UNIVERZITA KARLOVA

Právnická fakulta

Mgr. Zuzana Zajíčková

Ochrana osobních údajů v EU – práva subjektů údajů se zaměřením na právo na přístup

Rigorózní práce

Pověřený akademický pracovník: Doc. JUDr. Magdaléna Svobodová, Ph.D.

Tematický okruh: Evropské právo

Datum vypracování práce (uzavření rukopisu) : 21. 10. 2024

Prohlašuji, že jsem předkládanou rigorózní práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 539 409 znaků včetně mezer.

Mgr. Zuzana Zajíčková

rigorozantka

Poděkování

Ráda bych poděkovala Doc. JUDr. Magdaléně Svobodové, Ph.D. z katedry evropského práva Právnické fakulty UK v Praze za odborné vedení této práce, vstřícný přístup, cenné rady a věcné připomínky, které přispěly ke zkvalitnění této práce.

Poděkování patří také mé rodině za jejich trpělivost a kontinuální podporu při psaní této práce.

Obsah:

Úvod

„Náš informační a komunikační prostor je ve vlastnictví korporací, které používají predátorskou ekonomickou logiku, té říkám ‚kapitalismus dohledu'. Proměňuji intimní informace o nás na data, z nich potom dělají své soukromé vlastnictví a používají je, aby předpovídali naše chování a dokonce se naše chování snažili ovlivnit v budoucnosti. Tenhle byznys se za poslední desetiletí stal tak výnosným, že podobné korporace neuvěřitelně zbohatly. Stala se z nich mocenská centra a představují tak pro demokratické společnosti značný problém. Všichni jsme společně díky nim v určité pasti, protože v 21. století žijeme v informační civilizaci a pokud se jí chceme účastnit, musíme sami sebe reprezentovat jako informace. Pohybujeme se informačním prostředím, abychom si mohli naplánovat večeři s přáteli nebo se spojit se svým lékařem nebo získat informace o svém zdraví a spoustu dalších věcí. Pointou je, že my jsme na těchto technologiích závislí v našem každodenním životě. Pokud se chcete účastnit společenského života, neexistuje způsob, jak to obejít. Tyhle korporace stvořily zkrátka svět, ze kterého není úniku, takže se musíme ptát, co můžeme dělat[1]." Toto je přepis části rozhovoru s uznávanou emeritní profesorkou sociální psychologie, americkou spisovatelkou a vědkyní, Shoshanou Zuboff. Právě ta se od konce 80. let věnuje studiu digitálních technologií a jejich dopadu na společnost a v roce 2019 vydává zatím svou nejznámější knihu *Věk kapitalismu dohledu: Boj o budoucnost lidstva u nové hranice moci*. V knize přichází s teorií takzvaného dohledového kapitalismu, tedy nově vzniklého systému spjatého s internetovým prostředím a vyvíjející se digitální ekonomikou.

Kapitalismus dohledu podle ní funguje na základě bezprecedentní asymetrie ve znalostech a moci, která se k nim váže. Architektury kapitalismu dohledu vznikají začátkem 21. století (za přelom bývá považován rok 2002 a začátek masového využívání dat Googlem). Zatímco kapitalisté dohledu (technologické firmy) o nás uživatelích vědí všechno, tak my o jejich operacích zpracování nevíme nic. Dokážou předpovídat naši budoucnost, ale nikoliv v náš prospěch, nýbrž v zájmu maximalizace jejich zisku. Kapitalismus dohledu je v podstatě ekonomikou, která je postavená na poznatku, že předpovědi lidského chování lze prodávat jako zboží ve velkém objemu. Architektury kapitalismu dohledu v podstatě dnes ovládá 5 velkých korporací, které jsou zároveň obřími sledovacími impérii: je to Meta, Google, Microsoft, Amazon a Apple. Tyto společnosti využívají lidské zkušenosti jako volně dostupné

[1] Rozhovor s Shoshanou Zuboff na Radiu Wave ze dne 10. dubna 2023, podcast Vlna, *Soukromí, jak jsme ho znali ještě na přelomu tisíciletí, přestalo existovat, upozorňuje vědkyně Shoshana Zuboff*. Dostupné z: https://wave.rozhlas.cz/soukromi-jak-jsme-ho-znali-jeste-na-prelomu-tisicileti-prestalo-existovat-8966958. [cit. 2024-08-17].

suroviny k vytěžování uživatelských dat, vytváření predikcí o lidském chování a k prodeji získaných informací třetím stranám, které jsou z velké části zastoupeny marketingovými agenturami, ale patří mezi ně i státní bezpečnostní složky a další subjekty veřejného a soukromého sektoru. Prof. Zuboff dále vysvětluje, co představuje uživatel v procesu dohledového kapitalismu. Uživatelé nejsou zákazníky, ani v roli zaměstnanců, ani tzv. produkty těchto společností. Jsou pouze zdrojem potřebného materiálu. Produktem je pak až přeměna lidské zkušenosti v obchodovatelná data. Prof. Zuboff dokonce dnešní svět přirovnává k říši divů z populární knihy Alenka v říši divů. Uživatel je tou zmatenou Alenkou, která se králičí norou propadne do světa, kde se věci nenazývají pravými jmény. Firmy proklamují, že respektují naše soukromí a zaručují jeho ochranu, a přitom je pravdou úplný opak. Tyto společnosti proto podle prof. Zuboff zničily soukromí jednotlivce, jakoukoliv definici soukromí, která existovala a rozhodně zničily soukromí tak, jak jsme jej chápali v moderní společnosti[2].

O proměně paradigmatu soukromí a jeho vnímání se začíná mluvit i v „našich vodách“, pojednává o tom ve svém článku i prof. Kühn[3]. Za zásadní přelom chápe především příchod internetu, který přináší kvalitativní proměnu sdělování a sdílení informací a současně také největší proměnu soukromí. Zatímco v době před internetem byly zásahy do soukromí zpravidla fyzického charakteru (př. domovní prohlídka, sledování osob, odposlechy atd.) a jejich aktérem byla obvykle vláda, policie či zpravodajské služby; v době internetové převažují zásahy ve formě velmi sofistikované, jejichž aktérem bývají zpravidla nadnárodní soukromoprávní korporace. Tyto zásahy jsou velmi časté a dotčené osoby o nich zpravidla vůbec nic neví. Zásahy samy o sobě zpravidla nejsou příliš intenzivní, v důsledku snadného přístupu k informacím a kombinace různých dat ovšem nabývají na intenzitě. Typicky jsou to stopy, které dotčené osoby samy nebo prostřednictvím třetích osob zanechávají na internetu. Nebezpečí spočívá v možnostech nekontrolovaného šíření internetem i v nesmazatelnosti digitálních stop – internet na rozdíl od člověka nezapomíná. Dalším souvisejícím charakteristickým jevem je informační asymetrie mezi běžným uživatelem internetu a provozovatelem internetových služeb. Jakkoli přínosné pro nás mohou být nové digitální technologie, málokdy si plně uvědomujeme, že tím nejcennějším jsou právě naše osobní údaje, které tyto produkty o nás shromažďují a které zároveň tvoří ohromný zisk velkých firem. Jistý

[2] ZUBOFF, Shoshana, 2022. *Věk kapitalismu dohledu: Boj o budoucnost lidstva u nové hranice moci*. Argo, 728 s. ISBN 978-80-257-3936-5.
[3] KÜHN, Zdeněk, 2017. Transformace pojmu soukromí na počátku třetího milénia. Online. *Jurisprudence*. Roč. 2017, roč. 26, č. 2, s. 3-11. ISSN 1802-3843. Dostupné z: databáze ASPI. [cit. 2024-08-18].

vývojář softwaru pro „internet věcí“ prohlásil: „*Kolem určitého chování lze vytvořit kontext, a vynutit si tak změnu. Data závislá na kontextu nám umožňují propojit vaše emoce, kognitivní a životní funkce a podobně. Můžeme zjistit, že byste neměli řídit, a vaše auto zkrátka vypnout. Můžeme říct ledničce: ‚Zamkni se, protože by neměl jíst‘, nebo řekneme televizoru, aby se vypnul a přinutil vás jít spát, židli, aby se začala třást, protože byste na ní neměli sedět tak dlouho, nebo kohoutku, aby se otočil, protože musíte vypít víc vody*[4].“

Brzy se ukazuje, že rozsáhlé zpracování informací velkými korporacemi typu Google či Meta vyžaduje odpověď v podobě veřejné regulace. Vzhledem k tomu, že tyto firmy operují na globální úrovni a internet nezná hranice, roste význam veřejnoprávní ochrany. Jak píše prof. Kühn[5], ponechat úpravu na jednotlivých státech se neukazuje jako dostatečně účinné řešení. Odlišné národní regulace osobních údajů by představovaly překážku volnému pohybu poskytování služeb v rámci EU a současně by měly za následek nerovné postavení občanů států EU. Proto se přímo nabízí ochrana právem Evropské unie – jejím smyslem není aktivity zpracování dat znemožňovat, ale nastavit jasná pravidla a limity pro tyto aktivity s globálním či celoevropským dopadem. Evropská unie reagovala relativně dynamicky vytvořením veřejnoprávního institutu ochrany osobních údajů. Tento institut byl koncipován v polovině devadesátých let na základě směrnice 95/46. Směrnice tedy zavedla základní právní rámec, jehož cílem bylo ustavit rovnováhu mezi vysokou úrovní ochrany soukromí jednotlivců a volným pohybem osobních údajů v rámci EU.[6] Na tuto úpravu pak navázalo nařízení GDPR.

Struktura práce, výzkumné otázky a metodologie

Cílem této práce je komplexně uchopit a zpracovat právo subjektů údajů na přístup k osobním údajům podle článku 15 nařízení GDPR na úrovni EU. Tuto problematiku lze bezesporu označit za velice aktuální. V rámci široké odborné i laické veřejnosti se oblast práv subjektů údajů stává hojně diskutovanou, především po účinnosti nařízení GDPR. Dohromady jsou totiž tato práva chápána jako kontrolní mechanismus sloužící k zajištění souladu jednotlivých operací zpracování s právní úpravou na ochranu osobních údajů. Za tímto cílem

[4] ZUBOFF, Shoshana, 2022. *Věk kapitalismu dohledu: Boj o budoucnost lidstva u nové hranice moci*. Argo., 728 s. ISBN 978-80-257-3936-5.
[5] KÜHN, Zdeněk, 2017. Transformace pojmu soukromí na počátku třetího milénia. Online. *Jurisprudence*. Roč. 2017, roč. 26, č. 2, s. 3-11. ISSN 1802-3843. Dostupné z: databáze ASPI. [cit. 2024-08-18].
[6] MATEJKA, Ján, 2013. 4. Právní regulace ochrany soukromí, její limity a možnosti. In: MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, s. 57-156. ISBN 978-80-904248-7-6.

jsem formulovala několik výzkumných otázek (a v jejich rámci i podotázek), které jsou zde uvedeny v chronologickém sledu, jak jsou v práci zkoumány. **Zaprvé**, jaký je význam a účel práva na přístup? Odráží se to nějakým způsobem i ve vztahu k ostatním právům subjektů údajů? Právo na přístup podle článku 15 nařízení GDPR představuje vlastně rozvedení zásady transparentnosti, podobně jako právo subjektu údajů být informován podle článků 13 a 14 nařízení GDPR, v čem tedy spočívá základní rozdíl u těchto práv? **Zadruhé**, struktura článku 15 nařízení GDPR zahrnuje ve svém odstavci 3 právo získat kopii zpracovávaných osobních údajů, jak lze na toto právo na kopii pohlížet? Je to samostatné právo subjektu údajů, stojící vedle práva na přístup, nebo se jedná o jednu z komponent, příp. modalit práva na přístup? **Zatřetí**, je normativní úprava práva na přístup v článku 15 nařízení dostatečná? Je právo na přístup vhodně upraveno v unijních aktech *soft law*? **A začtvrté**, do jaké míry představuje právo na přístup k vlastním údajům skutečné posílení práv subjektů údajů? Jaké je jeho využití v praxi? Je ochrana prostřednictvím práva na přístup účinná?

Za účelem naplnění výše uvedeného cíle rigorózní práce jsou použity zejména základní metody[7], přičemž základními metodami jsou metoda deskriptivní, analytická, syntetická, částečně i komparativní (kapitola 5.3 Komparativní analýza geneze a implementace práva na přístup v právním řádu Německa, Francie a Velké Británie). Práce se částečně snaží opřít i o normativní a empirický přístup. Normativní z důvodu, že se pokouším právo na přístup poměřit z hlediska hodnot a principů. Empirický přístup je pak použit především v části šesté, kde zkoumám „společenskou realitu v souvislosti s právem na přístup“, resp. jeho uplatnění v praxi, za využití existujících empirických studií akademických pracovníků z Belgie a Nizozemska, Pierre Dewitta a Jefa Ausloose. Prostřednictvím analytické metody byla provedena analýza dostupné judikatury, a to zejména vrcholné evropské soudní instituce (Soudního dvora EU), částečně také zahraničních vnitrostátních soudů a českých soudů. Kritické analýze jsou podrobeny také relevantní materiály *soft law* (v podobě stanovisek, pokynů či vodítek) vytvořené Pracovní skupinou zřízenou dle čl. 29 Směrnice (neboli WP29) a jejím nástupcem – Evropským sborem pro ochranu osobních údajů (neboli EDPB), které, ačkoliv slouží v naprosté většině případů jako doporučení, jsou pro komplexní pohled nepostradatelné. Obsah a smysl ustanovení příslušných právních předpisů je vyložen prostřednictvím metody interpretační.

[7] BOBEK, Michal, 2016. Výzkum v Právu: Reklama na Nike anebo kvantová fyzika? Online. *Jurisprudence*. November 26, 2016, No. 6, 2016, s. 8 (3-10), Dostupné z: https://ssrn.com/abstract=2875982. [cit. 2024-09-25].

Na tomto místě bych jako autorka ráda představila strukturu své rigorózní práce spolu s důvody, které mě k napsání práce vedly. V první části jsem se rozhodla v první řadě mapovat historické pozadí práva na přístup a jeho výskyt v historických pramenech – předpisech na ochranu osobních údajů. V druhé části se zabývám základní terminologií ochrany osobních údajů, včetně vysvětlení základních zásad zpracování. To považuji za nezbytnou součást pochopení základního rámce ochrany osobních údajů. Ústředním bodem této práce je nicméně kritická analýza práva na přístup a jeho spolupůsobení s dalšími právy subjektu údajů. Třetí část tak byla pojata jako rozbor (byť nikoli podrobný) jednotlivých práv subjektu údajů, včetně uvedení *case law*. Je zde také zdůrazněn význam těchto dalších práv a jejich vztah k právu na přístup. Následující části se pak zabývají již samotným právem na přístup a tvoří nejrozsáhlejší část této práce, k čemuž uvádím i jednotlivé příklady z praxe dozorových úřadů, EDPB a *case law* Soudního dvora EU. Část čtvrtá se podrobně věnuje právně-teoretickému základu práva na přístup, jeho genezi, včetně komparativního exkurzu, účelu, významu, obecným principům a struktuře. Metodicky rovněž doporučuje, jakým způsobem lze podávat žádosti o právo na přístup a jak lze tyto žádosti vyřizovat. Část pátá více upřesňuje rozsah práva na přístup a jeho omezení, může mít využití zejména pro správce. Poslední část (část šestá) se soustřeďuje na uplatňování práva na přístup v praxi, zahrnuje obecné zhodnocení regulace a unijní zhodnocení nařízení GDPR, dále pak autorčiny úvahy nad některými normativními nedostatky a analýzu poznatků z provedených empirických studií k právu na přístup. Závěr obsahuje závěrečné úvahy, zejména ve vztahu k výzkumným otázkám.

Primárním důvodem, který mě k napsání této rigorózní práce vedl, je mé odborné profesní zaměření na ochranu osobních údajů. Již od března 2019 působím na českém Úřadu pro ochranu osobních údajů. V rámci své činnosti jsem se dostala také do kontaktu s několika evropskými materiály *soft law*, nejblíže pak k tehdy připravovaným Pokynům EDPB k právu na přístup. Tento materiál jsme v rámci tehdejšího analytického oddělení pomáhali dotvářet prostřednictvím rozsáhlých připomínek. Právě tehdy jsem si, nejspíše prvně, naplno uvědomila důležitost celé problematiky práv subjektů údajů, a především pak stěžejní význam práva na přístup, kterému zatím nebylo věnováno dostatek prostoru. Právo na přístup, které formálně již existovalo nějakou dobu, se jako samostatné právo vyprofilovalo až s účinností nařízení GDPR. I po účinnosti nařízení GDPR však nějakou dobu existovalo převážně jen „na papíře“. V praxi nebylo často realizovaným právem, neboť nikdo, ani subjekty údajů, ani správci samotní, nebyl obeznámen s možnostmi a způsoby jeho realizace. Jasnější „kontury“ tak začalo právo na přístup získávat až na podzim 2021 v souvislosti s přípravou zmíněných pokynů.

Dalším, neméně důležitým důvodem, je mé uvědomění, že i sama jsem jedním z těch subjektů údajů, který pořádně nemá přehled o tom, kde všude jsou jeho osobní údaje zpracovávány a jakým způsobem. Právo na přístup tak představuje jedinečný nástroj ochrany slabší strany subjektů údajů proti silnějším správcům, ať již soukromoprávním korporacím nebo orgánům veřejné moci. Od konce 20. století jsme svědky bezprecedentního obrovského nárůstu množství informací a prostředků, kterými je lze šířit. Ekonomika původně založená na průmyslu se transformovala na ekonomiku založenou na datech (hovoříme o konceptu data-driven economy). Pod vlivem možná trochu ponuré četby profesorky Shoshany Zuboff[8], jsem si uvědomila, jakým způsobem přistupují největší internetové společnosti – Google, Meta, Amazon, Apple, Microsoft k našim osobním datům, a že považují tato data za své hlavní aktivum a zdroj tvorby hodnot. Jak píše Helena U. Vrabec ve své monografii k *Právům subjektů údajů podle GDPR*[9], nejzřetelnější důkazy datového rozmachu můžeme pozorovat v našem každodenním životě. Ať již jde o okamžité zasílání zpráv pomocí mobilních telefonů (SMS, služby aplikace messenger), snadný přístup k dokumentům prostřednictvím cloudových služeb nebo personalizované reklamy – to vše je vývoj založený na široké dostupnosti a opakované použitelnosti dat. V ekonomice založené na datech se moc projevuje ve dvou rovinách: jednak v přístupu k datům a kontrolou nad nimi, jednak ve schopnosti sofistikovaného zpracování dat. Ani v jedné z těchto rovin nejsou jednotlivci ve výhodě. Jsme tak svědky výrazné asymetrie v oblasti moci a kontroly nad daty ve prospěch správců, která do značné míry vyplývá z architektury platforem pro shromažďování údajů. Vzhledem ke konstrukci těchto platforem je tak pro správce snadné převzít plnou kontrolu vstupních údajů uživatelů (fotografie, texty, komentáře atd.). Ukazuje se, že právě posílená kontrola ze strany subjektů údajů, kterou přineslo nařízení GDPR, je v dnešní době obzvláště důležitá.

[8] ZUBOFF, Shoshana, 2022. *Věk kapitalismu dohledu: Boj o budoucnost lidstva u nové hranice moci*. Argo., 728 s. ISBN 978-80-257-3936-5.

[9] VRABEC, Helena U., 2021. 1.2 The individual in the data-driven (big-data) economy. In: *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*. Oxford University Press, s. 3-9. Online. ISBN 9780191904851. Dostupné z: https://doi.org/https://doi.org/10.1093/oso/9780198868422.001.0001. [cit. 2024-08-29].

1. Právní rámec a kontext evropského práva ochrany osobních údajů

V rámci této části se budu věnovat úvodnímu historickému exkurzu. Na úvod se pokusím objasnit propojení mezi právem na ochranu osobních údajů a právem na respektování soukromého života. Poté se již přesunu k popisu jednotlivých mezinárodních a regionálních dokumentů a jejich významu pro pozdější formování unijní úpravy ochrany osobních údajů. Součástí této historicko-kulturní části bude samozřejmě mapování počátků práva na přístup v jednotlivých dokumentech.

1.1 Právo na respektování soukromého života a právo na ochranu osobních údajů – úvodní poznámky

Právo na respektování soukromého života a právo na ochranu osobních údajů, ačkoli spolu úzce souvisejí, jsou odlišná práva. Právo na soukromí – v evropském právu označované jako právo na respektování soukromého života – se v mezinárodním právu lidských práv objevuje poprvé ve Všeobecné deklaraci lidských práv, přijaté v roce 1948 jako jedno ze základních lidských práv. Vzápětí po přijetí Všeobecné deklarace se toto právo objevuje i na evropské úrovni Rady Evropy – v Evropské úmluvě o lidských právech (EÚLP). Úmluva byla vypracována v roce 1950 a je pro její smluvní strany právně závazná. V článku 8 je garantováno právo na respektování soukromého a rodinného života, obydlí a korespondence. Zásahy do tohoto práva ze strany orgánů veřejné moci jsou zakázány s výjimkou případů, kdy jsou v souladu se zákonem, sledují důležité a legitimní veřejné zájmy a jsou nezbytné v demokratické společnosti. Právo na ochranu soukromého života, rodiny, domova a korespondence je chráněno také v článku 17 Mezinárodního paktu o občanských a politických právech z roku 1966.

Právo na respektování soukromého života a právo na ochranu osobních údajů spolu úzce souvisejí. Obě se snaží chránit podobné hodnoty, tj. autonomii a lidskou důstojnost jednotlivců tím, že poskytují ochranu osobní sféry jednotlivce, v níž může svobodně rozvíjet svou osobnost, myslet a utvářet své názory. V této souvislosti se objevují dva významné prvky: potřeba zabránit nepřiměřeným zásahům do soukromých záležitostí a potřeba zajistit jednotlivcům přiměřenou kontrolu nad záležitostmi, které se jich mohou týkat. Obě práva jsou také nezbytným předpokladem pro uplatňování dalších základních práv a svobod. Tato dvě práva se ovšem liší svou formulací, rozsahem a působností. Právo na respektování soukromého života spočívá v obecném zákazu zasahování do soukromí, který podléhá určitým kritériím veřejného

zájmu, jež mohou v určitých případech zásah odůvodnit. Toto právo se týká situací, kdy je ohrožen nebo narušen soukromý život jednotlivce. Ovšem přesně určit obsah pojmu soukromý život není snadné. Pojem „soukromý život“ bývá v judikatuře SDEU i ESLP vykládán široce a zahrnuje intimní situace, citlivé nebo důvěrné informace, informace, které by mohly poškodit vnímání veřejnosti vůči jednotlivci, a dokonce i aspekty profesního života a chování na veřejnosti[10]. V základech tohoto práva je negativní koncept svobody, neboli „právo být nechán na pokoji“, tj. v podstatě existence nějaké soukromé zóny, do které by neměl nikdo vstupovat či zasahovat. Tuto zónu můžeme chápat jak prostorově, tak i z hlediska rozhodování o vlastní identitě[11]. Posouzení toho, zda se jedná o zásah do soukromého života, však vždy závisí na kontextu a okolnostech každého případu.

Oproti tomu právo na ochranu osobních údajů je fakticky moderně utvářeným a aktivním právem, které vzniklo v 70. letech 20. století z německého konceptu práva na informační sebeurčení, o němž bude podrobněji pojednáno dále. Právo na informační sebeurčení jednotlivce mu přiznává možnost podle vlastního uvážení rozhodnout, zda a případně v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace o jeho osobě a z jeho soukromí zpřístupněny jiným subjektům. Právo na ochranu osobních údajů vlastně zakotvuje systém brzd a protivah na ochranu jednotlivce při každém zpracování jeho osobních údajů[12]. Cílem práva na ochranu osobních údajů je poskytnout jednotlivcům právní ochranu před nevhodným používáním informačních technologií ke zpracování informací, které se jich týkají. Nebylo vytvořeno s cílem zabránit zpracování takových informací nebo omezit používání informačních technologií jako takových. Místo toho byl koncept práva na ochranu osobních údajů navržen tak, aby poskytoval záruky vždy, když se informační technologie použijí ke zpracování informací týkajících se fyzických osob. Vycházelo se z počátečního přesvědčení, že rozsáhlé využívání informačních technologií může mít dalekosáhlé dopady na práva a zájmy jednotlivců. Podle Petera Hustinxe je „právo na ochranu osobních údajů“ dokonce širší než „právo na ochranu soukromí“, protože se týká i dalších základních práv a svobod a všech druhů údajů bez ohledu na jejich vztah k soukromí, a

[10] FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2024-07-12].
[11] KRATOCHVÍL, Jan; KMEC, Jiří; KOSAŘ, David; KRATOCHVÍL, Jan a BOBEK, Michal, 2012. Kapitola XVIII Právo na respektování soukromého a rodinného života (čl. 8 EÚLP). Online. In: *Evropská úmluva o lidských právech*. Praha: C. H. Beck, s. 867-872. ISBN 978-80-7400-365-3. Dostupné z: databáze Beck online. [cit. 2024-07-20].
[12] FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2024-07-12].

zároveň omezenější, protože se týká pouze zpracování osobních údajů, přičemž ostatní aspekty ochrany soukromí nejsou zohledněny[13].

1.2 Mezinárodní právní rámec

Koncept práva na respektování soukromého života (resp. práva na soukromí) se poprvé objevuje v mezinárodním právu po druhé světové válce. V roce 1948 je v San Francisku Valným shromážděním Organizace spojených národů přijat první celosvětově významný mezinárodní dokument, Všeobecná deklarace lidských práv. Ačkoli se jednalo o právně nezávazný dokument (jde o rezoluci Valného shromáždění OSN), ovlivnil vypracování jiných mezinárodních dokumentů v oblasti lidských práv v Evropě, jeho autorita byla tedy značná. Právo na respektování soukromého a rodinného života bylo zakotveno v článku 12[14]. Po druhé světové válce také vzniká v roce 1949 organizace Rady Evropy, jejímž cílem je sdružovat evropské státy a podporovat hodnoty právního státu, demokracie, lidských práv a sociálního rozvoje. Za tímto účelem byla přijata v Římě v roce 1950 Evropská úmluva o lidských právech (EÚLP), která vstoupila v platnost v roce 1953 a která je pro smluvní strany závazná. Všechny členské státy Rady Evropy již začlenily EÚLP do svého vnitrostátního práva, což jim ukládá povinnost jednat v souladu s ustanoveními úmluvy. Hmotněprávní ochrana soukromého a rodinného života je zakotvena v článku 8 EÚLP[15]. K zajištění toho, aby smluvní strany dodržovaly své závazky vyplývající z EÚLP, byl v roce 1959 ve francouzském Štrasburku ustaven Evropský soud pro lidská práva (ESLP). Rozsahem a důsledky této ochrany se zabýval ESLP v řadě rozsudků. Ve všech případech ESLP posuzuje, zda došlo k zásahu do práva na respektování soukromého života, a pokud ano, zda měl odpovídající právní základ – tj. zda byl

[13] HUSTINX, Peter, Speeches and Articles EDPS. *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. Červenec 2013. Dostupné z: https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en. [cit. 2024-07-12].

[14] Článek 12: „*Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům*."

[15] Článek 8
Právo na respektování soukromého a rodinného života
„*1. Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.*
2. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných."

jasný, dostupný a předvídatelný, a zda byl nezbytný a přiměřený ve vztahu k dotčeným legitimním zájmům.

Jestliže shrnu tyto dva významné mezinárodní dokumenty, tak mohu konstatovat, že oba deklarovaly právo na ochranu soukromého života na obecné úrovni, zatímco právo na ochranu osobních údajů bylo zatím stále vnímáno jako jeho přirozená součást. Až později se z práva na soukromí postupně odděluje relativně samostatná oblast práva na ochranu osobních údajů jako nástroj ochrany člověka v rámci jeho práva na informační sebeurčení. ESLP se od 80. let začíná zabývat řadou situací, které se týkají otázek ochrany osobních údajů. Patří k nim odposlech[16], různé formy sledování[17] ze strany soukromého i veřejného sektoru a ochrana před ukládáním osobních údajů orgány veřejné moci (běžné i citlivé údaje – např. DNA[18], otisky prstů[19] atd.).

Pokud jde konkrétně o právo na přístup, tak také to začíná získávat rozměr základního lidského práva. Extenzivní výklad ze strany ESLP postupně zahrnuje právo na přístup do oblasti působnosti článku 8 EÚLP. ESLP již v řadě případů[20] zdůraznil, že odmítnutí nebo ignorování žádosti o přístup, ať už v případě informací, které mají k dispozici orgány veřejné moci nebo soukromé subjekty, by mohlo představovat nepřiměřený zásah podle čl. 8 odst. 2 EÚLP, pokud by toto rozhodnutí nezajistilo spravedlivou rovnováhu mezi konkurujícími si zájmy[21].

---

[16] Rozsudek ESLP ze dne 2. srpna 1984 Malone proti Spojenému království (stížnost č. 8691/79); Rozsudek ESLP ze dne 24. dubna 1990 Huvig proti Francii (stížnost č. 11105/84); Rozsudek ESLP ze dne 24. dubna 1990 Kruslin proti Francii (stížnost č. 11801/85) a Rozsudek velkého senátu ESLP ze dne 16. února 2000 Amann proti Švýcarsku (stížnost č. 27798/95).

[17] Rozsudek ESLP ze dne 6. září 1978 Klass a ostatní proti Německu (stížnost č. 5029/71); Rozsudek velkého senátu ESLP ze dne 4. května 2000 Rotaru proti Rumunsku (stížnost č. 28341/95); Rozsudek velkého senátu ESLP ze dne 4. prosince 2015 Roman Zakharov proti Rusku (stížnost č. 47143/06); Rozsudek velkého senátu ESLP ze dne 25. května 2021 Centrum för rättvisa proti Švédsku (stížnost č. 35252/08) a Rozsudek velkého senátu ESLP ze dne 25. května 2021 Big Brother Watch a ostatní proti Spojenému království (stížnosti č. 58170/13, 62322/14 a 24960/15).

[18] Rozsudek velkého senátu ESLP ze dne 4. prosince 2008 S. a Marper proti Spojenému království (stížnosti č. 30562/04 a 30566/04); Rozsudek pátého senátu ESLP ze dne 22. června 2017 Aycaguer proti Francii (stížnost č. 8806/12) a Rozsudek prvního senátu ESLP ze dne 13. února 2020 Trajkovski a Chipovski proti Severní Makedonii (stížnosti č. 53205/13 a 63320/13).

[19] Rozsudek velkého senátu ESLP ze dne 4. prosince 2008 S. a Marper proti Spojenému království (stížnosti č. 30562/04 a 30566/04) a Rozsudek pátého senátu ESLP ze dne 18. dubna 2013 M. K. proti Francii (stížnost č. 19522/09).

[20] Rozsudek ESLP ze dne 26. března 1987 Leander proti Švédsku (stížnost č. 9248/81); Rozsudek velkého senátu ESLP ze dne 7. července 1989 Gaskin proti Spojenému království (stížnost č. 10454/83); Rozsudek ESLP ze dne 25. února 1997 Z proti Finsku (stížnost č. 22009/93); Rozsudek druhého senátu ESLP ze dne 24. září 2002 M.G. proti Spojenému království (stížnost č. 39393/98); Rozsudek velkého senátu ESLP ze dne 13. února 2003 Odièvre proti Francii (stížnost č. 42326/98); Rozsudek čtvrtého senátu ESLP ze dne 17. července 2008 I proti Finsku (stížnost č. 20511/03) a Rozsudek třetího senátu ESLP ze dne 27. října 2009 Haralambie proti Rumunsku (stížnost č. 21737/03).

[21] AUSLOOS, Jef a DEWITTE, Pierre, 2018. Shattering One-Way Mirrors. Data Subject Access Rights in Practice. Online. *International Data Privacy Law*. March 2018, Volume 8, Issue 1, s. 25 (4–28). Dostupné z: https://doi.org/10.1093/idpl/ipy001. [cit. 2024-07-12].

Další mezinárodní smlouvou přijatou na zasedání Organizace spojených národů v New Yorku dne 19. prosince 1966 byl Mezinárodní pakt o občanských a politických právech (ICCPR). Ten vstoupil v platnost až v roce 1976 a svým obsahem navázal na Všeobecnou deklaraci lidských práv. Ochranu soukromí zakotvil v článku 17[22], který se obsahově zcela shoduje se zněním příslušného článku Všeobecné deklarace. ICCPR je právně závazná mezinárodní smlouva, která zavazuje 174 smluvních stran k respektování a zajištění výkonu občanských práv jednotlivců, včetně soukromí. V letech 2013 a 2014 pak v rámci Organizace spojených národů byly přijaty ještě dvě právně nezávazné rezoluce[23] o otázkách soukromí s názvem „Právo na soukromí v digitálním věku". Důvodem byla reakce na vývoj nových technologií a na odhalení případů hromadného sledování, prováděného v některých státech. Tyto rezoluce tak podnítily mezinárodní politickou debatu o soukromí, nových technologiích a sledování. Na ně pak navázaly rezoluce téže organizace z let 2016 a 2017, které potvrdily potřebu omezit pravomoci zpravodajských služeb a odsoudily hromadné sledování. Tyto rezoluce ovšem vedle odpovědnosti státních orgánů poukazují také na odpovědnost soukromého sektoru za dodržování lidských práv a vyzývají podniky, aby informovaly uživatele o veškerém zpracování osobních údajů a aby stanovily transparentní zásady zpracování[24].

1.3 Dokumenty OECD a Rady Evropy

Klíčovým orgánem pro počátek ochrany osobních údajů v Evropě byla Rada Evropy. Už v roce 1973 přijal Výbor ministrů Rady Evropy právně nezávaznou rezoluci (73) 22 – Ochrana soukromí fyzických osob ve vztahu k elektronickým databázím v soukromém sektoru. Důvodem, proč ji zmiňuji, je, že již zde bylo zařazeno právo na přístup jako šestá zásada[25]. Podle důvodové zprávy k této rezoluci lze právo na přístup – včetně informací o povaze údajů, o skutečných údajích a o tom, jak jsou tyto údaje využívány – považovat za „základní minimální

[22] Článek 17
„*1. Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence ani útokům na svou čest a pověst.*
2. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům."
[23] OSN. Rezoluce Valného shromáždění ze dne 18. prosince 2013 č. 68/167 Právo na soukromí v digitálním věku. Dostupné z: https://digitallibrary.un.org/record/764407?v=pdf. [cit. 2024-09-27]. OSN. Rezoluce Valného shromáždění ze dne 18. prosince 2014 č. 69/166 Právo na soukromí v digitálním věku. Dostupné z: https://documents.un.org/doc/undoc/gen/n14/707/03/pdf/n1470703.pdf. [cit. 2024-09-27].
[24] FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2024-07-12]
[25] 6. zásada: „*Obecně platí, že dotčená osoba by měla mít právo znát informace, které jsou o ní uchovávány; účel, pro který byly zaznamenány; a podrobnosti o každém zpřístupnění těchto informací*."

prvek ochrany soukromí“. O rok později byla přijata rezoluce (74) 29 – Ochrana soukromí fyzických osob ve vztahu k elektronickým databázím ve veřejném sektoru. Také zde již bylo upraveno právo na přístup, tentokrát jako pátá zásada[26]. Důvodová zpráva v tomto případě hovoří o tom, že „*účinná ochrana jednotlivce před zásahy do jeho soukromí v důsledku nesprávného použití údajů, které jsou o něm uchovávány, závisí na jeho právu znát tyto informace. Uznává se, že toto právo může podléhat určitým omezením, např. z důvodu bezpečnosti státu, veřejného pořádku nebo předcházení trestným činům nebo v případě informací, jejichž znalost by mohla samotnému jednotlivci způsobit újmu*.“ Všechny výjimky však musí být přísně vymezeny. V závěru důvodová zpráva připouští uložení určitých poplatků za náklady dotčeným subjektům nebo stanovení minimální periodicity sdělování informací, zdůrazňuje však, že se uplatňování zásady nesmí stát neúčinným nebo diskriminačním.

Prvními mezinárodně dohodnutými zásadami ochrany osobních údajů byla Směrnice o ochraně soukromí a přeshraničních tocích osobních údajů, kterou přijala Rada OECD v roce 1980[27]. Ačkoli jde formálně také o právně nezávazný dokument (má charakter doporučení), představuje vlastně první pokus o řešení přeshraničních toků údajů z globálního hlediska a obsahuje široce přijímané zásady ochrany osobních údajů. Druhá část této Směrnice obsahuje „zásadu účasti fyzických osob“, která zakotvuje právo na přístup (konkrétně jde o bod 13)[28]. Toto právo na přístup bylo omezeno na potvrzení, zda jsou údaje zpracovávány, a na samotné údaje. Navzdory tomuto omezenému rozsahu zásada stanoví důležité požadavky, které jsou

[26] 5. zásada: „*Každý člověk by měl mít právo vědět, jaké informace jsou o něm uchovávány. Jakákoli výjimka z této zásady nebo omezení výkonu tohoto práva by měly být přísně upraveny*.“

[27] OECD. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (23rd September, 1980). OECD Publishing, Paris. Dostupné z: https://doi.org/10.1787/9789264196391-en. [cit. 2024-09-25].

[28] Zásada účasti fyzických osob:
„13. Fyzická osoba by měla mít právo:
a) získat od správce údajů, nebo jiným způsobem, potvrzení o tom, zda má správce údajů k dispozici údaje vztahující se k jeho/její osobě, či nikoliv;
b) aby mu/jí byly sděleny údaje vztahující se k němu/ní, a to
1. *v přiměřené lhůtě;*
2. *za přiměřený poplatek nebo zdarma;*
3. *vhodným způsobem; a*
4. *formou této osobě snadno srozumitelnou;*

c) získat vysvětlení v případě zamítnutí žádosti předložené podle podčlánků a) a b) a měla by mít možnost vznést proti takovému zamítnutí námitku; a
d) vznést námitku proti údajům vztahujícím se k jeho/její osobě, a pokud je taková námitka úspěšná, nechat uvedené údaje vymazat, opravit, doplnit nebo pozměnit.“

dodnes relevantní: a) sdělení musí proběhnout v přiměřené lhůtě; b) bez nepřiměřeného poplatku; c) vhodným způsobem; a d) ve snadno srozumitelné formě[29].

Prvním skutečně společným evropským nástrojem ochrany osobních údajů se však stala Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (vyhlášená u nás pod č. 115/2001 Sb. m. s.), také nazývána jako Úmluva č. 108. Tato úmluva byla a stále je jediným právně závazným mezinárodním nástrojem v oblasti ochrany osobních údajů. Byla přijata Radou Evropy dne 28. ledna 1981, přičemž právě tento den bývá považován za počátek, kdy se právo na ochranu osobních údajů při jejich zpracování vyčlenilo jako zvláštní část práva na ochranu soukromí. Tento den se proto slaví jako mezinárodní den ochrany osobních údajů, a to právě na počest přijetí Úmluvy č. 108. Úmluva č. 108 vstoupila pro ČR v platnost v roce 2001, její Dodatkový protokol pak v roce 2003, přičemž ze strany ČR bylo učiněno prohlášení, jehož prostřednictvím byla rozšířena aplikace této úmluvy i na neautomatizované zpracování osobních údajů. Z pohledu ČR se tak úmluva vztahuje jak na automatizované tak i neautomatizované zpracování osobních údajů[30]. Úmluva definovala pojmy jako osobní údaj, automatizované zpracování nebo správce, stanovila požadavky na kvalitu údajů v podobě zásad zpracování osobních údajů, vymezila zvláštní skupiny údajů, nutnost osobní údaje zabezpečit a další hlediska týkající se automatizovaného zpracování. Pojmy jako osobní údaj, správce či zpracování se podobají znění současného nařízení GDPR[31] a od té doby se po významové stránce výrazně neměnily.

Pokud jde o právo na přístup, bylo zakotveno do článku 8 úmluvy (Dodatečné záruky pro subjekt údajů) pod písmeny a) a b)[32]. Obsahově se koncepce práva na přístup v článku 8

---

[29] AUSLOOS, Jef a DEWITTE, Pierre, 2018. Shattering One-Way Mirrors. Data Subject Access Rights in Practice. Online. *International Data Privacy Law*. March 2018, Volume 8, Issue 1, s. 25 (4–28). Dostupné z: https://doi.org/10.1093/idpl/ipy001. [cit. 2024-07-12].

[30] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 51-65. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-07-16].

[31] ŽŮREK, JUDr. Jiří. *Praktický průvodce GDPR (včetně rozhodovací praxe ÚOOÚ)* [online]. 2021 [cit. 2024-07-16].

[32] Článek 8 – Dodatečné záruky pro subjekt údajů

„Každé osobě musí být umožněno:

a) zjistit existenci automatizovaného souboru osobních údajů, jeho hlavní účely, jakož i totožnost a obvyklé sídlo nebo hlavní pracoviště správce souboru údajů;

b) získávat v přiměřených intervalech a bez přílišných průtahů nebo nákladů potvrzení o tom, zda jsou v automatizovaných souborech dat uloženy osobní údaje, které se jí týkají, jakož i sdělit jí tyto údaje ve srozumitelné formě;

c) docílit, podle povahy případu, opravu těchto údajů nebo jejich vymazání, jestliže byly zpracovány v rozporu s vnitrostátním právním řádem uplatňujícím základní zásady stanovené v článcích 5 a 6 této Úmluvy;

d) mít opravný prostředek, není-li vyhověno její žádosti o potvrzení, případně o sdělení, opravení nebo vymazání, jak je uvedeno v písmenech b) a c) tohoto článku.“

Úmluvy č. 108 značně podobá znění bodu 13 Směrnice OECD. Úmluva navíc přidala ještě možnost získat přístup k hlavním účelům zpracování, totožnosti a sídla správce a právo dostávat své osobní údaje v pravidelných intervalech. Jak vyplývá z důvodové zprávy k Úmluvě 108[33], ustanovení článku 8 má především umožnit subjektům údajů hájit jejich práva ve vztahu k automatizovaným souborům údajů. Třebaže ve vnitrostátních právních předpisech obsah článku 8 jednoznačně odpovídá subjektivním právům, znění v úmluvě je vyjadřuje formou záruk, které smluvní státy poskytují subjektům údajů, a to s ohledem na to, že úmluva není samostatně vykonatelná a ukládá smluvním stranám povinnost včlenit ustanovení o ochraně údajů do jejich vnitrostátních právních předpisů. Tyto záruky zahrnují čtyři hlavní body: a) vědomost o existenci automatizovaného souboru údajů; b) znalost obsahu případných informací uložených o subjektech údajů v souboru; c) opravu chybných nebo nevhodných informací; d) nápravu v případě, že některý z předchozích bodů není dodržen.

Všechny členské země EU Úmluvu č. 108 ratifikovaly. K Úmluvě č. 108 mohou navíc přistoupit i země, které nejsou smluvními stranami Rady Evropy. Úmluva má dodnes význam jako všeobecná norma a její otevřenost tvoří základ prosazování ochrany údajů na celosvětové úrovni. V roce 2018 prošla úmluva zásadní modernizací. Ukázalo se, že úmluva v původním znění přestává odpovídat požadavkům technologického vývoje, rostoucímu využívání nových informačních a komunikačních technologií, globalizaci operací zpracování a všudypřítomnému toku osobních údajů. V rámci modernizace úmluvy byly potvrzeny její původní zásady, některé byly posíleny a byly stanoveny nové záruky. Zásady transparentnosti, proporcionality, odpovědnosti, minimalizace údajů a záměrné a standardní ochrany údajů byly začleněny do úmluvy jako klíčové prvky mechanismu ochrany. Modernizovaná úmluva (tzv. Úmluva 108+) se již vztahuje na jakékoli zpracování (tj. nikoli pouze automatizované). Jsou zavedeny nové definice (např. pojem zpracovatel či příjemce osobních údajů), nová práva pro jednotlivce, a současně jsou zpřísněny povinnosti subjektů, které zpracovávají osobní údaje. Fyzické osoby, jejichž osobní údaje jsou zpracovávány, mají například právo seznámit se s důvody takového zpracování údajů. Další novinkou je právo nebýt předmětem rozhodnutí, které se týká subjektu údajů a které je založeno výhradně na automatizovaném zpracování, aniž by byly zohledněny názory subjektu údajů. Subjekt údajů má nově také právo kdykoli vznést námitku proti zpracování svých osobních údajů, pokud správce neprokáže závažné oprávněné důvody pro zpracování, které převažují nad jeho zájmy nebo právy a základními svobodami. Práva subjektu

[33] Důvodová zpráva k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat (*Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*). Dostupné z: https://rm.coe.int/16800ca434. [cit. 2024-09-01].

údajů jsou nově souhrnně zahrnuta do článku 9. Lze tak konstatovat, že Úmluva 108+ se značně přiblížila znění nařízení GDPR[34]. Úmluva 108+ nicméně ještě nevstoupila v platnost, neboť nebyla ratifikována všemi stranami. Od 11. října 2023 platí, že pro vstup v platnost stačí, aby byl ratifikován Protokol, kterým se mění Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (tzv. protokol č. 223) alespoň 38 státy Úmluvy, k čemuž ovšem stále nedošlo[35]. Důvodů, proč státy stále neratifikovaly tuto modernizovanou Úmluvu, může být více. Jedná se především o právní, politické a legislativně-technické důvody. Pomalá ratifikace může být spojena s právní složitostí. Proces harmonizace s vnitrostátními právními předpisy může být složitý a časově náročný, zejména v právních systémech, kde je vztah mezi vnitrostátním a mezinárodním právem složitý. Mnoho zemí navíc již má národní nebo regionální rámec ochrany údajů, jako je například nařízení GDPR v EU. Mohou tak vyvstat otázky, jak sladit Úmluvu s těmito předpisy, aby nedocházelo k překryvům nebo konfliktům mezi nimi. Z legislativně-technického hlediska může představovat problém zejména širší působnost Úmluvy oproti právnímu rámci nařízení GDPR. Úmluva zahrnuje i oblast zpracování osobních údajů za účelem národní bezpečnosti a obrany (jedná se o zpracování zpravodajskými službami a některými dalšími orgány, např. Ministerstvem obrany či Národním bezpečnostním úřadem). V případě ČR je tak podle gestora (Ministerstvo vnitra) nutné vyhodnotit potřebu přípravy legislativních opatření s ohledem na případné uplatnění některé z výjimek.[36] A konečně, ratifikační procesy závisí na politické vůli a prioritách vlády. Úmluva tak nemusí být vnímána jako urgentní politický problém, jako politická priorita, zejména pokud již státy mají robustní právní rámec, jako je právě nařízení GDPR.

1.4 Právo Evropské unie ochrany osobních údajů

V původních smlouvách Evropských společenství nebyla žádná zmínka o lidských právech nebo jejich ochraně. Soudní dvůr EU se však při výkladu smluv musel čím dál tím častěji zabývat případy údajného porušování lidských práv v oblastech spadajících do

[34] Důvodová zpráva k Úmluvě 108+ (*Explanatory Report)*, dostupné zde: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Modernizovaná Úmluva 108: novinky v kostce (*The modernised Convention 108: novelties in a nutshell*). Dostupné z: https://rm.coe.int/16808accf8. [cit. 2024-09-01].

[35] Aktuální přehled států, které ratifikovaly Protokol k Úmluvě 108+ je k dispozici zde: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223. Česká republika jej sice k 10. 10. 2018 podepsala, zatím ale stále ještě neratifikovala. [Stav ke dni 2024-08-03].

[36] LIPANOVÁ, Kateřina, 2020. K zásadní změně Úmluvy Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva č. 108). Online. *Jurisprudence*. 2020, Roč. 29, Č. 4, s. 10 (35-44). ISSN 1802-3843. Dostupné z: https://www.jurisprudence.cz/cz/casopis/k-zasadni-zmene-umluvy-rady-evropy-o-ochrane-osob-se-zretelem-na-automatizovane-zpracovani-osobnich-dat.m-443.html. [cit. 2024-09-25].

působnosti práva EU. Základní práva tak byla postupně zařazena mezi tzv. obecné zásady evropského práva. V roce 2000 byla přijata Listina základních práv Evropské unie, původně byla schválena jako nezávazný dokument o základních právech a svobodách. Na základě Lisabonské smlouvy však byla Listina inkorporována do primárního práva EU a získala tak právní závaznost.

Listina zaručuje nejen respektování soukromého a rodinného života (článek 7[37]), ale stanoví také právo na ochranu osobních údajů (článek 8[38]). Je tak skutečně významným, moderním a komplexním lidskoprávním dokumentem, který staví ochranu osobních údajů na úroveň základního práva v právu EU. Pokud se podíváme nejdřív na ustanovení článku 7, tak zjistíme, že je v porovnání s ostatními ustanoveními chránícími právo na soukromí v mezinárodním právu poměrně stručné[39]. Jeho smysl a rozsah je však stejný jako u EÚLP, jak ostatně vyplývá z tzv. Vysvětlení k článku 7 Listiny[40]. Toto právo tak může být omezeno stejnými omezeními, která jsou stanovena v článku 8 EÚLP. Ochrana osobních údajů je pojata v Listině jako samostatné právo pod článkem 8. Rozdělením ochrany soukromí a práva na ochranu osobních údajů do dvou na sebe navazujících článků tak evropský zákonodárce deklaroval, že tato práva spolu sice úzce souvisí, avšak jedná se o dvě samostatná základní práva[41]. Článek 8 Listiny byl formulován několik let po vzniku sekundární legislativy, a sice směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice 95/46“), tudíž reflektuje i její úpravu a částečně také úpravu z Úmluvy č. 108. Listina proto nejenže v čl. 8 odst. 1 výslovně zmiňuje právo na ochranu osobních údajů, ale v čl. 8 odst. 2 také uvádí základní

[37] Článek 7 Listiny: „*Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace.“*

[38] Článek 8 Listiny:

„1. Každý má právo na ochranu osobních údajů, které se ho týkají.

2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.

3. Na dodržování těchto pravidel dohlíží nezávislý orgán.“

[39] KOVÁČOVÁ, Lucia; NECHVÁTALOVÁ, Lucie a VÝBORNÝ, Štěpán, 2013. Kapitola 3 Ochrana soukromí versus svoboda projevu médií z mezinárodněprávní perspektivy. In: *Ochrana soukromí versus svoboda projevu médií*. Online. Spisy Právnické fakulty MU, Řada teoretická, Ed. S, 442. Brno: Masarykova univerzita, Právnická fakulta. ISBN 978-80-210-6521-5. Dostupné z: https://science.law.muni.cz/knihy/monografie/Ochrana_soukromi_vs_svoboda_projevu_medii.pdf. [cit. 2024-08-03].

[40] FRA. Vysvětlení Agentury FRA k jednotlivým ustanovením Listiny základních práv Evropské unie. Dostupné zde: https://fra.europa.eu/cs/eu-charter/. [cit. 2024-07-16].

[41] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 51-65. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-07-16].

zásady ochrany údajů a v odst. 3 pak vyžaduje, aby provádění těchto zásad kontroloval nezávislý orgán. Pokud jde konkrétně o právo na přístup, i to je v čl. 8 odst. 2 Listiny výslovně zmíněno jako právo subjektu údajů spolu s právem na opravu.

