osobných údajov týkajúcich sa dotknutej osoby ako v živom systéme alebo osobné údaje sa rôznia (pozorovateľné napríklad prostredníctvom záznamu o vymazaní v živom produkčnom systéme vykonanom v úplnom súlade so zásadou minimalizácie údajov), prevádzkovateľ musí byť v tejto situácii transparentný, a ak je to technicky možné, musí poskytnúť prístup, ako ho požaduje dotknutá osoba, vrátane prístupu k osobným údajom uchovávaným v zálohe. Napríklad s cieľom byť transparentný voči dotknutým osobám, ktoré si uplatňujú svoje právo, môže záznam o vymazaní v živom produkčnom systéme umožniť prevádzkovateľovi zistiť, že v zálohe sú údaje, ktoré už nie sú v živom systéme, pretože boli nedávno vymazané a ešte sa v zálohe neprepísali.

4.2.3 Rozsah novej žiadosti o prístup

111. Zostáva povedať, že dotknuté osoby majú právo na prístup k všetkým spracúvaným údajom, ktoré sa ich týkajú, alebo k častiam týchto údajov, a to v závislosti od rozsahu žiadosti (pozri aj oddiel 2.3.1 o úplnosti informácií a oddiel 3.1.1 ako analyzovať obsah žiadosti). V dôsledku toho, ak prevádzkovateľ už v minulosti vyhovel žiadosti o prístup, a za predpokladu, že žiadosť nie je neprimeraná, prevádzkovateľ nemôže zúžiť rozsah tejto novej žiadosti. Znamená to, že vo vzťahu k akejkoľvek ďalšej žiadosti o prístup tej istej dotknutej osoby by prevádzkovateľ nemal informovať dotknutú osobu iba o bežných zmenách spracúvaných osobných údajov alebo o samotnom spracúvaní od poslednej žiadosti, pokiaľ dotknutá osoba s tým výslovne nesúhlasí. V opačnom prípade by dotknuté osoby boli povinné zhromažďovať svoje poskytnuté osobné údaje s cieľom vytvoriť úplný súbor osobných údajov týkajúci sa ich informácií o spracúvaní a o právach dotknutých osôb.

4.3 Informácie o spracúvaní údajov a o právach dotknutých osôb

112. Okrem samotného prístupu k osobným údajom má prevádzkovateľ poskytnúť informácie o spracúvaní a o právach dotknutej osoby podľa článku 15 ods. 1 písm. a) až h) a článku 15 ods. 2 všeobecného nariadenia o ochrane údajov. Väčšina informácií o týchto konkrétnych bodoch je už zhromaždená, aspoň vo všeobecnej forme, a to v zázname prevádzkovateľa o spracovateľských činnostiach uvedenom v článku 30 všeobecného nariadenia o ochrane údajov a/alebo v jeho oznámení o ochrane osobných údajov vypracovanom v súlade s článkami 12 až 14 všeobecného nariadenia o ochrane údajov. Preto ako prvý krok môže byť užitočné nahliadnuť do Usmernení pracovnej skupiny zriadenej podľa článku 29 k transparentnosti podľa nariadenia 2016/679⁶⁷ týkajúcich sa obsahu informácií, ktoré sa majú poskytovať podľa článkov 13 a 14 všeobecného nariadenia o ochrane údajov.
113. V záujme dosiahnutia súladu s článkom 15 ods. 1 písm. a) až h) a článkom 15 ods. 2 môžu prevádzkovatelia s opatrnosťou použiť textové moduly svojho oznámenia o ochrane osobných údajov, pokiaľ zabezpečia, aby boli s ohľadom na požiadavku dotknutej osoby aktuálne a presné. Pred spracúvaním údajov alebo na začiatku ich spracúvania často ešte nie je možné poskytnúť niektoré informácie, ako napríklad identifikáciu konkrétnych príjemcov alebo konkrétnu dĺžku trvania spracúvania údajov. Niektoré informácie, ako napríklad právo podať sťažnosť dozornému orgánu [pozri článok 15 ods. 1 písm. f)], sa nemenia v závislosti od osoby, ktorá žiada o prístup. Preto sa môžu oznamovať všeobecným spôsobom, ako to je aj v oznámení o ochrane osobných údajov. Iné typy informácií, ako napríklad informácie o príjemcoch, kategóriách a zdroji údajov, sa môžu líšiť v závislosti od toho, kto podáva žiadosť a aký je rozsah žiadosti. V rámci žiadosti o prístup podľa článku 15 preto možno bude potrebné aktualizovať akékoľvek informácie o spracúvaní, ktoré má prevádzkovateľ k dispozícii a prispôbiť na účely spracovateľských operácií, ktoré sa skutočne vykonávajú v súvislosti so žiadosťou dotknutej osoby. Odvolávanie sa na znenie svojich zásad ochrany osobných údajov by teda nebolo pre prevádzkovateľa dostatočným spôsobom, ako poskytnúť informácie požadované podľa článku 15 ods. 1 písm. a) až h) a článku 15 ods. 2, pokiaľ „prispôsobené a aktualizované“ informácie nie sú rovnaké ako informácie poskytnuté na začiatku spracúvania. Pri vysvetľovaní toho, ktoré informácie sa týkajú žiadateľa, by sa prevádzkovateľ mohol v prípade potreby odvolať na určité činnosti (napríklad „ak ste využili túto službu...“, „ak ste zaplatili faktúrou“), pokiaľ je to pre dotknutú osobu zrejmé, ak sa ich to týka. Ďalej je vysvetlená miera špecifikácie požadovaná vo vzťahu k jednotlivým typom informácií.
114. Informácie o účeloch podľa článku 15 ods. 1 písm. a) musia byť konkrétne, pokiaľ ide o presný účel (účely) v skutočnom prípade žiadajúcej dotknutej osoby. Nestačilo by vymenovať všeobecné účely prevádzkovateľa bez objasnenia, ktorý účel (účely) prevádzkovateľ sleduje v aktuálnom prípade žiadajúcej dotknutej osoby. Ak sa spracúvanie vykonáva na niekoľko účelov, prevádzkovateľ musí objasniť, ktoré údaje alebo ktoré kategórie údajov sa spracúvajú na aký účel (účely). Na rozdiel od článku 13 ods. 1 písm. c) a článku 14 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov informácie o spracúvaní uvedené v článku 15 ods. 1 písm. a) neobsahujú informácie o právnom základe spracúvania. Keďže však niektoré práva dotknutých osôb závisia od platného právneho základu, tieto informácie sú pre dotknuté osoby dôležité na overenie zákonnosti spracúvania údajov a na určenie toho, ktoré práva dotknutej osoby sa v konkrétnej situácii uplatňujú. S cieľom uľahčiť výkon práv dotknutých osôb v súlade s článkom 12 ods. 2 všeobecného nariadenia o ochrane údajov sa teda prevádzkovateľovi odporúča informovať dotknutú osobu aj o príslušnom právnom základe pre každú spracovateľskú operáciu alebo uviesť, kde môže tieto informácie nájsť. V každom prípade sa na základe zásady transparentného spracúvania vyžaduje, aby informácie o právnych základoch

⁶⁷ Pracovná skupina zriadená podľa článku 29, WP 260 rev.01, 11. apríla 2018, Usmernenia k transparentnosti podľa nariadenia 2016/679 – schválené EDPB (ďalej len „usmernenia WP29 k transparentnosti – schválené EDPB“).

spracúvania boli poskytované dotknutej osobe dostupným spôsobom (napríklad v oznámení o ochrane osobných údajov).

115. Informácie o kategóriách údajov [článok 15 ods. 1 písm. b)] bude možno takisto potrebné prispôbiť situácii dotknutej osoby tak, že kategórie, ktoré sa ukázali ako nepodstatné v prípade žiadateľa, by sa mali odstrániť.

Príklad 19: V kontexte informácií uvedených v článkoch 13 a 14 všeobecného nariadenia o ochrane údajov hotel uvádza, že spracúva niekoľko kategórií údajov o zákazníkoch (identifikačné údaje, kontaktné údaje, bankové údaje, číslo kreditnej karty atď.). Ak sa žiadosť o prístup podáva na základe článku 15, dotknutá osoba, ktorá podáva žiadosť, musí byť okrem prístupu k samotným spracúvaným údajom (zložka 2) v súlade s článkom 15 ods. 1 písm. b) informovaná aj o konkrétnych kategóriách údajov, ktoré sa v konkrétnom prípade spracúvajú (napr. neuvedenie bankových údajov alebo údajov o kreditnej karte v prípade, že platba bola vykonaná v hotovosti).

116. Pri informáciách o „príjemcoch alebo kategóriách príjemcov“ [článok 15 ods. 1 písm. c)] sa v prvom rade musí zohľadňovať vymedzenie pojmu príjemca uvedené v článku 4 bode 9 všeobecného nariadenia o ochrane údajov. Vymedzenie pojmu príjemca vychádza z poskytovania osobných údajov fyzickej alebo právnickej osobe, orgánu verejnej moci, agentúre alebo inému orgánu⁶⁸. Z článku 4 bodu 9 všeobecného nariadenia o ochrane údajov vyplýva, že orgány verejnej moci konajúce v rámci konkrétneho zisťovania, na ktoré sa vzťahujú osobitné vnútroštátne predpisy, sa nepovažujú za príjemcov.
117. Pokiaľ ide o otázku, či si prevádzkovateľ môže slobodne vybrať medzi informáciami o príjemcoch alebo o kategóriách príjemcov, treba poznamenať, že „na rozdiel od článkov 13 a 14 všeobecného nariadenia o ochrane údajov, ktoré stanovujú povinnosť prevádzkovateľa (...), článok 15 všeobecného nariadenia o ochrane údajov stanovuje skutočné právo na prístup v prospech dotknutej osoby, pričom dotknutá osoba musí mať na výber, či chce získať, ak je to možné, informácie o konkrétnych príjemcoch, ktorým boli alebo budú uvedené údaje poskytnuté, alebo informácie o kategóriách príjemcov.“⁶⁹ Zároveň treba pripomenúť, ako je uvedené v spomínaných usmerneniach k transparentnosti⁷⁰, už podľa článkov 13 a 14 všeobecného nariadenia o ochrane údajov by informácie o príjemcoch alebo kategóriách príjemcov mali byť čo najkonkrétnejšie, s ohľadom na zásady transparentnosti a spravodlivosti. Podľa článku 15, ak si dotknutá osoba nezvolila inak, prevádzkovateľ je povinný uviesť skutočných príjemcov, iba ak nie je možné týchto príjemcov identifikovať alebo ak prevádzkovateľ nepreukáže, že žiadosti dotknutej osoby o prístup sú zjavne neopodstatnené alebo neprimerané v zmysle článku 12 ods. 5 všeobecného nariadenia o ochrane údajov^{71 72}. EDPB v tejto súvislosti pripomína, že uchovávanie informácií týkajúcich sa skutočných príjemcov je okrem iného potrebné na splnenie povinností prevádzkovateľa podľa článku 5 ods. 2 a článku 19 všeobecného nariadenia o ochrane údajov.

⁶⁸ Ďalej treba poznamenať, že rôzni prevádzkovatelia v zmysle vymedzenia v článku 4 bode 7 všeobecného nariadenia o ochrane údajov môžu existovať v rámci tej istej spoločnosti. V tejto konštelácii je možné poskytnutie údajov od jedného príjemcu druhému v rámci jednej spoločnosti.

⁶⁹ Rozsudok Súdneho dvora, Österreichische Post AG, C-154/21, bod 36.

⁷⁰ Pracovná skupina zriadená podľa článku 29, WP 260 rev.01, 11. apríla 2018, Usmernenia k transparentnosti podľa nariadenia 2016/679 – schválené EDPB (ďalej len „usmernenia WP29 k transparentnosti – schválené EDPB“), s. 37 (príloha).

⁷¹ Rozsudok Súdneho dvora, Österreichische Post AG, C-154/21.

⁷² Samotná skutočnosť, že údaje boli poskytnuté veľkému počtu príjemcov, by sama osebe nespôsobila, že žiadosť bude neprimeraná, pozri oddiel 6 bod 188.

Príklad 20: Zamestnávateľ vo svojom oznámení o ochrane osobných údajov informuje o tom, ktoré kategórie údajov sa v súlade s článkom 13 ods. 1 písm. e) a článkom 14 ods. 1 písm. e) všeobecného nariadenia o ochrane údajov odovzdávajú „cestovným kanceláriám“ alebo „hotelom“ v prípade služobných ciest. Ak zamestnanec požiada o prístup k osobným údajom po vykonaní služobnej cesty, zamestnávateľ by mal následne, pokiaľ ide o príjemcov osobných údajov podľa článku 15 ods. 1 písm. c), vo svojej odpovedi uviesť cestovnú kanceláriu a hotel, ktoré údaje prijali. Zatiaľ čo zamestnávateľ vo svojom oznámení o ochrane osobných údajov legitímne spomína kategórie príjemcov podľa článkov 13 a 14, pretože v tejto fáze ešte nebolo možné menovať príjemcov, mal by, pokiaľ zamestnanec ne zvolil inak, uviesť informácie o konkrétnych príjemcoch (názvy cestovných kancelárií, hotelov atď.), keď zamestnanec podáva žiadosť o prístup.

Ak prevádzkovateľ pri dodržaní vyššie uvedených podmienok, môže poskytnúť iba kategórie príjemcov, informácie by mali byť čo najkonkrétnejšie s uvedením typu príjemcu (t. j. odkazom na činnosti, ktoré vykonáva), odvetvia, sektora a podsektora a lokality príjemcov⁷³.