Důležitým mezníkem ve vývoji práva na ochranu údajů je právě přijetí Lisabonské smlouvy. Lisabonská smlouva výslovně stanovila právo na ochranu údajů do článku 16 SFEU v části první věnované obecným zásadám EU. Článek 16 rovněž vytvořil nový právní základ a udělil EU pravomoc přijímat právní předpisy v oblasti ochrany údajů. Je to právě článek 16, který vytvořil právní základ pro přijetí nové komplexní reformy pravidel ochrany údajů v roce 2016, a sice obecného nařízení o ochraně osobních údajů (nařízení GDPR) a tzv. trestněprávní směrnice.

Ačkoli Rada Evropy byla v oblasti ochrany údajů poměrně úspěšná, zejména při stanovení hlavních prvků právního rámce, nebyla už tolik úspěšná v otázce zajištění jednotné aplikace Úmluvy č. 108 ve všech členských státech. Evropská komise se velmi obávala, že tento nedostatek jednotnosti by mohl bránit rozvoji vnitřního trhu v oblastech, kde má zpracování osobních údajů hrát stále důležitější úlohu. Na konci roku 1990 proto předložila návrh směrnice s cílem harmonizovat vnitrostátní právní předpisy o ochraně údajů v soukromém a z větší části i veřejném sektoru. Po čtyřech letech jednání tak byla přijata směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů („směrnice 95/46“), která se tak stala hlavním předpisem unijního sekundárního práva v oblasti ochrany údajů až do května 2018. Jejím právním základem byl článek 100a Smlouvy o založení Evropského společenství (nynější článek 114 Smlouvy o fungování Evropské unie). Směrnice 95/46 vycházela ze zásad ochrany údajů, které již byly obsaženy ve vnitrostátních právních předpisech a v Úmluvě č. 108, které dále rozpracovala. Její cíl byl dvojí: zaprvé vyžadovala, aby všechny členské státy chránily základní práva a svobody fyzických osob, a zejména právo na soukromí v souvislosti se zpracováním osobních údajů v souladu s touto směrnicí. Zadruhé jim uložila, aby z důvodů souvisejících s touto ochranou neomezovaly ani nezakazovaly volný pohyb osobních údajů mezi členskými státy.[42] Směrnice 95/46 fakticky zavedla podrobný a komplexní systém ochrany údajů v EU. V souladu s právním systémem EU však neplatila přímo a musela být transponována do vnitrostátních právních předpisů členských států. Přestože směrnice měla

[42] HUSTINX, Peter, Speeches and Articles EDPS. *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. Červenec 2013. Dostupné z: https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en. [cit. 2024-07-12].

zajistit úplnou harmonizaci, v praxi byla v členských státech transponována odlišně. Navíc se vlivem prudkého nárůstu a vývoje technologií ukázalo, že právní ochrana, kterou poskytuje, není dostačující. Již v roce 2009 se tak začalo diskutovat o potřebě modernizovat pravidla EU pro ochranu údajů – v té době Komise zahájila veřejnou konzultaci o budoucím právním rámci pro základní právo na ochranu osobních údajů. Návrh nařízení GDPR Komise zveřejnila již v lednu 2012 a zahájila tak dlouhý legislativní proces jednání mezi Evropským parlamentem a Radou EU.[43]

Dne 27. dubna 2016 tak bylo přijato Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES („nařízení GDPR“ nebo též „obecné nařízení“), účinnosti nabylo až o dva roky později. Je součástí dosud největší reformy ochrany údajů v Evropské unii. Tato reforma zahrnuje také směrnici Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV („trestněprávní směrnice“). Dále zahrnuje nařízení Evropského parlamentu a Rady (EU) 2018/1725 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES („EUDPR“). Jako forma právního aktu tedy bylo v případě GDPR zvoleno nařízení, které přímo stanovuje povinnosti a přiznává práva přímo jeho adresátům, kterými jsou také jednotlivé vnitrostátní subjekty, nikoliv primárně státy. Nařízení tak lze zjednodušeně označit za obdobu zákona, jelikož na adresáty přímo dopadá. Nařízení GDPR zachovává a dále rozpracovává základní zásady a práva subjektu údajů stanovené ve směrnici 95/46. Kromě toho zavádí nové povinnosti, podle kterých organizace musejí zavést záměrnou a standardní ochranu údajů, za určitých okolností jmenovat pověřence pro ochranu osobních údajů, dodržovat nové právo na přenositelnost údajů a respektovat zásadu odpovědnosti. To, jaký mají nařízení GDPR a trestněprávní směrnice skutečně význam a jakým způsobem upravují jednotlivá práva (vč. práva na přístup) a povinnosti, však bude podrobně rozebráno v dalších částech této práce.

[43] FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2024-07-12]

2. Terminologie ochrany osobních údajů a základní zásady zpracování

V této části se budu zabývat terminologií, základními pojmy ochrany osobních údajů nařízení GDPR. Vyjasnění základních pojmů je stěžejní pro aplikaci nařízení. Bez toho, aniž bychom věděli, zdali se skutečně jedná o *osobní údaje* či údaje jiné, a zda se jedná o operaci *zpracování osobních údajů* či jakékoli nakládání s osobními údaji, není možné správně aplikovat nařízení GDPR. Samozřejmostí je, že musí být dána i věcná a místní působnost nařízení podle článku 2 a 3. Uvedu pouze základní pojmy, neboť pro rozebrání všech pojmů, které jsou obsaženy v hlavním definičním ustanovení, tj. článku 4 nařízení GDPR, zde není prostor. Ustanovení článku 4 nařízení obsahuje celkem 26 bodů, přičemž klíčovými pojmy jsou především „osobní údaj", „zpracování osobních údajů" a „uživatelé osobních údajů" (subjekt údajů, správce, zpracovatel). Poslední kapitola této části je pak věnovaná základním zásadám zpracování, což je základní kámen každé operace zpracování, které musí správce dodržovat.

2.1 Osobní údaj

Definice osobního údaje je pro aplikaci nařízení GDPR stěžejní, vzhledem k tomu, že zpracování osobních údajů se ze své podstaty týká pouze údajů osobních. Nařízení GDPR ve svém definičním ustanovení (článek 4 bod 1) definuje pojem „osobní údaje". Jedná se o „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů")"*, přičemž identifikovatelnou fyzickou osobou je „*fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor*." Následuje demonstrativní výčet, co vše může tímto identifikátorem být: jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Oproti definici ve směrnici 95/46 (konkrétně v článku 2 písm. a)) se definice v GDPR významově nezměnila. Pouze se rozšířil počet výslovně uvedených identifikátorů (např. lokační údaje nebo síťový identifikátor), což ale vzhledem k jejich demonstrativní povaze a skutečnosti, že zpravidla byly považovány za možné osobní údaje i před účinností nařízení, nemá zásadní význam.[44] Také Úmluva 108+ obsahuje de facto totožnou definici. Ochrana osobních údajů se tedy může vztahovat pouze na fyzické osoby, a to pouze za jejich života, neboť zemřelí již nejsou fyzickými osobami podle občanského práva. Při určování, zda je fyzická osoba identifikovatelná, musí správce nebo jiná

[44] ŽŮREK, JUDr. Jiří. *Praktický průvodce GDPR (včetně rozhodovací praxe ÚOOÚ)* [online]. 2021 [cit. 2024-04-14].

osoba podle 26. bodu odůvodnění přihlédnout ke všem prostředkům, o nichž lze rozumně předpokládat, že se použijí pro přímou či nepřímou identifikaci jednotlivce, například výběrem vyčleňováním nebo odlišením, které umožňují zacházet s jednou osobou jinak než s jinou. Tentýž bod odůvodnění zároveň hovoří o tom, že referenčním kritériem je pravděpodobnost, že budou k dispozici přiměřené prostředky k identifikaci. V úvahu musí být vzaty všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji.[45]

Jak je to s ochranou osobních údajů u právnických osob? Podle definice v nařízení GDPR se na ně tato ochrana nevztahuje. Ještě před působností nařízení to ovšem nebylo tak jednoznačné, jak lze ostatně doložit i rozdíly ve vnitrostátních právních předpisech. Předpisy Lucemburska, Norska a Rakouska připouštěly v této oblasti také ochranu pro právnické osoby. Bylo to zdůvodňováno rostoucí asymetrií mezi informační silou některých společností, a ve jménu ochrany svobody podnikání, ale také ochrany zaměstnanců malých podnikových struktur, aby tyto společnosti mohly využívat některých výsad, které nařízení v současné době vyhrazuje pouze fyzickým osobám. Také dnes stále rezonují úvahy o rozšíření ochrany na právnické osoby v určité části právnické obce, píše o tom např. prof. Yves Poullet ve své knize Ochrana soukromí v digitálním věku[46]. Vychází především z výkladu rozhodnutí štrasburského ESLP[47], který přiznal právnickým osobám určitou ochranu podle článku 8 EÚLP, zejména pokud šlo o ochranu obydlí (resp. sídlo společnosti, kanceláře a profesní prostory). Uznává však, že rozšíření ochrany osobních údajů na právnické osoby a její podřazení pod článek 8 EÚLP by bylo v rozporu se samotnou podstatou tohoto ustanovení. Zabývá se nicméně otázkou, jestli by nešlo vyjít z článku 10 EÚLP. Podle něj by takový základ legitimizoval pozitivní závazek Evropské unie nebo členských států chránit nezisková sdružení a malé a střední podniky před využitím jejich údajů některými správci údajů. Nemohlo by se sice jednat o „zkopírování“ všech stávajících ustanovení týkajících se fyzických osob, ale bezpochyby o přiznání určitých výsad dotčeným právnickým osobám, které jsou podobné výsadám fyzických osob (např. právo na přístup, opravu, právo být zapomenut atd.).

[45] FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2024-04-07]
[46] POULLET, Yves, 2019. « Chapitre 1 – Analyse critique du RGPD ». In: POULLET, Yves. *La vie privée à l'heure de la société du numérique*. 1ère éd. Bruxelles: Larcier, s. 97-168. ISBN 9782807911079.
[47] Rozsudek druhého senátu ESLP ze dne 16. dubna 2002 Société Colas Est a další proti Francii (stížnost č. 37971/97).

Pokud vyjdeme z dokumentu pracovní skupiny WP29[48], tak je obvyklé analyzovat definici „osobních údajů“ tak, že se rozdělí na čtyři hlavní složky: (1) „veškeré informace“; (2) „týkající se“; (3) „identifikované nebo identifikovatelné“; (4) „fyzické osoby“. Pokud jde o první z těchto prvků, Soudní dvůr EU ve věci *Nowak*[49] uvedl: „*Použití výrazu „veškeré informace“ v rámci definice pojmu „osobní údaj“[…] odráží cíl unijního zákonodárce přiznat tomuto pojmu široký význam, přičemž tento pojem se neomezuje na informace, které jsou citlivé nebo patří do soukromé sféry, ale potenciálně zahrnuje všechny druhy informací, a to jak objektivní, tak subjektivní ve formě názoru nebo hodnocení pod podmínkou, že jsou „o“ dotčené osobě.“* Poučné je v tomto ohledu rovněž stanovisko generální advokátky Sharpston ve věci *YS*[50]: „*Skutečný obsah těchto informací patrně nemá žádný význam, pokud se týkají identifikované či identifikovatelné osoby. Lze jej chápat tak, že se týká jakékoliv skutečnosti týkající se soukromého života této osoby a případně jejího profesního života (který může zahrnovat více veřejný aspekt tohoto soukromého života). Může být dostupný v písemné formě, nebo může být například zachycen na zvukovém záznamu nebo obrazově*.“ Nařízení GDPR pracuje s širokým pojetím pojmu „osobní údaj“, přičemž je nutné v tomto smyslu poukázat na judikaturu Soudního dvora EU, jakož i na rozhodovací praxi dozorových úřadů zemí EU, které k extenzivnímu výkladu přispívají.

Soudní dvůr EU v rámci své judikatury shledal, že různé typy informací mohou být osobními údaji. Nejedná se tedy pouze o identifikační údaje (jméno, příjmení, adresa bydliště), na jejichž základě lze konkrétní osobu jednoznačně určit, ale o veškeré informace, které se určeného či určitelného člověka týkají, byť jej ani samy o sobě, ani v kombinaci s dalšími informacemi přímo neidentifikují.[51] Není rozhodující, zda je informace negativní nebo pozitivní, objektivní (přítomnost určité látky v krvi) nebo subjektivní (názor nebo hodnocení osoby, např. posouzení bonity klienta bankou), ani zda se jedná o informaci pravdivou nebo prokázanou či nikoliv, případně zveřejněnou či nezveřejněnou. Předpisy ochrany osobních údajů ve skutečnosti počítají s tím, že údaje mohou být nesprávné, a proto stanovují právo subjektu údajů mít k těmto údajům přístup a napadnout je pomocí vhodných prostředků pro zajištění opravy nepřesných údajů. Mezi osobní údaje tak podle judikatury Soudního dvora

[48] WP29. *Stanovisko č. 4/2007 (WP136) k pojmu osobní údaje*, přijaté dne 20. června 2007, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf.
[49] Rozsudek ze dne 20. prosince 2017, Nowak, C-434/16, EU:C:2017:994, bod 34.
[50] Stanovisko generální advokátky Eleanor Sharpston ze dne 12. prosince 2013, YS a další, spojené věci C-141/12 a C-372/12, EU:C:2013:838, bod 45.
[51] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.

patří[52] mimo jiné telefonní číslo osoby nebo informace o jejích pracovních poměrech a zálibách[53]; údaje o osobních příjmech a daních[54]; identifikátory cookies[55]; otisky prstů[56]; snímky osob zaznamenané videokamerou[57]; písemné odpovědi účastníka odborné zkoušky a komentáře zkoušejících k těmto odpovědím[58]; údaje o provozu elektronických komunikací, včetně dynamické IP adresy[59]; identifikační číslo vozidla (tzv. VIN – vehicle identification number), tj. alfanumerický kód přidělený vozidlu výrobcem za účelem správné identifikace každého vozidla[60]. Pokud jde o prvek identifikovatelnosti osoby (údaj týkající se fyzické osoby), také v tomto případě zaujal Soudní dvůr EU široký přístup. Ve věci *Nowak*[61] uvedl, že tento prvek je splněn, pokud informace z důvodu svého účelu, obsahu nebo účinku souvisí s určitým jedincem. Jeden z posledních rozsudků, který se týkal pojmu „osobní údaje", je rozsudek ve věci *IAB Europe*[62]. Soudní dvůr zde rozhodl, že řetězec složený z kombinace písmen a znaků, jako je TC String (Transparency and Consent String), který obsahuje preference uživatele internetu nebo aplikace týkající se souhlasu tohoto uživatele se zpracováním osobních údajů, které se ho týkají, představuje osobní údaj, z důvodu možnosti jeho spojení s dalšími identifikátory (např. IP adresou), a umožňuje tak identifikovat subjekt údajů.

Nelze opominout ani vnitrostátní judikaturu, která rovněž zastává objektivní pojetí osobního údaje. Nález Ústavního soudu[63] například za osobní údaje považuje i tzv. metadata (tedy údaje provozního charakteru o činnosti osob): „*Tzv. ‚metadata' o uskutečněné komunikaci*

[52] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].
[53] Rozsudek ze dne 6. listopadu 2003, Lindqvist, C-101/01, EU:C:2003:596, bod 27.
[54] Rozsudek ze dne 20. května 2003, Österreichischer Rundfunk a další, spojené věci C-465/00, C-138/01 a C-139/01, EU:C:2003:294, bod 64. Rozsudek ze dne 1. října 2015, Bara a další, C-201/14, EU:C:2015:638, bod 29.
[55] Rozsudek ze dne 1. října 2019, Planet49, C-673/17, EU:C:2019:801, bod 45.
[56] Rozsudek ze dne 17. října 2013, Schwarz, C-291/12, EU:C:2013:670, bod 27.
[57] Rozsudek ze dne 11. prosince 2014, Ryneš, C-212/13, EU:C:2014:2428, bod 22. Rozsudek ze dne 14. února 2019, Buivids, C-345/17, EU:C:2019:122, bod 32.
[58] Rozsudek ze dne 20. prosince 2017, Nowak, C-434/16, EU:C:2017:994, body 36 a 42.
[59] Rozsudek ze dne 8. dubna 2014, Digital Rights Ireland a Seitlinger a další, spojené věci C-293/12 a C-594/12, EU:C:2014:238, bod 26. Rozsudek ze dne 19. října 2016, Breyer, C-582/14, EU:C:2016:779, bod 49. Rozsudek ze dne 6. října 2020, La Quadrature du Net a další, spojené věci C-511/18, C-512/18 a C-520/18, EU:C:2020:791, body 152 a 153.
[60] Rozsudek ze dne 9. listopadu 2023, Gesamtverband Autoteile-Handel (Přístup k informacím o vozidlech), C-319/22, EU:C:2023:837, body 46 a 48. Soud ovšem v tomto případě své vyjádření „korigoval", neboť uvedl, že VIN může představovat osobní údaj (resp. „získává tuto osobní povahu") pouze ve vztahu k jakékoli osobě, která má k dispozici prostředky, jež jí rozumně umožňují spojit tento údaj s konkrétní osobou.
[61] Rozsudek ze dne 20. prosince 2017, Nowak, C-434/16, EU:C:2017:994, bod 35.
[62] Rozsudek ze dne 7. března 2024, IAB Europe, C-604/22, EU:C:2024:214, body 43 až 45.
[63] Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17.

(tj. vše kromě obsahu) mohou být z hlediska zásahu do soukromí jednotlivce ve skutečnosti mnohem cennější a fakticky i ‚nebezpečnější' než znalost samotného obsahu komunikace, neboť jsou strojově zpracovatelná a analyzovatelná; z výsledků takového zpracování pak lze usuzovat budoucí chování jednotlivce." Podle Nejvyššího správního soudu[64] zase může být osobním údajem i registrační značka vozidla. Ten se nechal inspirovat také judikaturou dalších států EU a analogicky i rozsudkem Soudního dvora EU k IP adrese, která se vlastně také vztahuje pouze k zařízení. Při bližším zkoumání soudobé praxe ochránců dat a dozorových úřadů lze za osobní údaje považovat také personalizovanou emailovou adresu, historii prohlížení internetových stránek nebo informace o spotřebě (údaje týkající se teploty, spotřeby elektřiny nebo plynu, množství spotřebované teplé vody, stav elektrických spotřebičů atd.) v rámci jedné domácnosti[65]. Z hlediska ochrany není pro kvalifikaci osobního údaje rozhodný ani formát zachycených informací a nosič, který je obsahuje. Může jít o textovou, číselnou, grafickou, fotografickou, zvukovou či audiovizuální podobu.

Ve vztahu k osobním údajům je nutné zmínit také anonymní a anonymizované údaje. Anonymním údajem je jakákoli informace, na jejímž základě nelze vůbec identifikovat fyzickou osobu, nikdy tedy nebyla osobním údajem. Anonymizovaný údaj byl v minulosti osobním údajem, ale v současné době již identifikaci nelze provést. Důvodem je, že tento údaj byl předmětem nevratného technického procesu anonymizace[66]. Oproti těmto dvěma kategoriím stojí pseudonymizovaný údaj, který si zachovává status osobního údaje, neboť stále umožňuje (typicky nepřímou) identifikaci fyzické osoby. Pseudonymizace[67] je v podstatě technický proces, který napomáhá v zabezpečení osobních údajů.

V praxi zpracování údajů byla zaznamenána řada případů, kdy byly údaje, které byly nejprve považovány za anonymní, ve skutečnosti údaji osobními, neboť umožnily identifikaci. Na základě zdokonalující se datové analýzy lze ze zdánlivě technických dat získat poměrně přesné osobní informace. Rizika opětovné identifikace v čase rostou. Již v roce 2000 stačila kombinace PSČ, data narození a pohlaví k identifikaci 87 % obyvatel USA. Známé jsou

---

[64] Rozsudek Nejvyššího správního soudu ze dne 13. 8. 2020, č. j. 1 As 387/2019-56, bod 31.

[65] WP29. *Stanovisko č. 12/2011 k inteligentnímu měření (WP183)*, přijaté dne 4. dubna 2011, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_cs.pdf.
CNIL, 2014. Metodika francouzského dozorového úřadu CNIL k chytrému měření. *Pack de conformité – les Compteurs Communicants*. Online. Dostupné z: https://www.cnil.fr/sites/cnil/files/typo/document/Pack_de_Conformite_COMPTEURS_COMMUNICANTS.pdf [cit. 2024-04-14].

[66] WP29. *Stanovisko č. 5/2014 k technikám anonymizace (WP216),* přijaté dne 10. dubna 2014, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[67] Pseudonymizaci rozvádí body odůvodnění 26, 28 a 29 a je též přímo definována v článku 4 bodu 5 nařízení GDPR.

záznamy o hodnocení filmů 500 000 předplatitelů streamovací služby Netflixu, u nichž došlo v roce 2008 k re-identifikaci pomocí veřejně přístupné internetové filmové databáze. V roce 2013 byly z anonymizované veřejné databáze jízd newyorských taxíků, která neobsahovala žádné informace o cestujících, a paparazzi snímků odvozeny cestovní trasy některých celebrit, včetně konkrétních adres ulic a toho, zda zanechaly spropitné. V roce 2014 umožnila znalost polohy držitelů kreditních karet znovu identifikovat 90 % transakcí (za období tří měsíců) kreditní kartou, zaznamenávající útraty 1,1 milionu lidí v 10 000 obchodech, přičemž byl k dispozici pouze přístup k vynaloženým částkám, typu obchodu a kódu představující každou osobu. Tento experiment proběhl úspěšně ve čtyřech oddělených případech. Znalost konkrétních vynaložených částek v těchto případech vedla k opětovné identifikaci téměř všech držitelů karet.[68]

Na pojmu „osobní údaj“ ve světle výkladu judikatury Soudního dvora EU mohu velmi dobře ilustrovat prudký technologický vývoj a zároveň nutnost na tento vývoj regulativně reagovat. Pojem „osobní údaj“ se stal velmi nejednoznačným a rozhodně by neměl být považován za pojem statický. Informace mohou být spojeny s osobou v průběhu času, vůči různým subjektům a v různých kontextech. Je tak podle mého názoru nutné zaujmout flexibilní, poměrně široký a kazuistický přístup, který zohlední neustálou proměnu údajů (dat) jako takových[69]. Právo EU předpoklady pro široké pojetí tohoto pojmu vytvořilo. Soudní dvůr EU svojí judikaturou k tomuto širokému pojetí přispívá. Nekloním se ovšem k výše uvedenému názoru prof. Yves Poulleta. Domnívám se, že ochrana osobních údajů je inherentně spjata s člověkem, souvisí s právem na ochranu lidské důstojnosti a právem na informační sebeurčení. Podle mého názoru by tak neměla sloužit k ochraně právnických osob, a to ani malých podniků či neziskových sdružení. Tyto entity mají k dispozici jiné prostředky ochrany v soukromém právu, jako je ochrana jejich názvu nebo pověsti.

Ráda bych ještě upozornila na úvahy N. Purtové. Ta ve své práci[70] obecně podporuje široké pojetí osobních údajů, z hlediska budoucího vývoje nicméně varuje před situací, kdy téměř všechny údaje spadnou do kategorie osobní údaj, neboť najednou vše bude předmětem

[68] PURTOVA, Nadezhda, 2018. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. Online. *Law, Innovation and Technology*. Roč. 2018, č. 10(1), s. 35. Dostupné z: https://doi.org/10.1080/17579961.2018.1452176. [cit. 2024-07-12].
[69] AUSLOOS, Jef a DEWITTE, Pierre, 2018. Shattering One-Way Mirrors. Data Subject Access Rights in Practice. Online. *International Data Privacy Law*. March 2018, Volume 8, Issue 1, s. 25 (4–28). Dostupné z: https://doi.org/10.1093/idpl/ipy001. [cit. 2024-07-12].
[70] PURTOVA, Nadezhda, 2018. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. Online. *Law, Innovation and Technology*. Roč. 2018, č. 10(1), s. 35. Dostupné z: https://doi.org/10.1080/17579961.2018.1452176. [cit. 2024-07-12].

ochrany osobních údajů, a v důsledku toho to může vést k uložení stejně vysoké intenzity povinností správcům ve všech situacích zpracování údajů. Systém právní ochrany založený na všezahrnujícím pojetí a vysoké intenzitě pozitivních povinností správců v oblasti dodržování předpisů nebude podle ní dlouhodobě udržitelný. Podle ní existují dvě možnosti řešení. Zaprvé, zachovat široký výklad osobních údajů, ale snížit intenzitu povinností týkajících se dodržování předpisů, například přizpůsobením intenzity rizikům, vytvořit třeba různé soubory povinností pro různé druhy osobních údajů, nebo diferenciovat povinnosti správců podle různého stupně identifikovatelnosti informací. Zde vidí ovšem problém stanovit hranice pro režimy compliance různé intenzity. Proto se možná více kloní k druhé variantě, a sice zcela upustit od formálního rozlišování pojmu „osobní údaj" jako základního kamene ochrany údajů, čímž bude fakticky uznáno, že všechny údaje budou osobní. Ve výsledku totiž podle ní může mít každá informace potenciální dopad na lidi. Namísto toho by se mohlo pracovat s konceptem „újmy způsobené informacemi" chápané obecně jako jakékoli individuální nebo veřejné negativní důsledky zpracování informací. Měly by se tak především posuzovat jak pravděpodobné, tak fakticky zamýšlené a náhodné dopady zpracování údajů na subjekty údajů.

Osobně považuji tyto úvahy N. Purtové za opodstatněné, nicméně domnívám se, že rozlišování pojmů, vč. základního pojmu osobní údaj, má stále své místo, už kvůli významu právní úpravy chránit fyzické osoby. Souhlasím ovšem, že by se více měly rozvíjet koncepty újmy způsobené informacemi, stejně tak, že by se mělo v praxi více pracovat s posouzením dopadů zpracování údajů na lidi. Nařízení GDPR ostatně potřebné instituty má. Nařízení totiž zná institut posouzení vlivu na ochranu osobních údajů (tzv. DPIA), předpokládá navíc také obecný přístup založený na riziku (*risk based approach*), tedy povinnost správce provést základní posouzení rizik pro práva a svobody osob a s ohledem na míru rizika přijmout potřebná opatření.

2.2 Zpracování osobních údajů

Pro aplikaci nařízení GDPR je druhým klíčovým pojmem právě pojem „zpracování", upravený v článku 4 bodu 2 nařízení. Definice v nařízení se oproti dřívější směrnici nijak nerozšířila. Obě právní úpravy chápaly pojem široce, přičemž nařízení toto extenzivní pojetí zdůvodňuje cílem zajistit soudržnou a vysokou úroveň ochrany fyzických osob. Definice v podstatě zahrnuje jakoukoli operaci zpracování údajů, bez ohledu na dobu trvání operace,

množství zpracovávaných údajů, nebo zda je pořizován záznam.[71] Podle GDPR je zpracováním „*jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů.“* Následuje opět demonstrativní výčet pro ilustraci, co vše může zpracováním být: shromáždění, zaznamenání, uspořádání, strukturování, ale třeba také vyhledání, nahlédnutí, šíření nebo jakékoliv jiné zpřístupnění atd.

Prostředek a forma zpracování údajů jsou pro účely definice fakticky irelevantní. Definice totiž implicitně zahrnuje jak „zpracování osobních údajů zcela nebo částečně automatizovanými prostředky“, tak „zpracování jinými než automatizovanými prostředky“ (myšleno manuální zpracování osobních údajů, které jsou ale obsaženy v evidenci nebo do ní mají být zařazeny). Důležitým pojmem je tedy ve vztahu k manuálnímu zpracování právě pojem evidence, strukturovaný soubor osobních údajů, který je uspořádán podle zvláštních kritérií. Není-li splněna podmínka zařazení či úmyslu zařazení do evidence, není dána věcná působnost nařízení GDPR. Automatizované zpracování je pak veškeré zpracování prováděné pomocí výpočetní techniky. Definice automatizace však v nařízení obsažena není. Použitá technologie automatizovaného zpracování není rozhodující, neboť ochrana fyzických osob by měla být podle nařízení technologicky neutrální a nezávislá na použitých technologiích. Současně zpracování nesmí spadat do výjimky z rozsahu věcné působnosti nařízení podle čl. 2 odst. 2 nebo čl. 2 odst. 3 a 4 nařízení.

Dřívější vnitrostátní právní úprava v podobě zákona č. 101/2000 Sb., o ochraně osobních údajů kladla důraz na to, že zpracování osobních údajů musí být systematické a nikoli nahodilé.[72] Je však nutné doplnit, že tyto pojmy byly českou specialitou a neměly podklad v definici zpracování ve směrnici 95/46. Ani nařízení tuto otázku nahodilého a nesystematického zpracování osobních údajů neřeší. Český Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) nicméně tuto koncepci převzal i do současné praxe. ÚOOÚ k pojmu zpracování uvádí[73]: „*Zpracování ve smyslu obecného nařízení však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za*

[71] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

[72] Podle § 3 odst. 4 zákona se nevztahoval „*na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány*“. V § 4 písm. e) pak bylo vymezeno zpracování osobních údajů jako operace nebo soustava operací, systematicky prováděné s osobními údaji.

[73] ÚOOÚ. Základní příručka ÚOOÚ k ochraně údajů. Online. Dostupné z: https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju. [online]. [cit. 2024-04-14].

sofistikovanější činnost, nikoli nahodilou, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky. Pro nakládání s osobními údaji způsobem, který není zpracováním, poskytuje ochranu např. zákon č. 89/2012 Sb., občanský zákoník. Obecným nařízením se tak jako správci řídí pouze subjekty, které osobní údaje zpracovávají ve smyslu definice zpracování. Pojem zpracování má stejný význam, jako měl v zákoně č. 101/2000 Sb., o ochraně osobních údajů." Také podle JUDr. Jiřího Žůrka[74], odborníka v oblasti ochrany osobních údajů a dřívějšího ředitele odboru dozoru ÚOOÚ, nelze pod zpracování osobních údajů podle nařízení zařadit každou činnost spočívající v nakládání s osobními údaji. Mělo by to totiž za následek, že bychom každé lidské jednání, zahrnující interakci s osobními údaji, museli podřadit pod tento pojem, a to by bylo nereálné a též neúčelné. Zpracování tak podle něj musí být do jisté míry systematické, neboť musí probíhat za konkrétním účelem stanoveným správcem. Prvek systematičnosti tak naznačuje, že se již musí jednat o „kvalifikované" nakládání s osobními údaji za určitým účelem. Mgr. Nulíček a kol. zase uvádějí, že klíčem pro rozlišení, kdy se o zpracování osobních údajů jedná a kdy už nikoliv, je právě účel dané činnosti. Je-li účelem činnosti práce s osobními údaji jako takovými, i když v pasivní podobě (tzn. pouhé uchovávání) nebo jde o poslední činnost s těmito údaji (anonymizace nebo likvidace údajů), pak se o zpracování osobních údajů jedná. A naopak, pokud je přístup k údajům pouhým nepravidelným a nahodilým důsledkem jiné činnosti, jako je zejména servis či oprava technických prostředků pro zpracování osobních údajů, které mohou, ale nemusejí vždy zahrnovat i nárazový přístup k údajům, o zpracování podle GDPR se nejedná.[75] Někteří další odborníci v oblasti ochrany osobních údajů se nicméně domnívají, že by prvek systematičnosti neměl být přeceňován. Nařízení jej samo o sobě nestanoví a judikatura Soudního dvora EU má spíše tendenci vykládat jak pojem „osobní údaj", tak pojem „zpracování" extenzivně. Podle názorů těchto odborníků lze ovšem požadavek na znak systematičnosti vyvodit do jisté míry z čl. 2 odst. 1, neboť je imanentním znakem automatizovanosti zpracování či případně zpracování v evidenci.[76]

Jsem toho názoru, že by se pojmu zpracování měl přikládat široký význam, a to právě s ohledem na absenci těchto pojmů „systematičnost" či „nenahodilost" v unijních právních

[74] ŽŮREK, JUDr. Jiří. *Praktický průvodce GDPR (včetně rozhodovací praxe ÚOOÚ)* [online]. 2021 [cit. 2024-04-14].
[75] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.
[76] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 66-86. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

předpisech a na výkladovou linii Soudního dvora EU. V poslední řadě je podle mého názoru důležité připomenout cíl právní úpravy, kterým je právě poskytnutí vysoké míry ochrany subjektům údajů. Existují nicméně názory, že extenzivní výklad může vést ke zbytečné administrativní a právní zátěži pro některé osoby, které se takto stanou správci osobních údajů. Souhlasím, že se jedná o relevantní názor. Aby se předešlo tomu, že se tyto osoby stanou nechtěnými správci osobních údajů, existuje několik řešení. Základním řešením je zajistit jasný výklad prostřednictvím pokynů dozorových orgánů. To může snížit právní nejistotu a umožnit lepší rozlišení mezi správci a zpracovateli. Další řešení může představovat zjednodušený režim pro malé subjekty – správce. To je ostatně do jisté míry již v nařízení obsaženo, malí správci, kteří neprovádějí riziková zpracování, mají podstatně méně povinností než velcí správci. Navíc, mnou zastávané široké pojetí také předpokládá určité hranice. Domnívám se, že extenzivní pojetí tak, jak jej chápe Soudní dvůr EU, není tedy v současnosti systematický problém. Potřebné limity jsou z větší části již obsaženy v nařízení, ostatně souhlasím, že jako jistý prvek systematičnosti u pojmu zpracování lze chápat i požadavek zahrnutí či předpokladu zahrnutí osobních údajů v evidenci. To samo o sobě může hovořit o tom, že se pravděpodobně bude jednat o více či méně sofistikovanější činnost. Dalším důležitým limitem je, že ochrana osobních údajů je ryze veřejnoprávní regulací, zatímco ochrana osobnosti, včetně práva na soukromí, je řešena typicky v soukromoprávním kodexu, v případě ČR tedy v občanském zákoníku. V praxi ovšem může být někdy rozhraničení mezi veřejnoprávní a soukromoprávní regulací poměrně nejasné. Například v otázce používání kamerových systémů se český Úřad nezabývá kamerami instalovanými na pozemcích v soukromém vlastnictví v případě individuálních sporů mezi majiteli obydlí. To je zdůvodněno tím, že Úřad ze zákona (viz § 7 kontrolního řádu) nedisponuje oprávněním vstupovat do obydlí, které není používáno k podnikatelské činnosti, nemůže proto ověřit režim provozu kamery v obydlí, ani prostá tvrzení stran sporu. V této souvislosti proto Úřad pouze upozorňuje majitele nemovitostí na zákonná pravidla pro shromažďování a zpracování kamerových záznamů, neprovádí však kontrolu obydlí. Tato situace tak zpravidla nepodléhá prostředkům veřejného práva, s výjimkou, kdy se jedna ze stran dopouští šikanózního obtěžujícího jednání, které naplní skutkovou podstatu přestupku proti občanskému soužití podle zákona o některých přestupcích. V tomto případě je nicméně třeba oznámit jednání příslušné obci, aby bylo projednáno tzv. komisí k projednání přestupků. Ochrana je ovšem standardně ponechána prostředky soukromého práva.

Příklady operací zpracování jsou uvedeny v judikatuře Soudního dvora EU. Soudní dvůr tak shledal, že pojem „zpracování“ zahrnuje mimo jiné následující operace[77]: uvedení osobních údajů na internetové stránce[78]; shromažďování osobních údajů z veřejně přístupných dokumentů, zveřejňování osobních údajů v tištěné podobě, předání osobních údajů na CD-ROM nebo zasílání textových SMS zpráv obsahujících osobní údaje[79]; sdělení jména a adresy internetového účastníka nebo uživatele za účelem vedení civilních řízení[80]; činnosti vyhledávače, které spočívají v automatickém, neustálém a systematickém vyhledávání informací, které jsou na internetu zveřejněny, a ve zpřístupňování těchto informací ve formě seznamů výsledků vyhledávání[81]; uchovávání údajů za účelem jejich možného zpřístupnění příslušným vnitrostátním orgánům[82]; pořizování obrazového záznamu osob[83]; předávání osobních údajů z členského státu EU do třetí země[84]; zápis a uchovávání osobních údajů v rejstříku a jejich sdělení na žádost třetím osobám[85]; vyhotovení seznamu fyzických osob[86]; sběr a přenos osobních údajů návštěvníků internetových stránek prostřednictvím umístění sociálního modulu (plug-inu) třetí strany[87]. Široký výklad pojmu „zpracování“ použil Soudní dvůr i v jednom z posledních rozsudků ve věci *Endemol Shine Finland*.[88] Soud zde rozhodl, že i ústní sdělení informací o případných stávajících nebo předchozích odsouzeních fyzické osoby v trestních věcech představuje zpracování osobních údajů, pokud jsou tyto informace obsaženy v evidenci nebo do ní mají být zařazeny.

[77] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].
[78] Rozsudek ze dne 6. listopadu 2003, Lindqvist, C-101/01, EU:C:2003:596, bod 25. Rozsudek ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317, bod 26. Rozsudek ze dne 1. října 2015, Weltimmo, C-230/14, EU:C:2015:639, bod 37.
[79] Rozsudek ze dne 16. prosince 2008, Satakunnan Markkinapörssi a Satamedia, C-73/07, EU:C:2008:727, bod 37.
[80] Rozsudek ze dne 19. dubna 2012, Bonnier Audio a další, C-461/10, EU:C:2012:219, bod 52.
[81] Rozsudek ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317, bod 28.
[82] Rozsudek ze dne 8. dubna 2014, Digital Rights Ireland a Seitlinger a další, spojené věci C-293/12 a C-594/12, EU:C:2014:238, bod 29.
[83] Rozsudek ze dne 11. prosince 2014, Ryneš, C-212/13, EU:C:2014:2428, bod 25. Rozsudek ze dne 14. února 2019, Buivids, C-345/17, EU:C:2019:122, bod 35.
[84] Rozsudek ze dne 6. října 2015, Schrems, C-362/14, EU:C:2015:650, bod 45.
[85] Rozsudek ze dne 9. března 2017, Manni, C-398/15, EU:C:2017:197, bod 35.
[86] Rozsudek ze dne 27. září 2017, Puškár, C-73/16, EU:C:2017:725, bod 103.
[87] Rozsudek ze dne 29. července 2019, Fashion ID, C-40/17, EU:C:2019:629, bod 76.
[88] Rozsudek ze dne 7. března 2024, Endemol Shine Finland, C-740/22, EU:C:2024:216, body 30 až 32 a bod 35.

2.3 Uživatelé osobních údajů

Pojem „subjekt údajů“ není v definičním ustanovení nařízení GDPR uveden samostatně, ale v rámci definice pojmu „osobní údaje“, tj. v článku 4 bodu 1 nařízení. Jedná se o středobod ochrany osobních údajů, na který se tato ochrana vztahuje, přičemž subjektem údajů je jakákoli žijící fyzická osoba. Na tomto místě bych ráda zmínila jednu zajímavost z průběhu legislativního procesu přijetí nařízení. Komise původně navrhla, aby hlavním pojmem v definičním ustanovení byl právě „subjekt údajů“ a nikoli „osobní údaje“. Podstatu pojmu „osobních údajů“ (čl. 4 bod 2 návrhu nařízení) chtěla právě začlenit do definice „subjektu údajů“ (čl. 4 bod 1 návrhu nařízení). „Subjektem údajů“ tedy měla být „*identifikovaná fyzická osoba nebo fyzická osoba, kterou lze přímo či nepřímo identifikovat prostředky, o nichž lze důvodně předpokládat, že je správce nebo jakákoli jiná fyzická nebo právnická osoba použijí pro identifikaci dané osoby, zejména s odkazem na identifikační číslo, lokalizační údaje, elektronický identifikátor nebo s odkazem na jeden či více zvláštních prvků její fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo sociální identity*.“ „Osobními údaji“ pak měly být „*veškeré informace o subjektu údajů*.“ Tato navrhovaná struktura definice se ovšem v Parlamentu a Radě nesetkala s velkým pochopením, a proto byla nakonec vypuštěna.[89]

Hlavním odpovědným subjektem, tedy adresátem povinností uložených nařízením, je právě správce. Pojem „správce“ je definován v článku 4 bodu 7 nařízení. „Správcem“ tak může být „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení*.“ Původní návrh Komise počítal s tím, že správcem je subjekt, který určuje účel, podmínky a prostředky zpracování. Také od tohoto návrhu se nakonec upustilo, právě z důvodu, že podmínky jsou primárně určeny samotnou právní úpravou nařízení a nikoli správcem. Správce je tedy entita, jejímiž hlavními znaky jsou, že určuje účel a prostředky zpracování, tj. důvod a způsob zpracování, zjednodušeně proč se osobní údaje zpracovávají a jak se zpracovávají. Je klíčovým aktérem celé ochrany osobních údajů, neboť je nositelem povinností vůči subjektům údajů.

[89] Evropská komise 2012. *Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů)*, COM/2012/011 final, 25. ledna 2012. Dostupné zde: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A52012PC0011.

Jak uvedla pracovní skupina WP29 ve svém stanovisku[90], význam pojmu správce spočívá v určení, kdo je odpovědný za dodržování pravidel pro ochranu osobních údajů a jak mohou subjekty údajů uplatňovat svá práva v praxi. Také pozdější nástupce skupiny WP29, EDPB ve svých pokynech[91] zdůrazňuje význam správce jako orgánu, který rozhoduje o určitých klíčových prvcích zpracování, mezi něž patří zejména účel zpracování a právní základ (titul) zpracování. Prostředky zpracování může do určité míry zajistit další zapojený subjekt, tzv. zpracovatel, o kterém se podrobněji rozepíšu dále. V tomto smyslu lze odkázat opět na uvedené pokyny EDPB, které rozlišují tzv. podstatné a nepodstatné prostředky zpracování. Podstatné prostředky jsou vyhrazeny pro správce, mezi ně patří zejména druh zpracovávaných osobních údajů, doba zpracování, kategorie příjemců a kategorie subjektů údajů. Oproti tomu nepodstatné prostředky se týkají praktičtějších aspektů provádění, jako je volba konkrétního typu hardwaru nebo softwaru nebo podrobná bezpečnostní opatření, přičemž o těchto prostředcích může rozhodnout i zpracovatel. Pro snadnější pochopení lze správce popsat jako entitu, která má nad konkrétní operací zpracování vliv nebo kontrolu, proto se také používá anglický termín pro správce jako „controller“. Důležité je, že se jedná o tzv. funkční pojem, což znamená, že je nutné vždy zjistit, kdo má skutečně faktický vliv nad konkrétní operací zpracování, nikoli kdo je za správce formálně označen. Není rozhodující, zda má správce k údajům faktický přístup nebo zda je má k dispozici. Nařízení GDPR (stejně jako dřívější směrnice 95/46) navíc počítá s tím, že může dojít k určení účelu a prostředků zpracování na základě společné aktivity více aktérů, v tom případě se hovoří o tzv. společných správcích.

Soudní dvůr ve svých rozsudcích jasně uvedl, že pojmy „správce“ nebo „společní správci“ je třeba vykládat široce, aby bylo dosaženo „účinné a úplné ochrany subjektů údajů“[92]. Za správce tak musí být považován i provozovatel internetového vyhledávače[93]. Za tzv. společného správce musí být považován správce fanouškovské stránky (administrátor) na Facebooku spolu s Facebookem (dnes společnost Meta)[94], provozovatel internetových stránek,

[90] WP29. *Stanovisko č. 1/2010 (WP169) k pojmům „správce“ a „zpracovatel“*, přijaté dne 16. února 2010, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_cs.pdf.

[91] EDPB. *Pokyny 07/2020 k pojmům správce a zpracovatele v GDPR*. Verze 2.0. Přijato dne 7. července 2021, dostupné zde: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_cs.pdf.

[92] Rozsudek ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317, bod 34. Rozsudek ze dne 5. června 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, bod 28. Rozsudek ze dne 29. července 2019, Fashion ID, C-40/17, EU:C:2019:629, bod 66.

[93] Rozsudek ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317, bod 33.

[94] Rozsudek ze dne 5. června 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, body 34 až 37.

který začlení do uvedených stránek sociální modul společnosti Facebook spolu s Facebookem[95], nebo náboženská společnost Svědci Jehovovi společně s jednotlivými členy náboženské společnosti[96].

Dalším důležitým subjektem, kterého správce může, ale nemusí pro své zpracování využít, je „zpracovatel“. Zpracovatel je definován v čl. 4 bodu 8 nařízení jako subjekt, který zpracovává osobní údaje pro správce[97]. Stejně jako u definice správce, předpokládá i definice zpracovatele širokou škálu účastníků, může jím být fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt.[98] Základními pojmovými znaky zpracovatele jsou: a) je samostatným subjektem ve vztahu ke správci a b) osobní údaje jsou zpracovávány pro správce, resp. jménem správce[99]. Role zpracovatele je tedy neoddělitelně spjata s rolí správce, neboť jeho činnost je vlastně výsledkem delegování nebo outsourcingu úkolů stanovených správcem. Zpracovatel je zároveň vždy subjektem, který je právně oddělen od správce, nejedná se tedy o vztah mezi zaměstnavatelem a jeho zaměstnancem[100]. Platí proto, že např. personální oddělení firmy (HR) při vedení personální nebo mzdové agendy není zpracovatelem, pokud by ale firma využívala služeb externí společnosti, která by měla na starosti mzdové účetnictví, tak by tento externí dodavatel byl zpracovatelem. Činnosti svěřené zpracovateli mohou být omezené na konkrétní úkol nebo kontext nebo mohou být poměrně obecné a komplexní. Zpracovatel tedy v zásadě musí plnit pokyny správce, nemůže samostatně rozhodovat o účelu zpracování ani podstatných prostředcích tohoto zpracování. V případě, že zpracovatel překročí rámec pokynů správce a začne určovat své vlastní účely nebo podstatné prostředky zpracování, bude považován v souvislosti s tímto zpracováním za správce (čl. 28 odst. 10 nařízení).

Technologický vývoj zvýšil význam postavení zpracovatele. Význam tohoto postavení vzrostl s účinností nařízení GDPR, které zpracovatelům ukládá rozsáhlejší povinnosti. Na zpracovatele se tak vztahuje povinnost zabezpečení osobních údajů, dále povinnost spolupráce

---

[95] Rozsudek ze dne 29. července 2019, Fashion ID, C-40/17, EU:C:2019:629, body 80 a 81.
[96] Rozsudek ze dne 10 července 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, bod 73.
[97] Původně se předpokládal český překlad anglického „on behalf of the controller“ jako „jménem správce“, nakonec byl ale zvolen překlad „pro správce“.
[98] WP29. *Stanovisko č. 1/2010 (WP169) k pojmům „správce“ a „zpracovatel“*, přijaté dne 16. února 2010, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_cs.pdf.
[99] EDPB. *Pokyny 07/2020 k pojmům správce a zpracovatele v GDPR*. Verze 2.0. Přijato dne 7. července 2021, dostupné zde: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_cs.pdf.
[100] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

s dozorovým úřadem, povinnost v určených případech jmenovat pověřence pro ochranu osobních údajů, povinnost vést záznamy o všech kategoriích činností zpracování prováděných pro správce.[101] Vztah mezi správcem a zpracovatelem je definován v článcích 28 a 29 nařízení GDPR. Tento vztah se musí řídit smlouvou (tzv. zpracovatelská smlouva) nebo jiným právním aktem, který má písemnou formu, a to i v elektronické podobě, a je závazný. Právě typicky zpracovatelská smlouva je instrumentem, který by měl obsahovat podrobný popis pověření zpracovatele. Rozklíčovat postavení správce a zpracovatele je mnohdy velmi nesnadným úkolem, avšak stěžejním pro správné nastavení odpovědnostního vztahu, a tím i celé ochrany osobních údajů.

2.4 Zásady zpracování

Článek 5 nařízení GDPR stanoví v odstavci 1 a 2 všechny klíčové základní zásady zpracování, které jsou základem ochrany osobních údajů: zákonnost, korektnost a transparentnost (a), účelové omezení (b), minimalizace údajů (c), přesnost (d), omezení uložení (e), integrita a důvěrnost (f) a odpovědnost (g). Jsou to základní stavební kameny, na nichž je celé nařízení postaveno. Od těchto zásad se odvíjí veškeré zpracování osobních údajů, a správce s nimi musí být v souladu a zároveň být schopen kdykoli tento soulad doložit. S těmito zásadami jsou provázána také další ustanovení nařízení GDPR. Dá se říci, že jejich hlavní funkcí je interpretační funkce při výkladu nařízení GDPR. Tyto zásady se ovšem uplatní i při výkladu dalších právních předpisů, které se aplikují při zpracování osobních údajů. Většina z těchto zásad byla jako jednotlivé povinnosti vyjádřena i ve dřívější směrnici 95/46[102], až na dvě výjimky. Nařízení GDPR v porovnání se směrnicí nově zmiňuje jako jednu ze zásad zpracování zásadu integrity a důvěrnosti. Stejně tak je nově výslovně formulována zásada odpovědnosti (správce) v článku 5 odst. 2 nařízení GDPR. Dřívější směrnice nicméně obecně uváděla, že správce je povinen zajistit, aby byl dodržován článek 6 odstavec 1. V následujících odstavcích jen velmi stručně shrnu tyto základní zásady, neboť účelem této práce není komentářovým způsobem rozsáhle popisovat jednotlivé pojmy a zásady nařízení GDPR.

V článku 5 odst. 1 písm. a) jsou společně formulovány tři zásady: zákonnost (legalita), korektnost (též poctivost nebo férovost) a transparentnost (též průhlednost). Zákonnost představuje patrně nejdůležitější zásadu ochrany osobních údajů. Tato zásada stanoví, že

[101] ŽŮREK, JUDr. Jiří. *Praktický průvodce GDPR (včetně rozhodovací praxe ÚOOÚ)* [online]. 2021 [cit. 2024-04-14].
[102] Zásady zpracování byly nazvány jako zásady pro kvalitu údajů a upraveny v článku 6 směrnice.

zpracování musí vždy probíhat na základě alespoň jednoho z právních titulů vyjmenovaných v čl. 6 odst. 1 nařízení GDPR[103]. Tatáž zásada také stanoví, že zpracování nesmí být protiprávní, protiprávnost není myšlena jen jako rozpor s nařízením GDPR, ale rozpor s právním řádem obecně.[104] Podle Agentury Evropské unie pro základní práva (FRA) a Rady Evropy je třeba zásadu zákonného zpracování chápat také s odkazem na podmínky zákonného omezení práva na ochranu údajů nebo práva na respektování soukromého života s ohledem na čl. 52 odst. 1 Listiny základních práv Evropské unie a čl. 8 odst. 2 Evropské úmluvy o lidských právech. Korektnost bývá jako zásada chápána velmi obecně a mnoho autorů ji zaměňuje za zásadu transparentnosti[105]. Ačkoli jsou si zásady velmi podobné, tak se nejedná o tutéž zásadu. Korektnost by měla být dle zákonodárce vykládána obecně jako poctivost, tj. takový postup správce, který dodržuje dobré mravy, někdy je dávána do souvislosti s etikou zpracování osobních údajů. Správce tedy nezískává osobní údaje nekalými prostředky, podvodem nebo bez vědomí subjektu údajů a zohledňuje rozumná očekávání subjektů údajů. Transparentnost vyjadřuje povinnost otevřenosti vůči subjektu údajů a je vysvětlena v recitálu 39 nařízení GDPR. Zde se píše, že subjekty údajů by měly vědět, v jakém rozsahu jsou či budou jejich osobní údaje zpracovány. Tyto správcem poskytnuté informace by zároveň měly být snadno dostupné a srozumitelné. V praktické rovině se transparentnost realizuje především v informační povinnosti správce (články 12 až 14) a v odpovědi správce na subjektem údajů uplatněné právo na přístup (článek 15).