118. Podľa článku 15 ods. 1 písm. d) sa, ak je to možné, musia poskytnúť informácie o predpokladanej dobe uchovávaní osobných údajov. V opačnom prípade sa musia poskytnúť kritériá použité na určenie tejto doby. Informácie, ktoré poskytol prevádzkovateľ, musia byť dostatočne presné, aby dotknutá osoba vedela, ako dlho sa budú naďalej uchovávať údaje týkajúce sa dotknutej osoby. Ak nie je možné určiť čas vymazania, uvedie sa doba uchovávaní a jej začiatok alebo aktivujúca udalosť (napr. ukončenie zmluvy, uplynutie záručnej lehoty a pod.). Samotný odkaz, napríklad na „vymazanie po uplynutí zákonných lehôt uchovávaní“, nestačí. Údaje týkajúce sa dĺžky uchovávaní údajov budú musieť byť zamerané na konkrétne údaje týkajúce sa dotknutej osoby. Ak sa na osobné údaje dotknutej osoby vzťahujú rôzne doby vymazania (napríklad preto, že nie všetky údaje podliehajú zákonným povinnostiam uchovávaní), lehoty na vymazanie sa uvedú vo vzťahu k príslušným spracovateľským operáciám a kategóriám údajov.
119. Zatiaľ čo informácie o práve podať sťažnosť dozornému orgánu [článok 15 ods. 1 písm. f)] nezávisia od konkrétnych okolností, práva dotknutých osôb uvedené v článku 15 ods. 1 písm. e) sa líšia v závislosti od právneho základu spracúvania. Vzhľadom na povinnosť prevádzkovateľa uľahčiť výkon práv dotknutej osoby podľa článku 12 ods. 2 všeobecného nariadenia o ochrane údajov jeho odpoveď ohľadom týchto práv musí byť individuálne prispôbena prípadu dotknutej osoby a bude sa vzťahovať ku konkrétnym spracovateľským operáciám. Treba sa vyhnúť informáciám o právach, ktoré sa na dotknutú osobu v konkrétnej situácii nevzťahujú.
120. Podľa článku 15 ods. 1 písm. g) sa musia poskytnúť „akékoľvek dostupné informácie“, pokiaľ ide o zdroj údajov, ak sa osobné údaje nezískali od dotknutej osoby. Stupeň dostupných informácií sa môže časom meniť.

Príklad 21: V politike ochrany súkromia veľkej spoločnosti sa uvádza:

„Kontroly bonity nám pomáhajú predchádzať problémom pri platobných transakciách. Zaručujú ochranu našej spoločnosti pred finančnými rizikami, ktoré môžu mať v strednodobom až dlhodobom horizonte vplyv aj na predajné ceny. Kontrola bonity sa nevyhnutne vykonáva vtedy, keď sa chystáme odoslať tovar bez toho, aby sme súčasne získali príslušnú kúpnu cenu, napr. v prípade nákupu na účet. Bez vykonania kontroly bonity je možná iba platba vopred (okamžitý bankový prevod, poskytovateľ online platieb, kreditná karta).

⁷³ Usmernenia WP29 k transparentnosti – schválené EDPB, s. 37 (príloha).

Na účely kontroly bonity zašleme vaše meno, adresu a dátum narodenia týmto poskytovateľom služieb, napríklad: 1. finančná informačná agentúra X; 2. poskytovateľ obchodných informácií Y; 3. komerčná úverová referenčná agentúra Z.

Údaje sa postúpia uvedeným úverovým inštitúciám len v rozsahu, ktorý je zákonne prípustný, a len na účely analýzy vášho platobného správania v minulosti, ako aj na posúdenie rizika zlyhania na základe matematicko-štatistických postupov, pri ktorých sa využívajú údaje o adrese, ako aj na overenie vašej adresy (kontrola doručenia). V závislosti od výsledku kontroly bonity vám už možno nebudeme môcť ponúkať jednotlivé spôsoby platby, ako napríklad nákup na faktúry.“

Oznámenie o ochrane osobných údajov tak obsahuje všeobecné informácie o možnosti získať informácie od uvedených ekonomických informačných inštitúcií v súlade s článkami 13 a 14 všeobecného nariadenia o ochrane údajov. Ak nie je *ex ante* jasné, ktorá zo spoločností sa zapojí do spracúvania, stačí uviesť názvy oprávnených spoločností v politike ochrany súkromia. V rámci žiadosti na základe článku 15, okrem informácie, že bola získaná informácia o úverovej bonite, bude následne (*ex post*) potrebné poskytnúť, o ktorú z uvedených spoločností presne ide. V článku 15 ods. 1 písm. g) je jasne vyjadrené, že informácie o spracúvaní údajov zahŕňajú „akékoľvek dostupné informácie, pokiaľ ide o ich zdroj“, ak sa osobné údaje nezískali od dotknutej osoby.

121. V článku 15 ods. 1 písm. h) sa stanovuje, že každá dotknutá osoba by mala mať právo byť zmysluplným spôsobom informovaná, okrem iného, o existencii a základnom postupe automatizovaného rozhodovania vrátane profilovania týkajúceho sa dotknutej osoby a o význame a predpokladaných dôsledkoch, ktoré by takéto spracúvanie mohlo mať⁷⁴. Ak je to možné, informácie podľa článku 15 ods. 1 písm. h) musia byť konkrétnejšie vo vzťahu k odôvodneniu, ktoré vedie ku konkrétnym rozhodnutiam týkajúcim sa dotknutej osoby, ktorá požiadala o prístup.
122. Informácie o zamýšľaných prenosoch údajov do tretej krajiny alebo medzinárodnej organizácii vrátane informácie o existencii rozhodnutia Komisie o primeranosti alebo vhodných záruk sa musia poskytnúť podľa článku 13 ods. 1 písm. f) a článku 14 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov. V rámci žiadosti o prístup podľa článku 15 sa v článku 15 ods. 2 vyžadujú informácie o primeraných zárukách podľa článku 46 všeobecného nariadenia o ochrane údajov len v prípadoch, keď sa údaje skutočne prenášajú do tretej krajiny alebo medzinárodnej organizácii.

5 AKO MÔŽE PREVÁDZKOVATEĽ POSKYTNÚŤ PRÍSTUP?

123. Všeobecné nariadenie o ochrane údajov nie je veľmi normatívne, pokiaľ ide o to, ako musí prevádzkovateľ poskytnúť prístup. Uplatnenie práva na prístup môže byť v niektorých situáciách jednoduché a priame, napríklad keď malá organizácia disponuje obmedzenými informáciami o dotknutej osobe. V iných situáciách je právo na prístup komplikovanejšie, pretože spracúvanie údajov je zložitejšie; s ohľadom na počet dotknutých osôb, kategórie spracúvaných údajov, ako aj tok údajov v rámci rôznych organizácií a medzi nimi. Vzhľadom na rozdiely v spracúvaní osobných údajov sa môže vhodný spôsob poskytnutia prístupu následne líšiť.
124. Cieľom tohto oddielu je poskytnúť niekoľko usmernení a praktických príkladov o rôznych spôsoboch, ktorými môžu prevádzkovatelia vyhovieť žiadosti o prístup, ako aj o význame článku 12 ods. 1

⁷⁴ Pozri v tomto smere Usmernenia k transparentnosti podľa nariadenia 2016/679 (WP 260), bod 41, s odkazom na usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679 (WP 251).

všeobecného nariadenia o ochrane údajov vo vzťahu k právu na prístup. V tomto oddiele sú takisto uvedené určité usmernenia o tom, čo sa považuje za bežne používanú elektronickú podobu, ako aj o načasovaní poskytovania prístupu podľa článku 12 ods. 3 všeobecného nariadenia o ochrane údajov.

5.1 Ako môže prevádzkovateľ získať požadované údaje?

125. Dotknuté osoby by mali mať prístup k všetkým informáciám, ktoré o nich prevádzkovateľ spracúva. To napríklad znamená, že prevádzkovateľ je povinný vyhľadávať osobné údaje vo svojich IT systémoch a iných informačných systémoch. Pri vykonávaní takéhoto vyhľadávania by mal prevádzkovateľ použiť dostupné informácie v organizácii týkajúce sa dotknutej osoby, výsledkom čoho bude pravdepodobne zhoda v systémoch v závislosti od toho, ako sú informácie štruktúrované⁷⁵. Napríklad, ak sú informácie zoradené v súboroch v závislosti od názvu alebo referenčného čísla, vyhľadávanie sa môže obmedzovať na tieto faktory. Ak však štruktúra údajov závisí od iných faktorov, ako sú rodinné vzťahy alebo profesijné tituly alebo akékoľvek priame alebo nepriame identifikátory (napr. číslo zákazníka, používateľské meno alebo IP adresy), vyhľadávanie treba rozšíriť tak, aby zahŕňalo aj tieto identifikátory, za predpokladu, že prevádzkovateľ disponuje aj týmito informáciami týkajúcimi sa dotknutej osoby alebo mu tieto informácie poskytne dotknutá osoba. To isté platí, ak záznamy týkajúce sa tretích osôb pravdepodobne obsahujú osobné údaje týkajúce sa dotknutej osoby. Prevádzkovateľ však nemôže od dotknutej osoby požadovať, aby poskytla viac informácií, ako je potrebné na identifikáciu dotknutej osoby. Ak prevádzkovateľ na spracúvanie údajov využíva sprostredkovateľa, vyhľadávanie sa musí prirodzene rozšíriť aj o osobné údaje spracúvané týmto sprostredkovateľom.
126. V súlade s článkom 25 všeobecného nariadenia o ochrane údajov týkajúceho sa špecificky navrhutej a štandardnej ochrany údajov by mal mať prevádzkovateľ (a všetci sprostredkovatelia, ktorých využíva) už zavedené funkcie umožňujúce dodržiavanie práv dotknutej osoby. V tejto súvislosti to znamená, že pri vybavovaní žiadosti by mali existovať primerané spôsoby na nájdenie a získanie informácií o dotknutej osobe. Treba však poznamenať, že široký výklad v tomto smere by mohol viesť k funkciám na vyhľadávanie a získavanie informácií, ktoré samy osebe predstavujú riziko pre súkromie dotknutých osôb. Preto je dôležité mať na pamäti, že proces získavania údajov by mal byť navrhnutý tak, aby bol šetrný k ochrane údajov, aby neohrozoval súkromie iných, napríklad zamestnancov prevádzkovateľa.

5.2 Primerané opatrenia na zabezpečenie prístupu

5.2.1 Prijatie „primeraných opatrení“

127. V článku 12 všeobecného nariadenia o ochrane údajov sa stanovujú požiadavky na poskytnutie prístupu, t. j. na poskytnutie potvrdenia, osobných údajov a doplňujúcich informácií podľa článku 15 a zároveň sa určuje forma, spôsob a lehota vo vzťahu k právu na prístup. Usmernenia pracovnej skupiny zriadenej podľa článku 29 k transparentnosti podľa nariadenia 2016/679⁷⁶ obsahujú ďalšie usmernenia, pokiaľ ide o článok 12, väčšinou vo vzťahu k článkom 13 a 14 všeobecného nariadenia o ochrane údajov, ale aj vo vzťahu k článku 15 a k transparentnosti vo všeobecnosti. Preto to, čo je uvedené v týchto usmerneniach, môže často rovnako platiť aj pokiaľ ide o poskytovanie prístupu podľa článku 15.

⁷⁵ Takéto vyhľadávanie by malo samozrejme zahŕňať aj informácie, ktoré má sprostredkovateľ, pozri článok 28 ods. 3 písm. e) všeobecného nariadenia o ochrane údajov.

⁷⁶ Pracovná skupina zriadená podľa článku 29, WP 260 rev.01, 11. apríla 2018, Usmernenia k transparentnosti podľa nariadenia 2016/679 – schválené EDPB (ďalej len „usmernenia WP29 k transparentnosti – schválené EDPB“).

128. V článku 12 ods. 1 všeobecného nariadenia o ochrane údajov sa uvádza, že prevádzkovateľ prijme primerané opatrenia, aby dotknutej osobe poskytol všetky oznámenia podľa článku 15, ktoré sa týkajú spracúvania, a to v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho. V článku 12 ods. 2 sa stanovuje, že prevádzkovateľ uľahčuje dotknutej osobe výkon práva na prístup. Presnejšie požiadavky v tomto smere sa budú musieť posudzovať podľa jednotlivých prípadov. Pri rozhodovaní o tom, ktoré opatrenia sú primerané, musia prevádzkovatelia zohľadniť všetky relevantné okolnosti, okrem iného vrátane množstva údajov, ktoré sa spracúvajú, zložitosti nimi spracúvaných údajov a znalostí, ktoré majú o svojich dotknutých osobách, napríklad ak väčšinu dotknutých osôb tvoria deti, starší ľudia alebo osoby so zdravotným postihnutím. Okrem toho v situáciách, keď je prevádzkovateľ informovaný o akýchkoľvek konkrétnych potrebách dotknutej osoby, ktorá podáva žiadosť, napríklad prostredníctvom doplňujúcich informácií v podanej žiadosti, musí prevádzkovateľ tieto okolnosti zohľadniť. V dôsledku toho sa primerané opatrenia budú líšiť.
129. Pri posudzovaní je dôležité mať na pamäti, že výraz „primerané“ by sa nikdy nemal chápať ako spôsob obmedzenia rozsahu údajov, na ktoré sa vzťahuje právo na prístup. Pojem „primerané“ neznamená, že úsilie o poskytnutie informácií možno vyvážiť napríklad akýmkoľvek záujmom dotknutej osoby na získaní osobných údajov. Namiesto toho by sa posúdenie malo zamerať na výber najprimeranejšej metódy poskytovania všetkých informácií, na ktoré sa vzťahuje toto právo, v závislosti od konkrétnych okolností každého prípadu. Prevádzkovateľ, ktorý spracúva veľké množstvo údajov vo veľkom rozsahu, v dôsledku toho musí súhlasiť s tým, že vynaloží veľké úsilie na zabezpečenie práva na prístup pre dotknuté osoby v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho.
130. Treba sa vyhnúť tomu, aby bola dotknutá osoba v reakcii na žiadosť o prístup k údajom nasmerovaná na rôzne zdroje. Ako už bolo uvedené v usmerneniach WP29 k transparentnosti (v súvislosti s pojmom „poskytovať“ v článkoch 13 a 14 všeobecného nariadenia o ochrane údajov), pojem „poskytovať“ znamená, že *„dotknutá osoba nesmie mať potrebu aktívne vyhľadávať informácie, na ktoré sa vzťahujú tieto články, medzi inými informáciami, ako sú podmienky používania webového sídla alebo aplikácie“*⁷⁷. Dotknuté osoby preto musia pri rešpektovaní zásady transparentnosti získať od prevádzkovateľa informácie a osobné údaje požadované podľa článku 15 ods. 1, 2 a 3 spôsobom, ktorý umožňuje úplný prístup k požadovaným informáciám. Za osobitných okolností by bolo zdieľanie informácií v rámci prevádzkovateľa neprimerané alebo dokonca nezákonné, napríklad z dôvodu citlivej povahy informácií (ako sú informácie týkajúce sa oznamovania protispoločenskej činnosti). V týchto prípadoch by sa považovalo za vhodné rozdeliť informácie do niekoľkých odpovedí ako odpoveď na žiadosť dotknutých osôb o prístup. Metóda, ktorú zvolí prevádzkovateľ, musí skutočne poskytnúť dotknutej osobe požadované údaje a informácie, a preto by nebolo vhodné iba odkázať dotknutú osobu na kontrolu požadovaných údajov uložených na jej vlastnom zariadení vrátane napríklad kontroly histórie kliknutí a IP adresy na jej mobilnom telefóne.
131. V súlade so zásadou zodpovednosti musí prevádzkovateľ zdokumentovať svoj prístup, aby mohol za daných okolností preukázať primeranosť prostriedkov, ktoré si zvolil na poskytovanie potrebných informácií podľa článku 15.

⁷⁷ Usmernenia WP29 k transparentnosti – schválené EDPB, bod 33.

5.2.2 Rôzne spôsoby poskytovania prístupu

132. Ako už bolo vysvetlené v oddiele 2.2.2, pri podávaní žiadosti o prístup majú dotknuté osoby právo získať kópiu svojich údajov, ktoré sa spracúvajú podľa článku 15 ods. 3 spolu s doplňujúcimi informáciami, čo sa považuje za hlavný spôsob ako poskytnúť prístup k osobným údajom.
133. Za určitých okolností však môže byť vhodné, aby prevádzkovateľ poskytol prístup aj inými spôsobmi, než je poskytnutie kópie. Takýmito dočasnými spôsobmi [non-permanent modalities] prístupu k údajom môžu byť napríklad: ústne informácie, kontrola súborov, prístup na mieste alebo vzdialený prístup bez možnosti sťahovania. Tieto spôsoby môžu predstavovať vhodné formy udelenia prístupu, napríklad v prípadoch, keď je to v záujme dotknutej osoby alebo ak o to dotknutá osoba požiada. Prístup na mieste by mohol byť takisto vhodný ako prvotné opatrenie, keď prevádzkovateľ spracúva veľké množstvo nedigitalizovaných údajov, aby dotknutá osoba mohla byť informovaná o tom, aké osobné údaje sa spracúvajú, a aby mohla urobiť informované rozhodnutie o tom, aké osobné údaje chce prostredníctvom kópie poskytnúť. Dočasné spôsoby prístupu môžu byť v určitých situáciách postačujúce a primerané; môžu napríklad uspokojiť potrebu dotknutých osôb overiť správnosť údajov spracúvaných prevádzkovateľom tým, že dotknutým osobám poskytnú možnosť prezrieť si pôvodné údaje. Prevádzkovateľ nie je povinný poskytnúť informácie inou formou ako poskytnutím kópie, ale pri posudzovaní takejto žiadosti by mal zaujať primeraný prístup. Poskytnutím prístupu inými formami ako poskytnutím kópie sa nevylučuje právo dotknutých osôb mať aj kópiu, pokiaľ sa nerozhodnú o opaku.
134. Prevádzkovateľ sa môže v závislosti od danej situácie rozhodnúť poskytnúť kópiu údajov, ktoré sa spracúvajú, spolu s doplňujúcimi informáciami rôznymi formami, napr. e-mailom, fyzickou poštou alebo pomocou samoobslužného nástroja. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe uvedenej v článku 15 ods. 3, pokiaľ dotknutá osoba nepožiadala o iný spôsob. V každom prípade musí prevádzkovateľ pri poskytovaní informácií prostredníctvom e-mailu alebo online samoobslužnými nástrojmi zväžiť vhodné technické a organizačné opatrenia vrátane primeraného šifrovania.
135. V situácii, keď prevádzkovateľ spracúva osobné údaje týkajúce sa osoby, ktorá podáva žiadosť, len v malom rozsahu, kópia osobných údajov a doplňujúce informácie sa môžu a mali by sa poskytnúť prostredníctvom jednoduchého postupu.

Príklad 22: Miestne kníhkupectvo vedie záznamy o menách a adresách svojich zákazníkov, ktorí si objednali doručenie domov. Zákazník navštívi kníhkupectvo a požiada o prístup. V tejto situácii bude stačiť vytlačiť osobné údaje týkajúce sa zákazníka priamo z obchodného systému a zároveň poskytnúť doplňujúce informácie v článku 15 ods. 1 a 2.

Príklad 23: Mesačný darca charitatívnej organizácie požiada o prístup prostredníctvom e-mailu. Charitatívna organizácia uchováva informácie o daroch uskutočnených za posledných dvanásť mesiacov, ako aj mená a e-mailové adresy darcov. Prevádzkovateľ by mohol poskytnúť kópiu osobných údajov a doplňujúce informácie odpovedaním na e-mail za predpokladu, že sa použijú všetky potrebné záruky, berúc do úvahy napríklad povahu údajov.

136. Dokonca aj prevádzkovatelia, ktorí spracúvajú veľké množstvo údajov, sa môžu rozhodnúť spoliehať sa na manuálne procesy pri spracúvaní žiadostí o prístup. Ak prevádzkovateľ spracúva údaje vo viacerých rôznych oddeleniach, musí zhromaždiť osobné údaje z každého oddelenia, aby mohol odpovedať na žiadosť dotknutej osoby.

Príklad 24: Prevádzkovateľ vymenuje administrátora, aby sa zaoberal praktickými otázkami týkajúcimi sa žiadostí o prístup. Po prijatí žiadosti, administrátor odošle e-mailom otázku rôznym oddeleniam organizácie so žiadosťou o zhromaždenie osobných údajov o dotknutej osobe. Zástupcovia jednotlivých oddelení odovzdajú administrátorovi osobné údaje, ktoré spracúva ich oddelenie. Administrátor následne zašle všetky osobné údaje dotknutej osobe spolu s potrebnými doplňujúcimi informáciami, napríklad, ak je to vhodné, e-mailom.

137. Hoci manuálne procesy spracúvania žiadostí o prístup možno považovať za primerané, niektorí prevádzkovatelia môžu využívať automatizované procesy na spracovanie žiadostí dotknutých osôb. To by sa mohlo týkať napríklad prevádzkovateľov, ktorí prijímajú veľké množstvo žiadostí. Jedným zo spôsobov poskytovania informácií podľa článku 15 je poskytnutie samoobslužných nástrojov dotknutej osobe. To by mohlo uľahčiť efektívne a včasné vybavovanie žiadostí dotknutých osôb o prístup, a zároveň to prevádzkovateľovi umožní zahrnúť overovací mechanizmus do samoobslužného nástroja.

Príklad 25: Služba sociálnych médií má zavedený automatizovaný proces vybavovania žiadostí o prístup, ktorý umožňuje dotknutej osobe prístup k jej osobným údajom z jej používateľského konta. Ak chcú používatelia sociálnych médií získať osobné údaje, môžu pri prihlásení do svojho používateľského konta zvoliť možnosť „Stiahnuť vaše osobné údaje“. Táto samoobslužná možnosť umožňuje používateľom stiahnuť súbor obsahujúci ich osobné údaje priamo z používateľského konta do vlastného počítača.

138. Používanie samoobslužných nástrojov by nikdy nemalo obmedzovať rozsah prijímaných osobných údajov. Ak nie je možné poskytnúť všetky informácie podľa článku 15 prostredníctvom samoobslužného nástroja, zvyšné informácie je potrebné poskytnúť iným spôsobom. Prevádzkovateľ môže dokonca odporučiť dotknutej osobe, aby používala samoobslužný nástroj, ktorý prevádzkovateľ zaviedol na vybavovanie žiadostí o prístup. Treba však poznamenať, že prevádzkovateľ musí spracúvať aj žiadosti o prístup, ktoré sa neposielajú cez vytvorený komunikačný kanál⁷⁸.

5.2.3 Poskytnutie prístupu „v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho“

139. Podľa článku 12 ods. 1 všeobecného nariadenia o ochrane údajov prevádzkovateľ prijme primerané opatrenia s cieľom poskytnúť prístup podľa článku 15 v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho.
140. Požiadavka, že poskytnutie prístupu dotknutej osobe sa musí uskutočniť v stručnej a transparentnej forme, znamená, že prevádzkovatelia by mali informácie prezentovať efektívne a stručne, aby im dotknutá osoba ľahko porozumela, najmä ak ide o dieťa. Prevádzkovateľ musí pri výbere prostriedkov na poskytnutie prístupu podľa článku 15 zohľadniť množstvo a zložitosť údajov.

Príklad 26: Poskytovateľ sociálnych médií spracúva veľké množstvo informácií o dotknutej osobe. Veľkú časť týchto osobných údajov tvoria informácie nachádzajúce sa na stovkách strán súborov so záznamami [log files], kde sú evidované aktivity dotknutej osoby na webovom sídle. Ak dotknuté osoby požiadajú o prístup k svojim osobným údajom, na osobné údaje v týchto súboroch so záznamami sa tiež vzťahuje právo na prístup. Právo na prístup teda môže byť formálne splnené, ak sa dotknutej osobe poskytli tieto stovky strán súborov so záznamami. Bez opatrení prijatých na uľahčenie pochopenia informácií v súboroch so záznamami by však v praxi nemuselo byť splnené právo dotknutej osoby na prístup, pretože zo súborov so záznamami nie je možné ľahko získať žiadne poznatky, v dôsledku čoho

⁷⁸ Pozri oddiel 3.1.2.

nebola splnená požiadavka článku 12 ods. 1 všeobecného nariadenia o ochrane údajov. Prevádzkovateľ musí byť preto opatrný a dôkladný pri výbere spôsobu, akým sú informácie a osobné údaje dotknutej osobe prezentované.

141. Za okolností v uvedenom príklade by použitie viacúrovňového prístupu, podobného viacúrovňovému prístupu presadzovanému v usmerneniach k transparentnosti ohľadom oznámení o ochrane osobných údajov⁷⁹, mohlo predstavovať primerané opatrenie na splnenie oboch požiadaviek v článku 15 a článku 12 ods. 1 všeobecného nariadenia o ochrane údajov. Týmto sa bude podrobnejšie zaoberať oddiel 5.2.4. Požiadavka, že informácie sú „zrozumiteľné“, znamená, že by im mala porozumieť zamýšľaná cieľová skupina⁸⁰, pričom treba mať na pamäti všetky konkrétne potreby, ktoré môže mať dotknutá osoba a ktoré sú prevádzkovateľovi známe⁸¹. Keďže právo na prístup často umožňuje výkon iných práv dotknutej osoby, je dôležité, aby poskytované informácie boli zrozumiteľné a jasné. Dotknuté osoby totiž budú môcť zväziť, či sa odvolajú na svoje právo napríklad na opravu podľa článku 16 všeobecného nariadenia o ochrane údajov, len vtedy, keď budú vedieť, aké osobné údaje sa spracúvajú, na aké účely atď. V dôsledku toho môže byť potrebné, aby prevádzkovateľ poskytol dotknutej osobe doplňujúce informácie, ktoré vysvetľujú poskytnuté údaje. Treba zdôrazniť, že zložitosť spracúvania údajov zaväzuje prevádzkovateľa poskytnúť prostriedky na to, aby boli údaje zrozumiteľné a nemožno ju použiť ako argument na obmedzenie prístupu k všetkým údajom. Podobne nemožno ako argument na obmedzenie prístupu k všetkým údajom použiť povinnosť prevádzkovateľa poskytnúť údaje v stručnej forme.

Príklad 27: Webové sídlo elektronického obchodu zhromažďuje údaje o položkách zobrazených alebo zakúpených na jeho webovom sídle na marketingové účely. Časť týchto údajov budú tvoriť údaje v nespracovanom formáte⁸², ktoré neboli analyzované a nemusia byť pre čitateľa priamo zmysluplné (kódy, história aktivít atď.). Na takéto údaje súvisiace s činnosťami dotknutých osôb sa takisto vzťahuje právo na prístup a v dôsledku toho by sa tieto údaje mali dotknutej osobe poskytnúť v reakcii na žiadosť o prístup. Pri poskytovaní údajov v nespracovanom formáte je dôležité, aby prevádzkovateľ prijal potrebné opatrenia na zabezpečenie toho, aby dotknutá osoba údajom rozumela, napríklad poskytnutím vysvetľujúceho dokumentu, ktorým sa nespracovaný formát preloží do užívateľsky prívetivej formy. V takomto dokumente by sa zároveň mohlo vysvetľovať, že skratky a iné akronymy, napríklad „A“, znamená, že nákup bol prerušený a „B“ znamená, že nákup sa uskutočnil.

142. „Lahko dostupný“ prvok znamená, že informácie podľa článku 15 by mali byť prezentované spôsobom, ktorý je pre dotknutú osobu jednoducho prístupný. Týka sa to napríklad rozloženia, vhodných nadpisov a odsekov. Informácie by sa mali vždy poskytovať v jasnom a jednoduchom jazyku. Prevádzkovateľ, ktorý ponúka službu v krajine, by mal takisto ponúkať odpovede v jazyku, ktorému rozumejú dotknuté osoby v danej krajine. Odporúča sa aj používanie štandardizovaných ikon, ktoré uľahčujú zrozumiteľnosť a dostupnosť informácií. Ak sa žiadosť o informácie týka dotknutých osôb so zrakovým

⁷⁹ Usmernenia WP29 k transparentnosti – schválené EDPB, bod 35.

⁸⁰ Zrozumiteľnosť je úzko spojená s požiadavkou používať jasný a jednoduchý jazyk (Usmernenia WP29 k transparentnosti – schválené EDPB, bod 9). To, čo sa hovorí o jasnom a jednoduchom jazyku v bodoch 12 – 16, pokiaľ ide o informácie uvedené v článkoch 13 a 14 všeobecného nariadenia o ochrane údajov, sa rovnako vzťahuje na komunikáciu podľa článku 15.

⁸¹ Pozri bod 128.

⁸² Nespracovaný formát v tomto príklade treba chápať ako neanalyzované údaje, ktoré sú základom spracúvania, a nie ako najnižšiu úroveň nespracovaných údajov, ktoré môžu byť čitateľné iba strojovo (ako napríklad „bity“).

postihnutím alebo iných dotknutých osôb, ktoré môžu mať ťažkosti s prístupom k informáciám alebo s ich pochopením, očakáva sa, že prevádzkovateľ prijme opatrenia na uľahčenie pochopenia poskytovaných informácií, vrátane ústnych informácií, ak je to vhodné⁸³. Prevádzkovateľ by mal venovať osobitnú pozornosť tomu, aby zabezpečil, že starší ľudia, deti, zrakovo postihnuté osoby alebo osoby s kognitívnym alebo iným postihnutím môžu uplatňovať svoje práva, napríklad proaktívnym poskytovaním ľahko dostupných prvkov na uľahčenie uplatňovania týchto práv.