Porušení některé ze zásad zákonnosti, korektnosti a transparentnosti, příp. více těchto zásad, patří mezi nejčastěji konstatovaná porušení ze strany ÚOOÚ v rámci správních řízení. Úřad vedl správní řízení se společností, která v souvislosti s pronájmem motorových vozidel neposkytla subjektům údajů informace o zpracování osobních údajů prostřednictvím GPS lokátorů, které byly umístěny ve vozidlech, jakož ani informace o totožnosti a kontaktních údajích správce, účelu zpracování, pro který jsou osobní údaje určeny, a právním základu zpracování, o tom, že zpracování je nezbytné pro účely oprávněných zájmů správce nebo třetí strany, dále neposkytla informace ani o příjemci nebo kategorii příjemců osobních údajů, době uložení osobních údajů, právech subjektů údajů, ani informace o tom, zda je poskytnutí

[103] V případě zvláštní kategorie údajů (tzv. citlivých údajů), musí být dán kumulativně i právní titul neboli důvod uvedený v článku 9 odst. 2 nařízení GDPR.
[104] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.
[105] Dřívější směrnice 95/46 rozlišovala pouze zásadu zákonnosti a korektnosti, transparentnost chápala právě jako součást zásady korektnosti.

osobních údajů zákonným nebo smluvním požadavkem nebo požadavkem, který má být obsažen ve smlouvě, zda je subjekt údajů povinen osobní údaje poskytnout a o možných důsledcích neposkytnutí údajů, čímž byla porušena zásada zpracování osobních údajů stanovená v čl. 5 odst. 1 písm. a) nařízení 679/2016 (transparentnost). Úřad v tomto případě uložil pokutu ve výši 30 000 Kč.[106]

Zásada účelového omezení je další stěžejní zásadou, upravena je v článku 5 odst. 1 písm. b) nařízení GDPR. U každého zpracování totiž musí správce v první řadě určit účel a právní titul (neboli právní základ) – vymezí tak rozsah zpracování. Tato zásada vyžaduje, aby údaje byly shromažďovány pro určité, výslovně vyjádřené a legitimní účely (požadavek „specifikace účelu“) a aby nebyly dále zpracovávány způsobem, který je s těmito účely neslučitelný (požadavek „slučitelného použití“). Účely zpracování osobních údajů by měly být správcem stanoveny od samého počátku, nejlépe ještě před zahájením zpracování, nejpozději však v okamžiku shromažďování osobních údajů. Dojde-li ke splnění účelu zpracování, je povinností správce údaje zlikvidovat. Existují však výjimky, kdy je možné tzv. další zpracování. Dle tohoto ustanovení se jedná o zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Musí být nicméně současně splněny podmínky obsažené v čl. 89 odst. 1 nařízení GDPR.

Zásada minimalizace údajů úzce souvisí s předchozí zásadou účelového omezení. Je upravena v článku 5 odst. 1 písm. c) nařízení GDPR. Tato zásada znamená, že zpracovávané osobní údaje musí být přiměřené, relevantní a omezené na to, co je nezbytné vzhledem k účelům, pro které jsou zpracovávány. Tato zásada tedy obsahuje požadavek přiměřenosti (proporcionality), požadavek relevance a požadavek „omezení na nezbytnou míru“. Posledně uvedený požadavek se neposuzuje pouze ve vztahu k množství (kvantitě) údajů, ale také ve vztahu ke kvalitě údajů. Nejenže tak správce nesmí zpracovávat nadměrně velké množství údajů, nesmí ani zpracovávat takové osobní údaje, pokud by to znamenalo nepřiměřený zásah do práv a zájmů subjektu údajů.[107]

Další zásadou je zásada přesnosti, upravená v článku 5 odst. 1 písm. d) nařízení GDPR. Podle ní musí být osobní údaje zpracovávány v přesné podobě a v případě potřeby

[106] ŽŮREK, JUDr. Jiří. *Praktický průvodce GDPR (včetně rozhodovací praxe ÚOOÚ)* [online]. 2021 [cit. 2024-04-14]. ÚOOÚ. Anonymizovaný příkaz ÚOOÚ (UOOU-00178/19-3). Online. Dostupný z: https://uoou.gov.cz/media/poskytnute-informace/2019/3152019/uoou-0017819-3.pdf. [online]. 2019 [cit. 2024-04-14].

[107] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

aktualizované. Všechny nepřesné údaje by tak měly být opraveny nebo vymazány. Správce musí současně přijmout veškerá rozumná opatření, aby zajistil dodržování této zásady. Zásada přesnosti se prakticky projevuje v článku 16 nařízení (právo subjektu údajů na opravu jeho osobních údajů) a v článku 18 (právo subjektu údajů požadovat po správci omezení zpracování údajů v případě, kdy popírá jejich přesnost).

Následuje zásada omezení uložení, kterou obsahuje čl. 5 odst. 1 písm. e) nařízení GDPR. Tato zásada vlastně úzce souvisí se zásadou minimalizace údajů. Zatímco zásada minimalizace zdůrazňuje nezbytnost z hlediska rozsahu zpracovávaných údajů, zásada omezení uložení zdůrazňuje takovou nezbytnost z časového hlediska.[108] Tato zásada umožňuje zpracovávat osobní údaje ve formě, která umožňuje identifikaci subjektů údajů pouze po dobu nezbytnou k dosažení účelů zpracování. Jinými slovy, osobní údaje musí být správcem smazány nebo anonymizovány, jakmile již nejsou zapotřebí pro účely, ke kterým byly shromážděny. Základním kritériem je tedy účel zpracování. Uvedené ustanovení doplňuje recitál 39, který správce vyzývá, aby stanovil lhůty pro výmaz nebo pravidelný přezkum.

Zásada integrity a důvěrnosti neboli též zásada zabezpečení údajů stanoví, že osobní údaje musejí být zpracovány způsobem, který zajistí jejich náležité zabezpečení před neoprávněným či protiprávním zpracováním a zároveň před náhodnou ztrátou, zničením nebo poškozením, a to za použití vhodných technických nebo organizačních opatření. Jedná se o zásadu upravenou v čl. 5 odst. 1 písm. f) nařízení GDPR. Tato zásada v ustanovení upravující zásady v dřívější směrnici 95/46 chyběla, nicméně bezpečnost zpracování jako taková byla upravena i dříve, a to v článku 17 této směrnice. Tuto povinnost zabezpečení rozvíjí celý oddíl 2 kapitoly IV nařízení GDPR věnovaný správcům a zpracovatelům. Nařízení GDPR nově upravuje požadavek ohlašovat (oznamovat) porušení zabezpečení osobních údajů dozorovému úřadu a v určitých případech také subjektům údajů.

V článku 5 odst. 2 nařízení GDPR je také nově výslovně uvedena zásada odpovědnosti (správce). Seznam základních zásad zpracování tak končí prohlášením, že správce odpovídá za dodržování všech předchozích zásad. Oproti směrnici 95/46 se zavádí nový prvek: správce musí být nyní schopen prokázat, že zpracování je v souladu s těmito právními pravidly.[109] Zásada

[108] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 275-322. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].
[109] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

odpovědnosti je pak dále rozvedena v článku 24 nařízení GDPR. Správce tak musí přijmout příslušná opatření, která odpovídají míře rizika, které dané zpracování představuje. Zásada odpovědnosti posiluje porozumění a praktický závazek správce k ochraně údajů, neboť bude muset zavést vhodná technická a organizační opatření před zahájením operací zpracování, aby se zabránilo porušování nařízení GDPR. Vhodná opatření zahrnují přijetí interních zásad, používání škálovatelných programů k provádění zásad ochrany údajů a další opatření, která splňují zejména zásady záměrné a standardní ochrany osobních údajů.[110]

Základní zásady zpracování osobních údajů stanovené v nařízení GDPR jsou tedy vlastně pilíře celé ochrany osobních údajů. Tyto zásady tvoří základní rámec pro správné a zákonné nakládání s osobními údaji. Každý správce a zpracovatel musí tyto zásady dodržovat při jakémkoli zpracování osobních údajů. Tyto základní zásady zajišťují, že zpracování osobních údajů je prováděno eticky, zákonně a s maximální ochranou práv subjektů údajů. Dodržování těchto zásad je klíčové pro důvěru mezi subjekty údajů a organizacemi, které jejich údaje zpracovávají.

[110] VOIGT, Paul a VON DEM BUSSCHE, Axel, 2017. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, s. 180-187. Online. ISBN 978-3-319-57959-7. Dostupné z: https://doi.org/10.1007/978-3-319-57959-7. [cit. 2024-09-04].

3. Práva subjektů údajů

Významnou součástí nařízení GDPR jsou práva subjektů údajů. Účinnost právních předpisů obecně, a zejména práv subjektů údajů, závisí do značné míry na existenci vhodných mechanismů pro jejich vymáhání. V současné době, kdy je světová ekonomika založená na datech, se stává zpracování osobních údajů všudypřítomným a pro jednotlivce stále obtížněji pochopitelným jevem. Nařízení GDPR oproti předchozí právní úpravě zmírnilo nerovnováhu sil mezi subjekty údajů a správci, jednotlivci (subjekty údajů) získali určitá práva, která jim umožňují větší kontrolu nad zpracováním jejich osobních údajů.[111] Klíčovým pojmem v souvislosti s právy subjektů údajů je tedy kontrola. Helena U. Vrabec hovoří ve své monografii k *Právům subjektů údajů podle GDPR* o tom, že nařízení GDPR je ve své podstatě binární právní předpis, který obsahuje pravidla dvojího druhu: ustanovení se týkají buď kontroly nad osobními údaji, nebo ochrany osobních údajů. Zatímco první skupina ustanovení se týká jednotlivců (subjektů údajů) a posiluje jejich kontrolu nad osobními údaji, tak druhá skupina ustanovení je zaměřena na držitele údajů (zejména správce) a ukládá jim povinnost chránit osobní údaje. Cílem nařízení je pak omezit moc správců údajů tím, že jim ukládá povinnosti ochrany a vychyluje rovnováhu ve prospěch individuální kontroly jednotlivců, která vychází z osobní autonomie a dalších hodnot.[112]

V právním řádu EU má zásadní význam Listina základních práv EU, která představuje primární právo EU a která v čl. 8 odst. 2 zakotvuje právo na přístup k vlastním údajům a právo na opravu údajů. Sekundární právo EU – zejména nařízení GDPR – poměrně strukturovaným přístupem rozděluje práva do různých skupin, počínaje požadavky na transparentnost a právem na informace (články 12 až 14 nařízení GDPR), přes právo na přístup k údajům (článek 15 nařízení GDPR), právo na opravu údajů (článek 16 nařízení GDPR) a jejich výmaz (článek 17 nařízení GDPR), dále přes právo na omezení zpracování (článek 18 nařízení GDPR), až po (zcela nové) právo na přenositelnost údajů (článek 20 nařízení GDPR). Práva subjektů údajů ještě doplňují právo na námitku (článek 21 nařízení GDPR) a právo nebýt předmětem automatizovaného individuálního rozhodování (článek 22 nařízení GDPR). Tato systematika je logicky a prakticky navržena tak, aby zajistila, že jednotlivé kroky, které může subjekt údajů podniknout v souvislosti s ochranou svých osobních údajů, jsou prezentovány v pořadí, které

[111] FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2024-04-07]
[112] VRABEC, Helena U., 2021. 3.3 Control and EU data protection law. In: *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*. Oxford University Press, s. 59-63. Online. ISBN 9780191904851. Dostupné z: https://doi.org/https://doi.org/10.1093/oso/9780198868422.001.0001. [cit. 2024-04-14].

odpovídá jejich obvyklému využití a funkčnímu propojení. Začíná se základním právem na přístup, které má zásadní význam pro využití dalších práv, a pokračuje právy zaměřenými na opravu, výmaz, omezení zpracování, přenositelnost, až po specifická práva, jako je právo vznést námitku a právo nebýt předmětem automatizovaného rozhodování.

3.1 Obecné požadavky na transparentnost

Rozvinutí zásady transparentnosti v procesní rovině představuje článek 12 nařízení GDPR. Jeho účelem je sjednotit technické a procesní aspekty výkonu různých práv subjektu údajů na informace, včetně práva na přístup. Záměrem je posílit právní jistotu všech zúčastněných aktérů, a zejména pak právní jistotu subjektu údajů, včetně jeho postavení. Vzhledem k tomu, že ustanovení klade požadavky na správce, jakým způsobem komunikovat se subjektem údajů, tak subjektu údajů umožňuje snadněji pochopit obsah jeho práv, a tím pádem činit informovaná rozhodnutí. Konkrétní rozsah informací, které je třeba subjektu údajů poskytnout, upravují následující články 13 a 14 nařízení GDPR. Forma komunikace je pak upravena právě tímto ustanovením, které svojí strukturou patří mezi delší ustanovení nařízení. Požaduje se stručnost, transparentnost, srozumitelnost, snadno přístupný způsob, jasné a jednoduché jazykové prostředky, které lze souhrnně označit jako prvky transparentnosti. Mezi další prvky transparentnosti patří bezplatnost; povinnost poskytnout informace písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Posledně uvedený prvek je modifikován možností, že pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně.

Interpretace prvků transparentnosti může být v mnoha případech komplikovaná a nejasná, jistá výkladová vodítka poskytla tzv. pracovní skupina zřízená podle článku 29 (WP29), a to v Pokynech k transparentnosti podle nařízení 2016/679.[113] Stručnost zejména znamená, že by správce měl předcházet tzv. jevu zahlcení subjektu údajů informacemi. Doporučuje se proto využívat vícevrstvá prohlášení, resp. oznámení o ochraně soukromí. Další doporučení ke stručnosti jsou zejména členění textu, příp. vhodná vizualizace (např. různé ikony, loga nebo jiné grafické prvky), využívání metody otázky a odpovědi nebo využívání hypertextových odkazů. I tak může být požadavek na stručnost někdy poměrně náročným úkolem, např. v případě správců, kteří mají složitě strukturované a vzájemně propojené soubory

[113] WP29. *Pokyny k transparentnosti WP 260 rev.01*, přijaté dne 29. listopadu 2017 naposledy revidované a přijaté dne 11. dubna 2018. Strany 6–13. Dostupné z: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_cs.pdf.

údajů původně určené pro strojové čtení. Srozumitelnost je třeba chápat ve vztahu k cílové skupině, jiné požadavky budou u pracujících odborníků, jiné u dětí. Nařízení GDPR totiž na mnoha místech zdůrazňuje zvláštní zvýšenou ochranu nezletilých dětí vzhledem k jejich omezené schopnosti uvědomovat si rizika. Prvek snadné přístupnosti znamená, že nelze po subjektu údajů chtít, aby si musel tyto informace složitě dohledávat. Pokud jde o jasné a jednoduché jazykové prostředky, správci by měli nastavit zásady ochrany údajů, které jsou z jazykového hlediska uživatelsky přívětivé. Základní úvahou, která by měla provázet nastavení politiky ochrany údajů ze strany správce, je, že subjekt údajů by měl být schopen předem rozpoznat rozsah a důsledky zpracování a neměl by být následně zaskočen tím, jak jsou jeho osobní údaje používány.

V článku 12 je kromě výše zmíněných prvků transparentnosti upravena i otázka ověření totožnosti subjektů údajů při uplatnění práva, bezplatnost výkonu práv (a výjimky z ní) a také lhůty na odpověď správce. Obecně je také řečeno, že správce musí napomáhat, resp. usnadňovat uplatnění práv subjektů údajů (čl. 12 odst. 2).

3.2 Právo subjektu údajů být informován

Jak již bylo uvedeno výše, články 13 a 14 nařízení GDPR dále rozvádějí článek 12, a to tím, že konkrétně upravují soubor informací, které je třeba subjektu údajů poskytnout. Je v nich podrobně upravena informační povinnost správce v případě, že jsou osobní údaje získávány přímo od subjektu údajů (článek 13), a v případě, že osobní údaje nebyly získány od subjektu údajů, ale nejčastěji od třetí osoby (článek 14). Vzhledem ke složitosti a podrobné úpravě těchto článků se pokusím pouze zestručnit některé nejdůležitější body, které mají význam pro tuto práci. V podrobnostech lze určitě opět odkázat na Pokyny skupiny WP29 k transparentnosti podle nařízení 2016/679[114]. Základním rozdílem v porovnání s právem na přístup podle článku 15, který je předmětem zkoumání této práce, je, že články 13 a 14 se de facto týkají pasivního práva subjektu údajů. Jinými slovy, od subjektu údajů se zde nic neočekává, naopak u správce jde o aktivní povinnost, tuto informační povinnost musí plnit automaticky, a nikoliv až na požádání[115], a to s náležitou péčí. Tyto informace jsou obvykle obsaženy v oznámení, prohlášení nebo zásadách o ochraně osobních údajů (anglicky též nazýváno *privacy policy*).

[114] Tamtéž. Strany 14–33.
[115] ŽŮREK, JUDr. Jiří. *Praktický průvodce GDPR (včetně rozhodovací praxe ÚOOÚ)* [online]. 2021 [cit. 2024-04-14].

Článek 13 míří na situace, kdy jsou osobní údaje získávány přímo od subjektu údajů, jedná se tzv. o osobní údaje získané přímo. Poskytnutí informační povinnosti je vázáno na okamžik získání, resp. shromáždění údajů, což může být okamžik vyplnění formuláře nebo návrhu smlouvy, nikoli okamžik, kdy dojde akceptace zpět do sféry správce. Ustanovení se skládá celkem ze čtyř odstavců, přičemž první dva se týkají konkrétního rozsahu informací. Zatímco první odstavec upravuje informace, které musí správce poskytnout vždy (de facto informační minimum), tak druhý odstavec upravuje informace, které musí správce poskytnout, pokud je to nezbytné pro zajištění spravedlivého a transparentního zpracování. Pod odstavec 1 spadá: totožnost a kontaktní údaje správce, včetně kontaktních údajů případného pověřence pro ochranu osobních údajů (a) a b)); účely zpracování a právní základ pro zpracování (c)); oprávněný zájem správce, v případě, že je tento zájem základem pro zpracování (d)); informace o konečných příjemcích nebo kategorii příjemců osobních údajů (e)); případný úmysl správce předat osobní údaje do třetí země a právní podklad, na základě kterého dojde k předání (f)).

Podle odstavce 2 je pak správce povinen za výše uvedených okolností poskytnout navíc informace, mezi které patří: doba, po kterou budou osobní údaje uchovávány (a)); existence práv subjektu údajů (b)); právo kdykoli odvolat souhlas, pokud je zpracování založeno na souhlasu nebo výslovném souhlasu (c)); právo podat stížnost u dozorového úřadu (d)); zda je poskytnutí osobních údajů povinné, a pokud ano, jaké jsou důsledky jejich neposkytnutí (e)); existence automatizovaného rozhodování, včetně profilování (f)). Článek 13 odst. 3 výslovně upravuje situace, kdy správce hodlá osobní údaje dále zpracovat pro jiný účel, než pro který byly získány. Toto ustanovení se týká pouze zpracování údajů pro tzv. slučitelné účely. S tím se pojí povinnost správce aktualizovat oznámení subjektu údajů tak, aby obsahovalo informace o novém účelu. Článek 13 odst. 4 pak upravuje výjimku – jde o situace, kdy subjekt údajů již takovými informacemi disponuje. To znamená, že pokud tyto informace má a do té míry, co jimi disponuje, nemusí být správcem znovu informován. Může se jednat např. o situaci, kdy se uzavírá dodatek ke smlouvě, která sice mění předmět smlouvy, ale podstatné náležitosti zpracování osobních údajů (rozsah, účel, právní základ atd.) se nemění[116]. Zajímavostí a podle mého názoru nelogičností, kterou upravují Pokyny skupiny WP 29 k transparentnosti podle nařízení 2016/679, je okruh situací, které přiřazují pod článek 13. Podle skupiny WP 29 se tak jedná nejen o osobní údaje vědomě poskytnuté subjektem údajů, nýbrž i osobní údaje získané sledováním, např. kamerami, síťovým zařízením, sledováním přes Wi-Fi (k tomu blíže v části

[116] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.

čtvrté). Je totiž také otázkou, zdali v tomto smyslu nejsou uvedené Pokyny v rozporu se stále platným rozsudkem Soudního dvora EU, zvaném *Ryneš*[117]. Uvedený rozsudek se sice blíže nezabýval rozborem vztahu mezi článkem 10 a 11 směrnice 95/46 (de facto obdoba dnešního článku 13 a 14 nařízení), zařadil nicméně informační povinnost týkající se kamerového systému pod článek 11[118].

V článku 14 je zakotvena informační povinnost správce, pokud osobní údaje od subjektu údajů nezískal a získal je tak nepřímo. Osobní údaje tak mohou být získány z těchto zdrojů: od jiných správců údajů; z veřejně dostupných zdrojů; od zprostředkovatelů údajů nebo od jiných subjektů údajů. Struktura článku 14 je podobná struktuře článku 13 v tom smyslu, že rovněž stanoví dva obecné typy informací, které by měly být subjektu údajů poskytnuty, odpovídá na otázku, kdy by informace měly být poskytnuty, upravuje oznámení o dalším zpracování osobních údajů a řeší konkrétní výjimky z práva na informace (výjimky jsou nicméně podle článku 14 širší). Pokud jde o časový okamžik poskytování informací, je zde stanoveno obecné pravidlo (v čl. 14 odst. 3), že informace by měly být poskytnuty v přiměřené lhůtě po získání osobních údajů, nejpozději však do jednoho měsíce po jejich získání. Ustanovení má celkem pět odstavců. Opět platí, že první odstavec upravuje informace, které musí správce poskytnout vždy, a druhý odstavec zase informace, které musí správce poskytnout, pokud je to nezbytné pro zajištění spravedlivého a transparentního zpracování. Soubor informací, které mají být správcem sděleny, se významně překrývá s informacemi zakotvenými v článku 13 nařízení. Ve skutečnosti musí být všechny údaje požadované podle článku 13 uvedeny také podle článku 14 se třemi výjimkami. Zaprvé, jelikož osobní údaje nejsou shromažďovány přímo od subjektu údajů, vyplývá z toho, že by oznámení nemělo informovat o tom, zda je poskytnutí osobních údajů povinné. Zadruhé, správce je povinen pouze v případě nepřímého získání osobních údajů podle čl. 14 odst. 1 informovat subjekty údajů o tom, jaké kategorie osobních údajů o nich zpracovává. Zde platí, že by měl být popis kategorií dostatečně přesný a ne široký, aby umožnil subjektu údajů získat celkovou představu o zpracování údajů. Například osobní údaj týkající se zdraví bude často považován za příliš široký a neurčitý, vhodnější by bylo určení, že se jedná o údaj týkající se krevního tlaku nebo tělesné teploty apod. A konečně zatřetí pouze u nepřímého získání osobních údajů dle čl. 14 odst. 2 je správce povinen uvést i informace o zdroji osobních údajů, ledaže není možné tak učinit.

[117] Rozsudek ze dne 11. prosince 2014, Ryneš, C-212/13, EU:C:2014:2428, bod 34.
[118] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 450-474. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

3.3 Právo subjektu údajů na přístup k vlastním údajům – obecně

Nařízení GDPR upravuje právo na přístup a další práva subjektu údajů v článcích 15 až 22. Ačkoli tato práva nebyla seřazena podle významu, o primárním postavení práva na přístup v článku 15 nelze pochybovat, je totiž důležité i pro výkon dalších práv subjektu údajů. Systematika práv navíc, jak již bylo uvedeno, sleduje logický postup, jakým mohou být práva subjektů údajů uplatňována. Právo na přístup je neodmyslitelně spjato také s výše analyzovaným právem být informován, které umožňuje subjektu údajů získat „pasivně" celou řadu informací o zpracování. Naproti tomu právo na přístup umožňuje subjektu údajů zaujmout aktivní postoj, obrátit se na správce s žádostí a získat určité množství (spíše konkrétnějších) informací. Jeho účelem je vrátit subjektu údajů kontrolu, dát mu možnost ověřit si zákonnost zpracování prováděného správcem. Na právo na přístup lze pohlížet také jako na individualizovaný důsledek obecné informační povinnosti a povinnosti transparentnosti, které dopadají na správce údajů. V praxi také často slouží jako předpoklad pro pozdější podání stížnosti k dozorovému úřadu nebo pro podání návrhu k soudu, neboť umožňuje jednotlivci buď zjistit informace o zpracování jeho osobních údajů a rozsahu tohoto zpracování, nebo upozornit na riziko neoprávněného zpracování nebo zničení údajů. Právo na přístup je fakticky součástí kontrolního mechanismu, který má zajistit, aby osobní údaje nebyly zpracovávány bez vědomí jednotlivce.[119] Právo na přístup k údajům tedy nejenže předpokládá zapojení jednotlivce, ale také posiluje jeho informační sebeurčení jako projev širšího práva na soukromí, vybízí ke kontrole informačních postupů organizací a pomáhá odhalit potenciální zneužití údajů. A konečně, můžeme jej chápat také jako nástroj, který slouží k narovnání mocenské asymetrie mezi správci a subjekty údajů[120].

3.4 Právo na opravu

Jak již bylo uvedeno výše, články 15 až 22 nařízení upravují práva subjektů údajů, kterými jsou právo na přístup k osobním údajům; právo na opravu nepřesných osobních údajů;

[119] Collectif Dalloz, 2023. *Code de la protection des données personnelles 2024, annoté et commenté,* 1994 s., 6. vydání (z 11/2023). Online. Dalloz. ISBN 978-22-4723-215-4. Dostupné z: databáze Dalloz. [cit. 2024-04-14].

[120] VRABEC, Helena U., 2021. 5 The Right of Access under EU Data Protection Law. In: *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*. Oxford University Press, s. 104-106. Online. ISBN 9780191904851. Dostupné z: https://doi.org/https://doi.org/10.1093/oso/9780198868422.001.0001 [cit. 2024-04-14].

právo na výmaz, též známé jako „právo být zapomenut“; právo na omezení zpracování; právo na přenositelnost osobních údajů; právo vznést námitku proti zpracování osobních údajů a právo subjektu nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování. Většina těchto práv již byla upravena ve směrnici 95/46. Směrnice ovšem upravovala tato práva dohromady v jediném článku, a to článku 12. V tomto ustanovení tedy bylo upraveno právo na přístup, právo na opravu, právo na výmaz a právo na omezení zpracování (dříve ve směrnici označováno jako právo na blokování údajů). Posledně uvedené právo na omezení zpracování lze do jisté míry považovat za nové právo podle nařízení, a to z důvodu, že jeho předchůdce dopadal na užší okruh situací, jak bude blíže vysvětleno níže. Jediným ovšem skutečně novým právem, vzniklým spolu s unijní reformou ochrany osobních údajů, je právo na přenositelnost údajů.

Podle článku 16 nařízení GDPR má subjekt údajů v souladu se zásadou přesnosti, která stanoví, že osobní údaje musí být přesné a v případě potřeby aktualizované, právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje. Charakteristickým rysem práva na opravu je právě jeho provázání k právu na přístup. Jakmile subjekt údajů získá přístup ke svým osobním údajům a zjistí, že jsou nepřesné nebo neúplné s ohledem na účel zpracování, má související právo na opravu nebo doplnění údajů. Někdy se také uvádí, že má právo na opravu ještě druhou složku upravenou v článku 19 nařízení. Tou je oznamovací povinnost správce ohledně opravy nebo výmazu. Znamená to, že správce musí oznámit tyto opravy, doplnění nebo výmazy předchozím příjemcům údajů. Je otázkou, jak přistupovat k této povinnosti, pokud se jedná o zpracování spočívající v šíření nebo zpřístupňování údajů veřejnosti. Je třeba trvat na tom, aby oznámení bylo dosažitelné pro všechny původní příjemce i z řad veřejnosti? To může nastat typicky v situaci, kdy správcem bude například provozovatel internetové stránky Wikipedia, nebo poskytovatel sociální sítě, společnost Meta Platforms. Ustanovení pro tyto případy upravuje výjimku, pokud se oznámení ukáže jako nemožné nebo vyžadující nepřiměřené úsilí. Význam tohoto práva na předání oprav se projevuje v tom, že umožňuje subjektu údajů zastavit nebo alespoň omezit šíření chybných nebo nepravdivých informací.[121]

[121] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

3.5 Právo na výmaz („právo být zapomenut“)

Jedním ze stěžejních práv subjektu údajů je právo na výmaz, nazýváno též právo být zapomenut. Spolu s právem na přístup, jež jsou mimochodem často uplatňována právě spolu, je asi nejvýznamnějším nástrojem kontroly subjektu údajů. Je upraveno v článku 17 nařízení GDPR a jeho význam v poslední době vzrostl, obzvláště v souvislosti s rozvojem internetu, stává se tudíž často předmětem odborné diskuze a také četných zpracování akademických prací a publikací. Ačkoli se o něm často mluví jako o produktu modernizace evropských pravidel ochrany osobních údajů, není přímo novým institutem, jelikož v jednoduché podobě jej obsahovala i směrnice 95/46. Nařízení jej však upravuje v podstatně širší podobě.

Článek 17 obsahuje jak samostatné právo subjektu údajů požádat o výmaz údajů, tak samostatnou povinnost správce výmaz provést, pokud jsou pro něj dány důvody. Důvody, kdy je vyžadován výmaz, jsou uvedeny v odstavci 1 písm. a) až f), zahrnují všechny případy, kdy údaje neměly být zpracovávány nebo v žádném případě již nesmějí být zpracovávány. Údaje musí být vymazány, pokud již nejsou potřebné pro účel, pro který byly shromážděny (a správce by je tedy měl přestat zpracovávat samovolně); pokud fyzická osoba odvolala svůj souhlas a neexistuje žádný jiný právní základ; pokud fyzická osoba úspěšně uplatní své právo vznést námitku; pokud je zpracování údajů samo o sobě protiprávní (zejména z důvodu porušení základních zásad stanovených v článku 5 nařízení GDPR) a pokud je výmaz výslovně vyžadován pozitivním právem. Poslední důvod uvedený v písmenu f) se týká údajů osob, které byly v době shromažďování nezletilé. Konkretizaci tohoto důvodu přináší recitál 65 nařízení. Jedná se zejména o případy, kdy subjekt údajů udělil souhlas v době, kdy byl dítětem a nebyl si plně vědom rizik spojených se zpracováním, a následně chce proto tyto osobní údaje vymazat, zejména na internetu. V případě, že je splněna jedna z podmínek pro výmaz a správce, který osobní údaje zveřejnil, žádosti vyhoví, tak nastává podle čl. 17 odst. 2 pro správce další povinnost s tím související, a to povinnost informovat jiné správce (mateřské společnosti, dceřiné společnosti, obchodní partnery atd.) o výmazu osobních údajů. Správce je tak povinen informovat jiné správce o tom, že je subjekt údajů žádá, aby vymazali veškeré odkazy na dané osobní údaje, jejich kopie či replikace. Účelem tohoto ustanovení je zejména posílit právo být zapomenut v internetovém prostředí.

Právo na výmaz je široké, ale není absolutní. Nařízení upravuje celkem 5 výjimek v čl. 17 odst. 3. Vždy ale platí, že musí být dána nezbytnost k naplnění účelů uvedených v jednotlivých výjimkách, jinak se výjimky neuplatní. Všechny níže uvedené výjimky je nutné vykládat restriktivně, a navíc vždy posuzovat v souladu se základními zásadami, a to zejména

se zásadou minimalizace údajů. První výjimka se týká výkonu práva na svobodu projevu a informace. Jedná se o základní politická lidská práva, v tomto případě se tedy často bude muset provést vážení svobody projevu a práva na informace na straně jedné a ochrany osobních údajů, případně práva na soukromí, na straně druhé. Tato výjimka tedy souvisí s žurnalistickou činností (v širším smyslu slova, nikoli jen s činností profesionálních novinářů), s veřejnými rejstříky, dopadá nicméně i například na činnosti provozovatelů vyhledávače, kteří mají za určitých okolností povinnost odstranit odkazy na údaje. Druhá výjimka pak souvisí s plněním právní povinnosti či plněním úkolu ve veřejném zájmu či při výkonu veřejné moci. Třetí výjimku tvoří zpracování nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví. Začtvrté sem spadá výjimka v podobě zpracování nezbytného pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Poslední výjimkou, na jejímž základě může správce odmítnout výmaz údajů, je nezbytnost pro určení, výkon nebo obhajobu právních nároků. V praxi lze očekávat, že právě tuto výjimku budou správci využívat velmi často, možná nejčastěji. Z mého pohledu je ovšem velmi problematická právě tím, jak obecně je nastavena. Nařízení GDPR tuto výjimku blíže nerozvádí, dokonce ani nelze použít výklad v podobě *soft law*, neboť EDPB k právu na výmaz vydal pouze Pokyny ke kritériím práva být zapomenut v případech internetových vyhledávačů[122] (jako reakci na rozsudek *Google Spain*, ten bude v textu dále rozebrán). Správce by měl nicméně provést důkladnou úvahu a k této výjimce se uchýlit pouze tehdy, prokáže-li skutečně nezbytnost, faktickou potřebu údaje uchovávat. Správce tedy musí prokázat, že nelze určit, vykonat nebo obhájit určitý právní nárok bez zpracování daných údajů. Správce tedy nesmí výjimku používat plošně, automaticky, *pro futuro*. Taktéž z hlediska množství a kategorie údajů platí, že by se výjimka měla vztahovat jen na údaje dokládající zpracování a jeho zákonnost, nikoli na celé či rozsáhlé soubory dat.

Právo na výmaz se hodně rozvinulo především díky soudní judikatuře. Jedním z nejvýznamnějších rozhodnutí je rozsudek Soudního dvora EU ve věci *Google Spain*[123], který se dotýká práva na výmaz v internetovém prostředí a zdůrazňuje roli provozovatele vyhledávače, společnosti Google, jako správce osobních údajů. Pan González se domáhal po společnosti Google, aby jí byla uložena povinnost vymazat či skrýt jeho osobní údaje tak, aby se přestaly objevovat ve výsledcích vyhledávání a přestaly být propojeny s odkazy na

[122] EDPB. *Pokyny č. 5/2019 ke kritériím práva být zapomenut v případech vyhledávačů podle nařízení GDPR*, verze 2.0, přijaté dne 7. července 2020, dostupné zde: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_cs.pdf.

[123] Rozsudek ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317.

internetovém deníku. Soudní dvůr zde jasně rozlišil mezi odpovědností společnosti Google jako provozovatele vyhledávače na jedné straně a odpovědností vydavatele internetových stránek na straně druhé. Bylo konstatováno, že Google skutečně zpracovává osobní údaje a že tak činí na základě právního titulu v podobě oprávněného zájmu. Soud poté následně „vážil" jednotlivé zájmy: komerční zájem Googlu ve spojení s veřejným zájmem celé společnosti na svobodu informací, a oproti tomu zájem daného subjektu údajů v jeho konkrétní situaci. V posouzení došel Soudní dvůr k tomu, že v této konkrétní situaci je zájem pana Gonzáleze skutečně silnější a že osobní údaje musí Google z vyhledávání odstranit. Povinnosti provozovatele vyhledávače byly vyloženy velmi široce: Google tak může být povinen odstranit výsledky ze seznamu, a to i v případě, že zveřejnění informace, na kterou výsledek odkazuje, je samo o sobě zákonné. Činnost vyhledávače podle Soudu totiž hraje „*rozhodující roli v globálním šíření uvedených údajů*". Údaje jsou totiž přístupné všem uživatelům internetu provádějícím vyhledávání na základě jména dotčené osoby, navíc uspořádávání a seskupování informací zveřejněných na internetu do jisté míry usnadňuje uživatelům přístup k těmto informacím, ve výsledku je tedy možné obdržet strukturovaný přehled informací, týkající se této osoby, a sestavit profil dotčené osoby. Druhým významným rozsudkem ve vztahu k právu na výmaz je rozsudek Soudního dvora EU ve věci *Manni*.[124] Význam tohoto rozsudku tkví v tom, že Soud zde nastavil limit práva být zapomenut, a to ve vztahu k veřejným rejstříkům. Soud zde opět provedl vážení jednotlivých proti sobě stojících zájmů ve vztahu k účelu zápisu do obchodního rejstříku. Dospěl k závěru, že nad ochranou osobních údajů zapsaných v rejstříku převažuje zájem na ochraně zájmů třetích osob a zajištění právní jistoty a poctivosti obchodních transakcí, potvrdil tedy veřejný zájem na zachování údajů ve veřejných rejstřících. Na závěr ještě zmíním rozsudek ve věci *GC a další*[125]. Tento rozsudek je užitečný zkoumáním rozsahu práva na výmaz (zde práva na odstranění internetových odkazů) a snahou Soudu konkretizovat odpovědnost provozovatele vyhledávače. Soud zde připomíná, že právo na ochranu osobních údajů musí být posuzováno v souvislosti se svou funkcí ve společnosti, neboť není absolutním právem. Ačkoli mají obecně práva subjektu údajů přednost před ekonomickým zájmem provozovatele vyhledávače a rovněž i uživatelů internetu na svobodu informací, musí se při vážení brát v potaz další faktory: povaha dotčené informace a její citlivost, jakož i zájem veřejnosti mít k této informaci přístup, což se může lišit v závislosti na úloze, kterou má subjekt údajů ve veřejném životě. Provozovatel vyhledávače musí každopádně upravit seznam výsledků vyhledávání tak, aby celkový obraz, který se nabízí uživateli internetu, odrážel současný stav soudního řízení,

[124] Rozsudek ze dne 9. března 2017, Manni, C-398/15, EU:C:2017:197.
[125] Rozsudek ze dne 24. září 2019, GC a další, C-136/17, EU:C:2019:773.

jinými slovy poslední aktuální informace o soudním řízení ve věci musí být uvedeny na prvním místě.

3.6 Právo na omezení zpracování

Právo na omezení zpracování je fakticky staronovým právem nařízení GDPR, upraveným v článku 18 nařízení. Většinou se na něj jako na nové právo nepohlíží, protože existovalo ve směrnici 95/46 pod názvem právo na blokování údajů. Důvodem, proč by se na něj možná jako na nové právo pohlížet mělo, je srovnání zákonné úpravy práva na blokování údajů s úpravou práva na omezení zpracování v nařízení, neboť zjistíme, že toto právo ve své původní podobě mělo mnohem menší rozsah a uplatnění. Právo na blokování údajů bylo blíže rozvedeno v tehdejším § 21 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů. O toto právo mohl požádat pouze subjekt údajů, pokud zjistil nebo se domníval, že jsou jeho osobní údaje zpracovány v rozporu se zákonem nebo v rozporu s ochranou jeho soukromého a osobního života, a to zejména jestliže jsou jeho osobní údaje zpracovány nepřesně. Okruh případů, ve kterých je správce na žádost subjektu údajů povinen zpracování osobních údajů omezit podle nynější úpravy, je tedy podstatně širší.[126]

Co se rozumí omezením zpracování je upraveno v samotném definičním ustanovení, v čl. 4 bodu 3 nařízení, to ale není samo o sobě velmi přínosné.[127] V praxi je toto právo jakousi pojistkou nebo ochrannou doložkou, která za určitých okolností umožňuje omezit rozsah zpracování údajů. Rozlišujeme dva hlavní scénáře: buď je právo na omezení zpracování zamýšleno jako dočasné opatření, aby poskytlo subjektu údajů čas na uplatnění a vyhovění nebo nevyhovění práv (právo vznést námitku, právo na opravu údajů, právo podat žalobu), nebo umožňuje subjektu údajů, který čelí protiprávnímu zpracování, omezit rozsah a povahu zpracování. Subjekt údajů, jehož údaje byly zpracovány protiprávně, totiž může, má-li na tom zájem, požádat o zachování výhody „částečného“ zpracování svých údajů. Z praktického hlediska lze právo na omezení zpracování analyzovat jako právo na omezené uložení údajů, aniž by se s nimi jakkoli nakládalo, nebo jinými slovy právo na jejich „zmrazení“, zejména na

[126] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.

[127] „*Omezením zpracování“ [se rozumí] označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu.*

dobu potřebnou k určení, zda osoba má či nemá právo uplatnit svá práva.[128] Základním výslovně upraveným způsobem zpracování údajů po dobu omezení zpracování je tedy jejich uložení. Otázka, zdali by sem bylo možné zařadit i omezení zpracování, které nebude spočívat v pouhém uložení údajů (například nahlédnutí, ale bez obchodního využití údajů; obchodní využití, ale bez předání údajů atd.), zatím zůstává nejasná a bude muset být vyřešena soudní praxí. Jistý návod pro správce, pokud jde o způsoby, jak omezit zpracování osobních údajů, poskytuje recitál 67 nařízení. Zde se píše, že sem může spadat například přesun vybraných údajů do jiného systému zpracování, znepřístupnění údajů uživatelům nebo dočasné odstranění osobních údajů.

Zákonné důvody pro omezení zpracování jsou uvedeny v čl. 18 odst. 1 nařízení. Patří sem situace, kdy je subjektem popírána přesnost osobních údajů (a), zpracování je protiprávní a subjekt namísto o výmaz osobních údajů žádá o omezení jejich použití (b), subjekt chce údaje uchovat pro výkon nebo obhajobu svých právních nároků (c), subjekt vznesl námitku a dosud nebylo přijato rozhodnutí o tom, zda oprávněné důvody správce údajů převažují nad důvody subjektu údajů (d). Závěrem lze říci, že toto právo může být uplatněno jak v zájmu správce (pokud například chce prokázat, že existuje oprávněný důvod pro zpracování), tak v zájmu subjektu údajů (ostatní případy – povinnost správce uchovávat pro subjekt údajů důkazy o případném porušení). Otázkou protiprávnosti u omezení zpracování se zabývá rozsudek Soudního dvora EU ve věci *Bundesrepublik Deutschland*.[129] Soudní dvůr zde rozhodl, že nesplnění povinností stanovených v článcích 26 a 30 nařízení, které se týkají uzavření ujednání o vymezení společné odpovědnosti za zpracování a vedení záznamů o činnostech zpracování, ze strany správce nepředstavuje protiprávní zpracování, které přiznává subjektu údajů právo na výmaz nebo omezení zpracování [podle čl. 18 odst. 1 písm. b)], jelikož takové porušení samo o sobě neznamená, že správce porušil zásadu „odpovědnosti“.

3.7 Právo na přenositelnost údajů

Zcela novým a moderním institutem, právem subjektu údajů, je právo na přenositelnost údajů (též nazýváno jako právo na portabilitu), obsažené v článku 20 nařízení GDPR. Právě v něm se koncentruje snaha evropského zákonodárce vrátit v 21. století jednotlivcům kontrolu nad jejich osobními údaji. Právo na přenositelnost údajů bývá také někdy chápáno jako de facto

[128] Collectif Dalloz, 2023. *Code de la protection des données personnelles 2024, annoté et commenté,* 1994 s., 6. vydání (z 11/2023). Online. Dalloz. ISBN 978-22-4723-215-4. Dostupné z: databáze Dalloz. [cit. 2024-04-14].
[129] Rozsudek ze dne 4. května 2023, Bundesrepublik Deutschland, C-60/22, EU:C:2023:373.

rozšíření práva na přístup[130], neboť umožňuje jednotlivci získat zpět údaje shromážděné správcem, přenést je třetí straně (resp. novému správci) a znovu je použít ve svůj prospěch. Subjekt může buď požádat o přímé předání mezi správci (původním a novým), s výhradou technické proveditelnosti, nebo si sám převezme kopii údajů a případně zajistí předání konkurenční společnosti.[131] Smyslem tohoto práva, jak je ostatně objasněno i přímo v *Pokynech týkajících se práva na přenositelnost údajů*[132], je podporovat zdravé konkurenční prostředí a rozvíjet hospodářskou soutěž, v konečném důsledku pak i zvyšovat kvalitu služeb. EU od tohoto práva také očekává posílení postavení spotřebitele tím, že mu usnadní přechod mezi různými poskytovateli služeb v oblasti informačních technologií a e-commerce. Subjekt údajů by tak neměl být fakticky nucen zůstávat u jednoho poskytovatele služby, zejména kvůli časové a finanční nákladnosti.

Ani právo na přenositelnost samozřejmě není absolutním právem. Ve srovnání s právem na přístup má také užší rozsah a restriktivně dané podmínky. Toto právo se vztahuje pouze na operace zpracování založené na souhlasu subjektu údajů nebo na smluvním vztahu a zároveň pouze na automatizované operace zpracování. Z toho vyplývá, že tedy zpracování založené na jiném právním základě, např. na oprávněném zájmu správce, které je v digitálním světě běžné a potenciálně patří k těm nejvíce invazivním, toto právo nezakládá. Další podmínkou je, že se toto právo vztahuje pouze na osobní údaje, které se subjektu údajů týkají a zároveň které „poskytl" správci. Z uvedených Pokynů vyplývá, že WP29 preferuje v této otázce poměrně široký výklad. Patří sem tedy údaje aktivně a vědomě poskytnuté subjektem údajů, zejména údaje poskytnuté v rámci online formulářů (např. email, uživatelské jméno, věk atd.), tak údaje generované na základě aktivity subjektu údajů při používání služby nebo zařízení (např. provozní či lokalizační údaje osoby, historie prohlížení webových stránek, vyhledávání nebo nákupy na webu atd.). Naopak, údaje vytvořené přímo správcem, tzv. odvozené údaje (údaje získané profilováním subjektu údajů, údaje získané analýzou chování uživatele – typicky např. údaje o bonitě klienta) mezi tyto předávané údaje nepatří. Tyto údaje totiž tvoří jádro přidané hodnoty správce a často jsou spojeny s algoritmickým zpracováním chráněným profesním

[130] VANBERG, Aysem Diker a ÜNVER, Mehmet Bilal, 2017. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? Online. *European Journal of Law and Technology*. Roč. 2017, č. Vol 8, No 1. Dostupné z: https://www.ejlt.org/index.php/ejlt/article/view/546/726. [cit. 2024-04-14].
[131] Collectif Dalloz, 2023. *Code de la protection des données personnelles 2024, annoté et commenté,* 1994 s., 6. vydání (z 11/2023). Online. Dalloz. ISBN 978-22-4723-215-4. Dostupné z: databáze Dalloz. [cit. 2024-04-14].
[132] WP29. *Pokyny týkající se práva na přenositelnost údajů WP 242 rev.01*, přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017, zejména str. 3 a 4. Dostupné zde: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-tykajici-se-prava-na-prenositelnost-udaju-v-cestine.pdf.

tajemstvím. A konečně, právo na přenositelnost platí pouze za podmínky, že nejsou porušována práva třetích osob. Pokyny tuto podmínku vysvětlují poměrně logicky, aby nezbavovaly právo na přenositelnost reálného užitku, a to tak, že by práva a svobody těchto osob neměla být nepříznivě dotčena. To znamená, že předmětem práva na přenositelnost mohou být osobní údaje subjektu údajů, které zároveň obsahují i osobní údaje třetích osob, za předpokladu, že budou použity ke stejnému účelu. Například, subjekt údajů může požádat o přenos své e-mailové komunikace od jednoho poskytovatele e-mailové služby k jinému, ačkoli obsahuje i e-mailové adresy jiných osob. Nebo subjekt údajů může požádat o přenos telefonních záznamů k jinému telefonnímu operátorovi nebo o přenos informací o bankovním účtu k jiné bance, ačkoli zpravidla obsahují osobní informace dalších osob (údaje o příchozích a odchozích hovorech, historie transakcí na bankovním účtu).

Článek 20 obsahuje i formální požadavek, a sice, aby správce subjektu údajů poskytl údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, tedy takovém, který podporuje opakované použití. Takový formát se může mezi jednotlivými správci lišit (nařízení poskytuje určitá vodítka v recitálu 68), určitě sem ale nepatří formáty, jejichž zpracování s sebou nese vysoké náklady. Mělo by se jednat o běžně používané datové formáty. Skupina WP29 rovněž vyzvala průmyslové subjekty a profesní sdružení, aby používaly interoperabilní normy a formáty. V budoucnu lze pravděpodobně očekávat standardizaci některých datových formátů používaných provozovateli. Problematickým aspektem je, že interoperabilita může být, alespoň podle názoru některých expertů, současně faktorem, který zvyšuje pravděpodobnost porušení zabezpečení osobních údajů.[133] Na závěr je důležité zmínit vztah práva na přenositelnost k ostatním právům subjektu údajů. Uplatnění tohoto práva samo o sobě nemá vliv na ostatní práva. Právo na přenositelnost nevylučuje výkon jiných práv subjektu údajů, včetně práva vznést později námitku, ani není samo o sobě synonymem pro výmaz údajů správcem.

3.8 Právo vznést námitku

Nařízení přiznává subjektu údajů v některých případech možnost vznést tzv. námitku proti zpracování. Toto právo je významným projevem „kontrolní“ povahy unijního právního

[133] GASSER, Urs, 2015. Interoperability in the digital ecosystem. Online. *ITU – 15th Global Symposium for Regulators (GSR15)*. Roč. 2015, s. 33. Dostupné z: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/Discussionpaper_interoperability.pdf. [cit. 2024-04-14].

rámce pro ochranu údajů a jedno z nejsilnějších práv subjektů údajů, je vlastně jakousi vstupní branou pro právo na výmaz. Dopadá typicky na situace, kdy subjekt údajů neměl možnost ovlivnit to, že jsou jeho údaje zpracovány. Patří sem zpracování ve veřejném nebo oprávněném zájmu, zvláštní pravidla pak platí pro zpracování v rámci přímého marketingu nebo za určitých podmínek pro vědecký, historický výzkum či statistické účely. Častěji se setkáme s dělením tohoto práva na: a) obecné právo vznést námitku podle čl. 21 odst. 1 nařízení a b) právo vznést námitku proti přímému marketingu podle čl. 21 odst. 2 nařízení.