5.2.4 Veľké množstvo informácií si vyžaduje osobitné požiadavky týkajúce sa spôsobu poskytovania informácií

143. Bez ohľadu na prostriedky použité na poskytnutie prístupu môže existovať rozpor medzi množstvom informácií, ktoré musí prevádzkovateľ poskytnúť dotknutým osobám, a požiadavkou, že informácie musia byť stručné. Jedným zo spôsobov, ako dosiahnuť oboje, a príkladom primeraného opatrenia pre určitých prevádzkovateľov, keď sa má poskytnúť veľké množstvo údajov, je použiť viacúrovňový prístup. Tento prístup môže dotknutým osobám uľahčiť pochopenie údajov. Malo by sa však zdôrazniť, že tento prístup možno použiť len za určitých okolností a treba ho vykonávať spôsobom, ktorý neobmedzuje právo na prístup, ako je vysvetlené ďalej. Okrem toho by použitie viacúrovňového prístupu nemalo pre dotknutú osobu predstavovať ďalšiu záťaž. Preto by bolo najvhodnejšie vtedy, keď sa prístup poskytuje v online kontexte. Viacúrovňový prístup je len spôsob prezentácie informácií podľa článku 15 spôsobom, ktorý je v súlade aj s požiadavkami v článku 12 ods. 1 všeobecného nariadenia o ochrane údajov a nemal by sa zamieňať s možnosťou prevádzkovateľov požadovať, aby dotknutá osoba upresnila informácie alebo spracovateľské činnosti, ktorých sa týka jej žiadosť, ako je uvedené v odôvodnení 63 všeobecného nariadenia o ochrane údajov⁸⁴.
144. Viacúrovňový prístup vo vzťahu k právu na prístup znamená, že prevádzkovateľ môže za určitých okolností poskytnúť osobné údaje a doplňujúce informácie požadované podľa článku 15 v rôznych úrovniach. Prvá úroveň by mala obsahovať informácie o spracúvaní a právach dotknutej osoby podľa článku 15 ods. 1 písm. a) až h) a článku 15 ods. 2, ako aj prvú časť spracúvaných osobných údajov. V druhej úrovni by sa malo poskytnúť viac osobných údajov.
145. Pri rozhodovaní o tom, aké informácie by sa mali poskytnúť v rôznych úrovniach, by mal prevádzkovateľ zvážiť, ktoré informácie by dotknutá osoba vo všeobecnosti považovala za najrelevantnejšie. V súlade so zásadou spravodlivosti by prvá úroveň mala obsahovať aj informácie o spracúvaní, ktoré majú najväčší vplyv na dotknutú osobu⁸⁵. Prevádzkovatelia musia byť schopní preukázať zodpovednosť, pokiaľ ide o ich odôvodnenie uvedeného rozhodovania.

Príklad 28: Prevádzkovateľ analyzuje veľké súbory údajov [big data], aby zaradil zákazníkov do rôznych segmentov v závislosti od ich online správania. V tejto situácii možno predpokladať, že informácie, ktorých získanie je pre dotknuté osoby najdôležitejšie, sú informácie o tom, do akého segmentu boli zaradené. V dôsledku toho by tieto informácie mali byť zahrnuté v prvej úrovni. Údaje v nespracovanom formáte,⁸⁶ ktoré ešte neboli analyzované alebo ďalej spracúvané, ako napríklad aktivita používateľa na webovom sídle, sú takisto osobnými údajmi, na ktoré sa vzťahuje právo na prístup, v niektorých prípadoch by však mohlo stačiť poskytnúť tieto informácie v inej úrovni.

⁸³ Pozri Usmernenia WP29 k transparentnosti – schválené EDPB, bod 21.

⁸⁴ Pozri aj oddiel 2.3.1.

⁸⁵ Pozri Usmernenia WP29 k transparentnosti – schválené EDPB, bod 36.

⁸⁶ Pozri poznámku pod čiarou č. 82.

146. Aby sa použitie viacúrovňového prístupu mohlo považovať za primerané opatrenie, je potrebné, aby bola dotknutá osoba od začiatku informovaná, že informácie podľa článku 15 sú štruktúrované do rôznych úrovní a doplnené opisom toho, aké osobné údaje a informácie budú obsiahnuté v rôznych úrovniach. Týmto spôsobom bude pre dotknutú osobu jednoduchšie rozhodnúť, ku ktorým úrovniam chce mať prístup. Opis by mal objektívne odrážať všetky kategórie osobných údajov, ktoré prevádzkovateľ skutočne spracúva. Musí byť takisto jasné, ako môže dotknutá osoba získať prístup k rôznym úrovniam. Prístup k rôznym úrovniam nesmie pre dotknutú osobu predstavovať žiadne neprimerané úsilie a nesmie byť podmienený formulovaním novej žiadosti dotknutej osoby. To znamená, že dotknuté osoby musia mať možnosť vybrať si, či budú mať prístup k všetkým úrovniam naraz alebo k jednej či dvom z úrovní, ak im to vyhovuje.

Príklad 29: Dotknutá osoba požiada o prístup k službe streamovania videa. Žiadosť sa podáva prostredníctvom možnosti, ktorá je k dispozícii, keď sa dotknuté osoby prihlásia do svojho účtu. Dotknutá osoba má k dispozícii dve možnosti, ktoré sa na webovej stránke zobrazujú ako tlačidlá. Prvou možnosťou je stiahnutie časti 1 osobných údajov a doplňujúcich informácií. Táto časť obsahuje napríklad nedávnu históriu streamovania, informácie o účte a informácie o platbách. Druhá možnosť je stiahnuť si časť 2 osobných údajov, ktorá obsahuje súbory technických záznamov o činnostiach dotknutých osôb a historické informácie o účte. V tomto prípade prevádzkovateľ umožnil dotknutým osobám výkon ich práva spôsobom, ktorý pre dotknutú osobu nepredstavuje ďalšiu záťaž.

Obmena 1: V prípadoch, keď si dotknutá osoba zvolí iba tlačidlo na stiahnutie časti 1 osobných údajov, je prevádzkovateľ povinný poskytnúť iba časť 1 údajov.

Obmena 2: V prípadoch, keď si dotknutá osoba zvolí tlačidlá pre časť 1 aj časť 2 údajov, prevádzkovateľ nemôže oznámiť iba údaje časti 1 a požiadať o nové potvrdenie pred zaslaním údajov v časti 2. Namiesto toho musia byť dotknutej osobe poskytnuté údaje z oboch častí, ako to vyplýva z podanej žiadosti.

147. Použitie viacúrovňového prístupu sa nebude považovať za primerané pre všetkých prevádzkovateľov alebo vo všetkých situáciách. Mal by sa použiť len vtedy, keď by bolo pre dotknutú osobu ťažké porozumieť informáciám, ak by boli poskytnuté v celom rozsahu. Inými slovami, prevádzkovateľ musí byť schopný preukázať, že použitie viacúrovňového prístupu je pre dotknutú osobu prínosom, pretože jej pomáha pochopiť poskytované informácie. Viacúrovňový prístup by sa preto považoval za primeraný len vtedy, keď prevádzkovateľ spracúva veľké množstvo osobných údajov o dotknutej osobe, ktorá podáva žiadosť, a ak by dotknutá osoba mala zjavné ťažkosti s porozumením alebo pochopením informácií, ak by sa jej mali poskytnúť všetky naraz. Skutočnosť, že poskytnutie informácií podľa článku 15 by si od prevádzkovateľa vyžadovalo veľké úsilie a zdroje, nie je sama osebe argumentom pre použitie viacúrovňového prístupu.

5.2.5 Formát

148. Podľa článku 12 ods. 1 všeobecného nariadenia o ochrane údajov sa informácie podľa článku 15 poskytujú písomne alebo inými prostriedkami vrátane v prípade potreby elektronickými prostriedkami. Pokiaľ ide o prístup k osobným údajom, ktoré sa spracúvajú, v článku 15 ods. 3 sa uvádza, že ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob. Vo všeobecnom nariadení o ochrane údajov sa nestanovuje, čo je bežne používaná elektronická podoba. Existuje teda niekoľko prípadných formátov, ktoré možno použiť. To, čo sa považuje za bežne používanú elektronickú podobu sa bude takisto časom meniť.

149. To, čo možno považovať za bežne používanú elektronickú podobu, by malo vychádzať z objektívneho posúdenia a nie z toho, aký formát prevádzkovateľ používa pri svojej každodennej činnosti. S cieľom určiť, ktorý formát sa má v danej situácii považovať za bežne používaný formát, bude musieť prevádzkovateľ posúdiť, či existujú konkrétne formáty, ktoré sa všeobecne používajú v oblasti činnosti prevádzkovateľa alebo v danom kontexte. Ak takéto formáty vo všeobecnosti neexistujú, za bežne používané elektronické formáty by sa vo všeobecnosti mali považovať otvorené formáty stanovené v medzinárodnej norme, ako je ISO. EDPB však nevyklučuje možnosť, že aj iné formáty možno považovať za bežne používané v zmysle článku 15 ods. 3. Pri posudzovaní, či je formát bežne používaným elektronickým formátom, sa EDPB domnieva, že je dôležité, ako ľahko môže jednotlivец získať prístup k informáciám poskytovaným v aktuálnom formáte. V tejto súvislosti je potrebné poznamenať, aké informácie prevádzkovateľ poskytol dotknutej osobe o tom, ako má získať prístup k súboru, ktorý jej bol poskytnutý v konkrétnom formáte, napríklad aké programy alebo softvér by sa mohli použiť, aby bol formát prístupnejší pre dotknutú osobu. Dotknutá osoba by však nemala byť povinná kúpiť si softvér, aby získala prístup k informáciám.
150. Pri rozhodovaní o formáte, v ktorom bude kópia osobných údajov a informácií podľa článku 15 poskytnutá, musí mať prevádzkovateľ na pamäti, že formát musí umožňovať prezentáciu informácií spôsobom, ktorý je zrozumiteľný a ľahko dostupný. Je dôležité, aby sa dotknutej osobe poskytovali informácie v konkrétnej trvalej podobe (textová, elektronická). Keďže informácie by mali v priebehu času pretrvávajúť, v zásade sa uprednostňujú informácie v písomnej podobe, vrátane elektronických prostriedkov, pred inými podobami. Kópia osobných údajov by sa v prípade potreby mohla uložiť na elektronické pamäťové zariadenie ako je CD alebo USB kľúč.
151. Je potrebné poznamenať, že na to, aby sa prevádzkovateľ mohol domnievať, že dotknutým osobám bola poskytnutá kópia osobných údajov, nestačí im poskytnúť prístup k ich osobným údajom. Na splnenie požiadavky na poskytnutie kópie osobných údajov a v prípade, že sa údaje poskytujú elektronicky/digitálne, musia mať dotknuté osoby možnosť stiahnuť svoje údaje v bežne používanej elektronickej podobe.
152. Prevádzkovateľ je zodpovedný za rozhodnutie o primeranej podobe, v ktorej budú osobné údaje poskytnuté. Prevádzkovateľ môže, aj keď nemá nevyhnutne povinnosť, poskytnúť dokumenty, ktoré obsahujú osobné údaje o dotknutých osobách, ktoré podali žiadosť, v ich pôvodnej forme. Prevádzkovateľ by napríklad mohol v závislosti od jednotlivých prípadov poskytnúť prístup ku kópii média ako takého, vzhľadom na potrebu transparentnosti (napríklad na overenie presnosti údajov, ktoré uchováva prevádzkovateľ, v prípade žiadosti o nahliadnutie do zdravotnej dokumentácie alebo zvukového záznamu, ktorého prepis je sporný). Súdny dvor EÚ však vo svojom výklade práva na prístup podľa smernice 95/46/ES uviedol, že na to „aby sa vyhovelo [právu na prístup] stačí, aby sa tomuto žiadateľovi poskytol úplný súhrn týchto údajov v zrozumiteľnej forme, teda vo forme, ktorá tomuto žiadateľovi umožní oboznámiť sa s uvedeným údajmi a overiť, že tieto údaje sú správne a spracúvané v súlade s touto smernicou, aby prípadne mohol uplatniť práva, ktoré mu priznáva táto smernica“⁸⁷. Na rozdiel od smernice, všeobecné nariadenie o ochrane údajov výslovne obsahuje povinnosť poskytnúť dotknutej osobe kópiu osobných údajov, ktoré sa spracúvajú. To však neznamená, že dotknutá osoba má vždy právo získať kópiu dokumentov obsahujúcich osobné údaje, ale nezmenenú kópiu osobných údajov spracúvaných v týchto dokumentoch.⁸⁸ Takáto kópia osobných údajov by sa mohla poskytnúť prostredníctvom súhrnu obsahujúceho všetky osobné údaje, na ktoré sa vzťahuje

⁸⁷ Rozsudok Súdneho dvora, YS a i., spojené veci C-141/16 a C-372/12, bod 60.

⁸⁸ Otázky súvisiace s touto témou sú predmetom vecí, v ktorých v súčasnosti rozhoduje Súdny dvor Európskej únie (C-487/21 a C-307/21).

právo na prístup, pokiaľ súhrn umožňuje dotknutej osobe, aby si bola vedomá zákonnosti spracúvania a mohla si ju overiť. Preto neexistuje rozpor medzi znením všeobecného nariadenia o ochrane údajov a rozsudkom Súdneho dvora EÚ v tejto veci. Slovo zhrnutie v rozsudku by sa nemalo nesprávne vykladať v tom zmysle, že súhrn nezahŕňa všetky údaje, na ktoré sa vzťahuje právo na prístup, ale je len spôsobom, ako prezentovať všetky tieto údaje bez umožnenia prístupu k základným dokumentom, ktoré obsahujú osobné údaje. Keďže súhrn musí obsahovať kópiu osobných údajov, treba zdôrazniť, že ho nemožno urobiť spôsobom, ktorý by nejakým spôsobom upravoval alebo menil obsah informácií.

Príklad 30: Dotknutá osoba je mnoho rokov poistená v poisťovni. Došlo k niekoľkým poistným udalostiam. V každom jednotlivom prípade došlo k písomnej korešpondencii prostredníctvom e-mailu medzi dotknutou osobou a poisťovňou. Keďže dotknutá osoba musela poskytnúť informácie o konkrétnych okolnostiach každej udalosti, korešpondencia obsahuje množstvo osobných informácií o dotknutej osobe (záľuby, spolubývajúci, každodenné návyky atď.). V niektorých prípadoch vznikli nehody týkajúce sa povinnosti poisťovne odškodniť dotknutú osobu, čo spôsobilo veľké množstvo obojstrannej komunikácie. Všetku túto korešpondenciu uchováva poisťovňa. Dotknutá osoba požiada o prístup. V tejto situácii prevádzkovateľ nemusí nevyhnutne poskytnúť e-mailu v ich pôvodnej podobe tým, že ich pošle dotknutej osobe. Namiesto toho by sa prevádzkovateľ mohol rozhodnúť zostaviť e-mailovú korešpondenciu obsahujúcu osobné údaje dotknutej osoby do súboru, ktorý poskytne dotknutej osobe.

153. Bez ohľadu na formu, v akej prevádzkovateľ osobné údaje poskytuje, napr. poskytnutím skutočných dokumentov obsahujúcich osobné údaje alebo súhrnu osobných údajov, musia informácie spĺňať požiadavky na transparentnosť stanovené v článku 12 všeobecného nariadenia o ochrane údajov. Vykonanie nejakého druhu súhrnu a/alebo extrakcie údajov spôsobom, ktorým sa uľahčí pochopenie informácií, by v niektorých prípadoch mohlo predstavovať spôsob, ako splniť tieto požiadavky. V iných prípadoch sú informácie lepšie pochopiteľné poskytnutím kópie skutočného dokumentu obsahujúceho osobné údaje. O tom, ktorá forma je najvhodnejšia, sa teda musí rozhodnúť podľa okolností v jednotlivých prípadoch.
154. V tejto súvislosti je dôležité pripomenúť, že existuje rozdiel medzi právom na prístup podľa článku 15 všeobecného nariadenia o ochrane údajov a právom na získanie kópie administratívnych dokumentov upravených vnútroštátnym právom, pričom v druhom prípade ide o právo získať kópiu skutočného dokumentu. To neznamená, že právo na prístup podľa článku 15 všeobecného nariadenia o ochrane údajov vylučuje možnosť získať kópiu dokumentu/média, na ktorom sú osobné údaje uvedené.
155. V niektorých prípadoch samotné osobné údaje stanovujú požiadavky, v akom formáte sa majú osobné údaje poskytovať. Napríklad, ak osobné údaje predstavujú rukou písané informácie dotknutej osoby, môže byť potrebné poskytnúť dotknutej osobe fotokópiu tejto rukou písanej informácie, keďže samotný rukopis predstavuje osobný údaj. To by mohlo nastať najmä vtedy, keď je pri spracúvaní dôležitý rukopis, napr. analýza písma. To isté platí vo všeobecnosti aj pre zvukové záznamy, pretože samotný hlas dotknutej osoby predstavuje osobný údaj. V niektorých prípadoch však možno prístup poskytnúť poskytnutím prepisu konverzácie, napríklad ak sa tak dotknutá osoba a prevádzkovateľ dohodnú.
156. Treba poznamenať, že ustanovenia o požiadavkách na formát, pokiaľ ide o právo na prístup a právo na prenosnosť údajov sa líšia. Zatiaľ čo pri práve na prenosnosť údajov podľa článku 20 všeobecného nariadenia o ochrane údajov sa vyžaduje, aby boli informácie poskytnuté v strojovo čitateľnom formáte, pri práve na informácie podľa článku 15 sa to nevyžaduje. Formáty, ktoré sa nepovažujú za primerané pri plnení požiadavky na prenosnosť údajov, napríklad súbory pdf, by preto mohli byť stále vhodné pri plnení požiadavky na prístup.

5.3 Načasovanie poskytnutia prístupu

157. V článku 12 ods. 3 všeobecného nariadenia o ochrane údajov sa vyžaduje, aby prevádzkovateľ poskytol dotknutej osobe informácie o opatreniach prijatých v súvislosti so žiadosťou podľa článku 15 bez zbytočného odkladu a v každom prípade do jedného mesiaca od prijatia žiadosti. Túto lehotu možno predĺžiť najviac o dva mesiace s prihliadnutím na zložitosť a počet žiadostí za predpokladu, že dotknutá osoba bola informovaná o dôvodoch tohto oneskorenia do jedného mesiaca od prijatia žiadosti. Táto povinnosť informovať dotknutú osobu o predĺžení lehoty a jej dôvodoch by sa nemala zamieňať s informáciami, ktoré sa musia poskytnúť bezodkladne a najneskôr do jedného mesiaca, keď prevádzkovateľ nepodnikne žiadne kroky na základe žiadosti, ako sa uvádza v článku 12 ods. 4 všeobecného nariadenia o ochrane údajov.
158. Prevádzkovateľ reaguje a spravidla poskytne informácie podľa článku 15 bez zbytočného odkladu, čo znamená, že informácie by sa mali poskytnúť čo najskôr. To znamená, že ak je možné poskytnúť požadované informácie v kratšom čase ako jeden mesiac, prevádzkovateľ by tak mal urobiť. EDPB sa takisto domnieva, že načasovanie odpovede na žiadosť v niektorých situáciách musí byť prispôbené dobe uchovávanía, aby bolo možné poskytnúť prístup⁸⁹.
159. Lehota začína plynúť, keď prevádzkovateľ prijme žiadosť podľa článku 15, čo znamená, keď sa žiadosť dostane k prevádzkovateľovi prostredníctvom jedného z jeho oficiálnych kanálov.⁹⁰ Nie je potrebné, aby mal prevádzkovateľ skutočne o žiadosti vedomosť. Ak však prevádzkovateľ potrebuje komunikovať s dotknutou osobou z dôvodu neistoty týkajúcej sa totožnosti osoby, ktorá žiadosť podáva, môže dôjsť k pozastaveniu plynutia času, kým prevádzkovateľ nezíska od dotknutej osoby potrebné informácie, a to za predpokladu, že prevádzkovateľ požiadal o ďalšie informácie bez zbytočného odkladu. To isté platí, keď prevádzkovateľ požiada dotknutú osobu, aby špecifikovala spracovateľské operácie, ktorých sa žiadosť týka, ak sú splnené podmienky uvedené v odôvodnení 63.⁹¹

Príklad 31: Po prijatí žiadosti prevádzkovateľ okamžite zareaguje a požiada o informácie, ktoré potrebuje na potvrdenie totožnosti osoby, ktorá žiadosť podáva. Osoba odpovie až o niekoľko dní neskôr a informácie, ktoré dotknutá osoba posielala na overenie totožnosti, sa nezdajú dostatočné, a preto musí prevádzkovateľ požiadať o vysvetlenie. V tejto situácii dôjde k pozastaveniu plynutia času, kým prevádzkovateľ nezíska dostatok informácií na overenie totožnosti dotknutej osoby.

160. Lehota na odpoveď na žiadosť o prístup sa musí vypočítať v súlade s nariadením č. 1182/71⁹².

Príklad 32: Organizácia prijme žiadosť 5. marca. Lehota začína plynúť od toho istého dňa. Organizácia tak musí žiadosti vyhovieť najneskôr do 5. apríla vrátane.

Príklad 33: Ak organizácia prijme žiadosť 31. augusta a keďže nasledujúci mesiac je kratší, neexistuje zodpovedajúci dátum, dátumom odpovede je najneskôr posledný deň nasledujúceho mesiaca, teda 30. september.

⁸⁹ Pozri oddiel 2.3.3.

⁹⁰ V niektorých členských štátoch existujú vnútroštátne právne predpisy, v ktorých sa určuje, kedy sa správa považuje za prijatú, pričom sa berú do úvahy víkendy a štátne sviatky.

⁹¹ Pozri oddiel 2.3.1.

⁹² Nariadenie Rady (EHS, EURATOM) č. 1182/71 z 3. júna 1971, ktorým sa stanovujú pravidlá pre lehoty, dátumy a termíny.

161. Ak posledný deň tejto lehoty pripadne na víkend alebo sviatok, má prevádzkovateľ čas na odpoveď do nasledujúceho pracovného dňa.
162. Za určitých okolností môže prevádzkovateľ v prípade potreby predĺžiť čas na odpoveď na žiadosť o prístup o ďalšie dva mesiace, pričom zohľadní zložitosť a počet žiadostí. Treba zdôrazniť, že táto možnosť je výnimkou zo všeobecného pravidla a nemala by sa zneužívať. Ak sú prevádzkovatelia často nútení predĺžiť lehotu, mohlo by to naznačovať potrebu ďalej rozvíjať svoje všeobecné postupy na vybavovanie žiadostí.
163. To, čo predstavuje zložitú žiadosť, sa líši v závislosti od konkrétnych okolností každého prípadu. Niektoré z faktorov, ktoré možno považovať za relevantné, sú napríklad:
- množstvo údajov, ktoré prevádzkovateľ spracúva,
 - spôsob uchovávaní informácií, najmä ak je ťažké získať informácie, napríklad keď údaje spracúvajú rôzne oddelenia organizácie,
 - potreba upraviť informácie, keď sa uplatňuje výnimka, napríklad informácie týkajúce sa iných dotknutých osôb alebo informácie, ktoré predstavujú obchodné tajomstvo a
 - keď si informácie vyžadujú vykonanie ďalšej práce, aby boli zrozumiteľné.
164. Samotná skutočnosť, že vyhovie žiadosti by si vyžadovalo veľké úsilie, neznamená, že je žiadosť zložitá. Podobne by automaticky nespôsobila predĺženie lehoty skutočnosť, že veľká spoločnosť prijme veľký počet žiadostí. Ak však prevádzkovateľ dočasne prijme veľké množstvo žiadostí, napríklad z dôvodu mimoriadnej publicity o jeho činnostiach, možno to považovať za legitímny dôvod na predĺženie lehoty na odpoveď. Napriek tomu by prevádzkovateľ, najmä ten, ktorý vybavuje veľké množstvo údajov, mal mať zavedené postupy a mechanizmy, aby mohol za normálnych okolností vybaviť žiadosti v lehote.

6 LIMITY A OBMEDZENIA PRÁVA NA PRÍSTUP

6.1 Všeobecné poznámky

165. Právo na prístup podlieha obmedzeniam, ktoré vyplývajú z článku 15 ods. 4 všeobecného nariadenia o ochrane údajov (práva a slobody iných) a článku 12 ods. 5 všeobecného nariadenia o ochrane údajov (zjavne neopodstatnené alebo neprimerané žiadosti). Okrem toho sa v práve Únie alebo členského štátu môže v súlade s článkom 23 všeobecného nariadenia o ochrane údajov obmedziť právo na prístup. Výnimky týkajúce sa spracúvania osobných údajov na účely vedeckého, historického výskumu alebo štatistiky alebo na účely archivácie vo verejnom záujme môžu primerane vychádzať z článku 89 ods. 2 a 3 všeobecného nariadenia o ochrane údajov a výnimky pre spracúvanie vykonávané na novinárske účely alebo na účely akademickej, umeleckej alebo literárnej tvorby môžu vychádzať z článku 85 ods. 2 všeobecného nariadenia o ochrane údajov.
166. Je dôležité poznamenať, že okrem uvedených limitov, výnimiek a možných obmedzení nie sú vo všeobecnom nariadení o ochrane údajov povolené žiadne ďalšie výnimky alebo odchýlky z práva na prístup. To okrem iného znamená, že právo na prístup je bez akejkoľvek všeobecnej výhrady k proporcionality, pokiaľ ide o úsilie, ktoré musí prevádzkovateľ vynaložiť na zabezpečenie súladu so

žiadostou dotknutej osoby podľa článku 15 všeobecného nariadenia o ochrane údajov⁹³. Ďalej nie je dovolené limitovať alebo obmedziť právo na prístup v zmluve medzi prevádzkovateľom a dotknutou osobou.

167. Podľa odôvodnenia 63 sa právo na prístup udeľuje dotknutým osobám, aby si boli vedomé zákonnosti spracúvania a mohli si ju overiť. Právo na prístup okrem iného umožňuje dotknutej osobe dosiahnuť v závislosti od okolností opravu, vymazanie alebo zablokovanie osobných údajov⁹⁴. Dotknuté osoby však nie sú povinné uvádzať dôvody alebo odôvodňovať svoju žiadosť. Pokiaľ sú požiadavky článku 15 všeobecného nariadenia o ochrane údajov splnené, účely, ktoré sú dôvodom žiadosti, by sa mali považovať za irelevantné⁹⁵.

6.2 Článok 15 ods. 4 všeobecného nariadenia o ochrane údajov

168. Podľa článku 15 ods. 4 všeobecného nariadenia o ochrane údajov nesmie mať právo získať kópiu nepriaznivé dôsledky na práva a slobody iných. Vysvetlenia tohto obmedzenia sú uvedené v piatej a šiestej vete odôvodnenia 63. Uvedené právo by sa nemalo nepriaznivo dotknúť práv alebo slobôd iných osôb, ani obchodného tajomstva alebo práv duševného vlastníctva a najmä autorských práv týkajúcich sa softvéru.

Výsledkom zohľadnenia týchto prvkov by však nemalo byť odmietnutie poskytnutia akýchkoľvek informácií dotknutej osobe. Pri výklade článku 15 ods. 4 všeobecného nariadenia o ochrane údajov treba venovať osobitnú pozornosť tomu, aby sa neodôvodnene nerozšírili obmedzenia stanovené v článku 23 všeobecného nariadenia o ochrane údajov, ktoré sú prípustné len za prísnych podmienok.

169. Článok 15 ods. 4 všeobecného nariadenia o ochrane údajov sa vzťahuje na právo získať kópiu údajov, čo je hlavný spôsob poskytovania prístupu k spracúvaným údajom (druhá zložka práva na prístup). Platí to aj v prípade, ak je prístup k osobným údajom výnimočne umožnený iným spôsobom ako kópiou, pričom sa berú do úvahy práva a slobody iných. Napríklad neexistuje žiadny odôvodnený rozdiel v tom, či je obchodné tajomstvo dotknuté poskytnutím kópie alebo umožnením prístupu na mieste dotknutej osobe. Článok 15 ods. 4 všeobecného nariadenia o ochrane údajov sa nevzťahuje na doplňujúce informácie o spracúvaní uvedené v článku 15 ods. 1 písm. a) až h) všeobecného nariadenia o ochrane údajov.
170. Podľa odôvodnenia 63 medzi protichodné práva a slobody patria obchodné tajomstvá alebo duševné vlastníctvo a najmä autorské práva týkajúce sa softvéru. Tieto výslovne uvedené práva a slobody by sa mali považovať len za príklady, keďže v zásade všetky práva alebo slobody založené na práve Únie alebo členského štátu možno považovať za také, pri ktorých sa uplatňuje obmedzenie podľa článku 15 ods. 4 všeobecného nariadenia o ochrane údajov⁹⁶. Právo na ochranu osobných údajov (článok 8 Európskej charty základných práv) teda možno považovať aj za dotknuté právo v zmysle článku 15

⁹³ Ak prevádzkovateľ spracúva veľké množstvo informácií týkajúcich sa dotknutej osoby, ako je uvedené v odôvodnení 63 všeobecného nariadenia o ochrane údajov, prevádzkovateľ môže dotknutú osobu požiadať, aby spresnila, ktorých informácií alebo spracovateľských činností sa jej žiadosť týka. Pozri aj oddiel 2.3.1.