Obecné právo vznést námitku na jedné straně umožňuje subjektům údajů vznést námitku proti zpracování osobních údajů, které je zákonné, na základě jejich konkrétní situace – má tedy subjektivní povahu. Existuje bez ohledu na to, zda předmětné zpracování způsobuje subjektu údajů újmu nebo jej nějakým způsobem poškozuje. Situace jednotlivce totiž může odůvodňovat ukončení operace zpracování na žádost subjektu údajů, i když správce provádí zákonné zpracování. Touto situací může být něco, co je pro většinu subjektů údajů nepodstatné, ale pro daný subjekt údajů se ukáže jako kritické. Toto právo tak poskytuje kontextuální a individuální posouzení uplatněné na okolnosti námitky subjektu údajů[134]. Rozsah tohoto práva je však omezen na ty činnosti zpracování, kde je právním základem čl. 6 odst. 1 písm. e) (úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci) nebo f) (oprávněný zájem správce). Pokud je zpracování osobních údajů prováděno na jakémkoli jiném právním základě podle článku 6, toto obecné právo vznést námitku se neuplatní.[135] Toto obecné právo také nevyžaduje, aby subjekt údajů prokázal závažný oprávněný důvod pro vznesení námitky, je totiž na správci, aby odůvodnil závažnou potřebu zpracování a provedl tzv. test vážení zájmů (někdy též nazýváno balanční test). Toto je asi největší rozdíl oproti dřívější úpravě ve směrnici 95/46 (konkrétně v článku 14), a sice, že se obrátilo důkazní břemeno. U subjektu údajů je nyní pouze požadavek, že musí jít o důvody týkající se jeho konkrétní situace. Vlastní posouzení, jestli oprávněný zájem správce převáží nad právy a svobodami subjektů údajů, ale provádí sám správce. Pokud se námitka prokáže jako oprávněná, má správce povinnost tyto údaje „dále nezpracovávat“. V praxi to také znamená, že správce má pak povinnost vymazat osobní údaje „bez zbytečného odkladu“.

[134] VRABEC, Helena U., 2021. 8.3 How the GDPR tackles profiling on the individual level. In: *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*. Oxford University Press, s. 197-212. Online. ISBN 9780191904851. Dostupné z: https://doi.org/https://doi.org/10.1093/oso/9780198868422.001.0001. [cit. 2024-04-14].

[135] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

Právo vznést námitku proti přímému marketingu má v porovnání s obecnou námitkou absolutní účinek. Znamená to, že zde správce žádný test vážení zájmů neprovádí. Důvodem je to, že přímý marketing bývá považován za jeden z nejzávažnějších typů zásahů do soukromí subjektu údajů, zejména pokud je rozšířen o profilování a další techniky cílené reklamy. Jakmile subjekt údajů tento typ námitky vznese, musí správce ihned přestat osobní údaje subjektu údajů pro účely přímého marketingu zpracovávat. Zároveň to ale nutně neznamená, že musí správce všechny údaje automaticky vymazat nebo omezit jejich zpracování – musely by být naplněny podmínky práva na výmaz (článek 17) nebo práva na omezení zpracování (článek 18). Pro účinné uplatnění tohoto práva nejsou stanoveny žádné podmínky, a to ani s ohledem na konkrétní právní základ zpracování, ani s ohledem na existenci zvláštních okolností subjektu údajů. Tomuto typu námitky se také někdy říká zvláštní opt-out režim. Jak uvádí komentářová literatura, doplnění tohoto práva na námitku proti přímému marketingu představuje zvláštní úprava v zákoně č. 480/2004 Sb., o některých službách informační společnosti[136], která představuje v tomto vztahu *lex specialis*.

Podle čl. 21 odst. 6 nařízení má subjekt údajů právo podat námitku i v případě zpracování na základě čl. 89 odst. 1 nařízení, tedy pokud se jedná o zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to z důvodů týkajících se jeho konkrétní situace. Správce poté musí podle kritéria nezbytnosti posuzovat, jestli může daný úkol splnit i jiným způsobem, bez zpracování osobních údajů daného subjektu údajů[137].

Rovněž některé rozsudky Soudního dvora EU se zabývaly právem na námitku, byť zpravidla doplňkově k právu na výmaz. Patří sem zejména již jednou zmíněný rozsudek ve věci *Google Spain*[138]. Soudní dvůr zde k otázce posuzování práva subjektu údajů na námitku proti zpracování osobních údajů a práva na výmaz údajů podle směrnice 95/46 uvedl, že v tomto kontextu konstatování práva subjektu údajů na to, aby informace, která se ho týká, nebyla nadále spojena s jeho jménem prostřednictvím seznamu výsledků, nepředpokládá, že zahrnutí dotčené informace do dotčeného seznamu výsledků vyhledávání subjekt údajů poškozuje. Oprávněností námitky uplatněné subjektem údajů podle čl. 14 směrnice 95/46 se také zabýval Soud ve věci *Manni*[139], tento rozsudek byl také již rozebrán výše.

[136] Jedná se o § 7 uvedeného zákona, upravující šíření obchodních sdělení. Také toto ustanovení zakotvuje možnost opt-outu, a to konkrétně ve vztahu k šíření obchodních sdělení elektronickými prostředky.
[137] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.
[138] Rozsudek ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317.
[139] Rozsudek ze dne 9. března 2017, Manni, C-398/15, EU:C:2017:197.

3.9 Právo nebýt předmětem automatizovaného individuálního rozhodování

Posledním právem subjektu údajů je právo upravené v článku 22 nařízení GDPR, a sice právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Prvním předpokladem je tedy automatizované zpracování údajů, které je zpravidla určeno k vyhodnocení určitých osobních aspektů subjektu údajů. Druhou podmínkou je pak, že má takové zpracování pro subjekt údajů právní nebo obdobně významné účinky. Nařízení tedy nechrání subjekty údajů pouze proti právním důsledkům, ale také proti neprávním důsledkům, které ale mají pro ně významný dopad. Pokud je pravděpodobné, že tato rozhodnutí budou mít významný dopad na životy jednotlivců, jichž se týkají, například na jejich úvěruschopnost, elektronický nábor, pracovní výkon nebo analýzu chování či spolehlivosti, pak je nezbytná zvláštní ochrana, aby se předešlo negativním důsledkům. Ustanovení článku 22 lze chápat dvěma různými způsoby: buď jako právo, které může subjekt údajů uplatnit, nebo jako zákaz pro správce údajů.

Podle směrnice 95/46, která obsahovala podobné ustanovení v článku 15, se názory dozorových orgánů jednotlivých států na jeho výklad lišily. Státy tedy příslušné ustanovení transponovaly různým způsobem. Hlavním rozdílem bylo především koncepční pojetí automatizovaného rozhodování, a sice, zda jej vykládat jako činnost dopředu zákonem dovolenou, ledaže by s ní subjekt údajů vyslovil aktivně nesouhlas, tj. vznesl námitku proti takovému zpracování, nebo jako obecný zákaz takové činnosti, ledaže by se uplatnila některá z výjimek, která takové zpracování umožňuje. ČR, podobně jako některé další státy[140] transponovala ustanovení jako všeobecný zákaz s výjimkami pro některé případy. Oproti tomu druhou skupinu tvořily státy jako Velká Británie, Dánsko nebo Švédsko, ty tedy takové rozhodování obecně povolily s možností uplatnění námitky subjektem údajů.[141] Skupina WP29 se nakonec ve svých pokynech k automatizovanému individuálnímu rozhodování pro účely Nařízení 2016/679[142] přiklonila k výkladu, který považuje toto ustanovení za obecný zákaz, ze kterého existují výjimky. Co to tedy ve výsledku znamená? Znamená to, že ačkoli je ustanovení

[140] například Francie, Belgie, Nizozemsko, Itálie, Polsko atd.
[141] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 598-618. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].
[142] WP29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 (WP 251 rev.01)*, přijaté dne 3. října 2017, naposledy revidované a přijaté dne 6. února 2018. Dostupné zde: https://ec.europa.eu/newsroom/article29/items/612053.

koncepčně zařazeno mezi ostatní práva subjektu údajů, mělo by se na něj pohlížet spíše jako na pozitivní povinnost správců zaručit ochranu subjektů údajů. Tyto operace automatizovaného zpracování tedy zákonodárce považuje za natolik rizikové, že přenáší kontrolu na správce, než že by očekával, že subjekty údajů budou aktivně uplatňovat svá práva.

V praktické rovině míří ustanovení na situace, kdy o právech či povinnostech subjektu údajů (nebo o jiných skutečnostech, které na něj mají dopad) rozhoduje výlučně algoritmus. To lze chápat jako předem stanovený postup, který je následně prováděn automatizovaně. Cílem úpravy je tak zejména stanovit, ve kterých případech je automatizované individuální rozhodování přípustné, a pro případy, kdy přípustné je, poskytnout subjektu údajů záruky ochrany jeho práv. Některé z těchto záruk jsou uvedeny v samotném ustanovení a v recitálu 71, např. právo na lidský zásah ze strany správce, právo vyjádřit svůj názor, právo na získání vysvětlení o rozhodnutí učiněném po takovém posouzení a právo na napadnutí tohoto rozhodnutí. Právo na lidský zásah blíže konkretizují pokyny WP29, nelze jím chápat jen rutinní přezkum, správce musí fakticky zajistit, že jakýkoli dohled nad rozhodnutím bude smysluplný, nikoli jenom symbolický. Měl by jej provádět někdo, kdo má pravomoc a kompetenci rozhodnutí změnit, rozhodující je tedy pravomoc zpochybnit výsledky umělé inteligence.

Článek 22 odst. 2 nařízení obsahuje tři důležité výjimky. Právo – nebo přesněji řečeno zákaz – se neuplatní, pokud je zpracování: a) nezbytné pro uzavření nebo plnění smlouvy; b) povoleno právem EU nebo členského státu nebo c) založeno na výslovném souhlasu subjektu údajů. Tyto tři výjimky jsou tedy povoleny pouze v případě, že jsou zavedena vhodná ochranná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů. V případě první výjimky je důležité obzvláště zdůraznit, že musí být splněn prvek nezbytnosti, na to správci často zapomínají. Jinými slovy, pokud se ukáže, že pro konkrétní plnění smlouvy není automatizované rozhodování nezbytné a lze použít jiné prostředky, na základě kterých lze dosáhnout stejného účinku, měly by být použity tyto méně invazivní prostředky. Pokyny WP 29 uvádějí jako příklad situaci, kdy správce obdrží několik tisíc životopisů uchazečů v rámci vypsaného výběrového řízení. Dalším příkladem může být automatizované posouzení bonity žadatele o úvěr.[143] Pokud jde o druhou výjimku, recitál 71 uvádí několik scénářů, kdy lze takové předpisy nalézt. Může jít například o monitorování a předcházení podvodů a daňových úniků,

[143] Viz § 89 zákona č. 257/2016 Sb., o spotřebitelském úvěru: „*Odmítne-li poskytovatel poskytnout spotřebiteli spotřebitelský úvěr v důsledku posouzení jeho úvěruschopnosti, poskytovatel informuje spotřebitele bez zbytečného odkladu o tomto odmítnutí, a pokud je důvodem neposkytnutí výsledek automatizovaného zpracování údajů, nebo vyhledávání v databázi podle § 88 odst. 1, poskytovatel spotřebitele vyrozumí o tomto výsledku a o použité databázi.*“

jakož i zajištění bezpečnosti a spolehlivosti služby poskytované správcem. Zajímavá je také otázka personalizovaných reklam založených na profilování. Ty by podle názoru doktríny[144] také neměly spadat do oblasti působnosti zákazu podle čl. 22 odst. 1 nařízení. Důvodem má být skutečnost, že nevyvolávají ani právní účinky, ani srovnatelný rizikový potenciál, pokud jde o práva a svobody fyzických osob. Osobně si dovolím pochybovat o absenci rizikového potenciálu a právních či srovnatelných účinků personalizovaných online reklam, zejména behaviorální reklamy, které jsou podle mého názoru velmi rušivé. Na druhou stranu, tyto reklamy jsou velmi často součástí obchodních modelů společností, včetně Meta Platforms, dovedu si tedy představit jejich užívání za předpokladu platně získaného souhlasu uživatele. Otázku možného použití smlouvy jako právního titulu je podle mého názoru nutné odmítnout, s ohledem na rozsudek Soudního dvora ve věci C-252/21, *Meta Platforms a další (Všeobecné podmínky používání sociální sítě)*[145]. Soudní dvůr k tomu uvedl, že zpracování může být považováno za nezbytné pro splnění smlouvy, jejíž stranami jsou subjekty údajů, pouze za podmínky, že je toto zpracování objektivně nezbytné pro uskutečnění účelu, který je nedílnou součástí smluvního plnění určeného subjektům údajů. Správce tedy musí být schopen prokázat, proč by bez předmětného zpracování nemohlo být dosaženo hlavního předmětu smlouvy. K personalizaci obsahu následně Soud doplnil, že i když může být pro uživatele užitečná, nic to nemění na tom, že se nejeví být nezbytná k tomu, aby tomuto uživateli byly nabízeny služby sociální sítě.

Toto ustanovení článku 22 nařízení vyložil Soudní dvůr EU poprvé v rozsudku ve věci *SCHUFA Holding (Scoring)*[146]. Na tomto rozsudku lze demonstrovat, jakým způsobem Soud nahlíží na citlivé oblasti rozhodnutí založených výhradně na automatizovaném zpracování údajů, zde konkrétně automatizované posuzování bonity žadatele o úvěr. SCHUFA Holding je soukromá společnost založená podle německého práva, která poskytuje svým smluvním partnerům informace o úvěrové bonitě osob. Za tímto účelem přisuzuje každému subjektu údajů hodnotu, kterou vytváří z určitých charakteristických znaků této osoby na základě matematicko-statistických postupů. Stanovení hodnoty slouží k předpovědi budoucího chování osoby, například splácení úvěru, na základě jejího zařazení do skupiny jiných osob s určitými srovnatelnými znaky. Poté, co třetí osoba (banka) odmítla osobě na základě této hodnoty

[144] VOIGT, Paul a VON DEM BUSSCHE, Axel, 2017. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, s. 180-187. Online. ISBN 978-3-319-57959-7. Dostupné z: https://doi.org/10.1007/978-3-319-57959-7. [cit. 2024-09-04].
[145] Rozsudek ze dne 4. července 2023, Meta Platforms a další (Všeobecné podmínky používání sociální sítě), C-252/21, EU:C:2023:537, zejména body 98, 102, 115 až 117.
[146] Rozsudek ze dne 7. prosince 2023, SCHUFA Holding (Scoring), C-634/21, EU:C:2023:957.

poskytnout úvěr, požádala tato osoba společnost SCHUFA, aby jí poskytla přístup k jejím údajům, a vymazala údajně nesprávné údaje. Společnost SCHUFA jí však sdělila pouze její hodnotu a obecně způsoby jejího výpočtu, přičemž se ve zbývající části odvolávala na obchodní tajemství. Uváděla rovněž, že se ze strany společnosti SCHUFA vůbec nejedná o automatizované rozhodnutí. Subjekt údajů podal stížnost a následně i správní žalobu ke správnímu soudu. Věc nakonec skončila s předběžnou otázkou u Soudního dvora EU. Soudní dvůr konstatoval, že použitelnost ustanovení článku 22 podléhá třem kumulativním podmínkám, které byly v tomto případě splněny. Zaprvé musí existovat „rozhodnutí", zadruhé toto rozhodnutí musí být „založeno výlučně na automatizovaném zpracování, včetně profilování", a zatřetí musí mít „[pro subjekt údajů] právní účinky" nebo se ho musí „obdobným způsobem významně" dotýkat. Na prvním místě Soud upřesnil, že pojem „rozhodnutí" má široký rozsah, může zahrnovat i více aktů a může zahrnovat výsledek výpočtu solventnosti osoby ve formě hodnoty pravděpodobnosti týkající se schopnosti této osoby splnit v budoucnu své závazky. Na druhém místě, je zřejmé, že činnost dotčené společnosti odpovídá definici „profilování". A na třetím místě Soud uvedl, že jednání třetí osoby, které je poskytnuta hodnota pravděpodobnosti, se touto hodnotou „rozhodujícím způsobem" řídí. Pokud je hodnota nedostatečná, téměř vždy to vede k odmítnutí poskytnout úvěr. Soudní dvůr z toho tedy vyvodil, že toto formalizované sdělení hodnoty bance hraje rozhodující úlohu při poskytování úvěru, a proto musí být samo o sobě kvalifikováno jako automatizované rozhodnutí. Jedině tento široký výklad posiluje účinnou ochranu uvedenou v GDPR. Oproti tomu restriktivní výklad, podle něhož by stanovení hodnoty bylo považováno pouze za přípravný akt, a za „rozhodnutí" pouze akt přijatý třetí osobou (bankou), by vedl k mezeře v právní ochraně. Soud navíc zdůraznil, že by to vedlo i k omezení práva na přístup[147], neboť subjekt údajů by jej nemohl realizovat u společnosti SCHUFA, ale pouze u banky, u níž by nicméně zase nemohlo být fakticky naplněno, neboť v uvedeném případě třetí osoba těmito informacemi nedisponuje. V projednávané věci společnost SCHUFA na ústním jednání navíc uvedla (na dotaz soudce von Danwitze, zda používá samoučící se algoritmy ke stanovení úvěrového hodnocení), že sice v současné době nepoužívá samoučící se algoritmy, ale že tak může učinit v budoucnu. Význam tohoto rozsudku tak možná přesahuje i samotný rámec nařízení GDPR, neboť samoučící se

[147] Viz čl. 15 odst. 1 písm. h) nařízení GDPR, který v případě automatizovaného rozhodování přiznává subjektu údajů rozsáhlé právo na přístup, včetně smysluplných informací týkajících se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

algoritmy umělé inteligence, automatizovaná analytika a různé formy hodnocení se pravděpodobně stanou ještě běžněji používanými[148].

Význam práva podle článku 22 nařízení se odvíjí od vzrůstající implementace technologií umělé inteligence. Subjekty údajů si často nejsou vědomy množství a typu informací, které jsou o nich shromažďovány, ani toho, jak mohou být tyto informace propojeny prostřednictvím technologií umělé inteligence, aby bylo možné odvodit jejich charakteristiky. Klíčovým rizikem profilování je, že uživatelé nemají žádnou znalost nebo kontrolu nad kategorizací svých údajů nebo nad tím, jak s jejich údaji propojené systémy na základě této kategorizace zacházejí.[149] Stejně jako v případě práva vznést námitku je praktické uplatňování práva podle článku 22 nařízení GDPR náročné. V online prostředí navrhuje pracovní skupina WP 29 následující podobu odvolacího řízení: V okamžiku, kdy je subjektu údajů doručeno automatizované rozhodnutí, by správci údajů měli poskytnout odkaz na odvolací řízení, včetně dohodnutých lhůt pro přezkum a uvedení jmenného kontaktu pro případné dotazy. Příklad dobré praxe: webový prohlížeč Mozilla Firefox zavedl užitečnou samoregulační verzi kvaziodvolacího práva. Předtím, než systém umělé inteligence Mozilly odstraní komentář z důvodu jeho nevhodného charakteru nebo porušování pravidel, umožní autorovi příspěvku vyjádřit svůj názor a rozhodnutí napadnout.[150]

[148] HÄUSELMANN, Andreas, 2023. *The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber*. Online. European Law Blog. Dostupné z: https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/. [cit. 2024-06-23].

[149] KIESOW CORTEZ, Elif, 2021. 12.2 Automated Decision-Making and Artificial Intelligence. In: *Data Protection Around the World: Privacy Laws in Action*. T.M.C. Asser Press The Hague, s. 272. Online. ISBN 978-94-6265-407-5. Dostupné z: https://doi.org/10.1007/978-94-6265-407-5. [cit. 2024-09-25].

[150] VRABEC, Helena U., 2021. 8.3 How the GDPR tackles profiling on the individual level. In: *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*. Oxford University Press, s. 197-212. Online. ISBN 9780191904851. Dostupné z: https://doi.org/https://doi.org/10.1093/oso/9780198868422.001.0001. [cit. 2024-04-14].

4. Právo subjektu údajů na přístup k vlastním údajům (čl. 15 GDPR)

4.1 Obecné poznámky a význam práva na přístup

Těžiště této práce spočívá právě v bližším výzkumu práva subjektu údajů na přístup k vlastním údajům, obsaženému v článku 15 GDPR. Následující část si klade za cíl detailněji analyzovat toto právo. Abychom mohli hovořit o účinnosti právních předpisů obecně a práv subjektů údajů zvlášť, je důležité se zamyslet nad tím, zda vůbec a na jakém principu existují vhodné mechanismy k vynucování těchto práv. V digitálním věku se zpracování údajů stává všudypřítomným a pro jednotlivce je stále složitější je pochopit. Jednotlivci mohou být často ve znevýhodněném postavení, pokud jde o pochopení toho, jak jsou jejich osobní údaje zpracovávány, včetně technologie použité v konkrétním případě, ať už ze strany soukromého nebo veřejného subjektu. Ke zmírnění nerovnováhy moci mezi subjekty údajů a správci získali jednotlivci určitá práva na provádění větší kontroly zpracování svých osobních informací.[151]

Právo na přístup k osobním údajům je jedním z práv subjektu údajů, a je stanoveno jak v článku 8 Listiny, tak v kapitole III nařízení GDPR, konkrétně v článku 15 tohoto nařízení. Český překlad článku 15 je poněkud nepřesný, neboť zní „Právo subjektu údajů na přístup k osobním údajům“. Ve skutečnosti se ovšem nejedná pouze o právo na přístup k samotným údajům, ale také ke všem relevantním informacím o zpracování.[152] Výstižnější je proto obecné anglické znění „Right of access by the data subject“ nebo francouzské znění „Droit d'accès de la personne concernée“, které obecně pojednávají o právu subjektu údajů na přístup. Za vhodnou lze považovat i německou variantu „Auskunftsrecht der betroffenen Person“, což znamená „Právo dotčené osoby (subjektu údajů) na informace“.

Výkon práva na přístup se uskutečňuje v rámci práva na ochranu osobních údajů, konkrétně v rámci „*základních práv a svobod fyzických osob, a zejména jejich práva na ochranu osobních údajů*“, jak je uvedeno v čl. 1 odst. 2 nařízení GDPR. Právo na přístup je důležitým prvkem celého systému ochrany osobních údajů. Pokud jde o rozvoj práva na přístup v rámci právního rámce pro ochranu údajů, je třeba zdůraznit, že je součástí evropského systému ochrany osobních údajů od jeho počátku. Ve srovnání s předchozí právní úpravou,

[151] FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2022-03-07]
[152] FOŘT, Ferdinand, 2019. Kapitola III Práva subjektu údajů. In: PATTYNOVÁ, Jana; SUCHÁNKOVÁ, Lenka; ČERNÝ, Jiří a RŮŽIČKA, Miroslav. *Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář*. 2. vydání. Praha: Leges, s. 170-176. ISBN 978-80-7502-396-4.

směrnicí 95/46/ES, byl standard práv subjektů údajů stanovený v nařízení GDPR upřesněn a posílen, přičemž to platí i pro právo na přístup. Vzhledem k tomu, že modality (způsoby) poskytnutí práva na přístup jsou nyní vyjádřeny přesněji, byla posílena právní jistota jak pro subjekty údajů, tak pro správce. Kromě toho konkrétní znění článku 15 a přesná lhůta pro poskytnutí údajů podle čl. 12 odst. 3 nařízení GDPR ukládá správci povinnost připravit se na dotazy subjektů údajů tím, že vytvoří postupy pro vyřizování jejich žádostí. V této souvislosti je důležité dodat, že na právo na přístup by nemělo být nahlíženo izolovaně, neboť, podobně jako další ustanovení, působí ve vztazích k dalším normám. Právo na přístup je tak úzce spjato s dalšími ustanoveními nařízení GDPR, zejména se zásadami ochrany osobních údajů, povinností správce v oblasti transparentnosti a s dalšími právy subjektu údajů stanovenými v kapitole III nařízení GDPR. Právo subjektu údajů na přístup k jeho údajům je také podstatným prvkem k legitimnosti zpracování osobních údajů. Ačkoli subjekt údajů zpravidla nemá ve svém vlastnictví nosiče s osobními údaji, je určující právě vztah subjektu údajů k údajům o jeho osobě.[153]

Výkon práva subjektu údajů na přístup k jeho vlastním osobním údajům vede k nejčastějšímu důvodu stížností podaných dozorovým orgánům. Britský dozorový úřad, Úřad komisaře pro informace (ICO) zaznamenal za rok 2020–2021 celkem 2099 žádostí v porovnání s 1509 žádostmi za rok 2017–2018, jedná se tedy o 39% nárůst žádostí o přístup. Situace byla navíc silně ovlivněna nástupem pandemie, za rok 2019–2020 bylo žádostí o přístup evidováno dokonce 2747.[154] Irský dozorový úřad (DPC) zase evidoval celkem 4660 stížností za rok 2020, přičemž podle jeho údajů se největší počet, resp. 27 % stížností, týkalo právě práva na přístup k vlastním údajům, což činí cca 1258 stížností.[155] Český dozorový úřad bohužel takto detailní statistiku neobsahuje. Na základě výše uvedených čísel lze ovšem jednoznačně demonstrovat důležitost tohoto práva a také rostoucí povědomí subjektů údajů o jejich právech. Pokyny k transparentnosti skupiny WP29 uvádějí, že: „*smyslem požadavků stanovených obecným nařízením o ochraně osobních údajů, které se týkají výkonu uvedených práv a povahy*

[153] MORÁVEK, Jakub a BURIAN, David, 2012. 5. Směrnice Evropského parlamentu a Rady č. 95/46/ES. In: MORÁVEK, Jakub a BURIAN, David. *Předávání osobních údajů do zahraničí: česká a evropská právní úprava, otázky a odpovědi*. Praha: Linde, s. 60-61. ISBN 978-80-7201-878-9.

[154] ICO. Výroční zpráva britského dozorového úřadu ICO. *Information Commissioner's Annual Report and Financial Statements* 2020-21 [online]. Červenec 2021, 138 s. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf. [cit. 2022-03-07].

[155] DPC. Výroční zpráva irského dozorového úřadu DPC. *Data Protection Commission's Annual Report 2020* [online]. 98 s. Dostupné z: https://www.dataprotection.ie/sites/default/files/uploads/2021-02/DPC%202020%20Annual%20Report%20%28English%29.pdf. [cit. 2022-03-07].

požadovaných informací, je dát subjektům údajů takové postavení, aby mohly vymáhat svá práva a volat správce údajů k odpovědnosti za zpracování svých osobních údajů."[156]

Z hlediska významu má právo na přístup dvě hlavní funkce, a to posílení transparentnosti činnosti správce a usnadnění kontroly subjektu údajů nad jeho údaji. V čem takové posílení transparentnosti spočívá? Umožněním výkonu tohoto práva se totiž subjektu údajů poskytuje druhá, hlubší a podrobnější „vrstva" informací, které může získat nad rámec toho, co správce zveřejní podle článků 13 nebo 14 nařízení GDPR. Subjektu údajů je tak umožněno získat kopie zpracovávaných osobních údajů a aktualizované informace o sobě samém ve srovnání s tím, co bylo uvedeno v oznámení, a to kdykoli od okamžiku shromáždění těchto údajů a v zásadě bezplatně. Pro subjekt údajů je totiž naprosto zásadní objasnění toho, co se s jeho osobními údaji dělo dříve, k čemu dochází nyní a co se s nimi dít bude.

Druhou praktickou funkcí práva na přístup je umožnit fyzickým osobám mít kontrolu nad svými osobními údaji. V zájmu účinného dosažení tohoto cíle v praxi je cílem nařízení GDPR usnadnit tento výkon řadou záruk, které subjektu údajů umožní výkon tohoto práva snadno, bez zbytečných omezení, v přiměřených intervalech a bez zbytečných prodlev nebo nákladů. To vše by mělo vést k účinnějšímu prosazování práva subjektu údajů na přístup v době rychlého technologického rozvoje. Subjekt údajů získá potvrzení, že jeho osobní údaje jsou zpracovávány, a kopie těchto údajů, díky čemuž může případně uplatnit i veškerá svá další práva. Právo na přístup umožňuje subjektu údajů identifikovat nesprávné nebo neúplné informace, které jsou o něm zpracovávány, díky čemuž může realizovat své další právo, právo na opravu podle článku 16 nařízení GDPR. Subjekt údajů může prostřednictvím uplatnění práva na přístup získat také kopii svých osobních údajů, které si přeje následně nechat správcem vymazat (právo na výmaz podle článku 17 nařízení GDPR), čímž si zajistí, že o tyto informace navždy nepřijde.[157] Pro umožnění smysluplné kontroly má zásadní význam nastavit silný mechanismus transparentnosti. Za účelem přiměřeného výkonu práva na opravu nebo výmaz si bude muset být subjekt údajů vědom skutečného rozsahu svých osobních údajů a způsobu jejich zpracování. Jestliže správci naplňují řádně požadavek informování subjektů údajů (dodržují zásadu transparentnosti), subjekty údajů mohou správce volat k odpovědnosti a mohou mít

[156] WP29. *Pokyny k transparentnosti WP 260 rev.01*, přijaté dne 29. listopadu 2017 naposledy revidované a přijaté dne 11. dubna 2018, s. 27. Dostupné z: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_cs.pdf.
[157] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

kontrolu nad svými osobními údaji, například poskytnutím či odvoláním svého souhlasu a uplatněním svých práv jako subjektů údajů.[158]

Právo na přístup bývá také někdy nazýváno jako doplnění zásady transparentnosti, uplatněné následně, tedy *ex post*. Zásada transparentnosti (upravená v čl. 5 odst. 1 písm. a) GDPR) se konkretizuje jednou ze základních povinností správce, a to informační povinností. Obecná pravidla informační povinnosti jsou upravena v článku 12 GDPR. Samotná informační povinnost (informace poskytované správcem) je pak upravena v článcích 13 a 14, v těchto případech můžeme zase hovořit o zásadě transparentnosti *ex ante*.[159] Zásadním rozdílem práva na přístup v porovnání s informační povinností je pak to, že právo na přístup představuje prostředek, jak mohou subjekty údajů získat informace o již probíhajícím zpracování v jeho průběhu, vč. kopie zpracovávaných údajů.[160]

Články 13 a 14 se od sebe navzájem odlišují tím, že prvně uvedený se týká situace, kdy osobní údaje jsou získány od subjektu údajů, zatímco článek 14 dopadá na případy, kdy osobní údaje nebyly získány od subjektu údajů, nýbrž z jiného zdroje. Někdy se také ne zcela přesně hovoří o přímém (článek 13) a nepřímém (článek 14) získání osobních údajů. To ovšem není jediná odlišnost mezi těmito ustanoveními. Článek 13 klade v zásadě vyšší požadavky na správce z časového hlediska, neboť požaduje, aby správce subjektu údajů poskytl informace již v okamžiku získání osobních údajů (myšleno během procesu shromažďování osobních údajů). Oproti tomu článek 14 umožňuje správci informace poskytnout v přiměřené lhůtě po získání osobních údajů, nejpozději však do jednoho měsíce od okamžiku získání těchto osobních údajů. Předpokládá se totiž, že správci mají ztížený přístup k subjektům údajů, neboť do kontaktu s nimi teprve mohou vstoupit. Dalším významným rozdílem mezi články 13 a 14 je povinnost správce ve druhém případě doplnit informační povinnost o informace o zdroji osobních

[158] Viz například stanovisko generálního advokáta Pedra Cruz Villalóna ze dne 9. července 2015, Bara, C-201/14, EU:C:2015:461, bod 74: *„požadavek informování subjektů dotčených zpracováním jejich osobních údajů, který zaručuje transparentnost veškerého zpracování, je o to důležitější, že vytváří předpoklady pro to, aby dotyčné osoby mohly vykonat své právo na přístup ke zpracovávaným údajům upravené v článku 12 směrnice 95/46 a jejich právo na podání námitky proti zpracování uvedených údajů podle článku 14 této směrnice“.*

[159] NAUDTS, Laurens; DEWITTE, Pierre a AUSLOOS, Jef, 2022. 21 Meaningful transparency through data rights: A multidimensional analysis. In: KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research Handbook on EU Data Protection Law*. Cheltenham, UK: Edward Elgar Publishing, s. 530-571. Online. ISBN 9781800371682. Dostupné z: https://doi.org/10.4337/9781800371682.

[160] FOŘT, Ferdinand, 2019. Kapitola III Práva subjektu údajů. In: PATTYNOVÁ, Jana; SUCHÁNKOVÁ, Lenka; ČERNÝ, Jiří a RŮŽIČKA, Miroslav. *Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář*. 2. vydání. Praha: Leges, s. 170-176. ISBN 978-80-7502-396-4.

údajů.[161] To je logický požadavek, neboť u článku 13 je zdrojem právě samotný subjekt údajů. Úprava GDPR je ovšem nedostatečná, neboť již nekonkretizuje, jak moc podrobné musí tyto informace o zdroji být. Není proto jasné, zda by měly být informace o zdroji poskytovány v maximální možné detailní míře, či umožněno správci zvolit spíše obecnější informace s tím, že hlubší seznámení by bylo subjektu údajů umožněno právě prostřednictvím institutu práva na přístup podle článku 15 GDPR.

Třetím významným rozdílem mezi články 13 a 14 je povinnost správce informovat subjekty údajů o tom, jaké kategorie osobních údajů správce zpracovává, která se uplatní pouze v případě nepřímého získání osobních údajů. To sice může působit na první pohled také logicky, můžeme předpokládat, že subjekt údajů přeci ví, jaké osobní údaje sám správci poskytuje v prvním případě. Situaci ovšem paradoxně „zkomplikoval" samotný EDPB, který ve svých Pokynech k transparentnosti[162] pod režim článku 13 zařadil i osobní údaje, které správce získal prostřednictvím sledování zařízení, které subjekt údajů používá (např. za použití zařízení na automatizovaný sběr dat nebo softwaru na zachycování dat, jako jsou kamery, síťová zařízení, sledování přes Wi-Fi, RFID a další typy senzorů). To je podle mého osobního názoru nesprávný výklad v neprospěch subjektu údajů. Článek 13 se totiž na jeho základě vztahuje nejen na situace, kdy subjekt údajů své osobní údaje vědomě správci poskytl (např. při vyplňování elektronického formuláře), ale též na situace, kdy použité technice či zařízení na zpracování údajů nerozumí a nemusí tudíž vědět, jaké všechny osobní údaje jsou o jeho osobě zpracovávány a jakým způsobem. Domnívám se proto, že ačkoli tak nařízení GDPR výslovně nestanoví, měl by správce v zájmu transparentnosti a dobré praxe postupovat tak, že i v režimu podle článku 13 poskytne subjektu údajů informace o tom, jaké kategorie jeho osobních údajů zpracovává. V případě, kdyby tak neučinil, je pravděpodobné, že tyto informace o kategorii zpracovávaných osobních údajů bude muset stejně nakonec sdělit, a to právě v reakci na uplatnění práva na přístup konkrétní osoby podle článku 15 GDPR. Ve výsledku by tak situace mohla být i pro správce nakonec komplikovanější. Z předchozího rozboru článků 13 a 14 GDPR vyplývá zároveň podstatný rozdíl obou těchto článků v porovnání se mnou analyzovaným právem na přístup podle článku 15 GDPR. Právo na přístup umožňuje subjektům údajů jít nad rámec toho, co je uvedeno v zásadách zpracování osobních údajů, a požadovat více informací

[161] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 450-474. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

[162] WP29. *Pokyny k transparentnosti WP 260 rev.01*, přijaté dne 29. listopadu 2017 naposledy revidované a přijaté dne 11. dubna 2018, s. 15. Dostupné z: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_cs.pdf.

o tom, jak jsou jejich osobní údaje zpracovávány, a nabízí tak další individualizovanou úroveň transparentnosti. Informace, které správce poskytuje subjektu údajů podle článku 15 GDPR by měly být podrobnější a pokud možno přizpůsobené konkrétní situaci subjektu údajů, který uplatňuje své právo. Správci by proto neměli na právo na přístup odpovídat opakováním obecných informací, které jsou již k dispozici v rámci zásad ochrany údajů, ale měli by poskytnout podrobnosti týkající se konkrétní situace subjektu údajů uplatňujícího toto právo. Uplatnění práva na přístup by tak mohlo usnadnit pochopení složitých operací zpracování, jejichž vnitřní fungování může být příliš komplikované na to, aby se vešlo do běžných zásad ochrany údajů, nebo které se u jednotlivých subjektů údajů výrazně liší. Těžiště práva na přístup pak spočívá v očekávání subjektů údajů. Zatímco transparentnost *ex ante* může tato očekávání subjektů údajů formovat, jedině právo na přístup jim umožňuje proniknout hlouběji do operace zpracování a ověřit si rozsah postupů správců při zpracování údajů.[163]

Je důležité být schopen odlišit právo na přístup k vlastním osobním údajům od podobných práv s jinými cíli, jako je například právo na přístup k veřejným informacím, resp. veřejným dokumentům, které je projevem zásady otevřenosti veřejné správy. Tato dvě práva mají různé politické základy, z nichž jedno zaručuje transparentnost vůči osobě, jejíž osobní údaje správce shromažďuje a používá (transparentnost *inter partes*), zatímco druhé zajišťuje transparentnost vůči veřejnosti, pokud jde o informace, které mají hodnotu nebo význam pro veřejnost (transparentnost *erga omnes*), jedná se tedy o transparentnost rozhodování orgánů veřejné moci a řádnou správní praxi, což je legitimním zájmem veřejnosti[164]. Může ovšem dojít k situaci, kdy informace, které mají zvláštní hodnotu pro veřejnost a na něž se vztahuje právo na přístup k veřejným informacím, budou současně osobními údaji. Tyto situace jsou i v praxi českých soudů poměrně časté. V těchto situacích jsou oba právní režimy, jimiž se řídí tytéž údaje, v rozporu, a proto je třeba v každém jednotlivém případě hledat rovnováhu mezi veřejným zájmem a právy subjektu údajů. Jako příklad lze uvést diskuze, které se dlouhou dobu vedou ohledně zveřejňování informací o platech, či finančních odměnách konkrétních pracovníků veřejné správy a podmínek tohoto zveřejňování.

[163] NAUDTS, Laurens; DEWITTE, Pierre a AUSLOOS, Jef, 2022. 21 Meaningful transparency through data rights: A multidimensional analysis. In: KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research Handbook on EU Data Protection Law*. Cheltenham, UK: Edward Elgar Publishing, s. 530-571. Online. ISBN 9781800371682. Dostupné z: https://doi.org/10.4337/9781800371682.

[164] Z judikatorní praxe víme, že se často jednalo třeba o zájem veřejnosti na získání informací o nakládání s veřejnými financemi či informace o veřejných činitelích (platy, dosažené vzdělání, členství v KSČ nebo StB apod.).

Jedná se o oblast, která prošla rozsáhlým judikatorním vývojem. Žadatelé se s dotazy tohoto typu často obrací na povinné subjekty s odkazem na ustanovení § 8b zákona č. 106/1999 Sb., o svobodném přístupu k informacím (§ 8b – Příjemci veřejných prostředků). Dřívější judikatura správních soudů (především Nejvyššího správního soudu) zastávala dlouhodobě jednostrannou názorovou linii širokého pojetí přístupu k informacím (zejména rozsudek NSS, č. j. 8 As 55/2012-62). Základním pravidlem, které nastolila, je pravidlo informace o platech státních zaměstnanců zásadně poskytovat. Výklad byl v tomto pojetí extenzivní, a to jak z hlediska dotčených subjektů – pod § 8b zařazovala hromadně takřka všechny zaměstnance veřejné správy (s jedinou výjimkou zaměstnanců vykonávajících činnosti pomocné nebo servisní povahy). Takový radikální postup zdůvodnila, dle mého názoru ovšem velice neuspokojivě, veřejným zájmem, a sice zájmem nad kontrolou hospodárného a účelného nakládání s veřejnými prostředky, aniž by fakticky provedla třísložkový test proporcionality (test veřejného zájmu). Zpřesnění pak poskytly až nálezy Ústavního soudu.[165] Ústavní soud v nálezu IV. ÚS 1378/16 odmítl, i s odkazem na judikaturu Soudního dvora EU a Evropského soudu pro lidská práva[166], názorovou linii NSS a konstatoval, že ústavně konformní může být poskytnutí informací o platech pouze v případě, že budou splněny kumulativně tyto podmínky:

a) účelem vyžádání informace je přispět k diskusi o věcech veřejného zájmu;

b) informace samotná se týká veřejného zájmu;

c) žadatel o informaci plní úkoly či poslání dozoru veřejnosti či roli tzv. „společenského hlídacího psa“;

d) informace existuje a je dostupná.

Právo na přístup k informacím bývá vyvozováno z významově širšího pojmu právo na informace. Právo na informace lze totiž vnímat ve dvou rovinách. V první rovině (širší) je především součástí svobody projevu. Podle doc. M. Bartoně v této rovině neobsahuje pozitivní závazek veřejné moci k poskytování informací, pouze povinnost neklást překážky, které by bránily toku informací. Ve druhé rovině lze právo na informace vnímat jako právo na přístup

[165] Zejména nález ÚS ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16 a nález ÚS ze dne 3. 4. 2018, sp. zn. IV. ÚS 1200/16.

[166] Rozsudek ze dne 20. května 2003, Österreichischer Rundfunk a další, spojené věci C-465/00, C-138/01 a C-139/01, EU:C:2003:294; rozsudek ze dne 9. listopadu 2010, Volker und Markus Schecke a Eifert, spojené věci C-92/09 a C-93/09, EU:C:2010:662; rozsudek velkého senátu ESLP ze dne 8. listopadu 2016 Magyar Helsinki Bizottság proti Maďarsku (stížnost č. 18030/11).

k informacím, které jsou v dispozici veřejné moci.[167] V ústavním pořádku České republiky je právo na informace obsaženo v článku 17 Listiny základních práv a svobod a detailněji upraveno v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím.

Na evropské úrovni je právo na přístup k informacím zakotveno jako právo na přístup k dokumentům orgánů EU. Právo na přístup k dokumentům je upraveno v primárním právu EU v článku 15 Smlouvy o fungování EU a v článku 42 Listiny základních práv EU. Sekundární právo EU pak tvoří nařízení Evropského parlamentu a Rady EU (ES) č. 1049/2001 ze dne 30. 5. 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (dále jen „nařízení č. 1049/2001"). Účel nařízení č. 1049/2001 je vyjádřen v jeho článku 1: „*účelem tohoto nařízení je vymezit zásady, podmínky a omezení z důvodu veřejného nebo soukromého zájmu pro výkon práva na přístup k dokumentům Evropského parlamentu, Rady a Komise, aby se zajistil co nejširší přístup k dokumentům, vytvořit pravidla pro co nejsnadnější výkon tohoto práva a podporovat řádnou správní praxi při přístupu k dokumentům.*" Zpracování a přístup veřejnosti k úředním dokumentům je také upraveno samostatně v nařízení GDPR, konkrétně v článku 86 a odpovídajícím bodu odůvodnění 154. Právě tato ustanovení se zabývají střetem práva na informace a práva na ochranu osobních údajů. Předmětem této práce ovšem není vyčerpávajícím způsobem analyzovat právo na informace, tak si vystačíme jen se základním nastíněním jeho podstaty. Toto právo, které umožňuje získávat a dále využívat informace o činnosti orgánů veřejné moci tak představuje významný prostředek ke kontrole výkonu veřejné moci ze strany občanů. Ani zájem veřejnosti na přístupu k informacím, ani právo na ochranu osobních údajů však nejsou neomezená a absolutní. Bod odůvodnění 4 nařízení GDPR uvádí: *„Zpracování osobních údajů by mělo sloužit lidem. Právo na ochranu osobních údajů není právem absolutním; musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy. Toto nařízení ctí všechna základní práva a dodržuje svobody a zásady uznávané Listinou, jak jsou zakotveny ve Smlouvách, zejména respektování soukromého a rodinného života, obydlí a komunikace, ochranu osobních údajů, svobodu myšlení, svědomí a náboženského vyznání, svobodu projevu a informací, svobodu podnikání, právo na účinnou právní ochranu a spravedlivý proces, jakož i kulturní, náboženskou a jazykovou rozmanitost."* Je tedy nutné tato práva proporcionálně vyvažovat (provádět test proporcionality).

[167] BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*. Praha: Leges, 2010, s. 79-80. ISBN 978-80-87212-42-4.

Konflikt práva na přístup k dokumentům a práva na ochranu osobních údajů byl velmi dobře ilustrován ve věci *Bavarian Lager*.[168] Žalobce, společnost Bavarian Lager, požadoval po Evropské komisi zápis ze zasedání konaného v rámci řízení o nesplnění povinnosti, včetně jmen účastníků. Komise poskytla žalobci zápis ze svého zasedání bez uvedení jmen pěti účastníků, kteří s poskytnutím neudělili souhlas. Vznikla otázka, jak by se mělo zacházet s osobními údaji v dokumentu, na který se vztahují pravidla pro přístup veřejnosti stanovená v nařízení č. 1049/2001, a jak by měl být vykládán čl. 4 odst. 1 písm. b) uvedeného nařízení – zvláštní výjimka z práva na přístup veřejnosti, která vyžaduje, aby byla zvážena ochrana soukromí a osobních údajů. V případě, že jsou požadovány osobní údaje, nařízení o ochraně osobních údajů č. 45/2001[169] vyžaduje, aby příjemce prokázal potřebu, nezbytnost takového předání údajů, a subjekt má právo vznést kdykoli námitku.

Ve svém rozsudku ve věci *Bavarian Lager* dal za pravdu Soud prvního stupně (nyní Tribunál) žalobci a rozhodl, že výjimka stanovená v čl. 4 odst. 1 písm. b) musí být vykládána restriktivně. V důsledku toho bylo třeba přezkoumat, zda přístup veřejnosti ke jménu účastníků zasedání může skutečně a konkrétně narušit ochranu soukromí a osobní integritu dotčených osob. Soud prvního stupně měl za to, že nikoliv, a že pokud nebylo dotčeno soukromí, např. informace byly čistě profesního charakteru, nebylo nutné uplatňovat pravidla pro ochranu osobních údajů. Měl také za to, že soukromí zástupců pivovarnického průmyslu nebude narušeno odhalením skutečnosti, že byli na obchodním zasedání s Komisí, a proto by měla být zveřejněna jejich jména.

Ve svém rozhodnutí o kasačním opravném prostředku ale Soudní dvůr zaujal jiný přístup. Soudní dvůr rozhodl, že Soud prvního stupně nesprávně aplikoval článek 8 Evropské úmluvy o lidských právech (EÚLP), neboť nařízení o ochraně osobních údajů jasně stanoví, že EÚLP by měla být uplatňována pouze *„v případě, že […] zpracování [osobních údajů] probíhá […] v činnostech, které nespadají do oblasti působnosti [nařízení o ochraně osobních údajů]“* (bod 62). Pokud se žádost založená na nařízení o přístupu veřejnosti k dokumentům snaží získat dokumenty včetně osobních údajů, použije se nařízení o ochraně osobních údajů v plném rozsahu. Interpretoval čl. 4 odst. 1 písm. b) tak, že vyžadoval analýzu pravidel ochrany osobních údajů, a to i v případě, že nedošlo k porušení práva na soukromí. Na základě čl. 8 písm. b)

[168] Rozsudek ze dne 6. července 2010, Komise v. Bavarian Lager, C-28/08 P, EU:C:2010:378.
[169] Jedná se o dnes již neplatné nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů. Bylo nahrazeno nařízením Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES.

nařízení o ochraně osobních údajů č. 45/2001 Soudní dvůr konstatoval, že žalobce nepředložil jakékoliv výslovné a legitimní odůvodnění ani žádný přesvědčivý argument, který by Komisi umožnil posoudit nezbytnost předání osobních údajů účastníků nebo ověřit, zda mohou být poškozeny legitimní zájmy subjektů údajů (bod 78). Jména účastníků, kteří souhlas s předáním nedali, proto nemusela být odhalena a Komise tedy žádost o přístup k informacím právem zamítla. Dovolím si upozornit ještě na bod 49 tohoto rozsudku, ve kterém byly srovnány cíle nařízení č. 1049/2001 a nařízení č. 45/2001: „*První nařízení směřuje k zajištění co největší možné transparentnosti rozhodovacího procesu veřejných orgánů, jakož i informací, na kterých se jejich rozhodnutí zakládají. Jeho cílem je tedy co největší usnadnění výkonu práva na přístup k dokumentům, jakož i k podporování řádné správní praxe. Cílem druhého nařízení je zajištění ochrany základních práv a svobod fyzických osob, zejména pak práva na soukromí v souvislosti se zpracováním osobních údajů*.“ Soudní dvůr EU vyvozuje obecnou zásadu transparentnosti již z čl. 1 a čl. 10 odst. 3 Smlouvy o EU, přičemž tato zásada *„umožňuje občanům blíže se účastnit rozhodovacího procesu a zaručuje, že správní orgány budou mít ve vztahu k občanům v demokratickém systému větší legitimitu, účinnost a odpovědnost“* (bod 54). Ve věci *Bavarian Lager* tedy zásada otevřenosti veřejné správy nakonec ustoupila do pozadí. Právní rámec i judikatura se ovšem posunuly po vstupu v platnost Lisabonské smlouvy. Interpretace čl. 4 odst. 1 písm. b) nařízení č. 1049/2001 a článku 8 nařízení č. 45/2001 musí nyní plně zohlednit jak článek 8, tak článek 42 Listiny základních práv EU, které jsou rovnocennými základními právy. Při výkladu práva na ochranu osobních údajů musí být tak náležitě zohledněna zásada otevřenosti veřejné správy.[170]

Dalším rozsudkem, který se současně zabýval právem na přístup k dokumentům orgánů Evropské unie a právem na ochranu osobních údajů a pochází již z doby po Lisabonské smlouvě, je rozsudek ve věci *ClientEarth*.[171] V rozsudku šlo o rozhodnutí Evropského úřadu pro bezpečnost potravin (EFSA) neumožnit dvěma nevládním organizacím kompletní přístup k návrhům pracovních dokumentů vědeckých pokynů, neboť jim nebyla poskytnuta jména externích odborníků, kteří předložili vyjádření k vědeckým pokynům. Nevládní organizace si stěžovaly, protože úřad v návrzích zamaskoval jména externích vědeckých odborníků spojených s jejich připomínkami, obrátily se proto s návrhem na zrušení sporného rozhodnutí k Tribunálu, který ovšem jejich návrh zamítl. Organizace se proto obrátily na Soudní dvůr EU

[170] DOCKSEY, Christopher, 2016. Four fundamental rights: finding the balance. Online. *International Data Privacy Law*. August 2016, Volume 6, Issue 3, s. 15 (195–209). Dostupné z: https://doi.org/10.1093/idpl/ipw014. [cit. 2024-04-14].
[171] Rozsudek ze dne 16. července 2015, ClientEarth a PAN Europe v. EFSA, C-615/13 P, EU:C:2015:489.

s kasačním opravným prostředkem. Soudní dvůr připomněl, že obecný odkaz na zásadu otevřenosti nepostačuje ke splnění tohoto požadavku nezbytnosti, neboť obecně neexistuje žádná automatická přednost cíle transparentnosti před právem na ochranu osobních údajů. Zopakoval dvoustupňový test pro předávání osobních údajů: 1. Žadatel o informace musí nejprve prokázat nezbytnost. 2. Pokud se prokáže, že předání údajů je nezbytné, musí dotyčný orgán ověřit, že není důvod domnívat se, že mohou být dotčeným předáním poškozeny legitimní zájmy subjektu údajů. Soudní dvůr nicméně poznamenal, že žalobci založili svůj spor na přesném obvinění z podjatosti, které vycházelo ze studie prokazující, že si úřad najal odborníky s vazbami na průmyslnickou lobby. Soud dospěl k závěru, že nakonec bylo nezbytné zveřejnit jména těchto odborníků, aby bylo možné konkrétně ověřit nestrannost odborníků při plnění jejich odborných úkolů pro EFSA. Tribunál proto podle něj rozhodl nesprávně, když usoudil, že argumenty organizací nepostačují k prokázání nezbytnosti předání sporných informací.