⁹⁴ Rozsudok Súdneho dvora, YS a i., spojené veci C-141/12 a C-372/12.

⁹⁵ Nie sú tým dotknuté žiadne platné vnútroštátne právne predpisy, ktoré sú v súlade s požiadavkami stanovenými v článku 23 všeobecného nariadenia o ochrane údajov, pozri kapitolu 6.4.

⁹⁶ Váha alebo priorita protichodných práv a slobôd nie sú otázkou vymedzenia pojmov „práva a slobody“. Vyváženie takýchto záujmov je však súčasťou druhého kroku posudzovania, či je uplatniteľný článok 15 ods. 4. Pozri bod 173 ďalej.

ods. 4 všeobecného nariadenia o ochrane údajov. Pokiaľ ide o právo získať kópiu, právo na ochranu údajov iných osôb je typickým prípadom, pri ktorom treba posúdiť obmedzenie. Okrem toho je potrebné zohľadniť právo na dôvernosť korešpondencie, napríklad pokiaľ ide o súkromnú e-mailovú korešpondenciu v súvislosti so zamestnaním⁹⁷. Je dôležité poznamenať, že nie každý záujem predstavuje „práva a slobody“ podľa článku 15 ods. 4 všeobecného nariadenia o ochrane údajov. Napríklad, hospodárske záujmy podniku nezverejniť osobné údaje nedosahujú hranicu pre uplatnenie výnimky v článku 15 ods. 4, pokiaľ nie sú dotknuté obchodné tajomstvá, duševné vlastníctvo alebo iné chránené práva.

171. „Iných“ znamená akúkoľvek inú osobu alebo subjekt okrem dotknutej osoby, ktorá si uplatňuje svoje právo na prístup. Preto je možné zvážiť práva a slobody prevádzkovateľa alebo sprostredkovateľa (napríklad pri zachovaní dôvernosti obchodných tajomstiev a duševného vlastníctva). Ak by zákonodarca EÚ chcel vylúčiť práva a slobody prevádzkovateľov alebo sprostredkovateľov, použil by pojem „tretia strana“, ktorý je vymedzený v článku 4 bode 10 všeobecného nariadenia o ochrane údajov.
172. Všeobecná obava, že vyhovením žiadosti o prístup môžu byť dotknuté práva a slobody iných, nestačí na odvolanie sa na článok 15 ods. 4 všeobecného nariadenia o ochrane údajov. Prevádzkovateľ musí byť schopný preukázať, že v konkrétnej situácii by v skutočnosti boli dotknuté práva alebo slobody iných.

Príklad 34: O osobu, ktorá je dnes už dospelá, sa v minulosti niekoľko rokov staral úrad starostlivosti o mládež. S tým súvisiace súbory môžu prípadne obsahovať citlivé informácie o iných osobách (rodičoch, sociálnych pracovníkoch, iných maloletých osobách). Žiadosť o informácie od dotknutej osoby však vo všeobecnosti nemožno z tohto dôvodu odmietnuť s odkazom na článok 15 ods. 4 všeobecného nariadenia o ochrane údajov. Predovšetkým, úrad starostlivosti o mládež ako prevádzkovateľ musí podrobne preskúmať a preukázať práva a slobody iných. V závislosti od príslušných záujmov a ich relatívnej váhy môže byť poskytnutie takýchto konkrétnych informácií zamietnuté (napr. úpravou mien).

173. Vzhľadom na odôvodnenie 4 všeobecného nariadenia o ochrane údajov a zmysel článku 52 ods. 1 Európskej charty základných práv, právo na ochranu osobných údajov nie je absolútnym právom⁹⁸. Preto aj výkon práva na prístup musí byť vyvážený ostatnými základnými právami v súlade so zásadou proporcionality. Ak posúdenie článku 15 ods. 4 všeobecného nariadenia o ochrane údajov preukazuje, že vyhovenie žiadosti má nepriaznivé (negatívne) účinky na práva a slobody ostatných účastníkov (krok 1), treba zvážiť záujmy všetkých účastníkov s prihliadnutím na konkrétne okolnosti prípadu, a najmä pravdepodobnosť a závažnosť rizík prítomných pri oznamovaní údajov. Prevádzkovateľ by sa mal pokúsiť zosúladiť protichodné práva (krok 2), napríklad prostredníctvom vykonania primeraných opatrení na zmiernenie rizika pre práva a slobody iných. Ako je zdôraznené v odôvodnení 63, ochrana práv a slobôd iných na základe článku 15 ods. 4 všeobecného nariadenia o ochrane údajov by nemala viesť k odmietnutiu poskytnúť dotknutej osobe všetky informácie. To napríklad znamená, že tam, kde platí obmedzenie, informácie týkajúce sa iných musia byť v čo najväčšej možnej miere nečitateľné namiesto toho, aby sa odmietlo poskytnutie kópie osobných údajov. Ak však nie je možné nájsť riešenie zosúladenia príslušných práv, musí prevádzkovateľ v ďalšom kroku rozhodnúť, ktoré z protichodných práv a slobôd má prednosť (krok 3).

⁹⁷ ESĽP, Bărbulescu/Rumunsko, č. 61496/08, bod 80, 5. septembra 2017.

⁹⁸ Pozri napríklad aj rozsudok Súdneho dvora z 9. novembra 2010, Volker und Markus Schecke GbR a Hartmut Eifert/Spolková krajina Hesensko, spojené veci C-92/09 a C-93/09, [GC], bod 48.

Príklad 35: Predajca ponúka svojim klientom možnosť objednať si produkty prostredníctvom horúcej linky, ktorú prevádzkuje jeho zákaznícky servis. Na účely preukázania obchodných transakcií predajca uchováva záznam hovoru v súlade s prísnyimi požiadavkami platných právnych predpisov. Zákazník chce získať kópiu rozhovoru, ktorý mal so zástupcom zákazníckeho servisu. V prvom kroku predajca analyzuje požiadavku a zistí, že záznam obsahuje osobné údaje, ktoré sa týkajú aj niekoho iného, konkrétne zástupcu zákazníckeho servisu. V druhom kroku, s cieľom posúdiť, či by poskytnutie kópie malo vplyv na práva a slobody iných, musí predajca vyvážiť protichodné záujmy, najmä s prihliadnutím na pravdepodobnosť a závažnosť možných rizík pre práva a slobody zástupcu zákazníckeho servisu, ktoré sú prítomné pri oznamovaní záznamu klientovi. Predajca dospel k záveru, že v zázname sú len veľmi obmedzené osobné údaje týkajúce sa zástupcu zákazníckeho servisu, iba jeho hlas. Predajca/prevádzkovateľ zistí, že zástupca nie je ľahko identifikovateľný. Navyše obsah diskusie má odborný charakter a dotknutá osoba bola účastníkom rozhovoru. Na základe uvedených okolností prevádzkovateľ objektívne usudzuje, že právo na prístup nemá nepriaznivý vplyv na práva a slobody zástupcu zákazníckeho servisu, a preto môže prevádzkovateľ poskytnúť dotknutej osobe úplný záznam vrátane častí hlasového záznamu, ktorý sa týka zástupcu zákazníckeho servisu.

Príklad 36: Klientka predajne zdravotníckych potrieb chce mať prístup k výsledkom meraní týkajúcich sa jej nôh na základe článku 15 všeobecného nariadenia o ochrane údajov. Obchod so zdravotníckymi potrebami zmeral nohy dotknutej osoby, aby mohol vyrobiť individuálne lekárske kompresné pančuchy. Obchod so zdravotníckymi potrebami mal zrejme veľa skúseností a zaviedol špeciálnu techniku na presné meranie. Po premeraní v predajni zdravotníckych potrieb chce klientka využiť výsledky merania na nákup lacnejších ponožiek na inom mieste (objednávkou cez internet). Predajňa zdravotníckych potrieb čiastočne odmieta prístup k údajom na základe článku 15 ods. 4 všeobecného nariadenia o ochrane údajov a tvrdí, že vďaka ich špeciálnym a presným meracím technikám boli výsledky chránené ako obchodné tajomstvo. Ak a pokiaľ je prevádzkovateľ schopný preukázať, že:

- poskytnutie informácií o výsledkoch meraní dotknutej osobe nie je možné bez toho, aby sa prezradilo, ako boli merania uskutočnené a
- informácie o spôsobe vykonania meraní vrátane, ak je to relevantné, presného určenia meracích bodov sú obchodným tajomstvom

môže uplatniť článok 15 ods. 4 všeobecného nariadenia o ochrane údajov.

Prevádzkovateľ by aj tak musel poskytnúť čo najviac informácií o výsledkoch merania, ktoré by neprezradili jeho obchodné tajomstvo, aj keď by to znamenalo vyvinúť snahu o revíziu a úpravu výsledkov.

Príklad 37: HRÁČ X je registrovaný ako používateľ hernej platformy PLATFORMY Y. Jedného dňa HRÁČ X dostane upozornenie, že jeho online účet bol obmedzený. Keďže sa už nemôže prihlásiť, HRÁČ X požiada prevádzkovateľa o prístup ku všetkým osobným údajom, ktoré sa ho týkajú. Okrem toho HRÁČ X vyžaduje prístup k dôvodom obmedzenia účtu. PLATFORMA Y, prevádzkovateľ online hernej platformy, ktorej bola žiadosť podaná, informuje používateľov vo svojich všeobecných podmienkach dostupných na jej webovom sídle, že akýkoľvek druh podvádzania (najmä použitím softvéru tretích strán) bude mať za následok dočasný alebo trvalý zákaz využívania platformy. PLATFORMA Y takisto informuje používateľov vo svojich zásadách ochrany osobných údajov

o spracúvaní osobných údajov na účely odhaľovania herných podvodov v súlade s požiadavkami uvedenými v článku 13 všeobecného nariadenia o ochrane údajov.

Po prijatí žiadosti HRÁČAX o prístup by PLATFORMA Y mala HRÁČOVIX poskytnúť kópiu spracúvaných osobných údajov o HRÁČOVI X. Pokiaľ ide o dôvod obmedzenia účtu, PLATFORMA Y by mala potvrdiť HRÁČOVIX, že sa rozhodla obmedziť jeho prístup k online hrám z dôvodu použitia jedného alebo opakovaných herných podvodov, ktoré sú v rozpore so všeobecnými podmienkami používania. Okrem informácií poskytnutých o spracúvaní na účely odhaľovania herných podvodov by PLATFORMA Y mala HRÁČOVI X poskytnúť prístup k informáciám, ktoré má uložené o jeho herných podvodoch, ktoré viedli k obmedzeniu. PLATFORMA Y by mala HRÁČOVI X poskytnúť najmä informácie, ktoré viedli k obmedzeniu účtu (*napr.* prehľad záznamov, dátum a čas podvádzania, odhalenie softvéru tretej strany...), aby si dotknutá osoba (*t. j.* HRÁČ X) mohla overiť správnosť spracúvania údajov.

Podľa článku 15 ods. 4 a odôvodnenia 63 všeobecného nariadenia o ochrane údajov však PLATFORMA Y nie je povinná odhaliť žiadnu časť technickej prevádzky softvéru proti podvádzaniu, aj keď sa tieto informácie týkajú HRÁČA X, pokiaľ to možno považovať za obchodné tajomstvo. Nevyhnutné vyváženie záujmov podľa článku 15 ods. 4 všeobecného nariadenia o ochrane údajov bude mať za následok, že obchodné tajomstvá PLATFORMY Y bránia zverejneniu týchto osobných údajov, pretože znalosť technického fungovania softvéru proti podvádzaniu by takisto mohla používateľovi umožniť obísť budúce odhalenie podvodu alebo podvádzania⁹⁹.

174. Ak prevádzkovatelia odmietnu konať na základe žiadosti o právo na prístup úplne alebo čiastočne podľa článku 15 ods. 4 všeobecného nariadenia o ochrane údajov, bezodkladne a najneskôr do jedného mesiaca, musia dotknutú osobu informovať o dôvodoch (článok 12 ods. 4 všeobecného nariadenia o ochrane údajov). V zdôvodnení je potrebné odvolať sa na konkrétne okolnosti, aby sa umožnilo dotknutým osobám posúdiť, či chcú proti odmietnutiu prijať opatrenia. Zdôvodnenie musí obsahovať informácie o možnosti podať sťažnosť dozornému orgánu (článok 77 všeobecného nariadenia o ochrane údajov) a požiadať o súdny prostriedok nápravy (článok 79 všeobecného nariadenia o ochrane údajov).

6.3 Článok 12 ods. 5 všeobecného nariadenia o ochrane údajov

175. Článok 12 ods. 5 všeobecného nariadenia o ochrane údajov umožňuje prevádzkovateľom neprihliadať na žiadosti o právo na prístup, ktoré sú zjavne neopodstatnené alebo neprimerané. Tieto pojmy sa musia vykladať reštriktívne, pretože sa nesmú oslabiť zásady transparentnosti a bezplatnosť práv dotknutých osôb.
176. Prevádzkovatelia musia byť schopní preukázať jednotlivcovi, prečo sa domnievajú, že žiadosť je zjavne neopodstatnená alebo neprimeraná a na požiadanie vysvetliť dôvody príslušnému dozornému orgánu. Každá žiadosť by sa mala posudzovať v závislosti od prípadu k prípadu v kontexte, v ktorom bola podaná, aby sa rozhodlo, či je zjavne neopodstatnená alebo neprimeraná.

⁹⁹ Rozsah informácií poskytovaných jednotlivcom bude výrazne závisieť od kontextu, pričom sa zohľadní povaha prevádzkovateľa a povaha porušenia podmienok služby. V niektorých prípadoch majú prevádzkovatelia možnosť poskytnúť len základné informácie v odpovedi na žiadosť o prístup, na ktorú sa vzťahuje článok 15 ods. 4.

6.3.1 Čo znamená zjavne neopodstatnená?

177. Žiadosť o právo na prístup je zjavne neopodstatnená, ak pri uplatňovaní objektívneho prístupu jednoznačne a očividne nie sú splnené požiadavky článku 15 všeobecného nariadenia o ochrane údajov. Ako sa však vysvetľuje najmä v oddiele 3, existuje len veľmi málo takýchto predpokladov pre žiadosť o právo na prístup. EDPB preto zdôrazňuje, že pokiaľ ide o žiadosť o právo na prístup, existuje len veľmi obmedzený priestor na odvolávanie sa na „zjavne neopodstatnenú“ možnosť podľa článku 12 ods. 5 všeobecného nariadenia o ochrane údajov.
178. Okrem toho je dôležité pripomenúť, že pred uplatnením obmedzenia musia prevádzkovatelia dôkladne analyzovať obsah a rozsah žiadosti. Žiadosť by sa napríklad nemala považovať za zjavne neopodstatnenú, ak súvisí so spracúvaním osobných údajov, na ktoré sa nevzťahuje všeobecné nariadenie o ochrane údajov (v tomto prípade by sa žiadosť vôbec nemala posudzovať ako žiadosť podľa článku 15).
179. Iné prípady, v ktorých je uplatňovanie článku 12 ods. 5 všeobecného nariadenia o ochrane údajov sporné, predstavujú žiadosti súvisiace s informáciami alebo spracovateľskými činnosťami, ktoré jednoznačne a zjavne nepodliehajú spracovateľským činnostiam prevádzkovateľa.

Príklad 38: Dotknutá osoba sa obráti na obecný úrad so žiadosťou o údaje, ktoré spracúva štátny orgán. Namiesto tvrdenia, že žiadosť je zjavne neopodstatnená, by bolo pre oslovený orgán vhodnejšie a jednoduchšie potvrdiť, že tieto údaje orgán nespracúva (prvá zložka článku 15 všeobecného nariadenia o ochrane údajov: „či“ sa spracúvajú osobné údaje)¹⁰⁰.

180. Prevádzkovateľ by nemal predpokladať, že žiadosť je zjavne neopodstatnená, pretože dotknutá osoba už predtým predložila žiadosti, ktoré boli zjavne neopodstatnené alebo neprimerané alebo ak obsahuje neobjektívny alebo nevhodný jazyk.

6.3.2 Čo znamená neprimeraná?

181. Vo všeobecnom nariadení o ochrane údajov neexistuje žiadne vymedzenie pojmu „neprimeraný“. Na jednej strane znenie „najmä pre ich opakujúcu sa povahu“ v článku 12 ods. 5 všeobecného nariadenia o ochrane údajov umožňuje dospieť k záveru, že hlavný scenár na uplatnenie tohto tvrdenia vzhľadom na článok 15 všeobecného nariadenia o ochrane údajov súvisí s množstvom žiadostí dotknutej osoby o právo na prístup. Na druhej strane z uvedenej formulácie vyplýva, že nie sú *a priori* vylúčené iné dôvody, ktoré by mohli spôsobiť neprimeranosť.
182. Samozrejme, podľa článku 15 ods. 3 všeobecného nariadenia o ochrane údajov týkajúceho sa práva na získanie kópie môže dotknutá osoba podať prevádzkovateľovi viac ako jednu žiadosť¹⁰¹. V prípade žiadostí, ktoré by sa potenciálne mohli považovať za neprimerané, posúdenie „neprimeranosti“ závisí od analýzy, ktorú vykoná prevádzkovateľ a od špecifik odvetvia, v ktorom pôsobí.
183. V prípade následných žiadostí sa musí posúdiť, či bol alebo nebol prekročený prah primeraných intervalov (pozri odôvodnenie 63). Prevádzkovatelia musia starostlivo zvážiť konkrétne okolnosti každého prípadu.

¹⁰⁰ Iná otázka je, či orgán, ktorému bola žiadosť o prístup adresovaná, je oprávnený postúpiť žiadosť príslušnému štátnemu orgánu.

¹⁰¹ Podľa článku 15 ods. 3 druhej vety môže prevádzkovateľ za ďalšie požadované kópie účtovať primeraný poplatok.

184. Napríklad v prípade sociálnych sietí sa bude zmena súboru údajov očakávať v kratších intervaloch ako v prípade katastrov nehnuteľností alebo centrálnych registrov spoločností. V prípade obchodných partnerov treba zvážiť frekvenciu kontaktov so zákazníkom. V súlade s tým sú odlišné aj „primerané intervaly“, v rámci ktorých môžu dotknuté osoby znova uplatniť svoje právo na prístup. Čím častejšie sa v databáze prevádzkovateľa vyskytujú zmeny, tým častejšie môže byť dotknutým osobám umožnené žiadať o prístup k ich osobným údajom bez toho, aby sa žiadosť považovala za neprimeranú. Na druhej strane, druhá žiadosť tej istej dotknutej osoby by sa za určitých okolností mohla považovať za opakujúcu sa.
185. Pri rozhodovaní o tom či uplynul primeraný interval, by prevádzkovatelia mali z hľadiska primeraných očakávaní dotknutej osoby zvážiť toto:
- ako často sa údaje menia – je nepravdepodobné, že by sa medzi jednotlivými žiadosťami informácie zmenili? Ak súbor údajov zjavne nepodlieha inému spracúvaniu ako uchovávaniu a dotknutá osoba si je toho vedomá, napr. z dôvodu predchádzajúcej žiadosti o právo na prístup, môže ísť o znak neprimeranej žiadosti;
 - povaha údajov – môže sem patriť to, či sú údaje obzvlášť citlivé;
 - účely spracúvania – tieto účely môžu zahŕňať, či je pravdepodobné, že spracúvanie spôsobí žiadateľovi nepriaznivé následky (škodu), ak bude zverejnené;
 - či sa následné žiadosti týkajú rovnakého druhu informácií alebo spracovateľských činností alebo iných druhov informácií alebo spracovateľských činností¹⁰².

Príklad 39 (tesár): Dotknutá osoba podáva žiadosti o prístup **každé dva mesiace** tesárovi, ktorý pre ňu vyrobil stôl. Na prvú žiadosť odpovedal tesár úplne. Pri rozhodovaní o tom, či uplynul primeraný interval, treba brať do úvahy to, že tesár spracúva a zhromažďuje osobné údaje iba príležitostne (prvá zarážka v tomto bode) a nie ako súčasť svojej hlavnej činnosti a je ešte menej pravdepodobné, že stolár často poskytuje služby tej istej dotknutej osobe. V tomto prípade tesár skutočne neposkytol viac ako jednu službu dotknutej osobe, takže je nepravdepodobné, že by došlo k zmenám v súbore údajov týkajúcich sa dotknutej osoby. Najmä vzhľadom na povahu a množstvo spracúvaných osobných údajov možno riziká súvisiace so spracúvaním považovať za nízke (druhá zarážka v tomto bode), ako napríklad účel spracúvania (účely fakturácie a dodržiavanie povinnosti viesť záznamy) pravdepodobne nespôsobí nepriaznivé následky dotknutej osobe (tretia zarážka v tomto bode). Žiadosť sa okrem toho týka rovnakých informácií ako posledná žiadosť (štvrtá zarážka v tomto bode). Takéto žiadosti môžu byť následne považované za neprimerané z dôvodu ich opakovania.

Príklad 40 (platforma sociálnych médií): Platforma sociálnych médií, ktorej hlavnou činnosťou je zhromažďovanie a/alebo spracúvanie osobných údajov dotknutej osoby, vykonáva rozsiahle komplexné a nepretržité spracovateľské činnosti. Dotknutá osoba, ktorá využíva služby platformy, podáva žiadosti o prístup **každé tri mesiace**. V tomto prípade sú časté zmeny osobných údajov týkajúce sa dotknutej osoby vysoko pravdepodobné (prvá zarážka v tomto bode), široký rozsah zhromaždených údajov zahŕňa vyведенé citlivé osobné údaje (druhá zarážka v tomto bode) spracúvané na účely zobrazenia relevantného obsahu a členov siete dotknutej osobe (tretia zarážka). Žiadosti o prístup

¹⁰² Ak sa následná žiadosť týka rovnakého druhu informácií v rozsahu A čase, nejde o neprimeranosť, ale o otázku žiadosti o dodatočnú kópiu, pozri oddiel 2.2.2.2.

každé tri mesiace nemožno za týchto okolností v zásade považovať za neprimerané z dôvodu opakovania.

Príklad 41 (úverové agentúry): Rovnako ako v prípade sociálnych sietí nie je možné vylúčiť, že k úpravám relevantných údajov, ktoré majú úverové agentúry, dôjde v oveľa kratších intervaloch ako v iných oblastiach (prvá zarážka v tomto bode). Vyplýva to z mnohých faktorov, ktoré si dotknutá osoba ako osoba zvonka zvyčajne neuvedomuje z dôvodu zložitosti obchodného modelu. Odpoveď na otázku, aké typy údajov boli zozbierané na výpočet hodnoty skóre zo strany prevádzkovateľa a ktoré sú v súčasnosti zahrnuté do výpočtu, môže preto poskytnúť iba samotná úverová agentúra. Okrem toho spracúvanie údajov prostredníctvom úverových agentúr a výsledná hodnota skóre môže mať pre dotknutú osobu ďalekosiahle dôsledky, pokiaľ ide o zamýšľané právne transakcie, ako je uzatvorenie kúpnych, nájomných alebo lízingsových zmlúv (tretia zarážka v tomto bode).

Nie je možné všeobecne určiť konkrétny interval, v ktorom by sa podanie ďalšej žiadosti o prístup mohlo považovať za neprimerané podľa článku 12 ods. 5 druhej vety všeobecného nariadenia o ochrane údajov. Vyžaduje sa skôr celkové posúdenie okolností konkrétneho prípadu. Vzhľadom na význam spracúvania údajov pre realitu každodenného života dotknutých osôb sa však dá predpokladať, že **ročný interval** medzi informáciami poskytnutými bezplatne bude v každom prípade príliš dlhý na to, aby sa žiadosť považovala za neprimeranú. Ak je žiadosť podaná vo veľmi krátkom intervale, rozhodujúce by malo byť, či má dotknutá osoba dôvod domnievať sa, že sa informácie alebo spracúvanie od poslednej žiadosti zmenili. Napríklad, ak dotknutá osoba uskutočnila finančnú transakciu, ako je napríklad pôžička, dotknutá osoba by mala mať právo požiadať o prístup k informáciám o úvere aj keď bola takáto žiadosť predložená a zodpovedaná krátko predtým.

186. Ak je možné poskytnúť informácie jednoducho elektronickými prostriedkami alebo vzdialeným prístupom do zabezpečeného systému, čo znamená, že vyhovie takýmto žiadostiam v skutočnosti nezaťažuje prevádzkovateľa, je nepravdepodobné, že následné žiadosti možno považovať za neprimerané.
187. Ak sa žiadosť prekrýva s predchádzajúcou žiadosťou, prekrývajúca sa žiadosť možno vo všeobecnosti považovať za neprimeranú, ak sa týka presne tých istých informácií alebo spracovateľských činností a predchádzajúcej žiadosti prevádzkovateľ ešte nevyhovel, pričom zatiaľ nedosiahol stav „bez zbytočného odkladu“ (pozri článok 12 ods. 3 všeobecného nariadenia o ochrane údajov). V praxi by sa v dôsledku toho mohli obe žiadosti spojiť.
188. Skutočnosť, že poskytnutie informácií alebo kópie dotknutej osobe by si od prevádzkovateľa vyžadovalo obrovské množstvo času a úsilia, nemôže byť sama osebe dôvodom, že žiadosť bude neprimeraná¹⁰³. Veľký počet spracovateľských činností si zvyčajne vyžaduje väčšie úsilie pri vybavovaní žiadostí o prístup. Ako však už bolo uvedené, za určitých okolností možno žiadosti považovať za neprimerané z iných dôvodov, než je ich opakujúca sa povaha. Podľa názoru EDPB to zahŕňa najmä prípady nadmerného odvolávania sa na článok 15 všeobecného nariadenia o ochrane údajov, čo znamená prípady, keď dotknuté osoby neprimerane využívajú právo na prístup s jediným úmyslom, spôsobiť prevádzkovateľovi škodu alebo nepriaznivé následky.
189. V tejto súvislosti by sa žiadosť nemala považovať za neprimeranú z dôvodu, že:

¹⁰³ Žiadny test proporcionality, pozri bod 166.

- dotknutá osoba neuvedie žiadne dôvody žiadosti alebo prevádzkovateľ považuje žiadosť za nezmyselnú,
- dotknutá osoba používa nevhodný alebo nezdvorilý jazyk,
- dotknutá osoba má v úmysle použiť údaje na uplatnenie ďalších nárokov voči prevádzkovateľovi.¹⁰⁴

190. Na druhej strane sa môže žiadosť považovať za neprimeranú, napríklad ak:

- jednotlivец podá žiadosť, ale zároveň ponúkne jej stiahnutie výmenou za určitú formu výhody od prevádzkovateľa, alebo
- žiadosť má zlý úmysel a používa sa na obťažovanie prevádzkovateľa alebo jeho zamestnancov iba s jediným účelom, a to spôsobiť narušenie, napríklad na základe skutočnosti, že:
 - jednotlivец v samotnej žiadosti alebo v inej komunikácii výslovne uviedol, že má v úmysle spôsobiť narušenie a nič iné, alebo
 - jednotlivец v rámci kampane systematicky posiela prevádzkovateľovi rôzne požiadavky, napr. raz týždenne so zámerom a účinkom spôsobiť narušenie¹⁰⁵.

6.3.3 Dôsledky

191. V prípade zjavne neopodstatnenej alebo neprimeranej žiadosti o právo na prístup môžu prevádzkovatelia podľa článku 12 ods. 5 všeobecného nariadenia o ochrane údajov buď požadovať primeraný poplatok (zohľadňujúci administratívne náklady na poskytnutie informácií alebo na oznámenie alebo na uskutočnenie požadovaného opatrenia), alebo odmietnuť vyhovieť žiadosti.
192. EDPB poukazuje na to, že prevádzkovatelia na jednej strane nie sú vo všeobecnosti povinní účtovať primeraný poplatok predtým ako odmietnu konať na základe žiadosti. Na druhej strane, ani oni si medzi týmito dvoma alternatívami nemôžu úplne slobodne vybrať. V skutočnosti musia prevádzkovatelia prijať primerané rozhodnutie v závislosti od konkrétnych okolností prípadu. Zatiaľ čo je len ťažko predstaviteľné, že účtovanie primeraného poplatku je vhodným opatrením v prípade zjavne neopodstatnených žiadostí, pri neprimeraných žiadostiach bude – v súlade so zásadou transparentnosti – často vhodnejšie účtovať poplatok ako náhradu za administratívne náklady, ktoré opakujúce sa požiadavky spôsobujú.
193. Prevádzkovateľ musí byť schopný preukázať zjavne neopodstatnenú alebo neprimeranú povahu žiadosti (článok 12 ods. 5 tretia veta všeobecného nariadenia o ochrane údajov). Preto sa odporúča zabezpečiť riadne zdokumentovanie základných skutočností. V súlade s článkom 12 ods. 4 všeobecného nariadenia o ochrane údajov, ak prevádzkovatelia úplne alebo čiastočne odmietnu konať na základe žiadosti o prístup, musia dotknutú osobu bezodkladne, najneskôr však do jedného mesiaca od prijatia žiadosti informovať o
- dôvode nekonania,

¹⁰⁴ Nie sú tým dotknuté žiadne platné vnútroštátne právne predpisy, ktoré sú v súlade s požiadavkami stanovenými v článku 23 všeobecného nariadenia o ochrane údajov, pozri kapitolu 6.4.