4.2 Srovnání právní úpravy v nařízení GDPR s úpravou ve směrnici 95/46 a v trestněprávní směrnici

Dříve platná unijní právní úprava v podobě směrnice 95/46 upravovala právo na přístup k osobním údajům v čl. 12 písm. a)[172] a v recitálech 41 až 43 této směrnice. Tato úprava byla již na první pohled lakoničtější, zatímco dnešní článek 15 GDPR nabízí úpravu mnohem podrobnější a přesnější. Detailní rozbor článku 15 GDPR bude uveden v následujících kapitolách této práce. Ve stručnosti lze ale říct, že podle článku 15 GDPR má subjekt údajů

[172] Článek 12 - Právo na přístup

„Členské státy zaručí každému subjektu údajů právo získat od správce:

a) bez omezení, v rozumných intervalech a bez prodlení nebo nadměrných nákladů:

– potvrzení, že údaje, které se ho týkají, jsou či nejsou zpracovávány, jakož i informace týkající se alespoň účelů zpracování, kategorií údajů, na které se zpracování vztahuje, a příjemců nebo kategorií příjemců, kterým jsou údaje sdělovány,

– sdělení srozumitelnou formou o údajích, které jsou předmětem zpracování, a veškeré dostupné informace o původu údajů,

– oznámení postupu automatického zpracování údajů, které se ho týkají, alespoň v případě automaticky přijímaných rozhodnutí uvedených v čl. 15 odst. 1;

b) podle daného případu opravu, výmaz nebo blokování údajů, jejichž zpracování není v souladu s touto směrnicí, zejména z důvodů neúplné nebo nepřesné povahy údajů;

c) oznámení třetí osobě, které údaje byly sděleny, veškerých oprav, výmazů nebo blokování provedeného v souladu s písmenem b), pokud se to neukáže jako nemožné nebo to nevyžaduje nepřiměřené úsilí.“

právo požadovat po správci, aby mu sdělil informaci o tom, zda zpracovává osobní údaje, které se ho týkají. Pokud správce údaje zpracovává, má subjekt údajů právo tyto osobní údaje a informace o zpracování obdržet. V porovnání s tím článek 12 směrnice 95/46 obsahoval nejen samotné právo na přístup, ale také další práva subjektů údajů v podobě práva na opravu, práva na výmaz a práva na blokování údajů, uvedená pod písmenem b). Článek 12 písm. a) směrnice 95/46 členským státům ukládal povinnost zaručit subjektům údajů „právo získat od správce" tři druhy informací: I) potvrzení, že osobní údaje jsou zpracovávány či nikoli, a podrobnosti o zpracování, včetně jejich účelů, kategorií zpracovávaných údajů a příjemců nebo kategorií příjemců údajů; II) sdělení srozumitelnou formou o osobních údajích, které jsou předmětem zpracování; a III) znalost postupu jakéhokoli automatizovaného zpracování týkajícího se subjektu údajů, „alespoň", pokud vede k rozhodnutí, které vůči němu zakládá právní účinky nebo se ho významně dotýká.

Důležitost práva na přístup podle čl. 12 písm. a) směrnice 95/46 uznal Soudní dvůr Evropské unie ve svém rozsudku *Rijkeboer*[173]. Soudní dvůr se v tomto případě vyjádřil jednak k rozsahu práva na přístup, jednak k tomu, zda je přípustné časové omezení práva na přístup. Pan M. Rijkeboer požádal obecní úřad v Rotterdamu o poskytnutí přístupu k informacím o sdělování jeho osobních údajů třetím osobám v průběhu dvou předcházejících let, konkrétně k totožnosti těchto osob a obsahu informací, jež jim byly předány. Tuto žádost podal proto, že chtěl vědět, komu byla sdělena jeho předchozí adresa bydliště. Bylo mu vyhověno pouze částečně, když mu byly sděleny informace týkající se pouze období jednoho roku před podáním žádosti, neboť starší informace byly již z informačního systému vymazány. Nizozemský soud (Raad van State) podal k Soudnímu dvoru předběžnou otázku, zda zákonem stanovené omezení práva osoby na přístup je v souladu se směrnicí. Soudní dvůr při posouzení přiznal zásadní význam účelu tohoto ustanovení, a to je umožnit výkon dalších práv subjektů údajů. Právo na přístup se tak musí podle něj vztahovat i k minulosti. Pokud jde o stanovení lhůty, je třeba vzít v úvahu skutečnosti, jako je více či méně citlivá povaha základních údajů, doba jejich uchovávání a počet dotčených příjemců. Členské státy mají zajistit spravedlivou rovnováhu jednak mezi zájmem subjektu údajů na ochraně jeho soukromí a jednak zátěží, kterou pro správce představuje jeho povinnost tyto informace uchovávat. Soud dospěl k závěru, že v projednávaném případě nebylo dosaženo této spravedlivé rovnováhy, když základní údaje

[173] Rozsudek ze dne 7. května 2009, Rijkeboer, C-553/07, EU:C:2009:293.

byly uchovávány mnohem déle než údaje o příjemcích nebo kategoriích příjemců a obsahu předaných informací.[174]

Ve srovnání se směrnicí 95/46 tak nařízení GDPR rozšířilo povinné kategorie informací, které musejí být poskytnuty na základě žádosti subjektů údajů o přístup. Směrnice 95/46 totiž neurčovala žádné další podrobnosti: například pokud jde o způsoby výkonu tohoto práva; formu, v níž by měly být osobní údaje sdělovány; požadavky na ověření totožnosti žadatele o osobní údaje nebo lhůty pro odpověď na žádosti. Směrnice 95/46 byla do našeho vnitrostátního práva transponována do § 12 zákona č. 101/2000 Sb., o ochraně osobních údajů. Nařízení GDPR obsahuje širší rozsah poskytovaných informací a také právo na jednu bezplatnou kopii osobních údajů. Směrnice 95/46 ve své textaci vůbec ustanovení o poskytnutí kopie neobsahovala, ale odkazovala pouze na „sdělení o údajích, které jsou předmětem zpracování". Směrnice 95/46 proto neupravovala ani ustanovení o bezplatném poskytnutí první kopie zpracovávaných osobních údajů a některé členské státy EU včetně ČR tak do svých právních řádů zakomponovaly možnost stanovit poplatek za využití tohoto práva. Podle § 12 odst. 3 českého zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, bylo možné požadovat za poskytnutí informace přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace. Tento postup jistě nebyl vůči subjektům údajů nejvstřícnější a mohl do jisté míry odrazovat subjekty údajů od podávání žádostí o přístup. Některé státy EU proto výši takového poplatku regulovaly, např. Velká Británie stanovila maximální poplatek 10 liber za žádost. Otázkou poplatkové povinnosti a dalšími podmínkami výkonu práva na přístup se ostatně zabýval i Soudní dvůr EU ve svém starším rozsudku ve věci *X*.[175] Soudní dvůr v první řadě rozhodl, že k výkonu práva na přístup musí docházet bez omezení, bez nepřiměřeného prodlení a bez nadměrných nákladů. Jinak je na členských státech, které požadují úhradu poplatků protihodnotou za výkon práva na přístup k informacím uvedeným v čl. 12 písm. a) směrnice 95/46, aby určily výši těchto poplatků. Určení výše poplatků ale musí proběhnout takovým způsobem, že zajistí spravedlivou rovnováhu mezi zájmem subjektu údajů na ochraně jeho soukromí, zejména prostřednictvím jeho práva na sdělení údajů srozumitelnou formou, aby případně mohl využít svého práva na opravu, výmaz nebo zablokování údajů v případě nesouladu zpracovávání těchto údajů s uvedenou směrnicí,

[174] POKORNÁ, Andrea, DVOŘÁKOVÁ, Helena. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer ČR, 2020, 352 s. ISBN 978-80-7598-309-1.
[175] Rozsudek ze dne 12. prosince 2013, X, C-486/12, EU:C:2013:836.

jakož i práva na námitku a na podání soudní žaloby, na straně jedné, a zátěží, kterou pro správce představuje povinnost tyto informace sdělit, na straně druhé.

Nařízení GDPR od tohoto poplatku upustilo a výslovně zakotvilo v čl. 15 odstavci 3 právo na první bezplatnou kopii osobních údajů. Možnost správce účtovat přiměřený poplatek je stanovena v tomto odstavci až pro případné další kopie, které by subjekt žádal, s tím, že by poplatek měl reflektovat skutečné administrativní náklady. Lze proto očekávat, že právě tato změna povede ke zvýšení počtu žádostí o přístup k osobním údajům.[176]

Na základě provedené srovnávací analýzy deseti vnitrostátních právních předpisů, kterými byla směrnice 95/46 transponována, se zjistilo, že na vnitrostátní úrovni existovaly podstatné rozdíly, pokud šlo o způsob výkonu práva na přístup. Například v některých zemích mohly subjekty údajů předkládat své žádosti pouze písemně (Belgie, Maďarsko, Slovensko a Velká Británie), zatímco jiné země umožnily méně formální způsoby výkonu práva na přístup (Itálie, Rakousko nebo Česká republika)[177]. Existovaly rovněž rozdíly, pokud jde o lhůty pro odpověď na žádosti, a to od lhůty 15 dnů v Itálii, lhůty 30 dnů v Norsku, Španělsku, Maďarsku, Slovensku, lhůty 40 dnů ve Velké Británii, lhůty 45 dnů v Belgii až po lhůtu 56 dnů v Rakousku. Země jako Německo, Lucembursko a Česká republika žádnou konkrétní lhůtu vymezenou neměly.[178] Český zákon o ochraně osobních údajů pouze stanovil povinnost správce poskytnout subjektu údajů na jeho žádost a bez zbytečného odkladu informaci o zpracovávaných osobních údajích, které se ho týkají. Formulaci „*bez zbytečného odkladu*“ bylo nutné posuzovat s ohledem na rozsah, množství informací a možnosti správce požadovanou informaci vyhledat. Předpokládala se ovšem lhůta v řádu dní.[179]

---

[176] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.

[177] Podle italských právních předpisů bylo možné žádosti o přístup předkládat „bez jakýchkoliv zvláštních formalit“. V Rakousku se předpokládalo, že se žádosti o přístup budou obvykle podávat písemně správci údajů, nicméně ustanovení § 26 rakouského zákona o ochraně údajů umožňovalo i ústní podání takové žádosti se souhlasem správce údajů. Podle § 12 českého zákona o ochraně osobních údajů nebyla upravena forma žádosti o informace, vycházelo se tak z toho, že subjekt údajů byl oprávněn podat svoji žádost jakýmkoliv právem uznávaným způsobem, tj. když se žádost dostala do sféry vlivu správce. Žádost tak v zásadě bylo možné podat písemně, elektronicky, telefonicky nebo i např. osobně přímo u správce.

[178] GALETTA, Antonella, DE HERT, Paul, L'HOIRY, Xavier and NORRIS, Clive, 2017. Mapping the Legal and Administrative Frameworks of Informational Rights in Europe: A Cross-European Comparative Analysis. In: *The Unaccountable State of Surveillance*. Law, Governance and Technology Series, vol 34. Springer Cham, s. 22 (457–478). Online. ISBN 978-3-319-47573-8. Dostupné z: https://doi.org/10.1007/978-3-319-47573-8_15. [cit. 2022-03-07].

[179] POSPÍŠIL, Daniel, 2012. § 12 Přístup subjektu údajů k informacím. In: KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. *Zákon o ochraně osobních údajů*. 1. vydání. Online. Praha: C. H. Beck, 536 s. (s. 222). ISBN 978-80-7179-226-0. Dostupné z: databáze Beck online. [cit. 2022-03-07].

Pokud jde o reakci Evropské komise, tak její první zpráva z roku 2003 hodnotící provádění směrnice 95/46[180] nezmiňovala žádné větší problémy s transpozicí této směrnice a vyznívala vcelku příznivě. Její přístup se ovšem v následujících letech změnil a poukazoval více na rozdílnosti v transpozici. V roce 2010 již obsahovalo sdělení Komise k implementaci rámce ochrany osobních údajů [181] konkrétní výzvy k posílení individuálních práv subjektů údajů, včetně práva na transparentnost. Komise byla poměrně kritická – kritizovala zejména, že: „*Způsob jejich výkonu ale není harmonizován, a proto je v některých členských státech skutečný výkon těchto práv snazší než v jiných. Mimoto je zvlášť problematický v online prostředí, kde jsou údaje často uchovávány, aniž by o tom dotčená osoba byla informována anebo k tomu poskytla souhlas. Zvlášť dobrým příkladem jsou internetové sociální sítě, které mohou výrazně ohrožovat možnost fyzické osoby účinně kontrolovat své osobní údaje. Komise obdržela několik dotazů od osob, kterým se nepodařilo získat tyto údaje od poskytovatelů internetových služeb (například své fotografie), a jimž tak bylo zabráněno ve výkonu práva na přístup, opravu a vymazání údajů. Tato práva by proto měla být vyjádřena explicitněji, objasněna a případně posílena*.“

V roce 2016 bylo přijato nařízení GDPR, které nahradilo směrnici 95/46. Je výsledkem náročného procesu vyjednávání, který zahrnoval četné změny právního textu a který trval čtyři roky, než bylo přijato konečné znění nařízení. Roztříštěnost ochrany osobních údajů v jednotlivých členských státech EU a z ní vyplývající právní nejistota byly považovány za překážku výkonu ekonomických aktivit na úrovni EU. Dá se říct, že směrnice přestala odpovídat potřebám vyplývajícím z vnitřního trhu, docházelo ke značnému nárůstu přeshraničních toků osobních údajů. Nařízení je oproti směrnici přímo použitelným právním předpisem. EU si od sjednocení pravidel pro ochranu osobních údajů slibovala především větší právní jistotu a odstranění potenciálních překážek volného pohybu údajů. V tomto smyslu lze souhlasit, že nařízení je určitě vhodnější formou regulace pro tuto oblast, umožňuje totiž posílit důvěru lidí v odpovědné zacházení s jejich osobními údaji a posílit právní postavení subjektů údajů.[182] Také autorka této práce má za to, že nařízení poskytuje robustnější právní ochranu

[180] EC Report 2003: *Report from the Commission: First report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, 15 May 2003.
[181] EC Communication 2010: *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, 4 November 2010.
[182] VOIGT, Paul a VON DEM BUSSCHE, Axel, 2017. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, s. 180-187. Online. ISBN 978-3-319-57959-7. Dostupné z: https://doi.org/10.1007/978-3-319-57959-7. [cit. 2024-09-04].

subjektů údajů než směrnice a díky své přímé závaznosti umožňuje, aby v rámci EU nedocházelo k výrazným rozdílům.

Pro úplnost ještě rozeberu, jak je právo na přístup regulováno v oblasti vymáhání práva, konkrétně v oblasti trestního řízení. Zpracování osobních údajů v kontextu vyšetřování a stíhání trestné činnosti je upraveno ve směrnici Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (dále jen „trestněprávní směrnice“). Tato směrnice byla představena jako součást balíčku opatření EU pro reformu ochrany údajů společně s obecným nařízením o ochraně osobních údajů a jejím hlavním deklarovaným cílem bylo zajistit lepší ochranu osobních údajů v souvislosti s jejich zpracováním policií a orgány činnými v trestním řízení. Trestněprávní směrnice je *lex specialis* ve vztahu k nařízení GDPR, což je dáno specifickou povahou činností v oblasti trestního řízení. To ostatně vyplývá i z recitálu 19 nařízení GDPR a recitálu 11 trestněprávní směrnice. Recitál 19 nařízení GDPR uvádí, že toto nařízení by se nemělo uplatňovat na činnosti zpracování za těmito účely, a že na toto zpracování by se měl vztahovat konkrétnější právní akt Unie, totiž (trestněprávní) směrnice Evropského parlamentu a Rady (EU) 2016/680. Trestněprávní směrnice v recitálu 11 ovšem vysvětluje, že pokud orgán nebo subjekt jiný než příslušný orgán (zde typicky soukromoprávní subjekt) původně shromažďuje osobní údaje pro jiné účely a tyto údaje dále zpracovává pro účely vyšetřování, odhalování nebo stíhání trestných činů, i když na základě zákonné povinnosti, bude se na takové zpracování rovněž vztahovat nařízení GDPR.

Právo subjektu údajů na přístup k osobním údajům je v trestněprávní směrnici upraveno v článku 14[183]. Článek 14 má podobnou, i když trochu jednodušší strukturu v porovnání

[183] Článek 14 - Právo subjektu údajů na přístup k osobním údajům

„S výhradou článku 15 členské státy stanoví, že subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:

a) účely a právní základ zpracování;
b) kategorie dotčených osobních údajů;
c) příjemci nebo kategorie příjemců, kterým byly osobní údaje zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;
d) pokud možno předpokládaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování;
f) právo podat stížnost u dozorového úřadu a kontaktní údaje tohoto úřadu;

s článkem 15 GDPR. Subjekt údajů má právo získat od správce (jímž je v tomto případě orgán činný v trestním řízení) I) potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány (tedy pozitivní nebo negativní potvrzení o zpracování jeho osobních údajů); II) v případě pozitivního potvrzení, má právo získat přístup k těmto osobním údajům a III) poskytnutí informací, přičemž následuje výčet těchto informací. Tento výčet je v zásadě shodný s výčtem upraveným v článku 15 odst. 1 GDPR s jednou výjimkou, a sice, že nezahrnuje právo znát postup automatizovaného zpracování, jehož výsledkem je rozhodnutí nepříznivě ovlivňující subjekt údajů. Při bližším zkoumání však zjistíme, že rozhodnutí založená výhradně na automatizovaném zpracování, která mají pro subjekt údajů nepříznivé právní účinky, jsou také výslovně zakázána, jen na jiném místě, konkrétně v čl. 11 odst. 1 trestněprávní směrnice, nejsou-li taková rozhodnutí povolena právem EU nebo právem členského státu. Pracovní skupina WP29 ve svém doporučujícím materiálu k článku 14 trestněprávní směrnice zdůrazňuje, že subjektu údajů musí být v zásadě vždy poskytnuto alespoň negativní potvrzení o tom, že jeho osobní údaje zpracovávány nejsou. Politika „nepotvrdit ani nevyvrátit tyto informace“ je možná pouze v případě výjimek (omezení) podle článku 15. Informace by dále měly být poskytnuty bezplatně a bez zbytečného odkladu. Směrnice nedefinuje, co v tomto smyslu znamená pojem „bez zbytečného odkladu“, pracovní skupina WP29 však zastává názor, že by správce měl subjektu údajů poskytnout informace v reakci na žádost podle článku 14 co nejdříve, pokud možno do jednoho kalendářního měsíce. Správce subjektu údajů poskytne a sdělí tyto informace stručným, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, jak je uvedeno v čl. 12 odst. 1. této směrnice. Seznam informací, které musí správce uvést v reakci na žádost o právo na přístup, zahrnuje mimo jiné informace o příjemcích nebo kategoriích příjemců, kterým byly osobní údaje zpřístupněny. Směrnice ale neobjasňuje, jak konkrétní musí správce být při poskytování těchto informací. Pracovní skupina v tomto smyslu připomíná podstatu práva na přístup, kterou je možnost subjektu údajů získat potvrzení právního základu a ověřit, zda jsou údaje zpracovávány dovoleným (zákonným) způsobem. Správci by proto měli zajistit, aby byly poskytnuté informace přesné, jasné a dostatečné k dosažení tohoto účelu. Ačkoli článek 14 výslovně neobsahuje zmínku o právu na kopii, podle názoru pracovní skupiny by správce měl v rámci žádosti o přístup takovou kopii poskytnout, pokud je předmětem žádosti a pokud je to možné. V tomto smyslu je vhodné upozornit i na bod 43 odůvodnění trestněprávní směrnice,

g) sdělení osobních údajů, které jsou předmětem zpracování, a veškerých dostupných informací o jejich původu.“

který uvádí, že je možné k dodržení tohoto práva na přístup poskytnout subjektu údajů přehled jeho údajů ve srozumitelné formě.[184]

Článek 15 trestněprávní směrnice pak upravuje omezení práva na přímý přístup – tj. umožňuje členským státům omezit „zcela nebo částečně" právo subjektu údajů na přístup z několika důvodů, mimo jiné s cílem zabránit narušení prevence, odhalování, vyšetřování či stíhání trestných činů nebo výkonu trestů a chránit práva a svobody druhých. Nutno doplnit, že omezení práva na přístup je zákonné pouze „v takovém rozsahu a na takovou dobu", kdy představuje „nutné a přiměřené opatření v demokratické společnosti s náležitým přihlédnutím k základním právům a oprávněným zájmům dotčené fyzické osoby". Nejedná se tedy o „plošné" omezení. V těchto případech má subjekt údajů obvykle právo být informován o omezení přístupu, důvodech tohoto omezení a o možnosti podat stížnost dozorovému úřadu nebo se obrátit na soud. Taktéž zde platí, že správce informuje písemně subjekt údajů bez zbytečného odkladu, tj. pokud možno, do jednoho kalendářního měsíce od obdržení žádostí. V odpovědi může správce vynechat důvody omezení, pouze pokud by poskytnutí této informace ohrožovalo některý z právem chráněných účelů podle čl. 15 odst. 1. Pracovní skupina WP29 k povaze omezení v článku 15 připomíná, že by se jakékoli výjimky ze základních práv a oprávněných zájmů fyzické osoby měly vykládat a uplatňovat restriktivně, nikoli jako pravidlo, a zdůrazňuje, že neposkytnutí informací může být v rámci vyšetřování přípustné pouze tehdy, splňuje-li požadavky nezbytnosti a přiměřenosti. Stejně tak, v souladu s posudkem a judikaturou Soudního dvora Evropské unie[185], jakmile již nemohou tyto informace ohrozit probíhající vyšetřování, tak musí být subjektu údajů poskytnuty. V případě, že právo subjektu údajů na přístup bylo omezeno pouze částečně a odpověď lze poskytnout, je třeba, aby správce dostál své povinnosti a umožnil subjektu údajů přístup ke zpracovávaným osobním údajům a informacím. Dále platí, že je-li to možné, měly by být informace poskytnuty ve stejné formě jako žádost. Správce má navíc u omezení práva na přístup povinnost podle čl. 15 odst. 4 zdokumentovat věcné či právní důvody, na nichž se takové rozhodnutí o omezení zakládá, a tyto informace na žádost zpřístupnit dozorovým úřadům.

Transparentnost zpracování osobních údajů podpořená právem na přístup nepředstavuje pro subjekt údajů pouze „právo vědět", nýbrž je dále posílena právem na opravu nebo výmaz

[184] WP29. *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, wp258, Adopted on 29 November 2017. Dostupné zde: https://ec.europa.eu/newsroom/article29/items/610178/en.
[185] Posudek 1/15 Soudního dvora (velkého senátu) k návrhu dohody mezi EU a Kanadou o předávání údajů jmenné evidence cestujících ze dne 26. července 2017, EU:C:2017:592, body 218 až 220 a 223 až 225. Dále rozsudek ze dne 21. prosince 2016, Tele2 Sverige, spojené věci C-203/15 a C-698/15, EU:C:2016:970, bod 121 a citovaná judikatura.

osobních údajů nebo na omezení zpracování, jak je stanoveno v článku 16 trestněprávní směrnice. Jistou zvláštnost, v porovnání s nařízením GDPR, nabízí článek 17 trestněprávní směrnice, upravující fakticky právo na „nepřímý přístup“. Ve skutečnosti má však své opodstatnění. Pokud právní předpisy umožňují subjektu údajů omezit práva na získání informací, přístup nebo opravu/výmaz osobních údajů, má subjekt údajů (alespoň) právo na „nepřímý přístup“. V těchto případech musí vnitrostátní právní předpisy alespoň zachovat možnost výkonu práva na informace, na přístup nebo na informace o odmítnutí opravy nebo výmazu osobních údajů prostřednictvím příslušného dozorového úřadu. Toto právo tak v rámci trestněprávní směrnice představuje samostatné dodatečné právo a je třeba jej odlišit od práva na podání stížnosti dozorovému úřadu nebo práva žádat soudní ochranu. Je třeba jej pokládat za dodatečnou záruku, která je subjektům údajů poskytnuta pouze v rámci trestněprávní směrnice, neboť nařízení GDPR tuto možnost v případě omezení práv nestanoví. Podle čl. 17 odst. 3 musí příslušné dozorové úřady podílející se na výkonu tohoto práva subjekt údajů informovat přinejmenším o tom, že provedly veškerá nezbytná ověření nebo přezkum, a o právu subjektu údajů žádat soudní ochranu. Závěrem ještě pracovní skupina WP29 doporučuje, aby nejlépe samotní správci, případně dozorové úřady, vedli evidenci těchto žádostí o „nepřímý přístup“.[186]

Směrnice 95/46 umožňovala členským státům vyšší míru flexibility než současné nařízení GDPR. Nedokázala ale zajistit účinnou ochranu osobních údajů v celé Unii a především vysokou úroveň ochrany fyzických osob, subjektů údajů. Nařízení tato práva subjektů údajů posílilo (zavedlo například nově právo na přenositelnost údajů) a současně vytvořilo vhodný „tlak“ na správce, aby uspořádali své interní postupy v oblasti ochrany údajů a dosáhli tak souladu s nařízením. Zakotvilo totiž širokou oblast působnosti, výrazně navýšilo povinnosti správců (zavedlo například povinnost správce vést záznamy o zpracování údajů, za určitých okolností jmenovat pověřence pro ochranu osobních údajů a respektovat zásadu odpovědnosti) a stanovilo oprávnění dozorových úřadů ukládat za závažná porušení vysoké pokuty. To ovšem neznamená, že by regulace v podobě nařízení byla bezchybná. Již ze samotného názvu nařízení (obecné nařízení o ochraně osobních údajů) je jasné, že jedním z problematických aspektů je jeho značná „obecnost“. Nařízení totiž umožňuje členským státům v řadě případů přijmout speciální odchylnou úpravu (více v kapitole 5.3 Omezení práva na přístup). Konkrétně u práva na přístup neupravuje ani nařízení, ani v našem případě český

[186] WP29. *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, wp258, Adopted on 29 November 2017. Dostupné zde: https://ec.europa.eu/newsroom/article29/items/610178/en.

zákon o zpracování osobních údajů nějaké podrobnější podmínky pro podání a vyřízení žádosti o přístup, pouze v několika případech je upraveno omezení z práva na přístup.

Při srovnání nařízení GDPR a trestněprávní směrnice je základním rozdílem, kromě jiné formy zvoleného právního aktu, specifická povaha účelů směrnice. Směrnice má za cíl chránit osobní údaje shromážděné a zpracovávané pro účely trestního soudnictví, ke kterým patří za a) prevence, vyšetřování, odhalování či stíhání trestných činů, za b) výkon trestu a za c) případy, kdy policie a jiné donucovací orgány jednají za účelem dodržování práva a za účelem ochrany před hrozbami pro veřejnou bezpečnost. Jiná forma právního aktu byla zvolena z toho důvodu, že na rozdíl od zpracováním údajů pro obchodní účely, které je upraveno nařízením, bude zpracování pro bezpečnostní účely vyžadovat určitou míru flexibility. Směrnice také, na rozdíl od nařízení, nechrání osobní údaje všech fyzických osob, ale jednotlivců, kteří jsou účastníky trestního řízení, jako jsou svědci, informátoři, oběti, podezřelí a spolupachatelé. Příslušnými orgány působícími v oblasti policie a trestního soudnictví jsou orgány veřejné moci nebo orgány zmocněné vnitrostátním právem a veřejnou mocí. Směrnice do značné míry vychází ze zásad a definic uvedených v nařízení GDPR, zohledňuje nicméně zvláštní povahu policejního sektoru a sektoru trestního soudnictví. Směrnice, z důvodů své specifické povahy, poskytuje o něco nižší úroveň ochrany, pokud jde o právo na informace, právo na přístup k osobním údajům či jejich výmaz. Je to dáno důležitostí veřejného zájmu, který je u této směrnice pro činnosti policejního sektoru a sektoru trestního soudnictví dán. V konkrétní situaci sledování a zpracování osobních údajů pro účely trestního soudnictví může být tedy právo na přístup omezeno v podstatně větší míře.

4.3 Komparativní analýza geneze a implementace práva na přístup v právním řádu Německa, Francie a Velké Británie

Potřeba zaměřit se na ochranu lidských práv a svobod v souvislosti s automatizovaným zpracováním osobních údajů se objevila již koncem 60. let. Jedná se o období začátku užívání počítačové techniky pro účely správy ve veřejném a soukromém sektoru. Zpočátku byla počítačová technika dostupná jen ve vyspělých zemích a zpravidla sloužila pro veřejné instituce nebo velké korporátní společnosti. Mezi hlavní účely náležely: vedení mzdové, platové a personální agendy; vedení pacientských záznamů/ zdravotnické dokumentace v nemocnicích; veřejná sčítání lidu a statistické účely a také policejní spisy. Počátky práva na přístup lze v USA vystopovat již v 60. letech minulého století, individualizovaný přístup byl totiž vnímán jako

důležitá pojistka v souvislosti s rostoucím automatizovaným zpracováním dat ve velkém měřítku. Debata ohledně ochrany osobních údajů se začala více objevovat začátkem 70. let 20. století, a to zejména v Německu (ve spolkové zemi Hesensko), v Norsku, ve Švédsku, ve Francii (zde v souvislosti na stále živé vzpomínky na rozsáhlé nacistické spisy a záznamy z druhé světové války), ve Velké Británii a v USA. Jak v Evropě, tak v USA byly formulovány různé koncepce práva na přístup, od obecného práva vědět, že jsou osobní údaje zpracovávány, až po mnohem podrobnější „právo na kopii" (tj. právo automaticky dostávat všechny své informace v pravidelných intervalech). Ačkoli se v té době podrobnější pojetí práva na přístup nesetkalo s velkou podporou, bylo právě v této podobě později začleněno do Úmluvy Rady Evropy č. 108[187]. Nejrozšířenější formou „přístupu" v členských státech EU v oblasti ochrany údajů však bylo „právo být informován na požádání". Ačkoli měly vnitrostátní právní předpisy o ochraně osobních údajů podobné „základy", pochopitelně se začaly objevovat určité zvláštnosti. Rozdíly mezi jednotlivými státy, včetně oblasti práva na přístup, se odvíjí od různých historických a právních tradic. Prvním zákonem o ochraně osobních údajů byl zákon vydaný ve spolkové zemi Hesensko v roce 1970[188], který však měl omezenou územní působnost, neboť platil pouze v této spolkové zemi. Prvním celostátním zákonem o ochraně osobních údajů tak byl švédský zákon z roku 1973[189]. Do konce 80. let pak s přijetím právních předpisů ochrany osobních údajů následovaly i další evropské země (Francie, Německo, Nizozemsko a Velká Británie).[190] Některé země v této době právo na ochranu osobních údajů zakotvily dokonce i ústavně.[191] Na následujících řádcích blíže přiblížím jak etablování práva na ochranu osobních údajů, tak implementaci unijních pravidel v Německu, Francii a Velké Británii.

Německo

[187] AUSLOOS, Jef a DEWITTE, Pierre, 2018. Shattering One-Way Mirrors. Data Subject Access Rights in Practice. Online. *International Data Privacy Law*. March 2018, Volume 8, Issue 1, s. 25 (4–28). Dostupné z: https://doi.org/10.1093/idpl/ipy001. [cit. 2024-07-12].
[188] Datenschutzgesetz. Zákon o ochraně osobních údajů vydaný ve spolkové zemi Hesensko v roce 1970. Dostupné zde: https://starweb.hessen.de/cache/GVBL/1970/00041.pdf. [cit. 2024-08-24].
[189] Datalagen. Zákon o datech č. 289 z 11. května 1973. Dostupné zde: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289/. [cit. 2024-08-24].
[190] FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2022-07-18]
[191] Portugalsko (článek 35 portugalské ústavy z roku 1976), Španělsko (článek 18 španělské ústavy z roku 1978) a Rakousko (článek 1 rakouského zákona o ochraně údajů z roku 1978).

V Německu byla právní ochrana osobních údajů zpočátku úzce propojena se zásadou informační autonomie a sebeurčení. Tyto dvě zásady se zakořenily v německém právním systému po tzv. nálezu Ústavního soudu (*Bundesverfassungsgericht*) ke sčítání lidu z roku 1983[192], který lze považovat za přelomové rozhodnutí pro právní předpisy v oblasti ochrany údajů nejen v Německu, ale i dalších evropských zemích jako je Maďarsko, Slovensko a Estonsko. [193] Prvním celostátním zákonem v Německu byl federální zákon o ochraně osobních údajů (*Bundesdatenschutzgesetz*) z roku 1977[194]. Ten prošel četnými novelizacemi a je platný dodnes. Právo na přístup bylo ve znění německého zákona z roku 1977 zakotveno v § 4 odst. 1, který stanovil, že subjekt údajů má právo na „*informace o osobních údajích, které jsou uchovávány o jeho osobě*“[195]. Zákon tak fakticky zakotvil právo na transparentnost s prvky ze současného pojetí práva na informace a práva na přístup. Ustanovení § 4 bylo velmi stručné a ve zbylých odstavcích obsahovalo další práva subjektů údajů – právo na opravu (§ 4 odst. 2), právo na blokování údajů (§ 4 odst. 3) a právo na výmaz (§ 4 odst. 4). Další podrobnosti jako je například právo na přístup ke kopii osobních údajů ale ustanovení neobsahovalo.[196]

Ráda bych se ještě vrátila zpět k nálezu Ústavního soudu ke sčítání lidu z roku 1983. V roce 1983 německá federální vláda plánovala provést sčítání obyvatel. V německé společnosti ovšem panovaly velké obavy ze státem organizovaného sledování a pocit, že by takové statistické sčítání v důsledku vedlo k neodůvodněnému zásahu do soukromí. Případ se tak dostal až před federální Ústavní soud, který rozhodl, že zákon o sčítání lidu je protiústavní a zrušil jej, čímž došlo i k ukončení sčítání lidu, které bylo obnoveno až o 4 roky později. Nález je významný tím, že v něm Ústavní soud poprvé vymezil základy právní úpravy ochrany osobních údajů v německé Ústavě (*Grundgesetz*), v podobě základního práva na informační sebeurčení. Ústavní soud v Německu na tento nález s ohledem na jeho komplexní argumentaci

---

[192] Bundesverfassungsgericht. BVerfG. Rozsudek prvního senátu Ústavního soudu ze dne 15. prosince 1983 – 1 BvR 209/83; BVerfGE 65, 1 (1983). Dostupné z: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html;jsessionid=32644501620FBA0356ACCB64EA7006A5.internet962.

[193] GALETTA, Antonella, DE HERT, Paul, L'HOIRY, Xavier and NORRIS, Clive, 2017. Mapping the Legal and Administrative Frameworks of Informational Rights in Europe: A Cross-European Comparative Analysis. In: *The Unaccountable State of Surveillance*. Law, Governance and Technology Series, vol 34. Springer Cham, s. 22 (457–478). Online. ISBN 978-3-319-47573-8. Dostupné z: https://doi.org/10.1007/978-3-319-47573-8_15. [cit. 2022-03-07].

[194] Bundesdatenschutzgesetz. *Federální zákon o ochraně osobních údajů z 27. ledna 1977*. Dostupné zde: https://offenegesetze.de/veroeffentlichung/bgbl1/1977/7#page=1. [cit. 2024-08-24].

[195] § 4 - Rechte des Betroffenen:
„Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf:
(1). Auskunft über die zu seiner Person gespeicherten Daten,..“

[196] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

a četné právní i sociologické úvahy dodnes často odkazuje. Od té doby je základním kritériem pro nakládání s osobními údaji (ze strany orgánů veřejné správy i soukromých zpracovatelů) právo jednotlivce svobodně rozhodnout o použití svých vlastních údajů. Subjekt údajů má mít i nadále kontrolu nad svými vlastními údaji. Funkcí soukromí je dle soudu zejména důsledná ochrana individuality jednotlivce, přičemž důsledné sebevyjádření do značné míry závisí na oddělení společenských subsystémů. Soukromí a informační sebeurčení chrání tyto dělící linie, protože brání tomu, aby se citlivé informace z jedné oblasti (např. z profesní oblasti, lékařské péče, rodinného života atd.) propojily s jinými. Ochrana osobních údajů je tedy nezbytná pro svobodný a sebeurčený rozvoj jednotlivce. Zároveň je vývoj jednotlivce na základě sebeurčení předpokladem svobodného a demokratického pořádku. Lze tedy shrnout, že německý koncept práva informačního sebeurčení je velmi odlišný od konceptu soukromí jako „*práva být nechán o samotě*“, jedná se vlastně o výsledek soudcovské tvorby práva, odvozený od základních lidských práv.

V Německu byla ochrana osobních údajů primárně považována za odvozenou ze dvou základních lidských práv, „práva na rozvoj lidské osobnosti“ (*Persönliche Freiheitsrechte*), zaručeného čl. 2 odst. 1 Ústavy ve spojení s „právem na ochranu lidské důstojnosti“ (*Menschenwürde*), zakotveným v čl. 1 odst. 1 Ústavy. Z toho Ústavní soud ve svém nálezu ke sčítání lidu odvodil konkrétně právo na „informační sebeurčení“ (*Informationelle Selbstbestimmung*), které ovšem také zasadil do kontextu širších základních společenských norem: „*Individuální sebeurčení však předpokládá – a to i v podmínkách zpracování informací moderními technologiemi – že je jednotlivci umožněno svobodně se rozhodnout, zda určité kroky podnikne, či nikoli, včetně možnosti se podle tohoto rozhodnutí skutečně zachovat BVerfGE 65, 1 (42)BVerfGE 65, 1 (43). Každý, kdo není schopen s dostatečnou jistotou zjistit, jaké informace jsou o něm v určitých oblastech jeho společenského prostředí známy, a kdo nemůže rozumně posoudit znalosti možných komunikačních partnerů, může být významně omezen ve své svobodě plánovat nebo rozhodovat o vlastním sebeurčení. Společenský a z něj vycházející právní řád, v němž občan již nemůže vědět, kdo co o něm ví a kdy a v jaké situaci, je neslučitelný s právem na informační sebeurčení. Jednotlivec, který se obává, že nekonformní chování může být kdykoli zaznamenáno a poté trvale uloženo v záznamech, používáno nebo šířeno, se bude snažit takovým chováním nepřitahovat pozornost. Pokud jednotlivec očekává, že například jeho účast na setkání nebo občanské iniciativě bude oficiálně zaznamenána, a mohla by jej tak vystavit riziku, může se rozhodnout vzdát se výkonu svých příslušných základních práv (články 8 a 9 Ústavy). To by nejen omezovalo možnosti osobního rozvoje*

jednotlivce, ale mělo by to dopad i na obecné blaho, protože sebeurčení je základním předpokladem svobodné a demokratické společnosti, která je založena na aktivitě a participaci občanů.“[197]

V německém pojetí se klade důraz na dvojí účinky práva na informační sebeurčení a ochrany údajů. Jednotlivec je chráněn před zásahy do osobních záležitostí, čímž si vytváří soukromou sféru, ve které se může cítit v bezpečí před jakýmkoliv zásahem. Formulace se zaměřuje na zveřejňování informací: právo na informační sebeurčení je právo jednotlivce rozhodnout se sám o sobě, kdy a za jakých omezení zveřejnit osobní okolnosti („persönliche lebenssachverhalte“). Ochrana údajů má dle soudu ale i společenský cíl, informační sebeurčení je totiž klíčem k řádnému fungování svobodné a demokratické společnosti, která je založena na účasti jejích občanů. Demokratický právní stát se totiž do značné míry spoléhá na účast všech občanů a jeho legitimita je založena na respektování osobní svobody každého člověka. Právo na informační sebeurčení ani obecné právo na soukromí nejsou výslovně zmíněny v německé Ústavě. Ústavní soud však uznal obecné právo na ochranu osobnosti jako součást Ústavy ještě před přijetím nálezu ke sčítání lidu. Právní základ tohoto práva tedy tvoří dvě samostatná ustanovení Ústavy, a to právo na ochranu lidské důstojnosti (čl. 1 odst. 1) a právo na rozvoj vlastní osobnosti (čl. 2 odst. 1). Společně tyto články tvoří obecné právo na ochranu osobnosti, které každému jednotlivci zaručuje možnost rozvíjet svou vlastní osobnost podle sebe.[198] Klíčovými kritérii pro nakládání s osobními údaji se dle Ústavního soudu staly „nezbytnost“ a „zásada účelového omezení“.

Ústavní soud také v nálezu rozvinul řadu záruk na ochranu občanů před nepřiměřenými zásahy do jejich práva na informační sebeurčení. Vzhledem k tomu, že právo má postavení základního ústavního práva, jsou možné zásahy pouze u obecného právního zájmu (*rechtsgut*) na ústavní rovině. Navíc akty zasahující do práva občana na informační sebeurčení musí být založeny na zmocňovacím aktu, který sám o sobě musí splňovat vysoké standardy srozumitelnosti a určitosti. Za zmínku také stojí pozice Ústavního soudu k osobnostním profilům, které federální vláda plánovala v souvislosti se sčítáním obyvatel vést. Mělo se jednat

[197] Bundesverfassungsgericht. BVerfG. Rozsudek prvního senátu Ústavního soudu ze dne 15. prosince 1983 – 1 BvR 209/83; BVerfGE 65, 1 (1983). K právu na informační sebeurčení, § 146. Dostupné z: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html;jsessionid=32644501620FBA0356ACCB64EA7006A5.internet962.

[198] HORNUNG Gerrit, SCHNABEL Christoph, 2009. Data protection in Germany I: The population census decision and the right to informational self-determination. Online. *Computer Law & Security Review*. November 2008, Volume 25, Issue 1, s. 5 (84-88). ISSN 0267-3649. Dostupné z: https://doi.org/10.1016/j.clsr.2008.11.002. [cit. 2022-03-07].

o propojování údajů z více zdrojů, čímž mohly být generovány dodatečné informace – resp. osobní údaje mnohem citlivějšího charakteru, ještě více odhalující soukromý život obyvatel. Právě tento způsob shromažďování a následného propojování údajů může dle soudu představovat ohrožení práva jednotlivce na informační sebeurčení, kdy ztratí kontrolu nad tím sám rozhodovat o tom, které osobní údaje o sobě zveřejní. Dle dřívějšího nálezu Ústavního soudu, na nějž odkázal: „*Bylo by v rozporu s ústavní zárukou lidské důstojnosti, aby stát mohl využít práva registrovat a indexovat jednotlivce v celé jeho osobnosti, a to i v anonymitě statistického sčítání, protože s jednotlivcem by bylo zacházeno jako s objektem přístupným k inventarizaci ve všech směrech*."[199]

Ústavní soud rovněž v komentovaném nálezu z roku 1983 zakázal zavedení jedinečného osobního identifikátoru pro každého občana. Zde bych ráda připojila ještě poznámku. Německo se po dlouhou dobu (společně s Rakouskem) ostře vymezovalo proti používání jedinečného obecného identifikátoru v rámci veřejného sektoru, tedy obdoby našeho českého rodného čísla. Veřejné orgány využívaly do přijetí zákona o modernizaci rejstříků[200] v rámci příslušné agendy své „vlastní" agendové identifikátory, například číslo sociálního pojištění. Nakonec ale i v Německu přistoupili k variantě obecného, byť bezvýznamového identifikátoru s tím, že základem pro tento jednotný identifikátor je již existující daňové identifikační číslo.

Kromě toho, Ústavní soud v nálezu o sčítání lidu přijal několik zásad ochrany osobních údajů, které lze nyní považovat za klíčové zásady v celé Evropě, neboť všechny byly zakotveny do směrnice 95/46 a následně i do nařízení GDPR. Zejména se jedná o zásadu účelového omezení, minimalizace údajů a přiměřenosti, dále o povinnosti správce údajů a o práva subjektu údajů. Podle soudu by shromažďování neanonymizovaných údajů pro nespecifikované účely nebo účely, které budou upřesněny později, bylo porušením těchto zásad.

Francie

[199] Bundesverfassungsgericht. BVerfG (16. 7. 1969). Beschluss des Ersten Senats vom 16 Juli 1969 – 1 BvL19/63 (*Mikrozenzus*). Jedná se o nález Ústavního soudu z roku 1969, který předcházel nálezu ke sčítání lidu z roku 1983 a na nějž federální Ústavní soud odkázal. Dostupné z: https://openjur.de/u/183523.html. [cit. 2024-08-24].
[200] Registermodernisierungsgesetz. *Zákon o zavedení a používání identifikačního čísla ve veřejné správě a o změně některých zákonů (zákon o modernizaci rejstříků – RegMoG),* dostupné zde: https://www.gesetze-im-internet.de/regmog/BJNR059100021.html. [cit. 2024-08-24].

Pojem soukromí se ve Francii poprvé objevil v zákoně č. 70-643 ze 17. července 1970 o posílení záruky individuálních práv občanů[201]. Zákon obsahoval část nazvanou „ochrana soukromého života“, která změnila § 9 občanského zákoníku (Code Civil) a § 368 trestního zákoníku (Code Pénal) s cílem posílit ochranu soukromí a intimity jednotlivce. Obecnou definici ochrany soukromí však tento zákon, ani pozdější zákon o ochraně osobních údajů č. 78-17 z roku 1978[202] neobsahoval. V roce 1974 došlo ve Francii ke kontroverznímu odhalení plánu vlády vytvořit celostátní databázi všech francouzských státních příslušníků a dalších obyvatel na základě jedinečného identifikátoru. Francouzská vláda vytvořila projekt s názvem SAFARI, což byla zkratka pro „*système automatisé pour les fichiers administratifs et le répertoire des individus*“ (automatizovaný systém správních spisů a rejstříků osob). Projekt SAFARI spočíval v tom, že každému francouzskému občanovi měl být přidělen jedinečný identifikátor, který měl usnadnit komunikaci mezi existujícími veřejnými rejstříky, kde osoba figurovala. V rámci veřejného mínění vzbudil projekt rozruch, v souvislosti s jeho „nešťastně“ zvolenou zkratkou se poukazovalo na to, že předznamenává jakýsi „hon na francouzské občany“. Odhalení tohoto záměru a jeho následná medializace přispěly k tomu, že jen o několik dnů později vláda raději celý projekt zastavila a jmenovala *ad hoc* komisi, která celý problém prozkoumala a navrhla právní řešení. Pod vlivem těchto událostí byl přijat nový zákon a zřízen nový správní úřad Commission nationale de l’Informatique et des Libertés[203], který měl mít na starosti dozor v oblasti zpracování osobních údajů. Význam této problematiky, jakož i úkolů, které byly novému úřadu svěřeny, dokládá i fakt, že tento úřad byl de facto prvním správním úřadem ve Francii, který získal nezávislé postavení („autorité administrative indépendante“). Úřad je tedy oddělen od ostatních orgánů veřejné moci, ani vláda nemá vůči němu žádné kontrolní pravomoci, kromě pravomoci jmenovat 3 z jeho členů. Jeho postavení je natolik specifické, že se někdy hovoří dokonce o „kvazijudiciálním charakteru“, doktrína jeho postavení zase někdy připodobňuje k postavení Veřejného ochránce práv s tím rozdílem, že má na rozdíl od ombudsmana i rozhodovací pravomoc.[204]

[201] Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens (*Zákon č. 70-643 ze dne 17. července 1970 o posílení záruky individuálních práv občanů*). Dostupné zde: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000693897. [cit. 2024-08-24].
[202] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (*Zákon č. 78-17 ze dne 6. ledna 1978 o informačních technologiích, souborech a svobodách*). Dostupné zde: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/. [cit. 2024-08-24].
[203] Doslova Národní komise pro informační technologie a svobody, jde o francouzský úřad pro ochranu osobních údajů.
[204] HOLLEAUX, André, Conseiller d'État. Komentář k „*La Loi Du 6 Janvier 1978 Sur l'informatique et Les Libertés*“. Online. 181/31. La Revue administrative. 1978. [cit. 2024-08-24].

Francie měla svůj zákon o ochraně osobních údajů č. 78-17 od 6. ledna roku 1978 (*Loi relative à l'informatique, aux fichiers et aux libertés*, což lze doslova volně přeložit jako „zákon o informačních technologiích, souborech a svobodách"). Tento zákon prošel několika novelizacemi, ale je stále platný. Základní zásady a definice byly v původním verzi z roku 1978 upraveny v § 1 až 5. Ustanovení § 1 zákona, které je dodnes platné, stanoví: „*Informační technologie musí sloužit každému občanovi. Musí se rozvíjet v rámci mezinárodní spolupráce. Nesmí zasahovat do identity jednotlivce, lidských práv, soukromí ani do osobních či veřejných svobod*." Zákon v tomto ustanovení odkazuje na čtyři základní hodnoty; dvě z nich jsou tradiční – lidská práva a osobní či veřejné svobody, a dvě jsou poměrně nové, pokud jde o jejich vyjádření v legislativním textu: soukromí a identita jednotlivce.[205] Tento zákon byl na rozdíl od německého zákona již ve svém původním znění dosti podrobný. Rozlišoval mezi právem vědět, že osobní údaje jsou zpracovávány automatizovaně a právně je napadnout (ustanovení § 3 zákona)[206] a právem na přístup k osobním údajům[207]. Prvně jmenované ustanovení doslova upravovalo právo každého „*znát a napadnout informace a postupy použité při automatizovaných zpracováních, jejichž výsledky jsou použity proti němu*." Ustanovení § 34 pak zajistilo právo subjektů údajů, kteří prokážou svou totožnost, „obrátit se" na organizace, jež byly zapsány ve veřejném rejstříku správců údajů, s dotazem, zda osobní údaje fyzické osoby zpracovávají, a v tomto případě rovněž zaručilo právo na „sdělení" takových zpracovávaných osobních údajů. Následující ustanovení § 35 pak upravovalo způsob práva na přístup vč. práva na kopii za zaplacení poplatku, ale i třeba výjimku, kdy mohl správce požádat dozorový úřad o prodloužení lhůty na odpověď nebo o možnost některým žádostem ze zákonných důvodů nevyhovět:

§ 35 — „Nositel práva na přístup může získat informace, které se ho týkají. Sdělení informací musí být v jednoduchém jazyce a v souladu s obsahem vedených záznamů.

[205] Tamtéž.
[206] Art. 3 – „*Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés*."
Překlad: *„Každý má právo znát a napadnout informace a postupy použité při automatizovaných zpracováních, jejichž výsledky jsou použity proti němu."*
[207] Právu na přístup se věnovala celá kapitola V francouzského zákona s názvem Výkon práva na přístup, tedy ustanovení § 34 až 40. Stěžejní je ale ustanovení § 34 zákona:
Art. 34 – „*Toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en application de l'article 22 ci-dessus en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication*."
Překlad: *„Každá osoba, která prokáže svou totožnost, má právo dotázat se útvarů nebo orgánů odpovědných za provádění automatizovaných operací zpracování, jejichž seznam je veřejně přístupný podle článku 22 výše, aby zjistila, zda se tyto operace zpracování týkají jejích osobních údajů, a případně získat sdělení těchto údajů."*

Kopie se vydá nositeli práva na přístup, který o ni požádá oproti zaplacení paušálního poplatku, který se liší podle kategorie zpracování, a jehož výše je stanovena na základě rozhodnutí úřadu pro ochranu osobních údajů (dále jen „úřad“) a schválena vyhláškou ministra hospodářství.

Úřad, na nějž se obrátil správce odpovědný za zpracování, však může tomuto správci poskytnout:

– lhůty pro odpověď;

– povolení nepřihlížet k některým žádostem, které jsou zjevně zneužívající z hlediska jejich počtu, jejich opakující se nebo systematické povahy.

Pokud existuje důvodná obava, že informace uvedené v prvním odstavci tohoto článku mohou být zatajeny nebo vymazány, a to i před podáním opravného prostředku k soudu, může být podána žádost příslušnému soudu o nařízení veškerých opatření, která mohou zabránit takovému zatajení nebo vymazání.“

Další ustanovení zákona pak upravovaly podrobnosti dalších práv souvisejících s právem na přístup. Ustanovení § 36 tak zakotvovalo právo subjektu údajů na opravu, doplnění, objasnění, aktualizaci nebo výmaz nepřesných, neúplných, nejednoznačných nebo zastaralých informací, které se ho týkají, nebo jejichž sběr, použití, sdělování nebo uchovávání je zakázáno. Kromě toho, podle tohoto ustanovení nesl pro případ sporu důkazní břemeno (až na výjimky, kdy je prokázáno, že sporné informace byly sděleny samotným subjektem údajů nebo s jeho souhlasem) správce.

Ačkoli je ochrana osobních údajů součástí francouzského právního systému již od roku 1978, na ústavní úrovni nebyla dlouhou dobu zakotvena. Ústavní soud (*Conseil constitutionnel*) se vyslovil k řadě případů, které se nepochybně týkaly zpracování osobních údajů, především pro účely vymáhání práva, soudní nebo správní účely, přesto se v nálezech neobjevuje pojem zpracování osobních údajů, ale pracuje se pouze s pojmem práva na respektování soukromého života. Jakousi první vlaštovkou, kde Ústavní soud zmiňuje uznání ochrany osobních údajů, je nález z roku 1999, kdy soud přezkoumával ústavnost zákona o financování sociálního zabezpečení pro rok 2000.[208] V tomto případě bylo jedním ze sporných ustanovení zavedení lékařských potvrzení o pracovní neschopnosti, která vystavovali lékaři a předávali je orgánům

[208] BRAUCHART, Nina Maria. Master’s Thesis. LLM Law and Technology, Tilburg University, June 2019. *The constitutional right to personal data protection in the face of automated decision-making. A comparison between France and Germany*, str. 24-25. [cit. 2022-03-07].

sociálního zabezpečení. V reakci na to soud rozhodl, že právo na respektování soukromého života vyžaduje, aby byla při předávání osobních údajů zdravotní povahy vynaložena zvláštní péče.[209] Tato formulace „vynaložení zvláštní péče“ se znovu objevila v nálezu o všeobecném zdravotním pojištění z roku 2004, který zavedl elektronickou zdravotní dokumentaci. Zde se píše, že právo na respektování soukromého života vyžaduje vynaložení zvláštní péče při shromažďování a zpracování osobních údajů zdravotní povahy.[210]

Ochrana osobních údajů byla do seznamu ústavně chráněných práv výslovně zařazena až nálezem Ústavního soudu z roku 2012 k zákonu o ochraně totožnosti.[211] Napadena byla ustanovení zákona, která předpokládala zavedení biometrického průkazu totožnosti (s biometrickými osobními údaji) pro všechny francouzské občany. Zákon byl kritizován jak francouzským dozorovým úřadem, tak evropskou pracovní skupinou WP29. V bodě 8 nálezu Ústavní soud uvedl: „*Vzhledem k tomu, že svoboda proklamovaná článkem 2 Deklarace práv člověka a občana z roku 1789 zahrnuje právo na respektování soukromého života; musí být shromažďování, zaznamenávání, uchovávání, nahlížení a sdělování osobních údajů odůvodněno cílem veřejného zájmu a prováděno způsobem vhodným a přiměřeným tomuto cíli*.“ Požadavek cíle veřejného zájmu a vhodnosti a přiměřenosti pro umožnění zpracování osobních údajů tak svědčí o tom, že ochrana osobních údajů byla definitivně uznána jako součást práva na respektování soukromého života vyplývajícího z článku 2 Deklarace práv člověka a občana z roku 1789 a je tedy vyjádřením svobody. Na tomto místě je vhodné poznamenat, že francouzská Státní rada (*Conseil d'État*) v roce 2014 navrhla změnit koncepci práva na ochranu osobních údajů a přiblížit ji právě německému pojetí práva na informační sebeurčení (konkrétně citovala pragmatický přístup federálního Ústavního soudu).[212] Také francouzský úřad pro ochranu osobních údajů (CNIL) poukázal na toto doporučení ve své zprávě o umělé inteligenci a algoritmech[213], ke změně ovšem nakonec nedošlo.

---

[209] Conseil constitutionnel. Nález Ústavního soudu č. 99-422 ze dne 21. 12. 1999. Zejména bod 52 nálezu. Dostupné zde: https://www.conseil-constitutionnel.fr/decision/1999/99422DC.htm. [cit. 2022-03-07].
[210] Conseil constitutionnel. Nález Ústavního soudu č. 2004-504 ze dne 12. 8. 2004. Zejména body 4, 5 a 8 nálezu. Dostupné zde: https://www.conseil-constitutionnel.fr/decision/2004/2004504DC.htm. [cit. 2022-03-07].
[211] Conseil constitutionnel. Nález Ústavního soudu č. 2012-652 ze dne 22. 3. 2012. Dostupné zde: https://www.conseil-constitutionnel.fr/decision/2012/2012652DC.htm. [cit. 2022-03-07].
[212] Conseil d'Etat. *Etude Annuelle 2014 Du Conseil d'État – Le Numérique et Les Droits Fondamentaux* (La Documentation française 2014). 8. září 2014, str. 337. Dostupné zde: https://www.conseil-etat.fr/publications-colloques/etudes/le-numerique-et-les-droits-fondamentaux. [cit. 2022-03-07].
[213] CNIL. *'Comment Permettre à l'Homme de Garder La Main? Les Enjeux Éthiques Des Algorithmes et de l'Intelligence Artificielle'* (2017), str. 48. Dostupné zde: https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de. [cit. 2022-03-07].

Velká Británie

Také Velká Británie upravovala práva subjektů údajů ve svém prvním zákoně o ochraně osobních údajů (UK Data Protection Act z roku 1984)[214] poměrně komplexně. Práva subjektů údajů se nacházela v části III (§ 21 až 25) zákona. Ustanovení § 21 zákona tak stanovilo právo na přístup k osobním údajům, které mělo dvě složky: zaprvé, informování jednotlivce, zda uchovávané údaje, které má správce k dispozici, zahrnují osobní údaje, jejichž je tato fyzická osoba subjektem údajů, a zadruhé poskytnutí kopie informací, které tvoří takové osobní údaje, které má správce k dispozici.[215] Podobně jako francouzská úprava i Velká Británie již v právu na přístup zahrnula i právo na kopii zpracovávaných údajů, blíže upravila i způsob práva na přístup, lhůtu pro poskytnutí odpovědi (40 dnů) a výjimku, resp. možnost správce některým žádostem ze zákonných důvodů nevyhovět (z důvodu nepřiměřenosti – četnosti žádostí nebo z jakéhokoli jiného důvodu, v obou případech to ale musel posoudit soud). Terminologie tehdejšího zákona ještě nepracovala s pojmem správce, ale výslovně hovořila o uživateli údajů (data user), ačkoli z obsahového hlediska se nic nezměnilo, neboť se stále jedná o hlavní osobu odpovědnou za zpracování údajů. Těmito uživateli tedy byly různé veřejnoprávní i soukromoprávní organizace, které uchovávaly údaje a které se musely nejdříve nechat zaregistrovat u britského dozorového úřadu. Režim podle zákona z roku 1984 se dále opíral o určité základní zásady, které tvořily kodex pro řádné zpracování osobních údajů. Zásady, až na dvě výjimky, se nelišily od zásad, které jsou nyní obsaženy v nařízení GDPR.

Velká Británie potom implementovala směrnici 95/46 do zákona z roku 1998 (UK Data Protection Act 1998)[216], který vstoupil v účinnost 1. března 2000. Zákon obsahoval novou definici „zpracování“, která obsahově pojmula všechny činnosti, které mohly být prováděny s údaji, a začlenil několik prvků, jež představovaly významné změny ve srovnání s předchozí právní úpravou: 1) Manuální zpracování – zákon z roku 1998 se kromě elektronicky (automatizovaně) zpracovávaných osobních údajů vztahoval i na některé listinné záznamy. 2)

---

[214] UK Data Protection Act z roku 1984. Dostupné z: https://www.legislation.gov.uk/ukpga/1984/35/enacted. [cit. 2024-08-24].

[215] § 21 - Data Protection Act

(1) „*Subject to the provisions of this section, an individual shall be entitled:*

a) to be informed by any data user whether the data held by him include personal data of which that individual is the data subject; and

b) to be supplied by any data user with a copy of the information constituting any such personal data held by him;

and where any of the information referred to in paragraph (b) above is expressed in terms which are not intelligible without explanation the information shall be accompanied by an explanation of those terms.“ Dostupné z: https://www.legislation.gov.uk/ukpga/1984/35/enacted.

[216] UK Data Protection Act z roku 1998. Dostupné z: https://www.legislation.gov.uk/ukpga/1998/29/contents/enacted. [cit. 2024-08-24].

Legitimita zpracování – byly zavedeny nové podmínky pro zpracování jako minimální požadavky pro to, aby mohlo být zpracování prováděno zákonně. 3) Citlivé údaje – v zákoně byla vytvořena nová kategorie osobních údajů. Citlivé osobní údaje nebylo možné zpracovávat, pokud nebyla splněna jedna ze souboru zvláštních podmínek. 4) Export údajů – přenos osobních údajů do zemí mimo Evropský hospodářský prostor byl zakázán, pokud nebyly splněny určité podmínky. 5) Zabezpečení údajů – stávající bezpečnostní požadavky byly rozšířeny a byly stanoveny nové požadavky týkající se zpracovatelů údajů. 6) Práva subjektů údajů – do zákona bylo nově zařazeno více práv subjektů údajů a v silnější podobě, vč. práva na náhradu škody či imateriální újmy způsobené nezákonným zpracováním.[217]

Ukázalo se, že rozsah zákona z roku 1998 byl ještě širší než samotná směrnice 95/46, neboť pokrýval veškeré obecné zpracování údajů, včetně zpracování osobních údajů pro účely národní bezpečnosti, ačkoli s příslušnými výjimkami. Zákon upravoval celkem osm zásad ochrany osobních údajů, a sice zákonnost, účelové omezení, minimalizaci údajů, přesnost, omezení uložení, přístup, zabezpečení zpracování a přenos do zahraničí. V podrobnostech je přehledně uvedeno v tabulce v příloze na konci této práce. Pokud jde o právo na přístup, tak to bylo v zákoně z roku 1998 upraveno v ustanovení § 7 a opět bylo podrobnější než v předchozí úpravě. Zákon stanovil, že fyzická osoba, která podá písemnou žádost a zaplatí poplatek, má právo: a) být informována do 40 dnů, zda se zpracovávají nějaké osobní údaje; b) na uvedení popisu osobních údajů, důvodů jejich zpracování, a zda budou poskytnuty jiným organizacím nebo osobám; c) na poskytnutí kopie informací obsahujících osobní údaje; a uvedené podrobnosti o zdroji těchto údajů.

Později pak, pro zajištění souladu s rámcem ochrany údajů v podobě GDPR, byl přijat nový zákon UK Data Protection Act 2018[218]. Ten především aktualizoval práva subjektů údajů, usnadnil jejich uplatňování a v neposlední řadě se snažil zajistit, aby právní úprava adekvátním způsobem reagovala na technologicky pokročilejší metody zpracování údajů. 21. století je totiž navíc poznamenáno dvěma významnými fenomény – tím prvním je přesun podstatné části osobních údajů do internetového prostředí a tím druhým je obecně proces globalizace a internacionalizace. Na mezinárodní úrovni proto přijal Výbor ministrů Rady Evropy dne 18. května 2018 modernizovanou Úmluvu o ochraně jednotlivců v souvislosti se zpracováním osobních údajů („tzv. modernizovaná úmluva 108“). Britský zákon z roku 2018 tedy byl

[217] CAREY, Peter, 2018. *Data Protection: A Practical Guide to UK and EU law*. Oxford University Press. Fifth edition, 410 s. ISBN 978-0-19-881541-9.
[218] UK Data Protection Act z roku 2018. Dostupné z: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. [cit. 2024-08-24].

navržen tak, aby byl v souladu i s tímto mezinárodním instrumentem. Vzhledem k tomu, že Velká Británie oficiálně dne 31. ledna 2020 vystoupila z Evropské unie, byl přijat i zvláštní zákon, který právní důsledky brexitu řešil, a to European Union (Withdrawal) Act 2018 neboli zákon o vystoupení z Evropské unie[219]. Díky němu byl osud GDPR a dalších přímo použitelných právních norem EU účinných přede dnem vystoupení vyjasněn, byly inkorporovány do vnitrostátního práva. Z hlediska struktury je britský zákon z roku 2018 rozčleněn do sedmi částí. Část 1 obsahuje úvodní ustanovení. Část 2 je třeba číst společně s nařízením GDPR a dělí se dále na tři kapitoly, kapitolu 1 – rozsah a definice, kapitolu 2 – britské GDPR a kapitolu 3 – výjimky pro manuální nestrukturované zpracování a pro účely národní bezpečnosti a obrany. Část 3 pak obsahuje ustanovení o zpracování údajů v oblasti vymáhání práva a část 4 obdobně upravuje zpracování údajů zpravodajskými službami. Zbylé části se pak týkají postavení a fungování britského dozorového úřadu (část 5), vymáhání práva a úpravy přestupků (část 6) a závěrečných ustanovení (část 7). Definice a základní zásady zpracování osobních údajů tedy v zákoně upraveny nejsou, neboť jsou přímo upraveny v GDPR. Zákon pouze stanoví, že definice mají, až na výjimky, stejný význam jako v GDPR.

Základní zásady zpracování uvedené v GDPR se fakticky překrývají se zásadami uvedenými již ve znění britského zákona z roku 1998, pouze se dvěma výjimkami: přístup ani zahraniční předávání již nejsou formulovány jako zásady, přístupová práva jsou formulována jako zvláštní ustanovení upravené v kapitole III GDPR a zahraniční předávání nyní v podobě předávání údajů do třetích zemí nebo mezinárodním organizacím je upraven v kapitole V GDPR. Nicméně, v GDPR (čl. 5 odst. 2) je jeden princip, který předtím britský zákon z roku 1998 výslovně a samostatně uveden neměl, a tím je velice důležitý princip odpovědnosti správce („správce odpovídá za dodržení zásad a musí být schopen toto dodržení souladu doložit“). Práva subjektů údajů jsou opět z větší části obsažena v samotném nařízení GDPR: obecně lze říci, že byla ve srovnání s předchozí úpravou posílena. Nařízení upravuje právo na přístup podobným způsobem jako dřívější zákon, ovšem se dvěma podstatnými rozdíly. Zaprvé, informace musí být subjektu údajů poskytovány zdarma, výjimkou je možnost účtovat „přiměřený poplatek“, pokud je žádost zjevně nedůvodná nebo nepřiměřená, zejména pokud se opakuje. Zadruhé, lhůta na zaslání odpovědi subjektu údajů je delší, a sice jeden měsíc, přičemž ve složitých případech ji lze prodloužit nejvýše na tři měsíce. Britský adaptační zákon z roku 2018 v souvislosti s právy subjektů údajů ještě upravuje tři zvláštní ustanovení, a sice: 1) limity

[219] UK. European Union (Withdrawal) Act z roku 2018. Dostupné zde: https://www.legislation.gov.uk/ukpga/2018/16/contents. [cit. 2024-08-24].

poplatků, které si mohou správci výjimečně účtovat jako přiměřený poplatek; 2) povinnosti agentur pro hodnocení úvěruschopnosti a 3) automatizované rozhodování povolené zákonem: záruky.

Členské státy v rámci implementace směrnice 95/46 zavedly právo na přístup odlišným způsobem. Po přijetí obecného nařízení o ochraně osobních údajů (tzv. GDPR) se tento prostor ponechaný členským státům podstatně zúžil tím, že právo na přístup bylo zakotveno přímo v článku 15 nařízení GDPR. Větší prostor členským státům zůstal u ustanovení upravujících omezení a výjimky/ odchylky, která tak mohou pro subjekty údajů ve vymezených situacích znamenat omezení práva na přístup či dokonce i jeho odepření. Jedná se konkrétně o ustanovení článku 23 nařízení GDPR (omezení), který se zabývá obecnými omezeními práv subjektu údajů; dále článek 89 nařízení GDPR (záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, vědeckého či historického výzkumu nebo pro statistické účely); a článek 85 nařízení GDPR (zpracování a svoboda projevu a informací). V důsledku toho německý adaptační zákon k GDPR (federální zákon o ochraně osobních údajů) stanoví významné výjimky z práva na přístup, a to v § 34 zákona, který shrnuje všechny výjimky výše uvedené, jako je vědecký výzkum, historický výzkum, archivní účely a převažující oprávněné zájmy třetí osoby, a doplňuje cíle národní bezpečnosti a další cíle obecného veřejného zájmu. Britský zákon o ochraně osobních údajů z roku 2018 zavedl ještě početnější výjimky než německý prováděcí zákon, a to až do té míry, kdy si někteří experti začali klást otázku ohledně slučitelnosti těchto opatření s článkem 8 odst. 2 Listiny základních práv EU. Příloha 2 zákona uvádí omezení práv subjektu údajů, včetně práva na přístup, pro účely zdanění, trestního práva a soudního řízení, imigrační kontroly, ochrany veřejnosti, auditu, zdravotní služby, služeb pro děti, vědeckého výzkumu, historického výzkum, archivní účely atd. Zákon obsahuje navíc ještě i další výjimky v příloze 3 a 4.[220]

Shrnutí komparace

Co tedy vyplývá z provedené právní komparace, resp. jaké společné prvky a jaké odlišnosti lze z ní vyvodit? Pro Německo i Francii platí, že aby mohlo dojít k zásahu do práva na ochranu osobních údajů, resp. práva na informační sebeurčení dle německého konceptu, tak

[220] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

musí být tento zásah oprávněný – odůvodněn cílem veřejného zájmu, být přiměřený a být doprovázen řadou záruk. Obě země upravují zásadu účelového omezení a s ní spojený výmaz údajů, jakmile již nejsou údaje potřebné pro daný účel. Stejně tak obě země předpokládají určité situace omezení práva na přístup. Naopak, zásadní odlišnost lze spatřovat v jakémsi prvku „statičnosti" francouzské úpravy a v jejím užším pojetí ochrany osobních údajů. Francouzská úprava stojí především na negativním pojetí ochrany osobních údajů ve smyslu nevměšování se do osobní sféry jednotlivce. Německý právní rámec ovšem předpokládá mnohem širší, dynamičtější a aktivnější pojem: informační sebeurčení nejenže omezuje zásahy do osobní sféry, ale také zajišťuje rozvoj osobnosti a zapojení občanů do společnosti a veřejného dění. Francouzská úprava tento aktivní prvek postrádá.[221] Francie i Velká Británie měly také ve svých prvních zákonech o ochraně osobních údajů (ve Francii v roce 1978 a ve Velké Británii v roce 1984) poměrně komplexně řešeny práva subjektů údajů, tedy i práva na přístup, včetně práva na kopii. Francouzi dokonce upravovali již v původním zákoně právo být informován o automatizovaném zpracování, jakož i možnost se proti němu právně bránit, což bylo v případě Velké Británie řešeno až v zákoně z roku 1998.

Německo, oproti těmto dvěma zemím, mělo normativní úpravu v původním zákoně z roku 1977 velmi stručnou. Právo na informační sebeurčení je výtvorem Ústavního soudu. Ústavní soud jej odvodil ze dvou základních lidských práv, a to práva na rozvoj lidské osobnosti a práva na ochranu lidské důstojnosti. Ve Francii byla ochrana osobních údajů od počátku v rovině ochrany jednotlivce. Ústavní rovina ale dlouhou dobu absentovala, ochrana osobních údajů se neetablovala jako samostatné ústavní právo, ale jako prvek práva na respektování soukromého života, a tedy jako vyjádření svobody, a to navíc až v souvislosti s nálezem z roku 2012. Ve francouzském právním rámci obecně je totiž právě pojem svobody velmi úzce spojen s ochranou osobních údajů. Zaprvé se to promítá v názvu francouzského zákona o ochraně osobních údajů – zákon o informačních technologiích, souborech a svobodách. A zadruhé je pojem svobody obsažen i v názvu francouzského úřadu pro ochranu osobních údajů – Národní komise pro informační technologie a svobody.

[221] BRAUCHART, Nina Maria. Master's Thesis. LLM Law and Technology, Tilburg University, June 2019. *The constitutional right to personal data protection in the face of automated decision-making. A comparison between France and Germany*, str. 40. [cit. 2022-03-07].

4.4 Účel práva na přístup

Obecně řečeno, hlavním účelem práva na přístup je umožnit jednotlivcům mít kontrolu nad jejich osobními údaji. Právo na přístup je tedy navrženo tak, aby umožňovalo subjektu údajů být o zpracování svých osobních údajů informován a dalo mu možnost si ověřit zákonnost zpracování, jak je ostatně uvedeno i v recitálu 63 nařízení GDPR. Konkrétněji, účelem práva na přístup je umožnit subjektu údajů pochopit, jak jsou jeho osobní údaje zpracovávány, jakož i důsledky tohoto zpracování, a ověřit správnost zpracovávaných údajů, aniž by musel odůvodňovat svůj záměr. Jinými slovy, účelem práva na přístup je poskytnout fyzické osobě dostatečné, transparentní a snadno dostupné informace o zpracování údajů bez ohledu na použité technologie a umožnit jí ověřit různé aspekty konkrétní činnosti zpracování podle GDPR (např. zákonnost, korektnost, přesnost). V souladu s rozhodnutími Soudního dvora EU[222] slouží právo na přístup k zajištění ochrany práva subjektů údajů na soukromí a ochranu údajů v souvislosti se zpracováním údajů, které se jich týkají, a může usnadnit výkon jejich práv vyplývajících například z článků 16 až 19, 21 až 22 a 82 GDPR. Výkon práva na přístup je však právem jednotlivce a není podmíněn výkonem těchto jiných práv a výkon ostatních práv nezávisí na výkonu práva na přístup. Subjekt údajů je tedy třeba průběžně informovat o zpracování jeho osobních údajů. Je tak třeba v průběhu operace zpracování připomínat a opětovně potvrzovat subjektu údajů, jak je s jeho osobními údaji nakládáno. Výjimka, že informace není nutné poskytovat do té míry, v níž subjekt údajů již tyto informace má, jak je tomu v případě práva na informace podle článků 13 a 14, se v tomto případě nepoužije.[223]

Vzhledem k širokému účelu práva na přístup není účel práva na přístup vhodný k tomu, aby byl v rámci procesu posuzování žádostí o přístup správcem analyzován jako předpoklad pro výkon práva na přístup. Správce by proto neměl zkoumat důvody žádosti, posuzovat „proč“ subjekt údajů žádá o přístup, ale pouze „co“ subjekt údajů požaduje a zda má on jako správce k dispozici osobní údaje týkající se této osoby. Pokud tedy žádost splňuje všechny ostatní požadavky, musí správce žádosti vyhovět, ledaže se žádost ukáže jako zjevně nedůvodná nebo nepřiměřená podle čl. 12 odst. 5 nařízení GDPR, což ale musí správce prokázat. Správce by proto například neměl odepřít přístup na základě důvodů nebo podezření, že požadované údaje by subjekt údajů mohl použít k obhajobě u soudu v případě propuštění nebo pro případ

[222] Zejména rozsudek ze dne 20. prosince 2017, Nowak, C-434/16, EU:C:2017:994 a rozsudek ze dne 17. července 2014, YS a další, spojené věci C-141/12 a C-372/12, EU:C:2014:2081.
[223] FOŘT, Ferdinand, 2019. Kapitola III Práva subjektu údajů. In: PATTYNOVÁ, Jana; SUCHÁNKOVÁ, Lenka; ČERNÝ, Jiří a RŮŽIČKA, Miroslav. *Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář*. 2. vydání. Praha: Leges, s. 170-176. ISBN 978-80-7502-396-4.

obchodního sporu se správcem. Jak ale upozorňuje zároveň Evropský sbor pro ochranu osobních údajů (dále jen „EDPB“), tím však nejsou dotčena žádná aplikovatelná vnitrostátní procesní pravidla přijatá v souladu s článkem 23 nařízení GDPR (omezení), která určují například meze informací, které mají být poskytnuty nebo vyměňovány mezi stranami probíhajícího (soudního) řízení a jinými probíhajícími (právními) nároky.

Účelem práva na přístup, jeho rozsahem a pojmem kopie se Soudní dvůr zabýval v rozsudku ve věci *FT (Copies du dossier médical)*[224]. Jedná se o rozsudek z prostředí zdravotní péče. Pan DW nebyl spokojen se zdravotním ošetřením poskytnutým zubní lékařkou FT a měl podezření na pochybení. Požádal tak svou zubařku o bezplatnou kopii své zdravotnické dokumentace na základě práva na přístup podle nařízení GDPR, které zahrnuje rovněž právo obdržet kopii zpracovávaných osobních údajů. Zubařka FT ale odmítla vyhovět této žádosti bez zaplacení nákladů spojených s poskytnutím kopie, jak stanoví vnitrostátní německé právo. Tento poměrně jednoduchý případ se nakonec dostal až k Soudnímu dvoru EU. Předkládající německý soud v něm položil tři zásadní otázky. Zaprvé, zda se pan DW vůbec může dovolávat práva na přístup, vzhledem k tomu, že účelem jeho žádosti bylo uplatnění nároku z odpovědnosti lékařky, nikoli ochrana jeho osobních údajů. Zadruhé si položil otázku, zda vnitrostátní právní předpisy, které znemožňují volný přístup ke zdravotnické dokumentaci, mohou nějakým způsobem sloužit jako legitimní omezení práva na přístup v režimu článku nařízení 23 GDPR. Současně se ptá, zda má význam, že dotčený německý zákon byl přijat před vstupem GDPR v platnost. Poslední třetí otázka se týkala rozsahu práva na přístup v lékařském kontextu, konkrétně, zda musí být poskytnuty úplné dokumenty ze zdravotnické dokumentace či výpisy. K první otázce Soudní dvůr uvedl, že ze znění nařízení GDPR vyplývá zásada, že veškerý výkon práva na přístup je bezplatný. Poplatek může být naúčtován pouze v případě, že dojde ke zneužití práva, což však nebyl tento případ. Soudní dvůr se posléze zabýval argumentem důvodu žádosti o přístup, jinými slovy, zdali je podstatná vazba žádosti o přístup na účel ochrany osobních údajů, jak je uveden v bodě 63 odůvodnění nařízení[225]. Podle Soudního dvora tomu tak není, fyzické osoby nemusí uvádět žádný účel nebo odůvodnění pro využití svého práva na přístup, takže není důležité, zda tyto důvody souvisejí s ochranou osobních údajů či nikoli. Tím byl zpochybněn do té doby poměrně rozšířený názor odborné veřejnosti, že žádosti práva na přístup podané z jiných důvodů než kvůli ochraně osobních údajů

[224] Rozsudek ze dne 26. října 2023, FT (Copies du dossier médical), C-307/22, EU:C:2023:811.
[225] seznámit se se zpracováním údajů a ověřit jeho zákonnost.

mohou být právoplatně zamítnuty.[226] Soudní dvůr nadto připomněl, že body odůvodnění nejsou právně závazné, a tudíž nemohou omezit rozsah práv v samotných ustanoveních dotyčného aktu nařízení. Zadruhé, Soudní dvůr řešil, zda vnitrostátní právní úprava, která umožňuje veškerý přístup ke zdravotnické dokumentaci pouze za úplatu, může být legitimním omezením přístupu v rámci GDPR. GDPR předpokládá možnost omezit všechna práva subjektu prostřednictvím legislativních opatření, pokud takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti za účelem ochrany řady zájmů taxativně vyjmenovaných v čl. 23 odst. 1 GDPR. Soudní dvůr neviděl žádný problém v tom, že dotčený německý zákon byl přijat před vstupem GDPR v platnost. Mnohem přísněji však rozhodl o tom, zda dotčený německý zákon může odpovídat omezujícímu opatření přijatému za účelem čl. 23 odst. 1 písm. i) GDPR (ochrana práv a svobod druhých). V tomto případě je podle něj rozhodujícím faktorem účel daného zákona, což je v konkrétním případě ochrana ekonomických zájmů lékařů, a proto se na něj nemůže vztahovat čl. 23 odst. 1 písm. i) GDPR.

Pokud jde o poslední otázku, Soudní dvůr zdůraznil, že právo obdržet kopii jako součást práva na přístup má za cíl umožnit subjektu údajů „účinný výkon jeho práv“, což znamená, že tyto údaje musí být reprodukovány úplně a přesně. Takové informace musí být zároveň snadno pochopitelné, což může vyžadovat, aby správce poskytl také nezbytný kontext ve formě výpisů z dokumentů či celých dokumentů. Soudní dvůr poukázal na to, že GDPR v bodě 63 odůvodnění přímo uvádí přístup ke zdravotnické dokumentaci jako příklad (přístup k „údajům ve své lékařské dokumentaci, která obsahuje například informace o diagnóze, výsledky vyšetření, posudky ošetřujících lékařů a údaje o veškeré léčbě a provedených ošetřeních nebo zákrocích“). V této souvislosti odmítl poskytnutí jednoduchého shrnutí nebo kompilace těchto údajů lékařem, neboť by to v tomto případě mohlo vést ke vzniku rizika, že některé relevantní údaje budou opomenuty nebo reprodukovány nesprávně, stejně tak i pochopení pacientem by mohlo být ztíženo.

[226] KUGLER, Tobias a RÜCKER, Daniel, 2018. *New European General Data Protection Regulation: A Practitioner's Guide*. Hart/Nomos, Bloomsbury Collections, 285 s. First edition. Online. ISBN 978-1-5099-2059-4 Dostupné z: https://doi.org/10.5040/9781509920594. [cit. 2024-09-25].

4.5 Obecné principy práva na přístup

Jestliže subjekty údajů požádají o přístup ke svým údajům, musí být informace uvedené v článku 15 nařízení GDPR v zásadě poskytnuty v plném rozsahu. Pokud tedy správce zpracovává údaje týkající se subjektu údajů, poskytne veškeré informace uvedené v čl. 15 odst. 1 a případně informace uvedené v čl. 15 odst. 2, tj. pokud jde o předání do třetí země nebo předání mezinárodní organizaci. Jaké jsou obecné principy práva na přístup? Informace musí být úplné, správné a aktuální a musí co nejvíce odpovídat stavu zpracování údajů v době podání žádosti. Přístup k osobním údajům by zároveň měl být zajištěn tak, aby byl v souladu s požadavky na zabezpečení osobních údajů. Pokud správci zpracovávají údaje společně jako tzv. „společní správci“, nemá ujednání společných správců o jejich povinnostech, pokud jde o výkon práv subjektu údajů, a to zejména co se týká odpovědi na jeho žádost o přístup, vliv na práva subjektu údajů vůči správci, jemuž žádost adresuje. Principy tak lze shrnout do těchto kategorií: úplnost; správnost; časové hledisko posuzování žádosti a zajištění přístupu v souladu s požadavky na zabezpečení.

Subjekty údajů mají právo na úplné zveřejnění všech údajů, které se jich týkají, není-li uvedeno jinak. Platí tedy, že pokud subjekt údajů výslovně svou žádost nespecifikuje, resp. ji sám neomezí, je žádost o výkon práva na přístup chápána obecně a zahrnuje všechny osobní údaje, které se jej týkají. Nicméně, podle pokynů[227] lze o omezení přístupu k části informací uvažovat v těchto dvou případech[228]: zaprvé, subjekt údajů sám výslovně omezí svou žádost na podmnožinu údajů. V tomto případě může správce zvážit omezení žádosti subjektu údajů pouze tehdy, je-li jisté, že tento výklad odpovídá vůli subjektu údajů. Zadruhé, v situacích, kdy správce zpracovává velké množství údajů týkajících se subjektu údajů, může mít správce oprávněné pochybnosti, zda je skutečně cílem žádosti o přístup, vyjádřené velmi obecně, získat podrobné informace o všech druzích zpracovávaných údajů nebo o všech oblastech činnosti správce. Typicky se jedná o situace, kdy od počátku nebylo možné poskytnout subjektu údajů nástroje k upřesnění jeho žádosti nebo je subjekt údajů nevyužil. Správce pak čelí problémům s tím, jak poskytnout úplnou odpověď a zároveň zabránit „přehlcení“ subjektu údajů informacemi, o které nemá zájem a jež není schopen účinně zpracovat. Mohou sice existovat způsoby, jak tento problém vyřešit v závislosti na okolnostech a technických

[227] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 16-17. Dostupné z: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.

[228] Pozn.: v tomto smyslu je myšleno omezení k přístupu k údajům v jejich úplnosti, nikoli obecně omezení práva na přístup popsané v části páté, kapitole 5.3 této práce.

možnostech správce, například poskytnutím tzv. online samoobslužných nástrojů (může se jednat třeba o online formuláře). Nejsou-li ovšem taková řešení k dispozici, může správce, který zpracovává velké množství informací týkajících se subjektu údajů, požádat subjekt údajů, aby předem uvedl, jaké informace nebo činnosti zpracování po něm konkrétně požaduje (viz bod 63 odůvodnění nařízení GDPR). Tato výjimečná situace může nastat například v případě korporace s širší škálou různých činností nebo u orgánu veřejné moci s různými správními útvary, jestliže správce zjistí, že v těchto pobočkách či útvarech je zpracováváno mnoho údajů týkajících se subjektu údajů. Příklad č. 1: Orgán veřejné moci zpracovává údaje o subjektu údajů v několika různých odděleních, a to v rámci různých agend. Správa a uchovávání souborů jsou částečně zpracovávány manuálními neautomatizovanými prostředky a většina údajů je uložena pouze v listinných dokumentech. Žádost byla podána obecně, orgán veřejné moci má nicméně oprávněné pochybnosti, zda si je subjekt údajů vědom rozsahu své žádosti, zejména s ohledem na rozmanitost operací zpracování, které by žádost zahrnovala, množství informací a počet stran, které by subjekt údajů takto obdržel. Nejvhodnějším řešením je tedy vyzvat subjekt údajů, aby specifikoval rozsah své žádosti. Příklad č. 2: Velká korporace – pojišťovna obdrží od svého dlouhodobého zákazníka formou dopisu obecnou žádost o přístup. I když jsou z její strany řádně dodržovány lhůty pro výmaz, pojišťovna ve skutečnosti zpracovává velké množství údajů o zákazníkovi, protože zpracování je stále nezbytné pro plnění smluvních závazků vyplývajících ze smluvního vztahu, který se zákazníkem má (včetně např. pokračujících závazků, vzájemné komunikace se zákazníkem a s třetími stranami…) nebo k plnění právních povinností (archivované údaje, které je nutné uchovávat pro daňové účely atd.). Pojišťovna může mít pochybnosti, zda žádost, která byla podána velmi obecně, je skutečně určena k tomu, aby zahrnovala všechny druhy těchto údajů nebo všechny operace zpracování. To může být komplikovanější o to více, že pojišťovna má k dispozici jako kontaktní údaj pouze poštovní adresu subjektu údajů a musí tedy zasílat jakékoli informace klasickou poštou.

U obou výše uvedených příkladů je tedy vhodným způsobem řešení ze strany správce požádat subjekt údajů o upřesnění žádosti. Správce by měl současně za účelem splnění své povinnosti usnadnit výkon práva na přístup (čl. 12 odst. 2 nařízení GDPR) poskytnout smysluplné informace o všech operacích zpracování týkajících se subjektu údajů, jako jsou různá odvětví jeho činností, různé databáze atd. Správce by měl být v každém případě vždy schopen prokázat, že způsob vyřízení žádosti má za cíl poskytnout subjektu údajů co nejširší účinek práva na přístup. Pokyny EDPB zároveň zdůrazňují, že cílem žádosti o upřesnění není omezení odpovědi na žádost o přístup a nesmí se používat k zatajení jakýchkoli informací

o údajích nebo o zpracování, týkajícím se subjektu údajů. Současně platí, že pokud subjekt údajů, který byl požádán o upřesnění rozsahu své žádosti, potvrdí, že jsou předmětem jeho žádosti všechny osobní údaje, které se ho týkají, je správce samozřejmě povinen poskytnout tyto údaje v jejich úplnosti. Správce by tedy v první řadě měl poskytnout subjektu údajů jasný přehled o všech operacích zpracování, které se jej týkají, včetně zejména takových operací, které by subjekt údajů neočekával, dále by měl poskytnout přístup ke všem údajům, o které subjekt údajů jasně projevil zájem, a zároveň jednoznačně popsat způsoby, jakými lze získat přístup ke zbývajícím částem zpracovávaných údajů. [229]

Z hlediska principu správnosti platí, že informace obsažené v kopii osobních údajů poskytnuté subjektu údajů musí obsahovat osobní údaje skutečně uchovávané o subjektu údajů. Správce má tedy vůči subjektu údajů povinnost poskytnout informace o údajích, i když jsou nepřesné, stejně jako povinnost poskytnout informace o zpracování údajů, které nesplňuje požadavek zákonnosti.[230] Důvodem je, že jedním z hlavních účelů práva na přístup je právě možnost subjektu údajů dozvědět se o nezákonném zpracování, které se ho týká. Subjekt údajů může například využít práva na přístup k tomu, aby se dozvěděl o zdroji nepřesných údajů šířených mezi různými správci. Jestliže správce opraví nepřesné údaje ještě předtím, než o tom subjekt údajů informuje, připraví tak subjekt údajů o možnost ověřit si zákonnost zpracování. Zároveň platí, že touto povinností informovat o nezměněném stavu zpracování není dotčena povinnost správce ukončit nezákonné zpracování nebo opravit nepřesné údaje.

U posuzování žádosti je pak důležité i časové hledisko – odpověď správce na žádost o přístup by měla zahrnovat všechny údaje pro správce dostupné v daném okamžiku. Správce by se tak měl bez zbytečného odkladu pokusit získat informace o všech činnostech zpracování údajů týkajících se subjektu údajů. To zároveň znamená, že správce již není povinen poskytovat osobní údaje, které v minulosti zpracovával, ale které již nemá k dispozici. Správce například mohl osobní údaje vymazat v souladu se svými zásadami uchovávání údajů nebo právními předpisy, a proto již nemusí být schopen poskytnout požadované osobní údaje. V této souvislosti je důležité připomenout, že doba, po kterou jsou údaje uchovávány, by měla být stanovena v souladu s čl. 5 odst. 1 písm. e) nařízení GDPR (zásada časového omezení uložení), tedy nesmí být delší, než je nezbytné pro účely daného zpracování, neboť jakékoli uchovávání údajů musí být objektivně odůvodnitelné. Současně správce provede nezbytná opatření

[229] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 16-17.
[230] nebo již nesplňuje požadavek zákonnosti, ačkoli tomu dříve bylo jinak.

k usnadnění výkonu práva na přístup a k vyřízení těchto žádostí co nejdříve a před tím, než budou muset být údaje vymazány. V případě kratší doby uchovávání, než je časový rámec pro odpověď stanovený v čl. 12 odst. 3 nařízení GDPR, by měl být časový rámec pro odpověď na žádost přizpůsoben odpovídající době uchovávání, aby se usnadnil výkon práva na přístup a zabránilo se trvalé nemožnosti poskytnout přístup k údajům zpracovávaným v okamžiku podání žádosti. V tomto ohledu by tak měla být žádost o právo na přístup k osobním údajům vyřízena okamžitě před vymazáním osobních údajů. Také zde platí, že správce nemůže uniknout povinnosti poskytnout požadované osobní údaje vymazáním nebo úpravou osobních údajů v reakci na žádost o přístup. Pokud správce v průběhu zpracování žádosti o přístup zjistí nepřesné údaje nebo protiprávní zpracování, musí ještě před splněním svých dalších povinností posoudit stav zpracování a informovat o tom subjekt údajů. Je ve vlastním zájmu správce, aby dále doplnil informace o následných opravách nebo výmazech a byl tak v souladu se zásadou transparentnosti (vyjádřenou v čl. 5 odst. 1 písm. a) nařízení GDPR). V některých případech může dojít v čase mezi posouzením žádosti a odesláním odpovědi subjektu údajů k dalšímu zpracování nebo změnám osobních údajů. Pokud si je správce toho vědom, doporučuje se uvést informace o těchto změnách nebo informace o dalším zpracování subjektu údajů, v zájmu souladu se zásadou transparentnosti.[231]

Pokud jde o poslední obecný princip práva na přístup v této části – zajištění přístupu v souladu s požadavky na zabezpečení, jedná se vlastně o projev základní zásady zpracování, a sice zásady integrity a důvěrnosti (čl. 5 odst. 1 písm. f) nařízení GDPR). Dá se říci, že vlastně celé nařízení GDPR klade velký důraz na zabezpečení zpracování. Zásada integrity a důvěrnosti je novou zásadou zpracování, kterou dřívější směrnice 95/46 neobsahovala. Jedním z rizik vyskytujících se při zpracování osobních údajů je totiž riziko záměrného či neúmyslného zpřístupnění osobních údajů neoprávněným osobám, resp. riziko, že neoprávněné osoby získají k údajům přístup překonáním bezpečnostních opatření. V některých případech může být rizikem i pouhá ztráta údajů či jejich poškození. Odpověď na žádost o přístup, tedy sdělení a zpřístupnění osobních údajů subjektu údajů, je vlastně další operací zpracování, správce je proto povinen zavést vhodná technická a organizační opatření k zajištění úrovně zabezpečení odpovídající riziku zpracování (viz čl. 32 nařízení GDPR, kde je zabezpečení zpracování samostatně upraveno). To platí bez ohledu na způsob, v němž je přístup poskytován.

[231] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 19.

V případě, že je přístup, resp. předání údajů, poskytováno klasickou poštovní (neelektronickou) formou, může správce zvolit například zaslání zásilky doporučeně. Prostřednictvím doporučeného psaní lze bezpečně posílat písemná sdělení nebo i drobné balíčky, neboť provozovatel poštovních služeb za jejich řádné doručení odpovídá. V ČR lze odkázat na Poštovní podmínky České pošty, konkrétně článek 13 odst. 1 těchto podmínek stanoví: „*Podání doporučené zásilky podnik stvrzuje. Doporučenou zásilku dodá podnik jen za podmínky, že příjemce její převzetí potvrdí*.“ Alternativou, kterou může správce nabídnout, je pak osobní předání souboru s osobními údaji subjektu údajů oproti jeho podpisu. Musí se ale jednat o možnost, kterou lze subjektu údajů nabídnout, nelze do tohoto způsobu subjekt údajů nutit. Pokud jsou informace poskytovány elektronickými prostředky, správce musí zvolit takové prostředky, které splňují požadavky na zabezpečení údajů. To platí rovněž v případě poskytnutí kopie údajů v běžně používané elektronické formě (viz čl. 15 odst. 3 nařízení GDPR). Může se jednat o různá technická opatření, například použití šifrování, ochranu heslem, „zazipováním souboru“, certifikaci atd. Pokyny EDPB v tomto smyslu uvádí, že zasílání prostých emailů není vhodnou formou, neboť nezajišťuje tzv. koncové šifrování (anglicky *end-to-end encryption*). Správce by v takovém případě musel buď použít nějaký další protokol, aby takové koncové šifrování zajistil, nebo musel využít jinou formu, například předání datového souboru na USB klíči.[232] V českých podmínkách lze jako jednu z bezpečnějších forem předání údajů zmínit i informační systém datových schránek. Jedná se o jeden ze způsobů konkrétního a garantovaného doručení, se striktně vymezenou evidencí uživatelů, který umožňuje doručování zpráv konkrétnímu adresátovi do vlastních rukou. V současné době je tento informační systém povinný pro všechny státní instituce, právnické osoby a podnikající fyzické osoby (OSVČ).[233] Datové schránky mohou být spolu s osobním předáním asi nejvhodnějším způsobem předání údajů o zdravotním stavu (výpis či kopie zdravotnické dokumentace).

4.6 Struktura (hlavní komponenty) práva na přístup

Podle nařízení GDPR se právo na přístup v článku 15[234] skládá ze tří složek, tj. potvrzení, zda jsou osobní údaje zpracovávány, přístupu k nim a poskytnutí informace

[232] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 19-20.
[233] Systém nabízí tzv. dvoufaktorové přihlašování, tj. při přihlašování se na počítači musí uživatel mobilním telefonem vyfotit QR kód nebo mu přijde ověřovací SMS s číselným kódem.
[234] Článek 15 – Právo subjektu údajů na přístup k osobním údajům:

o samotném zpracování. Subjekt údajů může rovněž získat kopii zpracovávaných osobních údajů, zatímco tato možnost není dalším právem subjektu údajů, ale způsobem (modalitou) poskytnutí přístupu k údajům. Právo na přístup lze tedy chápat jak jako možnost subjektu údajů dotázat se správce, zdali dochází ke zpracování osobních údajů, které se ho týkají, tak jako možnost přístupu k těmto údajům a jejich ověření. Správce poskytne informace spadající do oblasti působnosti čl. 15 odst. 1 a 2 nařízení GDPR.[235]

4.6.1 Potvrzení o tom, zda jsou či nejsou zpracovávány osobní údaje

Při podání žádosti o přístup k osobním údajům musí subjekt údajů nejprve vědět, zda správce vůbec zpracovává údaje, které se ho týkají, či nikoli. Tyto informace proto představují první složku (komponentu) práva na přístup podle čl. 15 odst. 1 nařízení GDPR. Pokud správce nezpracovává osobní údaje týkající se subjektu údajů žádajícího o přístup, informace, které mají být poskytnuty, by se omezily na potvrzení, že osobní údaje týkající se subjektu údajů nejsou

---

„1. Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:

a) účely zpracování;

b) kategorie dotčených osobních údajů;

c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;

d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;

e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;

f) právo podat stížnost u dozorového úřadu;

g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

2. Pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách podle článku 46, které se vztahují na předání.

3. Správce poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob."

4. Právem získat kopii uvedenou v odstavci 3 nesmějí být nepříznivě dotčena práva a svobody jiných osob.“

[235] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 37.

zpracovávány. Pokud správce ovšem zpracovává údaje týkající se subjektu údajů, musí tuto skutečnost subjektu údajů potvrdit. Toto potvrzení může být sděleno samostatně nebo může být zahrnuto jako součást informací o zpracování.

4.6.2 Vlastní přístup ke zpracovávaným údajům

Přístup k osobním údajům je druhou složkou práva na přístup podle čl. 15 odst. 1 nařízení GDPR a představuje stěžejní část tohoto práva. Týká se pojmu osobních údajů, jak je vymezen v definičním ustanovení článku 4 bodu 1 nařízení GDPR. Kromě základních osobních údajů, jako je jméno a adresa, lze do této definice zahrnout neomezenou škálu údajů za předpokladu, že spadají do věcné působnosti nařízení GDPR (článek 2 GDPR), zejména pokud jde o způsob zpracování. Nařízení GDPR v recitálu 63 vysvětluje, že je zde zahrnuto právo na přístup k údajům o svém zdravotním stavu, například k údajům ve své lékařské dokumentaci, která obsahuje například informace o diagnóze, výsledky vyšetření, posudky ošetřujících lékařů a údaje o veškeré léčbě a provedených ošetřeních nebo zákrocích. Z hlediska pojmu zpracování zase platí, že se obecné nařízení vztahuje na zcela nebo částečně automatizované zpracování osobních údajů, a na neautomatizované neboli manuální zpracování těch osobních údajů, které jsou obsaženy v nějaké evidenci, rejstříku nebo seznamu nebo do nich mají být zařazeny. Manuálně zpracovávané údaje jsou tedy chráněny v momentě, kdy jsou systematicky uspořádány podle určených kritérií (např. podle nějakého klíče či indexu).

Přístupem k osobním údajům se zde rozumí skutečný přístup k samotným osobním údajům, a to nejen obecný popis údajů, ani pouhý odkaz na kategorie osobních údajů zpracovávaných správcem. Jestliže se neuplatní žádná omezení nebo výjimky, mají subjekty údajů právo na přístup ke všem zpracovávaným údajům, které se jich týkají, nebo k částem údajů, v závislosti na rozsahu jejich žádosti. Pokud ovšem subjekt údajů výslovně nepožaduje jinak, rozumí se žádostí o výkon práva na přístup obecný způsob, který zahrnuje všechny osobní údaje týkající se subjektu údajů. Povinnost správce poskytnout přístup k údajům dále nezávisí na typu nebo zdroji těchto údajů. Použije se v plném rozsahu i v případech, kdy žádající osoba původně poskytla správci tyto údaje, protože jejím cílem je informovat subjekt údajů o skutečném probíhajícím zpracování těchto údajů správcem. Právě v podstatě této „komponenty“ práva na přístup tkví zásadní rozdíl mezi současnou úpravou a úpravou dle dřívější směrnice 95/46. Dřívější ustanovení směrnice totiž neobsahovalo žádnou zmínku o tom, v jaké podobě má být takový přístup subjektu údajů umožněn, nehovořilo ani o právu

subjektu údajů získat kopii zpracovávaných osobních údajů, na rozdíl od současného znění čl. 15 odst. 3 nařízení GDPR. Dřívější ustanovení směrnice pouze odkazovalo na „sdělování“ zpracovávaných údajů a veškeré dostupné informace o původu údajů. Výslovným zakotvením práva na kopii tak bylo posíleno právo subjektu údajů na přístup, neboť rozsah tohoto práva není omezen tak, aby se vztahoval pouze na shrnutí zpracovávaných osobních údajů. K podobě poskytnutí takového přístupu se lze opět podívat do recitálu 63 nařízení GDPR: „*Je-li to možné, měl by mít správce možnost poskytnout dálkový přístup k bezpečnému systému, který by subjektu údajů umožnil přímý přístup k jeho osobním údajům*.“ Současně tento recitál upřesňuje, že by právem na přístup neměla být nepříznivě dotčena práva ani svobody ostatních, například obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení. Pokud jde o žádosti o přístup k videozáznamům, EDPB doporučuje správcům přijmout technická opatření, aby mohli těmto žádostem vyhovět (například úprava záznamu, jako je maskování nebo šifrování, resp. zakódování oblastí, které nejsou relevantní pro záznam, nebo dokonce i odstranění záběrů třetích osob).[236] Použití těchto technologií může být v některých případech dokonce dle EDPB i povinné pro dosažení souladu s čl. 5 odst. 1 písm. c) nařízení GDPR (zásada minimalizace údajů), aby se zabránilo identifikaci jiných subjektů údajů.