¹⁰⁵ „Systematicky odosielané ako súčasť kampane“ znamená, že žiadosti, ktoré by sa dali ľahko spojiť do jednej, dotknutá osoba umelo rozdelí nielen na niekoľko, ale aj množstvo jednotlivých častí, so zjavným úmyslom spôsobiť narušenie.

- práve podať sťažnosť dozornému orgánu,
- možnosti domáhať sa súdneho prostriedku nápravy.

194. Pred účtovaním primeraného poplatku na základe článku 12 ods. 5 všeobecného nariadenia o ochrane údajov by prevádzkovatelia mali dotknutým osobám poskytnúť informácie o svojom pláne požadovať poplatok. Dotknuté osoby musia mať možnosť rozhodnúť sa, či stiahnu žiadosť, aby sa vyhli spoplatneniu.
195. Neodôvodnené zamietnutie žiadostí o právo na prístup možno považovať za porušenie práv dotknutej osoby podľa článkov 12 až 22 všeobecného nariadenia o ochrane údajov, a preto môže podliehať výkonu nápravných právomocí zo strany príslušných dozorných orgánov vrátane správnych pokút na základe článku 83 ods. 5 písm. b) všeobecného nariadenia o ochrane údajov. Ak sa dotknuté osoby domnievajú, že došlo k porušeniu ich práv dotknutej osoby, majú právo podať sťažnosť na základe článku 77 všeobecného nariadenia o ochrane údajov.

6.4 Prípustné obmedzenia v práve Únie alebo členských štátov na základe článku 23 všeobecného nariadenia o ochrane údajov a výnimky

196. Rozsah povinností a práv stanovených v článku 15 všeobecného nariadenia o ochrane údajov môže byť obmedzené prostredníctvom legislatívnych opatrení v práve Únie alebo členských štátov¹⁰⁶.
197. Prevádzkovatelia, ktorí plánujú využiť obmedzenie založené na vnútroštátnom práve, musia dôkladne skontrolovať požiadavky ustanovenia príslušných vnútroštátnych právnych predpisov. Ďalej je dôležité poznamenať, že obmedzenia práva na prístup v práve členských štátov (alebo Únie), ktoré sú založené na článku 23 všeobecného nariadenia o ochrane údajov, musia prísne spĺňať podmienky stanovené v tomto ustanovení. EDPB vydal usmernenia 10/2020 k obmedzeniam podľa článku 23 všeobecného nariadenia o ochrane údajov s ďalšími vysvetleniami. Pokiaľ ide o právo na prístup, EDPB pripomína, že prevádzkovatelia by mali obmedzenia zrušiť hneď ako zaniknú okolnosti, ktoré odôvodňujú ich zavedenie¹⁰⁷.
198. V legislatívnych opatreniach, ktoré sa týkajú obmedzení podľa článku 23 všeobecného nariadenia o ochrane údajov, sa môže takisto uvádzať, že uplatňovanie práva sa oneskorí, že právo sa bude uplatňovať čiastočne alebo sa zameria len na určité kategórie údajov alebo že právo bude možné uplatniť nepriamo prostredníctvom nezávislého dozorného orgánu¹⁰⁸.

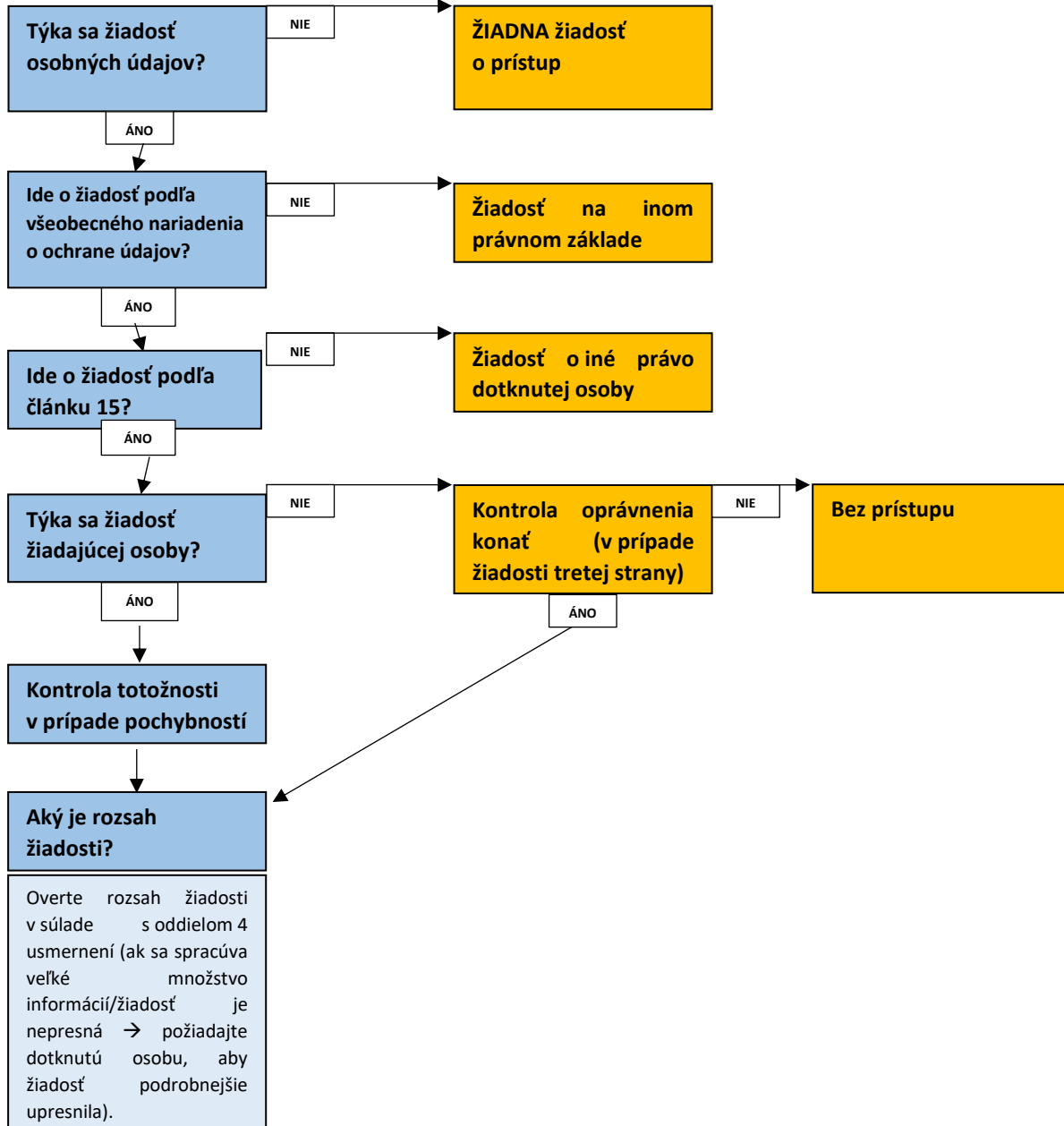
¹⁰⁶ Pozri napríklad oddiely 32 až 37 nemeckého spolkového zákona o ochrane údajov (BDSG), oddiely 16 a 17 nórskeho zákona o osobných údajoch a kapitolu 5 švédskeho zákona o ochrane údajov.

¹⁰⁷ Bod 76, Usmernení 10/2020 k obmedzeniam podľa článku 23 všeobecného nariadenia o ochrane údajov, verzia 2.0, prijaté 13. októbra 2021.

¹⁰⁸ Bod 12, Usmernení 10/2020 k obmedzeniam podľa článku 23 všeobecného nariadenia o ochrane údajov, verzia 2.0, prijaté 13. októbra 2021. V oddiele 34 ods. 3 nemeckého spolkového zákona o ochrane údajov sa napríklad uvádza, že ak orgán verejnej moci neposkytne informácie dotknutej osobe vyhovujúcej žiadosti o právo na prístup z dôvodu určitých obmedzení, tieto informácie poskytne spolkový dozorný orgán na žiadosť dotknutej osoby, pokiaľ zodpovedný najvyšší spolkový orgán (orgánu, ktorý bol predmetom žiadosti) v konkrétnom prípade nerozhodne, že by to ohrozilo bezpečnosť spolkovej republiky alebo spolkovej krajiny. Taliansky DPCode poskytuje nepriamy prístup (prostredníctvom orgánu) v prípade, že by prístup mohol mať nepriaznivý vplyv na množstvo záujmov (napr. záujem na porovnanie s praním špinavých peňazí), pozri článok 2-L talianskeho DPCode.

PRÍLOHA – VÝVOJOVÝ DIAGRAM

Krok 1: Ako vykladať a posudzovať žiadosť?



Krok 2: Ako odpovedať na žiadosť (1)?

Tri hlavné zložky práva na prístup (štruktúra článku 15)

Potvrdenie, či sa osobné údaje spracúvajú alebo nie

Prístup k osobným údajom

Ďalšie informácie o účeloch, príjemcoch atď. [článok 15 ods. 1 písm. a) – h)]

Krok 2: Ako odpovedať na žiadosť (2)?

Prijatie primeraných opatrení

Článok 12 ods. 1: stručné, transparentné, zrozumiteľné, ľahko dostupné

Článok 12 ods. 2: uľahčiť výkon práva na prístup

Výber z spomedzi rôznych prostriedkov

Poskytnite kópiu, ak nie je dohodnuté inak (článok 15 ods. 3)

Ak je to vhodné, použite viacúrovňový prístup (najrelevantnejšie v online kontexte)

Načasovanie – bez zbytočného odkladu, v každom prípade do jedného mesiaca (vo výnimočných prípadoch predĺženie o ďalšie dva mesiace) (článok 12 ods. 3)

Krok 2: Ako odpovedať na žiadosť (3)?

Ako môže prevádzkovateľ získať všetky údaje o dotknutej osobe?

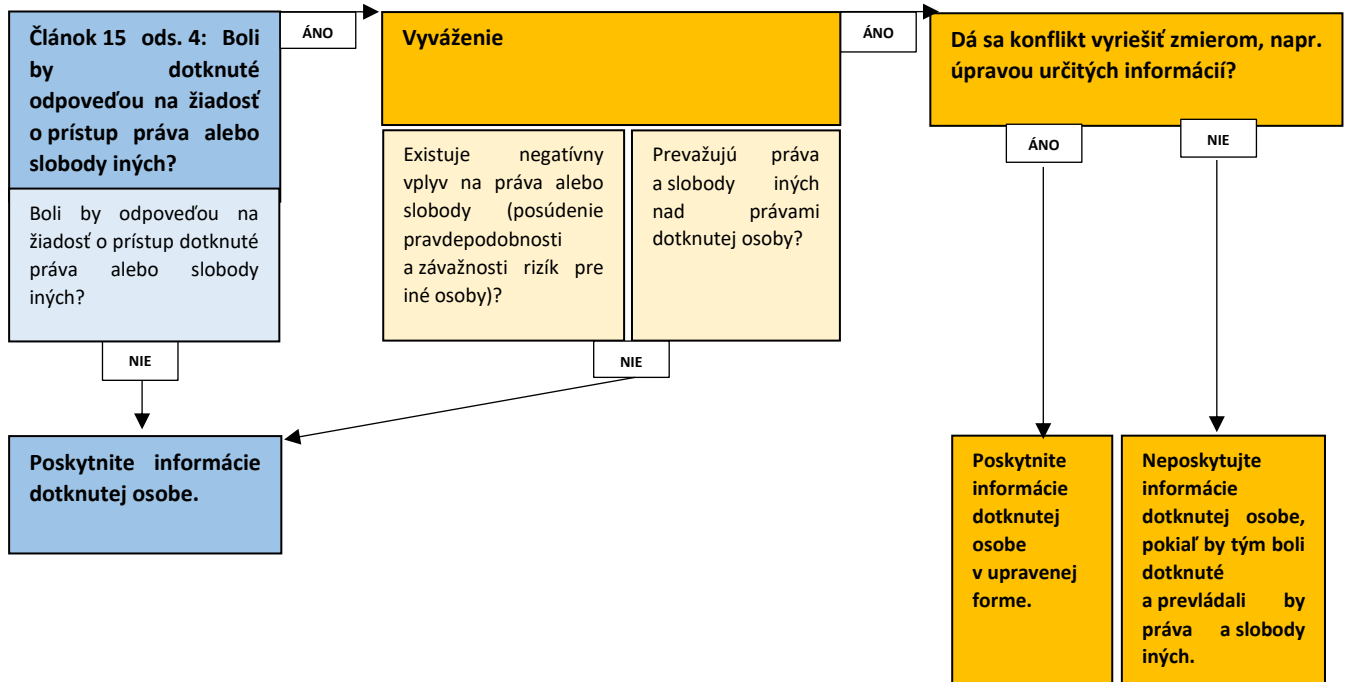
Definujte kritériá vyhľadávania – na základe toho, čo dotknutá osoba poskytla, ďalších informácií, ktoré má prevádzkovateľ o dotknutej osobe a faktorov, na základe ktorých sú údaje štruktúrované (napríklad číslo zákazníka, IP adresy, profesijný titul, rodinné vzťahy atď.).

Identifikujte všetky technické funkcie, ktoré môžu byť k dispozícii na získanie údajov.

Prehľadávajte všetky relevantné IT systémy alebo informačné systémy, ktoré nepatria do IT.

Zostavte, extrahujte alebo inak zhromaždite údaje, ktoré sa týkajú dotknutej osoby, a to spôsobom, ktorým sa v plnej miere odzrkadľuje spracúvanie, t. j. zahŕňa všetky osobné údaje týkajúce sa dotknutej osoby a umožňuje dotknutej osobe poznať a overiť si zákonnosť spracúvania. Získavanie informácií by sa mohlo uskutočniť od prípadu k prípadu alebo ak je to možné, pomocou nástroja špecificky navrhnutej ochrany súkromia, ktorý už prevádzkovateľ zaviedol.

Krok 3: Kontrola limitov a obmedzení (1)



Krok 3: Kontrola limitov a obmedzení (2)