4.6.3 Informace ke zpracování

Třetí složkou práva na přístup jsou informace o zpracování a právech subjektu údajů, které musí správce poskytnout podle čl. 15 odst. 1 písm. a) až h) a čl. 15 odst. 2. Tyto informace se částečně překrývají s typem informací, které musí být uvedeny v oznámeních o ochraně osobních údajů správce podle článků 13 a 14 nařízení GDPR (neboli ustanovení o informační povinnosti správce) nebo se záznamy správce o činnostech zpracování uvedených v článku 30 nařízení GDPR, ale pravděpodobně bude nutné je aktualizovat a přizpůsobit subjektu údajů, který žádost podal. Ustanovení článků 13 a 14 předpokládají informace, jako je například účel zpracování; kategorie dotčených osobních údajů; příjemci nebo kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny; veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány přímo od subjektu údajů; a právo podat stížnost u dozorového

[236] EDPB. *Guidelines 03/2019 on processing of personal data through video devices*, version 2.0, Adopted on 29 January 2020, s. 22 a 31. Dostupné zde: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

úřadu. Mimoto čl. 15 odst. 1 ještě předpokládá poskytnutí informací o dalších právech subjektu údajů, jako je právo na opravu nebo výmaz, právo na omezení zpracování a právo vznést námitku proti tomuto zpracování. Čl. 15 odst. 2 pak dále stanoví, že pokud byly osobní údaje předány do třetí země nebo mezinárodní organizaci, u nichž nebylo zjištěno, že poskytují odpovídající ochranu, musí správce zveřejnit vhodné záruky, na jejichž základě se předání uskutečnilo, jako jsou položky uvedené v seznamu podle článku 46 GDPR (závazná podniková pravidla, standardní smluvní doložky atd.). Důležité je, že na rozdíl od informací obsažených v oznámeních musí být údaje poskytnuté subjektu údajů na základě žádosti o přístup podle článku 15 nezbytně podrobnější a strukturovanější, konkrétně „přizpůsobené na míru" přesným osobním údajům osoby podávající žádost a jejich zpracování. Oznámení jsou oproti tomu ze své povahy obecná v tom smyslu, že obvykle zahrnují zpracování osobních údajů více subjektů údajů. Jsou to informace *a priori*, což znamená, že jde o informace o tom, co se v budoucnu plánuje s osobními údaji získanými přímo od subjektu údajů nebo od třetích stran, na rozdíl od informací, co se již stalo se zpracovávanými osobními údaji. Odpověď na žádost o přístup se naopak bude muset konkrétně zaměřit na informace o položkách osobních údajů týkajících se osoby podávající žádost, například individualizovat konkrétní příjemce nebo kategorie příjemců, kteří obdrželi údaje této osoby, nebo zveřejnit přesnou dobu uložení osobních údajů, které se vztahují na konkrétní údaje žadatele.

Při sdělování podrobností o zpracování subjektu údajů má v současné době digitalizace zvláštní význam jeden druh informací uvedený v čl. 15 odst. 1 písm. h) nařízení GDPR, a sice „*skutečnost automatizovaného rozhodování, včetně profilování*", a „*přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů*". Ačkoli by se mohlo zdát, že tato část reflektuje vývoj v oblasti moderních technologií a umělé inteligence, její původ je mnohem starší. Vztahuje se již k prvnímu vydání francouzského zákona o ochraně osobních údajů č. 78-17 z roku 1978, jehož tehdejší ustanovení § 3 upravovalo právo každého „*znát a napadnout informace a úsudky použité při automatizovaných zpracování, jejichž výsledky jsou vůči němu namířeny*." Také původní právní úprava na evropské úrovni, směrnice 95/46, obsahovala ve svém článku 12 (právo na přístup) právo subjektu údajů získat od správce „*oznámení postupu automatického zpracování údajů…alespoň v případě automaticky přijímaných rozhodnutí*", která významně ovlivňují subjekt údajů. Tento bod byl považován za dostatečně důležitý, a proto byl umístěn samostatně a uveden v čl. 12 písm. a) třetím pododstavci směrnice 95/46 namísto toho, aby byl vyjmenován podle čl. 12 písm. a) prvního

pododstavce směrnice 95/46 spolu s dalšími podrobnostmi o zpracování, které musí být subjektu údajů, jenž podal žádost, sděleny. Proto právo vědět o postupu spojeném s určitým automatizovaným rozhodováním není regulatorní reakcí na současný vývoj v používání algoritmů a umělé inteligence. Lze dokonce říct, že evropský zákonodárce uvažoval o otázkách automatizovaného zpracování a dopadu automatizovaného rozhodování již od počátků právních předpisů o ochraně osobních údajů.

Pokud jde o to, co by mělo být subjektu údajů v tomto ohledu sděleno podle čl. 15 odst. 1 písm. h) nařízení GDPR, měl by správce v první řadě potvrdit, zda osoba, která žádost podává, podléhá automatizovanému rozhodování podle čl. 22 odst. 1 a 4 nařízení GDPR, tj. automatizovanému rozhodování založenému výhradně na automatizovaném zpracování, které má pro ni právní účinky nebo má podobný významný dopad pro ni, včetně takových rozhodnutí založených na zpracování citlivých údajů. V souladu se svými povinnostmi týkajícími se odpovědnosti by měl správce v okamžiku obdržení žádosti o přístup okamžitě ověřit, zda je subjekt zapojen do takového druhu zpracování, neboť z toho pro něj vyplývají některé zvláštní povinnosti. Například v případě, že správce provádí systematické a rozsáhlé hodnocení osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování a na nichž se zakládají rozhodnutí, která mají právní účinky vůči dané osobě nebo mají podobný významný dopad na ni, musí být provedeno posouzení vlivu na ochranu osobních údajů (dále jen „DPIA“). Zadruhé, pokud tento typ zpracování existuje, správce musí sdělit smysluplné informace o příslušném postupu zpracování. Podle názoru EDPB však nařízení GDPR nevyžaduje zbytečně složité vysvětlení použitých algoritmů. EDPB dále doporučil, aby správce poskytl subjektu údajů obecné informace, například o faktorech zohledněných v rozhodovacím procesu a o tom, jaký význam je jim souhrnně přikládán. V každém případě by informace měly být dostatečně komplexní, aby bylo možné porozumět důvodům rozhodnutí. Kromě toho je třeba zohlednit i bod 58 odůvodnění nařízení GDPR, a sice, že sdělování informací subjektům údajů musí být stručné, snadno přístupné a srozumitelné, a to s použitím jasných a jednoduchých jazykových prostředků. Zatřetí, správce by měl vysvětlit význam a předpokládané důsledky tohoto typu zpracování. Pokud je například předpokládaným důsledkem vyloučení subjektu údajů z požívání nějaké výhody nebo z účasti na pohovoru do zaměstnání, měly by být tyto důsledky upřesněny.[237]

[237] KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 1488. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

4.7 Realizace práva na přístup

Modality, resp. způsoby poskytnutí práva na přístup, jsou upraveny v nařízení GDPR, ovšem pouze ve velmi omezené podobě. Článek 15 v odstavci 3 a 4 tohoto nařízení totiž hovoří jen o právu na kopii zpracovávaných osobních údajů. Je tedy třeba se ponořit i do materiálů *soft law* a podívat se, zdali ke způsobům poskytnutí práva na přístup neobsahují nějaká bližší vysvětlení. Zde je asi nejlepší vyjít z Pokynů EDPB č. 1/2022 k právům subjektů údajů.[238] Na tomto místě bych ráda zmínila i některé „diskuzní perličky" z pracovní skupiny pro práva subjektů údajů, jíž se pracovně v rámci svého zaměstnání účastníme. Bylo tam vzneseno několik otázek, z nichž uvedu dvě nejzajímavější: 1) Je právo získat kopii dle čl. 15 odst. 4 samostatným právem nebo součástí obecného práva subjektu údajů na přístup dle článku 15? 2) Je omezení právy jiných osob (znění čl. 15 odst. 4) vztáhnuto jen k právu získat kopii nebo k celému právu na přístup? Osobně považuji první otázku za vyjasněnou, právo získat kopii je jednoznačně jedním ze způsobů poskytnutí přístupu subjektu k jeho osobním údajům a nikoli samostatným právem. To ostatně potvrdila i judikatura Soudního dvora EU. Stejný názor zastávala v průběhu procesu vytváření pokynů k právům subjektů údajů (právu na přístup) i zástupkyně německého dozorového úřadu a ukázal se jako nejpřesvědčivější, byl přijat a promítnul se do výsledné podoby pokynů. Pro tento názor slouží podle mě několik důvodů: Jednak hledisko systematické, tj. členění ustanovení článku 15. Právo na kopii je až ve třetím a čtvrtém odstavci článku 15, systematicky se s ním pracuje jako s něčím odvislém od obecného práva na přístup. Nelze si totiž dost dobře logicky představit, že by mohlo být realizováno bez uplatnění obecného práva na přístup. Zadruhé, subsidiárně lze využít i přístup anglického dozorového úřadu ICO, který uvádí: „*The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully...*" Také toto pojetí svědčí názoru, že je právo na kopii úzce spojeno s obecným právem na přístup. Pokud jde o druhou otázku, byla podle mého názoru nakonec v pokynech vyřešena „šalamounsky". Z koncepce znění odstavce 4 se skutečně omezení vztahuje jen k právu získat kopii. Nelze ovšem opomenout, že omezení právy jiných osob je obsaženo i na řadě jiných míst nařízení GDPR, nejjasněji asi v již zmíněném recitálu

[238] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023.

63, kde se o omezení hovoří i v obecné rovině práva na přístup. Tolik tedy malé přiblížení k diskuzím, které předcházely přijetí pokynů k právům subjektů údajů.

Jak se tedy uvádí i v samotných pokynech, povinnost poskytnout kopii by neměla být chápána jako dodatečné právo subjektu údajů, ale jako jeden ze způsobů poskytování přístupu k údajům. Jedná se o projev posílení práva na přístup k údajům a pomáhá při výkladu práva na přístup – poskytnutí pouhého shrnutí údajů ve většině případů nebude dostačující odpovědí.[239] Zároveň se ale v pokynech píše, že cílem není rozšířit rozsah práva na přístup, odkazuje se totiž na kopii osobních údajů, které jsou předmětem zpracování, a nikoli nutně na reprodukci původních dokumentů. EDPB chápe pojem kopie v širokém smyslu – podle něj může zahrnovat různé druhy přístupu k osobním údajům, za předpokladu, že je tento přístup úplný (tj. zahrnuje všechny požadované osobní údaje) a subjekt údajů má možnost si údaje o sobě uchovávat. Požadavek poskytnout kopii tedy znamená, že informace o osobních údajích týkajících se subjektu údajů, který žádost podává, jsou mu poskytnuty způsobem, který mu umožňuje uchovávat veškeré informace a vrátit se k nim. Je tedy důležité i časové hledisko – má se za to, že ve většině případů bude subjekt údajů potřebovat informace o sobě nejen na omezenou určitou dobu, ale trvale. Ačkoli bude zpravidla hlavním způsobem poskytnutí práva na přístup poskytnutí kopie dokumentu, který má správce o subjektu údajů u sebe, existují také další způsoby. Za určitých okolností totiž může být vhodné, aby správce poskytl přístup jinými způsoby než poskytnutím kopie, a to tzv. dočasnými způsoby. Takovými způsoby mohou být dle pokynů například: poskytnutí ústní informace; nahlížení do spisů; poskytnutí přístupu na místě nebo vzdáleného přístupu bez možnosti stahování. Tyto způsoby mohou být dostačující a rozumné, a to v případech, kdy je to v zájmu subjektu údajů nebo o to subjekt údajů požádá. Důležité je totiž, aby byl splněn cíl práva na přístup, a sice aby byl subjekt údajů informován a ověřil si zákonnost zpracování. Podle okolností tedy může být v dané situaci dostačující, pokud správce subjektu údajů umožní uspokojit jeho potřebu ověřit si správnost údajů tím, že mu dá možnost nahlédnout do původního (originálního) záznamu. Je tedy na správci, aby rozumně posoudil žádost subjektu údajů.

SDEU odkázal na svou dřívější judikaturu[240] týkající se práva na získání kopie osobních údajů i v usnesení ve věci *Addiko Bank*[241]. Soud opětovně potvrdil, že subjektu údajů musí být poskytnuta věrná a srozumitelná reprodukce údajů bez ohledu na to, zda je žádost odůvodněná

[239] Viz výše citovaný rozsudek ze dne 26. října 2023, FT (Copies du dossier médical), C-307/22, EU:C:2023:811, bod 78.
[240] Tamtéž.
[241] Usnesení ze dne 27. května 2024, Addiko Bank, C-312/23, EU:C:2024:458, body 29 a 48 až 49.

či nikoli. V praxi je tak důležité, že Soud potvrdil, že práva podle článku 15 nařízení GDPR lze uplatnit i v případě, že subjekt údajů sleduje účely, které nesouvisejí s ochranou údajů. V tomto konkrétním případě šlo o situaci, kdy požádalo několik klientů banky, aby jim poskytla kopie dokumentů obsahujících jejich osobní údaje, a to včetně úvěrových smluv, které uzavřeli; splátkových kalendářů; dokumentů týkajících se změn úrokových sazeb a výpisů z účtu. Některé z těchto žádostí byly výslovně odůvodněny vůlí subjektů údajů podat proti správci stížnost nebo přímo žalobu. Správce odmítl k těmto dokumentům poskytnout přístup. Subjekty údajů proto podaly stížnosti k chorvatskému dozorovému úřadu s tvrzením, že toto odmítnutí představuje porušení čl. 15 odst. 3 nařízení GDPR. Správce se domníval, že čl. 15 odst. 3 nařízení GDPR přiznává pouze právo na kopii zpracovávaných osobních údajů, a ne nutně dokumentů, které je obsahují. Konkrétně to zdůvodnil tak, že požadované dokumenty se týkají ukončených úvěrových vztahů, a proto není nutné je zpřístupňovat. Jelikož správce nesplnil příkazy vydaný úřadem, byla mu uložena pokuta. Správce proto poté podal žalobu ke správnímu soudu v Záhřebu. Správní soud rozhodl o přerušení řízení a předložil SDEU předběžné otázky: Za 1) „Je správce podle čl. 15 odst. 3 [nařízení GDPR] povinen poskytnout subjektu údajů kopii dokumentu obsahujícího jeho osobní údaje?“ Za 2) „Je správce oprávněn odmítnout žádost o kopii osobních údajů, kterou subjekt údajů podal podle čl. 15 odst. 3 [nařízení GDPR], nikoliv za účelem získání poznatků o operaci zpracování a ověření její zákonnosti ve smyslu 63. bodu odůvodnění uvedeného nařízení, ale k získání podkladů, které mu mohou pomoci při podání žaloby proti správci, nebo je účel, pro který jsou údaje požadovány, irelevantní pro rozhodnutí správce o dotčené žádosti?“

Soudní dvůr Evropské unie rozhodl, že pojem „kopie“ ve smyslu čl. 15 odst. 3 nařízení GDPR se nevztahuje na dokument jako takový, ale na osobní údaje v něm obsažené, které musí být úplné. Kopie proto musí obsahovat všechny osobní údaje, které jsou předmětem zpracování, pokud je to nezbytné pro zajištění přesnosti a srozumitelnosti údajů. To závisí na kontextu zpracovávaných údajů. Článek 15 nařízení GDPR má za cíl posílit a vyjasnit práva subjektů údajů. Právo na přístup k informacím stanovené v tomto článku má tedy subjektu údajů umožnit ujistit se, že osobní údaje, které se ho týkají, jsou věcně přesné a že jsou zpracovávány v souladu se zákonem. Kromě toho musí kopie osobních údajů, které jsou předmětem zpracování a které je správce povinen poskytnout podle čl. 15 odst. 3 věty 1 nařízení GDPR, obsahovat všechny vlastnosti, které subjektu údajů umožňují účinně uplatnit jeho práva podle tohoto nařízení. SDEU dále znovu potvrdil, že poskytnutí kopie osobních údajů nemůže být podmíněno tím, zda subjekt údajů sleduje konkrétní účel. Článek 15 nařízení GDPR přiznává subjektu údajů

rozsáhlé právo na přístup, které existuje bez ohledu na důvody žádosti. Pokud tedy rozhodnutí ve věci *Addiko Bank* mám shrnout, subjekty údajů by měly mít plný přístup ke svým osobním údajům, aby mohly účinně uplatňovat svá práva podle GDPR. Správci musí být připraveni reagovat na žádosti o kopie osobních údajů v plném rozsahu a nemohou tak učinit na základě účelu informací.

Vrátím se ale ještě zpět k obecnému doporučení vhodného postupu pro správce ve vztahu k poskytování kopií. Správce se může v závislosti na dané situaci rozhodnout poskytnout kopii údajů, které jsou předmětem zpracování, spolu s doplňujícími informacemi, přičemž oboje poskytne různými způsoby, např. e-mailem, poštou nebo použitím online samoobslužného nástroje[242]. V každém případě musí správce zvážit vhodná technická a organizační opatření, včetně odpovídajícího šifrování. Pokyny EDPB uvádí pro ilustraci několik příkladů. Příklad č. 3: Malé lokální knihkupectví vede záznamy o jménech a adresách svých zákazníků, kteří používají online objednávky nebo objednávky domů. Zákazník navštíví knihkupectví a požádá o přístup ke zpracovávaným údajům o své osobě. V této situaci je přiměřené, pokud správce vytiskne osobní údaje týkající se zákazníka přímo z informačního systému, tuto kopii zákazníkovi poskytne, a zároveň poskytne doplňující informace dle článku 15 odst. 1 a 2. Příklad č. 4: Dárce přispívající pravidelně na charitu požádá o přístup prostřednictvím e-mailu. Charitativní organizace jako správce uchovává informace o darech uskutečněných za posledních dvanáct měsíců, jakož i jména a e-mailové adresy dárců. Správce může poskytnout kopii osobních údajů a doplňující informace zasláním odpovědi na e-mail, pokud budou přijaty všechny nezbytné záruky, například s ohledem na povahu údajů. V případě správců, kteří mohou čelit velkému počtu žádostí o přístup, hovoří pokyny i o možnosti správců využívat automatizované postupy pro vyřizování žádostí subjektů údajů. Typicky lze využít tzv. online samoobslužné nástroje, které budou integrovat mechanismus ověřování, a zároveň zajistí účinné a včasné vyřizování žádostí subjektů údajů o přístup. Důležité je, aby tyto nástroje neomezovaly rozsah správcem přijatých osobních údajů. Příklad č. 5: Služba sociálních sítí má zaveden automatizovaný proces vyřizování žádostí o přístup, díky němuž může subjekt údajů přistupovat ke svým osobním údajům ze svého uživatelského účtu. Aby mohl uživatel sociálních sítí znovu získat své osobní údaje, může zvolit možnost „Stáhnout vaše osobní údaje“ po přihlášení do svého uživatelského účtu. Tento „samoobslužný“ nástroj umožňuje uživateli

[242] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 43-44.

stáhnout soubor obsahující jeho osobní údaje přímo z uživatelského účtu do vlastního počítače.[243]

Otázku formátu budu podrobněji rozebírat v části **5.8 Posuzování žádosti práva na přístup**, proto zde uvedu ve stručnosti jen pár poznámek. Nařízení GDPR se k formátu vyjadřuje velmi úsporně, a to v článku 12 a 15. Podle čl. 12 odst. 1 se informace podle článku 15 poskytují písemně nebo jinými prostředky, případně i elektronickými prostředky. Pokud jde o přístup ke zpracovávaným osobním údajům, čl. 15 odst. 3 nařízení stanoví, že pokud subjekt údajů podá žádost v elektronické formě, a pokud subjekt údajů nepožádá o jiný způsob, poskytnou se informace v běžně používaném elektronickém formátu. Nařízení GDPR ovšem neupřesňuje, co je běžně používaným elektronickým formátem. Existuje tedy několik možných formátů, které lze použít a jež se navíc v průběhu času mohou vyvíjet a tedy lišit. Pokud není subjektem údajů požadováno jinak, je na správci, aby rozhodl o vhodném formátu, v němž budou osobní údaje poskytnuty. Správce může, i když není nutně povinen, poskytnout dokumenty, které obsahují osobní údaje o subjektech údajů, které žádost podaly, jako takové a v jejich původní podobě. Správce může například případ od případu poskytnout přístup ke kopii nosiče vzhledem k potřebě transparentnosti. Pokyny uvádějí jako příklad možnost subjektu údajů ověřit přesnost údajů v držení správce v případě žádosti o přístup ke zdravotnické dokumentaci nebo ke zvukovému záznamu, jehož přepis je zpochybněn.

Podstatu práva na přístup k osobním údajům, jeho vztah k právu na svobodný přístup k informacím a především pak rozsah práva subjektu údajů na přístup byl upřesněn judikaturou Soudního dvora EU, ačkoli se tak stalo za působnosti dřívější úpravy ochrany údajů – směrnice 95/46. Konkrétně bylo řešeno, jestli má subjekt údajů právo na přístup k údajům uvedeným v protokolu, které se jej týkají, a v případě, že ano, zda toto právo znamená, že mu musí být poskytnuta kopie protokolu, nebo postačí poskytnutí úplného a srozumitelného přehledu uvedených údajů. V rozsudku *YS a další*[244] Soudní dvůr uvedl, že „*aby bylo právo na přístup dodrženo, postačí, aby tento žadatel obdržel úplný přehled těchto údajů ve srozumitelné formě, tedy ve formě, která tomuto žadateli umožní seznámit se s uvedenými údaji a ověřit, že tyto údaje jsou přesné a že jsou zpracovány v souladu s touto směrnicí, aby případně mohl uplatnit svá práva, která mu přiznává uvedená směrnice*“. Zde je nutné poznamenat, že ve znění směrnice nebylo výslovně upraveno právo na kopii, jako je upraveno právě v nařízení GDPR.

[243] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 42.
[244] Rozsudek ze dne 17. července 2014, YS a další, spojené věci C-141/12 a C-372/12, EU:C:2014:2081, bod 60.

Výše jsem napsala, že EDPB je toho názoru, že ve většině případů podle současné úpravy přitom nebude poskytnutí pouhého shrnutí údajů dostatečné. Není takové tvrzení ovšem v rozporu s názorem Soudního dvora EU obsaženém ve zmíněném rozsudku? Respektive, není rozsudek v důsledku změny formulace v nařízení GDPR již překonán? EDPB v pokynech tedy koriguje svůj postoj a uvádí, že takový rozpor zde není. Výraz „přehled údajů" uvedený v rozsudku by neměl být nesprávně vykládán v tom smyslu, že by nezahrnoval všechny údaje, na které se vztahuje právo na přístup, ale je pouze způsobem, jak tyto údaje prezentovat, aniž by byl systematicky umožněn přístup ke skutečným dokumentům. Vzhledem k tomu, že shrnutí (resp. přehled) musí obsahovat kopii osobních údajů, je třeba zdůraznit, že nemůže být poskytnuto způsobem, který nějakým způsobem mění obsah informací. Proto je dle EDPB rozsudek zcela aplikačně použitelný i nyní a poskytnutí takového shrnutí údajů, které obsahuje všechny zpracovávané údaje, může být adekvátní odpovědí subjektu údajů na jeho žádost.

Příklad č. 6: Subjekt údajů je pojištěn u jedné pojišťovny již několik let, během nichž došlo k několika pojistným událostem. V každém případě přitom došlo k písemné komunikaci prostřednictvím e-mailu mezi subjektem údajů a pojišťovnou. Vzhledem k tomu, že subjekt údajů musel poskytnout informace o konkrétních okolnostech každé pojistné události, jejich vzájemná komunikace zahrnuje mnoho osobních informací o subjektu údajů (záliby, spolubydlící pojištěného, jeho každodenní návyky atd.). U několika případů přitom dojde k neshodě ohledně povinnosti pojišťovny uhradit subjektu údajů škodu, což ještě navýšilo množství písemné korespondence. Veškerá tato korespondence je uchovávána pojišťovnou. Subjekt údajů podá žádost o přístup. V této situaci nemusí správce nutně poskytnout e-maily v jejich původní podobě tím, že je přepošle subjektu údajů. Namísto toho se správce může rozhodnout zkompilovat e-mailovou korespondenci obsahující osobní údaje subjektu údajů do jednoho souboru, který zašle subjektu údajů.[245]

Poskytování dalších kopií je upraveno v článku 15 odstavci 3 větě druhé nařízení GDPR. Ustanovení se týká situací, kdy subjekt údajů požádá správce o více než jednu kopii, například v případě ztráty nebo poškození první kopie nebo pokud chce zkrátka kopii předat jiné osobě nebo dozorovému úřadu. V případě vyžádání těchto dalších kopií si může správce v souladu s výše uvedeným ustanovením účtovat přiměřený poplatek s ohledem na administrativní náklady s tím spojené. K této problematice se vyjadřuje i čl. 12 odst. 5 nařízení GDPR. Podle tohoto ustanovení je správce primárně povinen poskytnout úkony podle čl. 15 až

[245] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 49.

22 a 34 bezplatně. Dále stanoví, že jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, má správce dvě možnosti, jak na tuto skutečnost reagovat. Jednak může uložit přiměřený poplatek, který bude zohledňovat administrativní náklady, anebo může takové žádosti odmítnout. Předtím, než správce jednu z uvedených možností vybere, musí posoudit, že dané žádosti subjektu údajů jsou skutečně nedůvodné a nepřiměřené, a toto posouzení musí být schopen doložit.[246] Důvodem je, že takové podávání opakovaných žádostí uplatňovaných krátce po sobě, jehož smyslem je správce jen „zahltit", by bylo možné kvalifikovat jako zneužívání tohoto práva. Pokud subjekt údajů požádá o další kopii po podání první žádosti, může vyvstat otázka, zda by to mělo být považováno za novou žádost, nebo zda subjekt údajů chce další kopii údajů ve smyslu čl. 15 odstavce 3 věty druhé, přičemž v druhém případě může být účtován poplatek za další kopii. Řešení je obsaženo v pokynech EDPB, které uvádějí, že odpověď závisí výhradně na obsahu žádosti: Žádost by měla být vykládána jako žádost o další kopii, pokud se z hlediska času a rozsahu týká stejného souboru osobních údajů jako předchozí žádost. Pokud si však subjekt údajů klade za cíl získat informace o údajích zpracovávaných v jiném časovém okamžiku nebo týkajících se jiného rozsahu údajů, než bylo původně požadováno, platí znovu, že má právo získat bezplatnou kopii podle čl. 15 odst. 3. Typicky tedy po delším časovém úseku, kdy je důvodné očekávat změny v údajích a jejich zpracování, nebo po každé takové skutečně proběhlé změně ve zpracování, měla by být žádost považována za novou s právem na bezplatnou kopii.

Příklad č. 7: Klient obchodní společnosti podá žádost o přístup ke zpracovávaným osobním údajům o své osobě. Rok po získání odpovědi od společnosti podá tentýž klient žádost o přístup podle článku 15 nařízení GDPR u téže společnosti. Bez ohledu na to, zda od předchozí žádosti došlo mezi stranami k novým obchodním transakcím nebo výměně kontaktů, je třeba tuto druhou žádost považovat za novou žádost. Subjekt údajů má tedy právo získat bezplatnou kopii údajů, i kdyby nenastala žádná změna ve zpracování údajů společností, tato skutečnost totiž nemusí být subjektu údajů známá. Varianta č. 1: Pokud klient podá novou žádost například pouze týden po první žádosti, záleží na okolnostech. I tato žádost by mohla být považována za novou žádost. Pokud nebylo první žádosti vyhověno, mohla by být také vykládána jako pouhé připomenutí první žádosti. S ohledem na krátký časový interval a v závislosti na konkrétních okolnostech by ale mohla být posouzena i jako nepřiměřená – podle Pokynů je tato otázka

[246] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 474-491. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

sporná. Varianta č. 2: Pokud klient podá žádost o novou kopii v reakci na přechozí žádost v případě, že ztratil dříve obdrženou kopii, měla by být fakticky považována za žádost o další kopii, protože z hlediska rozsahu a doby zpracování odkazuje na předchozí žádost. Klient tedy nemá právo na bezplatné poskytnutí kopie.

4.8 Posuzování žádosti práva na přístup

Co vše musí správce při posuzování žádosti práva na přístup zohlednit a jaké jsou možné scénáře takového posouzení, jakož i jeho důsledky, je předmětem této části. Evropské dozorové úřady vydaly četné materiály, které se procesu posuzování žádostí práva na přístup věnují, příkladem mohou být tyto pokyny irského dozorového úřadu[247], pokyny francouzského dozorového úřadu (včetně vzorů žádostí o přístup)[248] nebo video britského dozorového úřadu ICO[249] shrnující základní principy. Obecný konsensus a základní shrnutí jsou obsaženy také v Pokynech EDPB.[250]

Oprávněnou osobou práva na přístup je subjekt údajů, korelativně tomu odpovídá, že příslušné povinnosti dopadají na správce zpracování. To znamená, že správce je právně odpovědný za dodržování práva na přístup. Aby správce splnil své povinnosti, může se se zpracovateli smluvně dohodnout, že zpracovatelé poskytují podporu při vyřizování žádostí o přístup podle čl. 28 odst. 3 písm. e) nařízení GDPR. Povinná smlouva mezi správcem a zpracovatelem může zejména zahrnovat ujednání, podle něhož má zpracovatel „pomoci správci vhodnými technickými a organizačními opatřeními“, aby správce splnil svou povinnost reagovat na žádosti o přístup. V praxi by to mohlo znamenat, že zpracovatel má například za úkol vyhledat osobní údaje, které jsou předmětem žádosti o přístup, ve svých systémech a zpřístupnit příslušné osobní údaje správci. Zpracovatel by rovněž mohl mít za úkol vytvořit rozhraní svých systémů, které by správci umožnilo přímo vyhledávat dotčené osobní údaje. Bez ohledu na jakékoli smluvní ujednání by správce měl mít vždy možnost posoudit jakoukoli

[247] DPC (říjen 2022). *Subject Access Requests: A Data Controller's Guide* (Žádosti subjektu údajů o přístup: Průvodce pro správce údajů). Dostupné zde: https://www.dataprotection.ie/sites/default/files/uploads/2022-10/20221005%20Subject%20Access%20Requests%20A%20Data%20Controller%27s%20Guide.pdf. [cit. 2024-04-14].
[248] CNIL (září 2023). *Le droit d'accès: connaître les données qu'un organisme détient sur vous* (Právo na přístup: zjistěte, jaké údaje o vás organizace uchovává). Dostupné zde: https://www.cnil.fr/fr/comprendre-mes-droits/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous. [cit. 2024-04-14].
[249] ICO (listopad 2022). How to deal with Subject Access Requests. (Video britského dozorového úřadu – Jak vyřizovat žádosti o přístup k informacím). Dostupné zde: https://www.youtube.com/watch?v=WY98d-wUn5w. [cit. 2024-04-14].
[250] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 20.

žádost o přístup ve věci samé a měl by rovněž rozhodnout o rozsahu platných žádostí o přístup. Jakákoli smluvní ujednání mezi správcem a zpracovatelem o dodržování práva na přístup budou záviset na povaze zpracování a na druhu služeb, které zpracovatel poskytuje správci.

Základní premisou je, že správce musí každou žádost posoudit individuálně, na principu *case-by-case*. Správce vezme v úvahu mimo jiné tyto otázky: Zda se žádost týká osobních údajů souvisejících s žádající osobou a kdo je touto žádající osobou. Jak je uvedeno v čl. 12 odst. 2 nařízení GDPR, správce má povinnost usnadňovat výkon práv subjektu údajů podle článků 15 až 22, přičemž musí mít na paměti i odpovídající zabezpečení osobních údajů. Obecně také platí, že správce nemůže odmítnout vyhovět žádosti subjektu údajů za účelem výkonu jeho práv, ledaže doloží (při vynaložení přiměřeného úsilí), že nemůže zjistit totožnost subjektu údajů, k tomu ale podrobněji později. Pokyny EDPB také vyzývají správce, aby u vyřizování žádostí práva na přístup byli proaktivní. Článek 15 nařízení GDPR sice předpokládá, že subjekt údajů musí právo na přístup aktivně uplatnit. Současně se ale od správce očekává, že by měl být v první řadě připraven takovou žádost obdržet, řádně ji posoudit a bez zbytečného odkladu poskytnout žadateli vhodnou odpověď. Způsob, jakým se správce připraví na uplatnění žádosti o přístup, by měl být vhodný a přiměřený a měl by záviset na povaze, rozsahu, kontextu a účelech zpracování, jakož i na rizicích pro práva a svobody fyzických osob v souladu s článkem 24 nařízení GDPR (princip odpovědnosti správce). Nedodržení povinností správce, včetně těch, které se týkají práva na přístup, může vyústit k tomu, že subjekt údajů podá stížnost u dozorového úřadu, což může vést k uložení pokuty a/nebo dalších nápravných opatření správci osobních údajů. Dozorový úřad může rovněž zahájit vlastní kontrolu u správce, jejímž cílem je zjistit, zda je v souladu s právními předpisy na ochranu osobních údajů.

4.8.1 Požadavky na formu žádosti

Jak již bylo uvedeno výše v kapitole **4.7 Realizace práva na přístup**, v této části se také zaměřím více na požadavky na formu, resp. formát žádosti. Požadavky na formu žádosti jsou uvedeny v článku 12 a 15 nařízení GDPR, z větší části právě ve článku 12. Článek 12 nařízení GDPR totiž neobsahuje pouze obecné požadavky na informační povinnost správce a formu komunikace správce se subjekty údajů, nýbrž také určitá procesní pravidla, která správci musejí dodržovat při výkonu práv subjektů údajů dle čl. 15 až 22 nařízení GDPR. Několikrát již bylo dříve řečeno, že správce by měl výkon práv subjektům údajů usnadňovat.[251] Od správce

[251] Viz první věta čl. 12 odst. 2 nařízení GDPR.

se tedy předpokládá, že umožní dostatek způsobů, jakými mohou subjekty údajů práva uplatnit, především by měl umožnit výkon práv subjektům údajů prostřednictvím všech běžných komunikačních kanálů, jimiž se subjekty údajů komunikuje, např. prostřednictvím webového formuláře, telefonicky, v prostředí své aplikace (např. v elektronickém bankovnictví či po přihlášení k uživatelskému účtu), příp. i osobní návštěvou na pobočce.[252] Nařízení GDPR neukládá subjektům údajů žádné zvláštní požadavky týkající se formy žádosti o přístup k osobním údajům. Neexistují proto žádné požadavky podle nařízení GDPR, které by musely subjekty údajů dodržovat při výběru komunikačního kanálu, jehož prostřednictvím hodlají vstoupit do kontaktu se správcem.

Pokud jde o otázku komunikačních kanálů, obecně platí, že je primárně na rozhodnutí subjektu údajů, jak s ním má správce při výkonu práv komunikovat. Jestliže ale subjekt údajů formu blíže neupřesní a není to jasné ani na základě podané žádosti, je pak na správci, aby rozhodl o vhodném formátu, v němž budou osobní údaje poskytnuty. Čl. 12 odst. 1 nařízení GDPR stanoví, že informace jsou poskytovány písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Subjekt údaje si však může vyžádat i poskytnutí informací ústně, a to za předpokladu, že je identita subjektu údajů prokázána jinými způsoby. Na základě jazykového výkladu ustanovení lze usuzovat, že zákonodárce pravděpodobně předpokládal, že nejčastější formou odpovědí na žádosti subjektů údajů bude písemná podoba. V praxi současné doby lze vzhledem k technologickému rozvoji usuzovat, že převládající podobou poskytnutí informací bude elektronická forma, neboť žádosti o přístup jsou často podávány v souvislosti s elektronicky (online) poskytovanými službami. Ostatně, význam elektronické podoby zdůrazňuje i samotné nařízení GDPR ve svém čl. 12 odst. 3, kdy říká, že správce poskytne informace v elektronické podobě, je-li to možné, pokud zároveň subjekt údajů nepožádá o jiný způsob. Obdobně je význam elektronické formy zdůrazněn i v čl. 15 odst. 3, zde je akorát zdůrazněno, že má jít o elektronickou formu, *která se běžně používá*. Správce by měl mít nicméně nastaveny vnitřní procesy pro všechny varianty, tedy pro komunikaci elektronickou, písemnou i ústní. Zároveň musí být správce schopen vždy v souladu se zásadou odpovědnosti dle čl. 5 odst. 2 nařízení GDPR doložit, co a jak subjektům sdělil a jaká opatření přijal, včetně způsobu, jakým byla ověřena jeho totožnost. To má zejména význam v případě, že byla informace subjektu údajů poskytnuta ústně. Skupina WP29 ve svých Pokynech

[252] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.

k transparentnosti dále uvádí, že správce by měl být připraven umožnit subjektu údajů i opětovný poslech předem nahraných zpráv. To je nezbytným požadavkem, pokud žádost o poskytnutí informací ústní formou vznesl subjekt údajů se zrakovým postižením nebo jiný subjekt údajů, pro nějž může být obtížné získat přístup k informacím v písemné formě či takovým informacím porozumět.[253]

EDPB povzbuzuje správce, aby poskytovali takové komunikační kanály, které se jeví jako nejvhodnější a uživatelsky nejpřívětivější, aby subjekt údajů mohl podat účinnou žádost. Pokud však subjekt údajů podá žádost prostřednictvím komunikačního kanálu poskytnutého správcem, který se liší od toho, který je uveden jako nejvhodnější, musí být i tato žádost obecně považována za účinnou a správce by se měl touto žádostí zabývat. Správci by měli vynaložit veškeré přiměřené úsilí, aby zajistili, že výkon práv subjektu údajů bude usnadněn (například v případě, že subjekt údajů zašle žádost zaměstnanci, který se za standardních okolností žádostmi zabývá a ukáže se, že je na dovolené, může být vynaložení přiměřeného úsilí ze strany správce chápáno jako vytvoření automatické informace zaslané subjektu údajů o alternativním komunikačním kanálu pro řešení jeho žádosti). Pokyny EDPB[254] dále upřesňují, že za situace, kdy subjekt údajů zašle žádost na náhodnou nebo zjevně nesprávnou e-mailovou (nebo poštovní) adresu, kterou správce přímo neposkytuje jako vhodný komunikační kanál, přičemž takový vhodný komunikační kanál správce vytvořil, není správce povinen se touto žádostí zabývat. Tím je myšleno i zaslání žádosti zjevně nezpůsobilým zaměstnancům/ pracovníkům správce (např. řidiči, uklízečky). EDPB zároveň správcům doporučuje, aby s ohledem na cíl usnadnění výkonu práv subjektů údajů zavedli takové mechanismy, které zajistí lepší interní komunikaci mezi zaměstnanci, tedy včetně těch, v jejichž kompetenci není vyřizovat žádosti o přístup. EDPB dále rozhodně správcům doporučuje, aby měli zavedeno více komunikačních kanálů. Příklad č. 8: Poskytovatel zdravotnických služeb nabízí elektronický formulář na svých internetových stránkách i tištěné formuláře na recepcích klinik, takže žádosti o přístup k osobním údajům lze podat jak elektronicky, tak osobně. I přes tyto možnosti poskytovatel nadále přijímá žádosti podané jinými způsoby, jako například poštou nebo e-mailem. Kromě toho má navíc určenou kontaktní osobu, kterou lze oslovit e-mailem nebo telefonicky a která pomáhá subjektům údajů s uplatňováním jejich práv.[255]

[253] WP29. *Pokyny k transparentnosti WP 260 rev.01*, přijaté dne 29. listopadu 2017 naposledy revidované a přijaté dne 11. dubna 2018, s. 13. Dostupné z: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_cs.pdf.
[254] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 23.
[255] WP29. *Pokyny k transparentnosti WP 260 rev.01*, přijaté dne 29. listopadu 2017 naposledy revidované a přijaté dne 11. dubna 2018, s. 27. Dostupné z: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_cs.pdf.

4.8.2 Vztah mezi subjektem údajů a osobními údaji, o jejichž přístup žádá

Právo na přístup se týká „subjektu údajů“ a může jej vykonávat pouze subjekt údajů, příp. osoba, která jej právně zastupuje. Článek 12 odst. 6 nařízení GDPR zejména umožňuje správcům, kteří mají „důvodné pochybnosti“ o totožnosti „fyzické osoby podávající žádost“, požádat o dodatečné informace, pokud se domnívají, že je „nezbytné potvrdit totožnost subjektu údajů“. Recitál 64 nařízení GDPR dále požaduje, aby správce použil „*všechna vhodná opatření k ověření identity subjektu údajů, který žádá o přístup*“, se zvláštní pozorností věnovanou „*on-line službám a síťovým identifikátorům*“. Zpřístupnění osobních údajů někomu jinému než subjektu údajů na základě žádosti o přístup by mohlo totiž představovat porušení zabezpečení osobních údajů, které je rovněž definováno jako „*neoprávněné poskytnutí nebo zpřístupnění přenášených osobních údajů*“[256]. Mohlo by rovněž porušit zásadu integrity a důvěrnosti zpracování těchto údajů a právo na respektování soukromého života subjektu údajů. Je proto důležité, aby se správce ujistil, že žadatel je subjektem údajů. Nařízení GDPR neukládá žádné požadavky týkající se metod pro určení totožnosti subjektu údajů. Články 11 a 12 však stanoví podmínky pro výkon všech práv subjektu údajů, včetně práva na přístup k osobním údajům. Žádost o dodatečné informace za účelem vyhovění žádosti o přístup je však zákonná pouze tehdy, jsou-li tyto informace nezbytné k identifikaci subjektu údajů (proto jsou uchovávány tak dlouho, jak je to nezbytné pro identifikaci subjektu údajů), a pokud splňují test proporcionality.

Je třeba mít na paměti, že správce zpravidla nemůže požadovat více osobních údajů, než je nezbytné pro umožnění této identifikace a že použití těchto informací by mělo být přísně omezeno na splnění žádosti subjektů údajů. Příklad č. 9: U požadavku kopie cestovního pasu nebo dokladu totožnosti osoby, která žádá o přístup ke všem osobním údajům zpřístupněným třetím osobám prostřednictvím mobilní aplikace instalované v jejich telefonu, nebude pravděpodobně splněna nezbytnost. Správce totiž může zajistit ověření totožnosti subjektu údajů jiným a pro subjekt údajů méně zatěžujícím způsobem. V důsledku toho je v tomto případě nepřiměřené požadovat kopii dokladu totožnosti. To ostatně potvrzují i Pokyny týkající se práva na přenositelnost údajů[257], když hovoří o tom, že možnost správce vyžádat si dodatečné informace pro posouzení totožnosti osoby nemůže vést k nadměrným požadavkům a ke

[256] Viz článek 4 bod 12 nařízení GDPR.
[257] WP29. *Pokyny týkající se práva na přenositelnost údajů WP 242 rev.01*, přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017, s. 15. Dostupné zde: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-tykajici-se-prava-na-prenositelnost-udaju-v-cestine.pdf.

shromažďování osobních údajů, které nejsou relevantní ani nezbytné na posílení propojení mezi fyzickou osobou a požadovanými osobními údaji. Pokyny uvádí jako příklad dobré praxe ověření totožnosti pro vyřízení žádosti o přístup k údajům subjektů údajů v jejich e-mailových účtech, účtech na sociálních sítích a účtech používaných pro různé jiné služby, použití uživatelských jmen a hesel, z nichž některá si uživatelé sami volí, aniž by odhalili své celé jméno a totožnost. Pokud je tedy zpracování spojeno s uživatelským účtem, může k identifikaci subjektu údajů stačit poskytnutí příslušného přihlašovacího jména a hesla. Na možnosti digitální identifikace subjektu údajů poukazuje i recitál 57 nařízení GDPR, který říká, že: *„součástí identifikace by měla být digitální identifikace subjektu údajů, například prostřednictvím mechanismu autentizace na základě stejných pověřovacích údajů, které subjekt údajů používá pro přihlášení k on-line službám poskytovaným správcem údajů*.“ Pokyny k právu na přístup vyzdvihují zejména roli dvoufázového ověřování, kdy po přihlášení uživatele (za předpokladu, že byl jeho účet zřízen), správce vytvoří ve svém systému jednorázový jedinečný kód, který odešle na číslo mobilního telefonu uživatele a ten jej pak potvrdí či zadá znovu do systému.[258]

Jak již jsem uvedla výše, problematika důslednější minimalizace osobních údajů při kopírování občanských průkazů nebo cestovních dokladů je v poslední době předmětem pozornosti EDPB, viz doporučení v Pokynech k právu na přístup.[259] Pokyny jasně zdůrazňují, že použití kopie dokladu totožnosti v rámci procesu ověřování totožnosti představuje riziko pro zabezpečení osobních údajů a může vést k neoprávněnému nebo protiprávnímu zpracování, a jako takové by mělo být považováno za nevhodné, pokud to není nezbytně nutné, vhodné a v souladu s vnitrostátními právními předpisy. V takových případech by správci měli mít zavedeny systémy, které zajistí úroveň zabezpečení vhodnou formou ke zmírnění vyšších rizik pro práva a svobody subjektu údajů, pokud jde o přijímání těchto údajů. Je rovněž důležité poznamenat, že identifikace prostřednictvím průkazu totožnosti nemusí být vhodnou identifikací zejména v on-line kontextu (např. s použitím pseudonymů), pokud subjekt údajů nemůže poskytnout žádné jiné důkazy, např. další prvky nebo vlastnosti umožňující propojení k jeho uživatelskému účtu. Ačkoli řada soukromoprávních organizací (např. hotely, banky, půjčovny aut) dnes požaduje kopie průkazu totožnosti svých klientů, nemělo by to být obecně považováno za vhodný způsob ověřování, jak uvádí Pokyny. Správce může totiž zavést rychlé

[258] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 26.
[259] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 27-29.

a účinné bezpečnostní opatření k identifikaci subjektu údajů, který byl správcem dříve ověřen, např. prostřednictvím e-mailu nebo textové zprávy obsahující potvrzovací odkazy, prostřednictvím bezpečnostních otázek nebo potvrzovacích kódů. V každém případě mohou být informace o identifikačním dokladu, které nejsou nezbytné pro potvrzení totožnosti subjektu údajů, jako je státní příslušnost, rodné číslo, velikost/ výška, barva očí, fotografie a strojově čitelná zóna, před jejich předložením správci začerněny nebo skryty (např. prostřednictvím zvláštní šablony), s výjimkou případů, kdy vnitrostátní právní předpisy vyžadují úplnou neupravenou kopii průkazu totožnosti.

Pokyny hovoří dokonce o tom, že dobrou praxí by ze strany správců měla být jejich snaha být maximálně nápomocni subjektům údajů (pokud subjekt údajů například neví, jak nebo není schopen tyto zbytné informace skrýt). Příklad č. 10: Uživatelka paní Nováková si založila účet v internetovém obchodě (eshopu) s použitím svého e-mailu a uživatelského jména. Následně tato uživatelka požádá správce o informace, zda zpracovává její osobní údaje, a pokud ano, požádá o přístup k nim podle článku 15. Správce požaduje doklad totožnosti této žádající osoby (zaslání kopie dokladu), aby mohl ověřit její totožnost. Požadavek správce je v tomto případě dle Pokynů nepřiměřený a vede k nadbytečnému sběru údajů. Místo toho může správce (v souladu se zásadou minimalizace údajů, tj. zabránit nadbytečnému sběru údajů) k ověření totožnosti osoby využít (neinvazivní) bezpečnostní otázky, které byly nastaveny již v okamžiku registrace účtu subjektu údajů, nebo může implementovat vícefaktorovou autentizaci pro vyřízení žádosti o přístup.

Názor, že k ověřování totožnosti subjektu údajů pro potřeby vyřízení žádosti o přístup není vhodné požadovat kopie dokladů totožnosti, si postupně osvojují i někteří zástupci z praxe. Upozorňuje na to například Brendan Quinn, autor praktické příručky k implementaci ochrany údajů[260]. Ten uvádí, že v počátcích GDPR se přístupy jednotlivých unijních států lišily, přičemž ovšem řada z nich tuto praxi považovala za přípustnou. Jiné přístupy, třeba nizozemský dozorový úřad, však od počátku viděly potenciální rozpor se zásadou minimalizace údajů v článku 5 GDPR a nyní se zdá, že se postupně stávají převládajícím názorem ostatních regulačních orgánů. Správci by si však vždy měli ověřit osvědčené postupy u příslušných regulačních orgánů svého členského státu a u vnitrostátních soudů. Quinn proto také doporučuje raději využít alternativní opatření, např. ověření identity prostřednictvím přihlašovacího

[260] QUINN, Brendan, 2021. Chapter 9: Data Subject Rights. Online. In: *Data Protection Implementation Guide: A Legal, Risk and Technology Framework for GDPR*. Wolters Kluwer, s. 171-184. ISBN 978-9403529004. Dostupné z: Kluwer Law International. [cit. 2024-08-24].

systému (loginu) nebo dvoufaktorové ověřování. Jeho další doporučení se převážně shodují s doporučeními v Pokynech EDPB. Quinn nad rámec ještě uvádí jako relativně bezpečné možnost správce vyžádat si poslední tři číslice čísla účtu subjektu údajů, jeho datum narození a/nebo zákaznické číslo; případně klasicky požádat subjekt údajů, aby se zastavil osobně a předložil svůj doklad totožnosti, aniž by se u něj pořizovala kopie.

O významu této problematiky svědčí také stále probíhající spory českého Úřadu pro ochranu osobních údajů (dále jen „Úřad“) s Finančním analytickým úřadem (dále jen „FAÚ“). Ten v rámci svého zaměření – boje proti praní špinavých peněz nebo financování terorismu (tzv. AML účel) vydal již několik verzí metodických pokynů k otázce kopírování průkazů totožnosti pro účely AML zákona.[261] Aniž bych chtěla detailně rozebírat předmět tohoto sporu, Úřad trvá na svém dříve přijatém postoji, že pořizování kopií by nemělo být plošné, ale v konkrétních případech odůvodněné, zejména podezřením na možné porušování zákona, jehož účelem je zabránění zneužívání finančního systému k legalizaci výnosů z trestné činnosti a k financování terorismu a vytvoření podmínek pro odhalování takového jednání. V souladu s principy GDPR (především principem minimalizace, obsaženým v čl. 5 odst. 1 písm. c) nařízení GDPR, a tzv. konceptem záměrné a standardní ochrany osobních údajů, obsaženým v článku 25 nařízení GDPR) musí podle Úřadu povinná osoba v postavení správce již od počátečních fází zpracování, tedy již od návrhu operací zpracování, zavést taková technická a organizační opatření, která od samého počátku zajišťují ochranu soukromí a principů ochrany osobních údajů klientů. Povinná osoba by tedy měla zaujmout proaktivní přístup založený na riziku (*risk based approach*) a provést základní posouzení rizik pro práva a svobody klientů z hlediska ochrany osobních údajů, především principů nezbytnosti a přiměřenosti, a to ještě před pořízením takových kopií dokladů totožnosti. Pokud povinná osoba v konkrétním případě dospěje k tomu, že pořízení a uchování kopie dokladu totožnosti nebude nezbytným nebo přiměřeným opatřením (v konkrétním případě bude zcela dostačující pro daný účel předcházet legalizaci výnosů z trestné činnosti a financování terorismu pouze ověřit a zaznamenat identifikační údaje klienta), pak takovou kopii pořídit nesmí. Tomuto postoji ostatně odpovídá i fakt, že AML zákon sice pracuje s povinností identifikace a hloubkové kontroly klienta[262], ve

[261] Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.
[262] Viz ustanovení § 7 a 9 AML zákona. [cit. 2024-08-24].

vztahu k přímému pořizování kopií však hovoří pouze o oprávnění, resp. fakultativní možnosti povinných osob pořizovat kopie průkazů totožnosti.[263]

Právním základem AML problematiky na úrovni EU je směrnice Evropského parlamentu a Rady (EU) 2015/849 (tzv. „4. AML směrnice“) ze dne 20. května 2015, o předcházení využívání finančního systému k praní peněz a financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES, konkrétně ve znění směrnice Evropského parlamentu a Rady (EU) 2018/843 (tzv. „5. AML směrnice“) ze dne 30. května 2018. Tento unijní předpis upravuje povinnost vést příslušné identifikační údaje v kapitole V, v čl. 40 odst. 1 písm. a) (Ochrana údajů, vedení záznamů a statistické údaje), kde se hovoří o povinnosti povinných osob uchovávat následující dokumenty a informace: „*v případě hloubkové kontroly klienta kopii dokumentů a informací, které jsou zapotřebí ke splnění požadavků na hloubkovou kontrolu klienta podle kapitoly II, případně včetně informací získaných elektronickými prostředky identifikace*.“ Je proto důležité doplnit, že vzhledem k tomu, že i v samotné směrnici se hovoří o kopii dokumentů, nezbývá odpůrcům plošného kopírování dokladů příliš manévrovacího prostoru. Také na úrovni členských států EU je výklad různorodý. Velké země jako Německo, Rakousko a Francie uplatňují totiž výklad ve prospěch kopírování dokladů totožnosti. AML směrnici transponovaly do svých vnitrostátních právních řádů oproti ČR odlišně. Německo vydalo nový zákon o sledování výnosů ze závažné trestné činnosti, přičemž v § 8 odst. 2 stanovilo, že je-li při identifikaci fyzické osoby předložen doklad totožnosti, „*má povinná osoba právo a povinnost pořídit si kopie těchto dokladů nebo záznamů nebo je zaznamenat v digitální podobě*.“[264] Důvodová zpráva k citovanému ustanovení uvádí, že nová úprava na rozdíl od předchozího znění zákona, které upřesňovalo, že kopie dokladů předložených ke zjištění totožnosti se považuje za záznam údajů v nich obsažených, je nyní stanoveno právo a povinnost pořizovat kopie dokladů předložených ke zjištění totožnosti. Touto úpravou je tak transponován článek 40 odst. 1 písm. a) AML směrnice. Kromě toho důvodová zpráva uvádí, že se zde odráží názor zastávaný v ustálené správní praxi, že předpisy o praní špinavých peněz týkající se povinnosti uchovávat záznamy představují *lex specialis* k ustanovení o ochraně údajů v zákoně o cestovních pasech a zákoně o občanských průkazech,

[263] Viz poslední věta § 8 odst. 11 AML zákona: „*Povinná osoba <u>může</u> pro účely tohoto zákona pořizovat kopie nebo výpisy z předložených dokladů a zpracovávat takto získané informace k naplnění účelu tohoto zákona, a to bez souhlasu klienta*.“ [cit. 2024-08-24].

[264] Jedná se o ustanovení § 8 odst. 2 větu druhou zákona o sledování výnosů ze závažné trestné činnosti (Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten). Dostupné zde: https://www.gesetze-im-internet.de/gwg_2017/BJNR182210017.html. [cit. 2024-08-24].

která zakazují pořizování kopií dokladů totožnosti.[265] Francie transponovala ustanovení směrnice do článků R.561-5 až R.561-6 měnového a finančního zákoníku.[266] Zde se uvádí, že se ověří totožnost klienta jedním z těchto způsobů: „*3. je-li zákazník fyzickou osobou, fyzicky přítomnou pro účely identifikace v okamžiku navázání obchodního vztahu, předložením originálu platného úředního dokladu s fotografií a pořízením kopie tohoto dokladu*.“ Z toho podle mého názoru vyplývá jediné, že ačkoli je mi blízký přístup českého dozorového úřadu zastávající v první řadě hledisko ochrany subjektů údajů, lze i na evropské úrovni pozorovat silný tlak na plošné pořizování kopií dokladů totožnosti. V zájmu právní jistoty a předvídatelnosti práva by však bylo jistější, kdyby unijní regulace (spíše příslušná AML směrnice nežli nařízení GDPR) přímo upravovala, zda se jedná o povinnost či oprávnění povinného subjektu.

O tom, že je AML problematika velice aktuální, svědčí i dění na evropské úrovni. Dne 20. července 2021 představila Evropská komise legislativní balíček čtyř legislativních návrhů, jehož cílem je posílit opatření EU v oblasti boje proti praní peněz a financování terorismu („AML/CFT“). Tento balíček obsahuje návrh nařízení Evropského parlamentu a Rady o předcházení využívání finančního systému k praní peněz nebo financování terorismu (tzv. „návrh nařízení vztahujícího se na soukromý sektor“), návrh nařízení Evropského parlamentu a Rady, kterým se zřizuje Orgán pro boj proti praní peněz a financování terorismu (tzv. „návrh nařízení, kterým se zřizuje AMLA“), návrh směrnice o mechanismech boje proti praní peněz a návrh revize nařízení o převodech peněžních prostředků. V reakci na tyto evropské návrhy nezůstaly pozadu ani evropští ochránci údajů, a sice EDPB, ani Evropský inspektor ochrany údajů[267], které k balíčku zaslaly své připomínky[268]. EDPB sice uznalo významný veřejný zájem na zajištění boje proti praní peněz a financování terorismu, zdůraznilo však nutnost zajistit soulad s GDPR, zejména základními zásadami zpracování (především zásada účelového

[265] Důvodová zpráva k německému zákonu o sledování výnosů ze závažné trestné činnosti. Dostupná zde: https://dserver.bundestag.de/btd/18/115/1811555.pdf. [cit. 2024-08-24].
[266] Způsoby ověření totožnosti klienta (je-li klientem fyzická osoba) jsou v bodě 3. článku R. 561–5–1 Code monétaire et financier (Měnový a finanční zákoník). Dostupné zde: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043332956. [cit. 2024-08-24].
[267] Tzv. European Data Protection Supervisor, zkráceně „EDPS“. Jedná se o orgán, který dohlíží na to, aby orgány a instituce EU dodržovaly při zpracovávání osobních údajů právo občanů na soukromí.
[268] Např. Dopis EDPB adresovaný Evropské komisi ze dne 12. května 2022, dostupné zde: https://www.edpb.europa.eu/system/files/2022-05/edpb_letter_out2022-0035_aml_cft_proposal_ec_en.pdf. Dále Dopis EDPB Evropskému parlamentu, Radě a Evropské komisi ze dne 28. března 2023 ke sdílení údajů pro účely boje proti praní peněz a financování terorismu s ohledem na mandát Rady k jednání, dostupné zde: https://www.edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0018_aml_cft_council_en.pdf. Dále Stanovisko evropského inspektora ochrany údajů 12/2021 ze dne 22. září 2021 k balíčku legislativních návrhů týkajících se boje proti praní peněz a financování terorismu (AML/CFT), dostupné zde: https://www.edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf. [cit. 2024-08-24].

omezení, přesnosti a zásada minimalizace údajů). Povinné subjekty totiž zpracovávají osobní údaje, které umožňují vyvodit intimní závěry o jednotlivcích a které mohou vést zejména k vyloučení právnických a fyzických osob z poskytnutí práva nebo služby (např. poskytování bankovních služeb). V rámci připomínek zároveň vyzvalo orgány EU, aby více zapojily EDPB a EDPS do diskuzí o legislativních návrzích. EDPB kromě toho kritizovalo nedostatečné zakotvení záruk, zejména pokud jde o zpracování zvláštních kategorií údajů (tzv. citlivých údajů) a údajů týkajících se rozsudků v trestních věcech, patřících pod články 9 a 10 nařízení GDPR. Legislativní návrhy navíc nestanoví konkrétní pravidla ve vztahu ke zdrojům, které mají povinné subjekty používat pro shromažďování informací. Rizika také EDPB spatřuje ve vztahu k informacím získaným zapojením externích poskytovatelů služeb.

Pokud jde o EDPS, tak ten ve svém šířeji pojatém stanovisku obecně uvítal cíle legislativního AML balíčku, stejně jako přístup založený na posouzení rizik, připojil ovšem několik doporučení. Aby byl zajištěn soulad se zásadami nezbytnosti a přiměřenosti ochrany údajů, měly by legislativní návrhy určit kategorie osobních údajů, které mají povinné osoby zpracovávat za účelem splnění povinností v oblasti AML/CFT. Dále by měly návrhy poskytnout jasné informace o podmínkách a omezeních zpracování zvláštních kategorií osobních údajů a osobních údajů souvisejících s rozsudky v trestních věcech a trestnými činy. Ve vztahu ke zvláštní kategorii osobních údajů by návrhy měly zejména stanovit, který typ údajů by měly povinné osoby zpracovávat a v jaké přesné fázi procesu pro účely boje proti praní peněz a financování terorismu. V tomto ohledu se EDPS domnívá, že by nemělo být povoleno zpracování osobních údajů týkajících se sexuální orientace nebo etnického původu. EDPS kromě toho ještě doplnil několik dílčích doporučení konkrétně ve vztahu k registrům informací o skutečných majitelích. Zaprvé, že seznam informací by měl být úplným (taxativním) seznamem. Zadruhé, že přístup správců daně i orgánů stavovské samosprávy k registrům informací by měl být omezen pouze na účel boje proti praní peněz a financování terorismu. A zatřetí, EDPS uplatnil rezervovaný postoj k všeobecnému přístupu veřejnosti k informacím o skutečných majitelích. Podle něj jsou totiž účelem identifikace a předcházení praní peněz a financování terorismu pověřeny pouze příslušné orgány, které jsou pověřeny vynucováním práva, a povinné osoby při přijímání opatření hloubkové kontroly klienta. EDPS dále ve vztahu ke zpracování osobních údajů souvisejících s rozsudky v trestních věcech doporučil vypustit odkaz na „nařčení“ (kromě „vyšetřování“, „řízení“ a „odsouzení“), vzhledem k jeho neurčitosti. Kromě toho EDPS doporučil jasně a vyčerpávajícím způsobem vymezit kategorie osobních údajů, ke kterým mohou mít finanční zpravodajské jednotky

přístup (finanční informace). Také právní uspořádání finančních zpravodajských jednotek by mělo být, aby bylo zcela v souladu se zásadami ochrany údajů, založeno na vyšetřování namísto uspořádání založeného na zpravodajských informacích. Posledním důležitým doporučením, které stojí za to zmínit, je že návrh by měl především vyjasnit, ve kterých případech by povinné osoby měly využívat tzv. kontrolní seznamy a uvést, že povinné osoby by měly řádně ověřovat informace z těchto seznamů, zejména s ohledem na jejich spolehlivost a přesnost.

K rozlišení, kdy správce může potřebovat po subjektu údajů uvedení „dodatečných informací" a kdy nikoliv, si dovolím uvést jeden příklad, tentokrát z aktuální oblasti informačních technologií, na nějž odkazují Pokyny k právu na přístup.[269] Příklad č. 11: Správce zpracovává osobní údaje za účelem behaviorálního marketingu (adresování behaviorální reklamy) vůči svým internetovým uživatelům. Osobní údaje shromažďované pro behaviorální reklamu jsou obvykle shromažďovány pomocí souborů cookies a jsou spojeny s pseudonymními náhodnými identifikátory. Subjekt údajů pan Novák uplatní u správce právo na přístup prostřednictvím jeho internetových stránek. Správce je schopen za těchto okolností přesně identifikovat pana Nováka, neboť mu může ukázat behaviorální reklamu tak, že propojí koncové zařízení pana Nováka s jeho reklamním profilem prostřednictvím souborů cookies zanechaných v koncovém zařízení. Správce by měl být také schopen přesně identifikovat pana Nováka, aby mu umožnil přístup k jeho osobním údajům, neboť lze nalézt spojení mezi zpracovávanými údaji a subjektem údajů. Z tohoto důvodu a s ohledem na zásady GDPR, jako je zásada korektnosti, by výše uvedený příklad nespadal do oblasti působnosti článku 11 nařízení GDPR a žádné dodatečné informace by správce nepotřeboval. Jinou situací by ovšem bylo, pokud by pan Novák uplatnil své právo na přístup e-mailem nebo obyčejným dopisem zaslaným správci, pak v této souvislosti nebude mít správce jinou možnost, než požádat pana Nováka, aby poskytl „dodatečné informace" (čl. 12 odst. 6 nařízení GDPR), aby mohl identifikovat reklamní profil spojený s panem Novákem. V tomto případě bude dodatečnými informacemi identifikátor souborů cookie uložený v koncovém zařízení pana Nováka.

Za určitých okolností může být pro správce velmi problematické subjekt údajů identifikovat, resp. jej vyhledat v datasetu, v němž jeho údaje zpracovává. To je typicky problém u kamerových záznamů. K tomu existuje vyjádření EDPB v podobě Pokynů

[269] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 24-25.

k videotechnice, týkajících se kamerových systémů.[270] Podle EDPB, pokud se ve videozáznamu nedají vyhledat osobní údaje (tj. správce by musel projít velké množství uchovávaného materiálu, aby nalezl příslušný subjekt údajů), správce nemusí být schopen identifikovat subjekt údajů. Z těchto důvodů by subjekt údajů měl v žádosti o přístup správci uvést, kdy – v rámci přiměřeného časového období v poměru k počtu zaznamenaných subjektů údajů – vstoupil do monitorované oblasti. Správce by měl ovšem předem subjekt údajů informovat o tom, jaké údaje jsou k nalezení příslušných informací potřebné. V tomto smyslu tak EDPB připouští to, že subjekt údajů může být v určitých situacích povinen poskytnout pro kladné vyřízení své žádosti potřebnou součinnost, přičemž její neposkytnutí může vést v krajním případě k tomu, že jeho právo nebude možné realizovat. Jestliže tak subjekt údajů v rámci své žádosti o přístup uvede, že se v kamerami monitorované oblasti vyskytoval v roce 2020, aniž by poskytl další specifikaci, nebude pravděpodobně možné jej ve videozáznamech vyhledat a poskytnout mu kopii tohoto videozáznamu. Obecně platí, že čím je monitorovaný prostor exponovanější na veřejnosti, tj. vystaven většímu počtu pohybujících se osob, tím více informací (a obsahově přesnější informace) bude správce od subjektu údajů potřebovat, aby mohl jeho právu na přístup vyhovět.

Příklad č. 12: Subjekt údajů požádá o přístup a o kopii svých osobních údajů zpracovaných prostřednictvím monitoringu pomocí videokamer při vstupu do obchodního centra. Jde o obchodní centrum, které navštíví cca 30 000 osob denně, subjekt údajů by proto měl upřesnit, kdy prošel monitorovanou oblastí v časovém rámci přibližně jedné hodiny. Pokud správce materiál stále zpracovává, měla by být poskytnuta kopie videozáznamu. Jestliže je možné ve stejném materiálu identifikovat další subjekty údajů, měla by být tato část materiálu anonymizována (například rozmazáním kopie nebo jejích částí), a to před poskytnutím kopie subjektu údajů, který podal žádost. Jde o projev omezení obsaženého v čl. 15 odst. 4 nařízení GDPR, které říká, že právem získat kopii nesmějí být nepříznivě dotčena práva a svobody jiných osob. K tomu Pokyny[271] uvádí: „*Ochrana práv třetích osob by však neměla být využívána jako výmluva s cílem zabránit oprávněným nárokům na přístup jednotlivců, správce by v těchto případech měl zavést technická opatření ke splnění žádosti o přístup (například úprava záznamu, jako je maskování nebo šifrování). Správci však nejsou povinni tato technická opatření zavádět, pokud mohou jiným způsobem zajistit, že jsou schopni reagovat na žádost*

[270] EDPB. *Guidelines 03/2019 on processing of personal data through video devices*, version 2.0, Adopted on 29 January 2020, s. 22-23, body 94, 95 a 96. Dostupné zde: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.
[271] Tamtéž.

podle článku 15 ve lhůtě stanovené v čl. 12 odst. 3.“ Pokyny dále uvádí, že pokud správce automaticky maže všechny záznamy, například do dvou dnů, není tak schopen po těchto dvou dnech subjektu údajů záznam poskytnout. Pokud správce po těchto dvou dnech obdrží žádost, měl by být subjekt údajů odpovídajícím způsobem o této faktické nemožnosti informován.

4.8.3 Analýza obsahu žádosti

Způsob, jakým lze přistoupit k analýze obsahu žádosti o přístup lze demonstrovat položením následujících pěti otázek:

A) Týká se žádost osobních údajů?

Podle nařízení GDPR se oblast působnosti žádosti o přístup vztahuje pouze na osobní údaje. Žádost o informace o dalších otázkách, včetně obecných informací o správci, jeho obchodních modelech nebo činnostech zpracování nesouvisejících s osobními údaji, se proto nepovažuje za žádost podanou podle článku 15 nařízení GDPR. Kromě toho žádost o informace o anonymních údajích nebo údajích, které se netýkají žádající osoby nebo osoby, jejímž jménem oprávněná osoba podala žádost, nebude spadat do rozsahu práva na přístup. K tomu si dovolím ještě jedno zpřesnění. Podle generálního advokáta Manuela Campos Sánchez-Bordony se struktura článku 15 nařízení GDPR skládá z: *potvrzení zda osobní údaje, které se subjektu údajů týkají, jsou či nejsou zpracovávány* (1); *přístupu k těmto osobním údajům* (2) *a přístupu k následujícím informacím* (3), tedy k těm, které jsou uvedeny v písmenech a) až h) tohoto ustanovení. Podle generálního advokáta tedy ustanovení rozlišuje mezi „*osobními údaji*“ na jedné straně a „*informacemi*“, na které odkazují písmena uvedená v odstavci 1 na straně druhé. Informace, které mají být subjektu údajů poskytnuty podle čl. 15 odst. 1 písm. a) až h) nařízení GDPR, tedy nelze zaměňovat s osobními údaji subjektu údajů ve smyslu čl. 4 odst. 1 nařízení GDPR. Stručněji řečeno, oblast působnosti žádosti o přístup je širší a nejedná se tak jen o osobní údaje subjektu údajů. Subjekt údajů má podle článku 15 nařízení GDPR fakticky právo na přístup nejen ke svým osobním údajům, ale i k informacím o samotném zpracování a jeho okolnostech, které jsou vyjmenovány pod písmeny a) až h) nařízení GDPR.[272] Pokud jde o pseudonymizované údaje[273], tak na rozdíl od anonymních údajů (které nejsou osobními údaji)

[272] Stanovisko generálního advokáta Manuela Campos Sánchez-Bordony ze dne 15. prosince 2022, Pankki S, C-579/21, EU:C:2022:1001. V této věci byl dne 22. června 2023 vydán rozsudek Soudního dvora EU. Rozsudek přinesl detailnější rozbor článku 15 nařízení GDPR a bude podrobně analyzován v další části páté.
[273] Viz recitál 26 nařízení GDPR. WP29. *Stanovisko č. 4/2007 WP136 k pojmu osobní údaje*, přijaté dne 20. června 2007, s. 18-21. Dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf.

jsou pseudonymizované údaje, které by mohly být přiřazeny fyzické osobě použitím dodatečných informací, osobními údaji. Pseudonymizované údaje, které mohou být spojeny se subjektem údajů (např. tím, že tento subjekt údajů poskytne příslušné identifikační informace, viz čl. 11 odst. 2 nařízení GDPR), proto spadají do oblasti působnosti žádosti. [274]

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

Obecně platí, že žádost se může týkat pouze osobních údajů osoby, která žádost podala. O přístup k osobním údajům jiných osob lze požádat, pouze pokud se jedná o žádosti podané třetími osobami/ prostřednictvím zástupců (k tomu podrobněji v části **5.9 Právo na přístup učiněné třetími osobami/ prostřednictvím zástupců**).

C) Použijí se jiná ustanovení než nařízení GDPR upravující přístup k určité kategorii údajů?

Podle nařízení GDPR nemusí subjekty údajů ve své žádosti uvádět právní základ. Pokud však subjekty údajů objasní, že jejich žádost vychází z odvětvových právních předpisů[275] nebo z vnitrostátních právních předpisů upravujících konkrétní otázku přístupu k určitým kategoriím údajů, a nikoli z nařízení GDPR, pak správce posoudí tuto žádost v souladu s těmito odvětvovými nebo vnitrostátními předpisy, a ustanovení GDPR se na tuto žádost nepoužijí. Pokud subjekty údajů rovněž požádají o přístup ke svým údajům podle článku 15 a správce současně již poskytl údaje podle jiných právních předpisů, měl by správce ověřit, zda již byly splněny povinnosti podle nařízení GDPR (tj. zda již byly poskytnuty všechny informace podle článku 15) či nikoli (v takovém případě musí správce poskytnout další informace). Má-li správce pochybnosti o tom, jaké právo si subjekt údajů přeje uplatnit, může požádat subjekt údajů, který žádost podal, o vysvětlení, resp. specifikaci předmětu žádosti. Tím ovšem není dotčena povinnost správce jednat bez zbytečného odkladu. Pokud však správce v případě pochybností požádá subjekt údajů o další vysvětlení a neobdrží žádnou odpověď, měl by (s přihlédnutím k povinnosti usnadňovat výkon práva na přístup) přesto provést výklad obsahu

[274] WP29. *Pokyny týkající se práva na přenositelnost údajů WP 242 rev.01*, přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017, s. 10. Dostupné zde: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-tykajici-se-prava-na-prenositelnost-udaju-v-cestine.pdf.

[275] Viz WP29. *Pokyny týkající se práva na přenositelnost údajů WP 242 rev.01*, přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017, s. 9, poznámka pod čarou 15: „*Například je-li konkrétním cílem žádosti subjektu údajů poskytnout přístup k historii transakcí na svém bankovním účtu poskytovateli služeb informování o účtu, a to pro účely uvedené v druhé směrnici o platebních službách, měl by být tento přístup udělen podle ustanovení této směrnice*.“ Dostupné zde: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-tykajici-se-prava-na-prenositelnost-udaju-v-cestine.pdf.

žádosti a jednat na jeho základě. Správce může stanovit vhodný časový rámec, během něhož může subjekt údajů poskytnout další vysvětlení. Při stanovení tohoto časového rámce by měl správce ovšem počítat s dostatkem času na řešení žádosti o přístup. Pokud je žádost zaměřena na získání přístupu podle nařízení GDPR, tak skutečnost, že existuje zvláštní právní úprava, neznamená, že tato zvláštní právní úprava převáží nad obecným uplatňováním práva na přístup, jak je stanoveno v nařízení GDPR. K tomu je ale nutné doplnit, jak uvádí článek 23 nařízení GDPR, že mohou existovat omezení stanovená právními předpisy EU nebo vnitrostátními právními předpisy, přičemž tato omezení se mohou vztahovat i k právu na přístup (více v části 6.3 – Omezení práva na přístup).

D) Spadá žádost do oblasti působnosti článku 15?

Nařízení GDPR nezavádí žádné zvláštní formální požadavky na žádost o přístup k osobním údajům či na osoby žádající o přístup. K podání žádosti o přístup stačí, aby žádající osoby upřesnily, že chtějí vědět, jaké osobní údaje, které se jich týkají, správce zpracovává. I z hlediska obsahu může být žádost neformální, nemusí ani obsahovat výslovně odkaz na ustanovení článku 15, bude-li z jejího obsahu zřejmé, že se jedná o uplatnění práva na přístup. Správce proto nemůže odmítnout poskytnutí údajů odkazem na nedostatek uvedení právního základu žádosti, zejména na neexistenci konkrétního odkazu na právo na přístup nebo na nařízení GDPR. Pokyny EDPB[276] konkrétně uvádí, že zcela dostačující je, pokud subjekty údajů nebo jejich zástupci uvedou, že:

— chtějí získat přístup k osobním údajům, které se jich týkají;

— uplatňují své právo na přístup; nebo

— chtějí znát informace, vztahující se k jejich osobě, které správce zpracovává.

Správci by si zároveň měli uvědomit jednak svou povinnost usnadňovat výkon práv subjektů údajů, jednak skutečnost, že žadatelé zpravidla nemusí být obeznámeni se složitostí nařízení GDPR. Správci by proto měli zaujmout vstřícný a shovívavý přístup, tím spíše, pokud jsou žádající osoby zároveň zranitelné osoby (zejména děti, starší osoby, osoby s hendikepem). Obecně platí, že v případě jakýchkoli pochybností se vždy správci doporučuje, aby požádal subjekt údajů, který žádost podal, o upřesnění předmětu žádosti.

[276] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 22.

E) Chtějí subjekty údajů získat přístup ke všem zpracovávaným informacím o nich, nebo jen k jejich částem, resp. jen k některým informacím?

Správce musí vždy posoudit, zda žádosti podané žádajícími osobami odkazují na všechny informace, nebo jen části informací o nich zpracovávaných. Pokyny EDPB uvádí, že jakékoli omezení rozsahu žádosti na konkrétní ustanovení článku 15 nařízení GDPR ze strany subjektů údajů musí být jasné a jednoznačné. Pokud ale subjekty údajů vyžadují doslovné „informace o údajích zpracovávaných v souvislosti s nimi“, měl by správce předpokládat, že subjekty údajů hodlají uplatnit své právo podle čl. 15 odst. 1 až 2 nařízení GDPR v plné míře. Taková žádost by neměla být vykládána v tom smyslu, že si subjekty údajů přejí získat pouze kategorie osobních údajů, které jsou zpracovávány, a vzdát se svého práva obdržet informace uvedené v čl. 15 odst. 1 písm. a) až h). Jiným případem je, pokud subjekty údajů výslovně specifikují, že si přejí získat přístup ke zdroji nebo původu svých osobních údajů nebo ke stanovené době uchovávání. V takovém případě může správce omezit svou odpověď na konkrétní požadované informace.

4.9 Právo na přístup učiněné třetími osobami

Právo na přístup svědčí subjektu údajů, subjekt údajů jej zpravidla vykonává osobně, poměrně často však mohou nastat situace, kdy bude toto právo za subjekt údajů vykonávat jiná osoba. Právo na přístup tak může být realizováno **prostřednictvím smluvního zmocněnce**[277] nebo **zákonných zástupců jménem nezletilých osob**, Pokyny EDPB[278] hovoří i o **realizaci práva na přístup jinými entitami prostřednictvím platforem – internetových portálů**. Pokyny dále hovoří o tom, že pokud je to vhodné a přiměřené, respektive, má-li správce důvodné pochybnosti, může být za určitých okolností vyžadováno ověření totožnosti osoby oprávněné k výkonu práva na přístup a k jednání jménem subjektu údajů. V tomto smyslu je však třeba dodat, že zpřístupnění osobních údajů neoprávněné osobě, může představovat porušení zabezpečení osobních údajů. Podle mého názoru by tak v případě zastoupení subjektu údajů mělo být vyžadováno ověření totožnosti zmocněnce či zákonného zástupce vždy. Pokyny v této části nepochopitelně opomíjejí článek 80 nařízení GDPR. Jedná se o článek upravující zastupování subjektů údajů, a to prostřednictvím neziskového subjektu, organizace nebo

[277] Podle právního řádu ČR se jedná o smluvní zastoupení, které se prokazuje na základě plné moci, § 441 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.
[278] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 29-30.

sdružení, jež byly řádně založeny v souladu s právem některého členského státu, jejichž statutární cíle jsou ve veřejném zájmu a jež vyvíjejí činnost v oblasti ochrany práv a svobod subjektů údajů ohledně ochrany jejich osobních údajů. Subjekt údajů tak může tuto nezávislou (např. spotřebitelskou organizaci nebo odborovou organizaci) pověřit, aby jeho jménem podala stížnost, uplatnila práva uvedená v článcích 77, 78 a 79[279] a, pokud tak stanoví právo členského státu, uplatnila právo na odškodnění podle článku 82 nařízení GDPR.

Ustanovení článku 80 nařízení GDPR tak má za cíl především posílit postavení subjektů údajů jako slabší „strany". V praxi často pouze takto vyvíjený větší tlak prostřednictvím více subjektů údajů či samotná existence rizika takovéhoto spojování se subjektů údajů k prosazení jejich společného zájmu představuje pro správce dostatečnou motivaci rychle a efektivně řešit vzniklý problém.[280] Ustanovení článku 80 nařízení GDPR sice nemá přímý odkaz na článek 15 (právo na přístup), ale vzhledem k tomu, že subjekt údajů podává stížnost k dozorovému úřadu či žalobu k soudu až v případě, kdy není spokojen s vyřízením svých práv, je jeho význam nezpochybnitelný. Nic také nebrání tomu, aby v případě, že subjekt údajů řádně pověří tuto organizaci zastoupením ve své záležitosti, tato jednala v zájmu subjektu údajů a jeho jménem podala i přímo žádost o přístup. Je tedy škoda, že se této otázce zastoupení neziskovým subjektem či odborovou organizací Pokyny nevěnují.[281] Otázku právních požadavků zastoupení neřeší ani nařízení GDPR, ani Pokyny EDPB. Záleží totiž na vnitrostátní právní úpravě členských států, jaké stanoví požadavky na prokázání oprávnění podat žádost jménem subjektu údajů. Podle zásady odpovědnosti správce a v souladu s ostatními zásadami ochrany osobních údajů je i zde důkazní břemeno na správci. Je to správce, kdo musí prokázat existenci příslušného zmocnění k podání žádosti jménem subjektu údajů, s výjimkou případů, kdy vnitrostátní právní předpisy stanoví jinak.

Výzkumu uplatnění práva na přístup a významu jeho kolektivního uplatnění se věnovali poměrně zevrubně Mahieu, Asghari a Van Eeten[282] z Technické univerzity v Delftu. Podle nich

[279] Článek 77 – právo podat stížnost u dozorového úřadu, článek 78 – právo na účinnou soudní ochranu vůči dozorovému úřadu a článek 79 – právo na účinnou soudní ochranu vůči správci nebo zpracovateli.
[280] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 1177-1186. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].
[281] Ostatně tato připomínka také zazněla i ze strany neziskových subjektů ve veřejné konzultaci k Pokynům k právu na přístup – např. připomínka ředitele neziskové organizace Worker Info Exchange, Jamese Farrara. Dostupné z: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en. [cit. 2024-04-14].
[282] MAHIEU, René L.P., ASGHARI, Hadi a VAN EETEN, Michel, 2018. Collectively Exercising the Right of Access: Individual Effort, Societal Effect. Online. *Internet Policy Review*. Roč. 2018, č. 7(3). Dostupné z: https://doi.org/10.14763/2018.3.927. [cit. 2024-06-23].

může kolektivní využívání práva na přístup pomoci změnit nerovnováhu sil mezi jednotlivými občany a organizacemi ve prospěch občanů, což může zároveň organizace motivovat k tomu, aby s údaji nakládaly transparentnějším způsobem. Nařízení GDPR totiž má nástroje (především právě v podobě článku 80), které umožňují jednotlivci – subjektu údajů získat sílu prostřednictvím společného úsilí, kolektivní akce. Mahieu a Ausloos[283] ve své dřívější práci hovořili o tzv. fenoménu '*architecture of empowerment'* (architektuře posílení) se silným kolektivním rozměrem, který byl doposud podceňován. K tomu uváděli, že právo na přístup je klíčové pro demokratizaci kontroly nad zpracováním údajů v digitální společnosti. Mahieu, Asghari a Van Eeten tuto myšlenku posléze rozvíjejí a tvrdí, že, pokud je právo využíváno kolektivním způsobem, vytváří to kontext pro posuzování kvality odpovědí a zákonnosti postupů při zpracování údajů porovnáním odpovědí na podobné žádosti o přístup. Také účastníci vnímali při uplatňování tohoto práva kolektivním způsobem mnohem více jeho společenskou než individuální hodnotu, a to zejména díky posunu nerovnováhy ve prospěch subjektů údajů. Výzkum v počátku vedli tak, že požádali několik dobrovolných účastníků, aby zaslali celkem více než sto žádostí o přístup ke svým osobním údajům a podělili se o odpovědi získané od správců. Odpovědi byly podrobeny analýze a vlastnímu hodnocení účastníků. Přibližně 80 % žádostí o přístup k osobním údajům bylo nakonec zodpovězeno. Pokud jde o klasifikaci správců podle odvětví, až 35 % žádostí adresovaných správcům v odvětví dopravy (Car2Go, NS, Letiště Amsterdam Schiphol) zůstalo zcela bez odpovědi, v odvětví telekomunikací (KPN, T-Mobile, Ziggo) a maloobchodu (Happy Socks, Ikea, Bol.com) zůstalo nezodpovězeno až 25 %, v odvětví online platforem (Mi, Skype, Spotify) až 20 %. Bylo zjištěno, že ve většině případů byly i zaslané odpovědi kvalitativně stále nedostatečné, účastníci byli výsledkem také zklamáni. Řešením podle autorů je právě kolektivní uplatnění práva subjektu údajů či kolektivní stížnost. Řada neziskových organizací subjektům údajů pomáhá, ať už se sestavením online stížností, např. organizace Bits of Freedom prostřednictvím online projektu My Data Done Right[284], nebo přímo za subjekty údajů stížnosti podává, v současné době asi nejznámější nezisková organizace NOYB (None of Your Business)[285] vytvořená kolem rakouského aktivisty a právníka Maxe Schremse. Jako příklad úspěšného kolektivního

[283] MAHIEU, René L.P. a AUSLOOS, Jef, 2020. Harnessing the collective potential of GDPR access rights: towards an ecology of transparency. Online. *Internet Policy Review*. Roč. 2020. Dostupné z: https://policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487. [cit. 2024-06-23].
[284] Bits of Freedom. Projekt *My Data Done Right*. Dostupné z: https://www.mydatadoneright.eu/. [cit. 2024-06-23].
[285] NOYB. *Your right of Access (Article 15)*. Dostupné z: https://noyb.eu/en/your-right-access-article-15. [cit. 2024-06-23].

postupu lze uvést skupinové stížnosti podané sdružením NOYB a La Quadrature du Net, které vedly až k uložení pokuty ve výši 50 milionů eur francouzským dozorovým úřadem společnosti Google LLC[286]. Francouzské sdružení La Quadrature du Net mělo dokonce mandát od 10000 osob. Porušení francouzský dozorový úřad shledal v oblasti povinnosti transparentnosti; informační povinnosti a absence platného právního základu pro zpracování osobních údajů uživatelů pro účely personalizace reklam[287].

Ve vztahu k zemřelým osobám se nařízení GDPR neuplatňuje, jak je uvedeno v recitálu 27. Ustanovení zároveň umožňuje členským státům stanovit si vlastní vnitrostátní pravidla týkající se zpracování osobních údajů zesnulých osob. V tomto smyslu je důležité si uvědomit, že osobní údaje zemřelých osob se často mohou zpracovávat ve spojení s osobními údaji živých, na něž se ochrana podle nařízení GDPR vztahovat může (např. korespondence zesnulého).

Děti jsou zvláště chráněnými subjekty údajů z důvodu své zranitelnosti. Proto se na řadě místech nařízení objevují specifické limity zpracování osobních údajů aplikovatelné právě jen na děti. Již některé recitály nařízení GDPR výslovně zmiňují, že děti mají požívat zvláštní ochrany. Recitál 38 nařízení GDPR hovoří přímo o tom, že: „*zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů…*“ Dále také v článku 58 recitálu je zakotvena nutnost zvláštního přístupu k ochraně osobních údajů dětí, který říká, že v případech, kdy je zpracování osobních údajů zaměřeno na děti, měly by být všechny informace a sdělení podávány prostřednictvím *jasných a jednoduchých jazykových prostředků, aby jim děti snadno porozuměly*. Toto znění je dále reflektováno v článku 12 nařízení GDPR věnovaném transparentnosti a postupům pro výkon práv subjektu údajů, kde je správci stanovena povinnost přijmout vhodná opatření, aby subjekt údajů stručně, jasně, srozumitelně a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků informoval o účelu zpracování osobních údajů, právech subjektu údajů a dalších souvisejících skutečnostech. Také v tomto ustanovení je znovu zdůrazněno, že zvláště důležité je ho dodržet, jde-li o informace určené dítěti. Jak již bylo řečeno, nařízení GDPR obsahuje zvláštní ochranu dětí na několika

[286] NAUDTS, Laurens; DEWITTE, Pierre a AUSLOOS, Jef, 2022. 21 Meaningful transparency through data rights: A multidimensional analysis. In: KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research Handbook on EU Data Protection Law*. Cheltenham, UK: Edward Elgar Publishing, s. 530-571. Online. ISBN 9781800371682. Dostupné z: https://doi.org/10.4337/9781800371682.

[287] EDPB. 21. 1. 2019. *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. Dostupné z: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. [cit. 2024-06-23].

místech, tato práce se však zaměřuje na právo subjektu údajů na přístup. Z hlediska práva na přístup náleží samozřejmě i dětem jako subjektům údajů toto právo. Hlavním hlediskem v souvislosti s výkonem práva na přístup musí být nejlepší zájem dítěte, což je dlouhodobý koncept vycházející z mezinárodního práva. Jak uvádí čl. 8 odst. 3 nařízení GDPR, ustanovením není dotčeno obecné smluvní právo členských států, například pravidla týkající se platnosti, uzavírání nebo účinků smlouvy vzhledem k dítěti. Úprava právního jednání dítěte tedy spadá do vnitrostátních právních řádů členských států. Pokyny pouze poukazují na to, že dítě může být způsobilé k právnímu jednání v závislosti na jeho zralosti a schopnosti, jinak za něj jedná jeho zákonný zástupce. V ČR se dle § 31 občanského zákoníku obecně předpokládá, že nezletilý je svéprávný v rozsahu, který odpovídá rozumové a volní vyspělosti nezletilého jeho věku.

Pokud jde o realizaci práva na přístup jinými entitami, a to prostřednictvím platforem – internetových portálů, EDPB k tomu ve svých Pokynech zaujímá dosti obezřetný přístup. O co se jedná? Existují společnosti, které poskytují služby, které subjektům údajů umožňují podávat žádosti o přístup prostřednictvím internetového portálu. Subjekt údajů se přihlásí a získá přístup k portálu, jehož prostřednictvím může podat například žádost o přístup, požádat o opravu údajů nebo výmaz údajů od různých správců. Pro subjekty údajů se tak může jednat o nástroj, který jim výrazně pomáhá při uplatňování jejich práv (časová úspora, nemusí pokaždé znovu absolvovat proces ověřování jejich totožnosti atd.). Subjekty údajů mohou na tyto portály nahrát své osobní údaje a dokonce i doklad své totožnosti, portály pak jejich jménem zašlou žádosti vybraným organizacím správců. Problematickou stránkou je to, že provozovateli těchto portálů bývají třetí strany, tedy entity odlišné od správce. Správce musí tedy v první řadě ověřit, zda skutečně třetí strana jedná jménem subjektu údajů oprávněně. Je jeho povinností zajistit, aby nedošlo k porušení zabezpečení a osobní údaje subjektu údajů nebyly sděleny neoprávněným osobám. Spornou se pak může jevit ta část v Pokynech EDPB, kde se hovoří o tom, že správce nemá povinnost poskytovat údaje podle článku 15 přímo portálu, a to např. pokud zjistí, že portál nezajišťuje dostatečná bezpečnostní opatření. Za této situace Pokyny uvádějí, že správce může sám od sebe rozhodnout o použití jiných postupů pro vyřízení žádostí o přístup. Je ovšem otázkou, zda je toto doporučení dostatečně opodstatněné a zdali není v rozporu s výše uvedeným principem, že subjekt údajů se může svobodně rozhodnout, jak uplatní své právo na přístup. Jak bylo uvedeno, ustanovení čl. 12 odst. 3 nařízení GDPR jasně stanoví, že: „*Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob*“. Pokud se subjekt údajů rozhodl

vyžádat si své osobní údaje prostřednictvím konkrétního internetového portálu, tak by neměl existovat žádný důvod, proč by správce údajů mohl mít právo být osvobozen od povinnosti usnadnit výkon práv subjektu údajů tím, že by záměrně odmítl poskytnout přístup k údajům a informace prostřednictvím takového elektronického prostředku, jaký si subjekt údajů sám zvolil. Za nejvhodnější řešení bych osobně považovala, kdyby správce upozornil přímo subjekt údajů na bezpečnostní riziko v souvislosti s konkrétním portálem a podle jeho reakce postupoval dále (tj. poskytl údaje podle jeho přání, pokud by subjekt údajů na tomto prostředku trval, nebo prostřednictvím alternativně dohodnutého prostředku). Jinou otázkou je, jak postupovat, pokud by správce žádnou reakci subjektu údajů ve stanovené lhůtě neobdržel.

5. Rozsah práva na přístup

Část pátá navazuje na předchozí část pojednávající o právu subjektu údajů na přístup k vlastním údajům. V této části bude vyjasněn především rozsah informací, na něž se vztahuje právo na přístup obecně (**kapitola 5.1 Posouzení rozsahu práva na přístup**). Další kapitoly se pak soustředí na aktivitu správce (**kapitola 5.2 Poskytnutí přístupu správcem**) a na omezení tohoto práva (**kapitola 5.3 Omezení práva na přístup**). Na tomto místě je vhodné připomenout, že správce musí pro posouzení žádosti o přístup nejdříve posoudit tři významné skutečnosti: zaprvé, zda dotčené zpracování osobních údajů spadá do věcné a místní působnosti nařízení GDPR (a). Zadruhé, zdali jsou údaje, o jejichž přístup subjekt údajů žádá, skutečně osobními údaji (b). A zatřetí, zda se osobní údaje, o jejichž přístup subjekt údajů žádá, skutečně týkají subjektu údajů (c).

5.1 Posouzení rozsahu práva na přístup

5.1.1 Posouzení věcné a místní působnosti nařízení

První úvaha správce tedy musí směřovat na věcnou a místní působnost nařízení GDPR, které jsou upraveny v článku 2 a 3 tohoto nařízení. Právo na přístup se proto nevztahuje na osobní údaje, které nejsou zpracovávány automatizovanými prostředky nebo které nejsou součástí evidence[288] podle čl. 2 odst. 1 nařízení GDPR, stejně tak se nevztahuje na osobní údaje, jež jsou zpracovávány fyzickou osobou v rámci její výlučně osobní činnosti podle čl. 2 odst. 2 nařízení GDPR. Místní působnost byla pro účely nařízení stanovena široce. Nařízení GDPR se oproti dřívější směrnici vztahuje nejen na správce, ale i na zpracovatele, usazené v EU, ať již zpracovávají osobní údaje kdekoli, a za splnění určitých podmínek i na správce nebo zpracovatele usazené mimo EU. Právě druhý případ je projevem tzv. extrateritoriální působnosti nařízení GDPR. Za účelem zajištění ochrany subjektů údajů se nařízení GDPR vztahuje i na správce a zpracovatele, kteří na území EU usazeni nejsou a svou činnost zde

[288] Pojem „evidence“ je pro účely nařízení definován v článku 4 bodu 6 tohoto nařízení. Rozumí se jím jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska. Evidence (nebo jinými slovy rejstřík, kartotéka či seznam) je tedy jakýkoliv způsob strukturování, umožňující vyhledávání podle předem daných kritérií, například roku vzniku, abecedního pořadí apod. UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 66-86. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

nevykonávají ani prostřednictvím faktické provozovny (čl. 3 odst. 2), pokud se jimi prováděné zpracování týká jedné z následujících činností, jejíž podstatou je cílení na subjekty údajů: buď se musí jednat o nabídku zboží nebo služeb nebo o monitorování jejich chování.

5.1.2 Posouzení kvality shromážděných informací jako osobních údajů

Druhé posouzení vedené správcem má význam k určení rozsahu údajů, k nimž je subjekt údajů oprávněn získat přístup. Jedná se o rozlišení mezi osobními údaji a jinými údaji, které kvalitu osobních údajů nemají. Čl. 15 odst. 1 a odst. 3 nařízení GDPR odkazují na „*osobní údaje*“ a „*osobní údaje, které jsou předmětem zpracování*“. Rozsah práva na přístup je proto určen především rozsahem pojmu „*osobní údaje*“, který je definován v čl. 4 odst. 1 nařízení GDPR.[289] Samotný pojem „*osobních údajů*“ již byl předmětem podrobnějšího rozboru v několika dokumentech pracovní skupiny WP29[290] a byl i předmětem výkladu Soudního dvora EU, a to i v souvislosti s právem na přístup podle článku 12 směrnice 95/46. Pojmem osobní údaj, resp. osobní údaje, jsem se blíže zabývala v části druhé. Nyní se proto omezím na konstatování, že pojem „osobní údaje“ je klíčovým pojmem z hlediska aplikace nařízení GDPR. I zpracování jiných údajů může být (a zpravidla také je) regulováno právem, například u zpracování údajů tvořících obchodní tajemství či utajované skutečnosti, nicméně pouze pokud se jedná o zpracování osobních údajů, bude se aplikovat nařízení GDPR.

5.1.3 Posouzení vztahu osobních údajů k subjektu údajů

Podle čl. 15 odst. 1 nařízení GDPR „*subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím*“. Ustanovení tedy výslovně odkazuje na osobní údaje, které se týkají subjektu údajů. Právo na přístup lze uplatnit výhradně ve vztahu k osobním údajům, které se týkají subjektu údajů, který žádá o přístup, nebo případně, pokud je právo uplatněno prostřednictvím zmocněnce nebo zákonného zástupce. Je proto třeba

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

[290] Především dokument WP29. *Stanovisko č. 4/2007 WP136 k pojmu osobní údaje*, přijaté dne 20. června 2007. Dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf.

vyloučit osobní údaje, které se týkají výhradně jiné osoby. Pokyny týkající se práva na přenositelnost údajů, které lze do jisté míry obdobně použít i v oblasti práva na přístup, uvádí: „*Do oblasti působnosti žádosti spadají pouze osobní údaje. Všechny údaje, které jsou anonymní, nebo které se netýkají subjektu údajů, nespadají do působnosti tohoto práva. Do jeho působnosti však spadají pseudonymní údaje, které mohou být jasně spojeny se subjektem údajů (např. tím, že tento subjekt údajů poskytne příslušné identifikační informace, viz čl. 11 odst. 2)*."[291] V rámci třetího kroku posouzení přísluší současně posoudit správci, zda jsou osobní údaje jím skutečně zpracovávány. Dalším klíčovým pojmem je proto pojem „*zpracování*"[292]. Tento pojem již byl předmětem detailnějšího vymezení v této práci, konkrétně v části druhé.

Jak ostatně uvádí Pokyny k právu na přístup[293], klasifikace údajů jako osobních údajů týkajících se subjektu údajů však nezávisí na tom, zda se tyto osobní údaje týkají i někoho jiného. To potvrdil i Soudní dvůr EU ve svém rozsudku ve věci *Nowak*[294], kdy Soud přiznal kvalitu osobních údajů i informacím týkajícím se zkoušeného obsaženým v jeho odpovědích při odborné zkoušce a v korekturních poznámkách zkoušejícího, a to i přesto, že tyto korekturní poznámky představovaly také informace týkající se zkoušejícího. Je tedy možné, že se osobní údaje týkají více než jedné osoby současně. V důsledku to neznamená, že by měl být subjektu údajů automaticky umožněn přístup k osobním údajům, které se týkají i někoho jiného, protože správce musí respektovat postup podle čl. 15 odst. 4 nařízení GDPR, podle něhož *nesmějí být nepříznivě dotčena práva a svobody jiných osob*. Jak ale vyplývá z několika rozsudků Soudního dvora, výjimky z povinnosti poskytnout subjektu údajů informace by měly být vykládány restriktivně, a nemělo by tak například dojít k odepření přístupu ke všem osobním údajům subjektu údajů, nýbrž pouze k poskytnutí přístupu k užšímu rozsahu údajů. O tom, že by správci údajů neměli přijímat příliš restriktivní výklad věty „*osobní údaje, které se týkají subjektu údajů*", hovoří i EDPB v Pokynech týkajících se práva na přenositelnost údajů. Příklad č. 13: Uživatel požádá svého telefonního operátora o výpis všech svých hovorů za poslední měsíc. Správce by mu proto měl poskytnout informace nejen o čase uskutečnění příchozích a

[291] WP29. *Pokyny týkající se práva na přenositelnost údajů WP 242 rev.01*, přijaté dne 13. prosince 2016 naposledy revidované a přijaté dne 5. dubna 2017, s. 10. Dostupné zde: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-tykajici-se-prava-na-prenositelnost-udaju-v-cestine.pdf.

[292] Pojem „zpracování" je pro účely nařízení definován v článku 4 bodu 2 tohoto nařízení jako jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

[293] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 34-36.

[294] Rozsudek ze dne 20. prosince 2017, Nowak, C-434/16, EU:C:2017:994, bod 44.

odchozích hovorů a jejich délce, ale také o čísle, na které uživatel volal a které mu volalo. EDPB hovoří o tom, že uživatelé by měli být schopni tyto záznamy v návaznosti na svou žádost získat, jelikož tyto záznamy se (rovněž) týkají subjektu údajů. Obdobný výklad zaujímá nejen ve vztahu k záznamům telefonních hovorů a jejich výpisům, ale také u interpersonálního přenosu zpráv nebo u záznamů služeb VoIP (tzv. „Voice over IP“, služby telefonního volání prostřednictvím internetového protokolu, např. Skype).[295] V tomto smyslu považuje EDPB za důležité, aby byl subjekt údajů upozorněn na to, že pokud tento záznam (např. záznam, kde je zaznamenán hlas druhé osoby, s kterou subjekt údajů telefonicky hovořil) použije k účelům jdoucím nad rámec obecného účelu práva na přístup (a sice informovat subjekt údajů o zpracování, které se ho týká a dát mu možnost si ověřit zákonnost tohoto zpracování), stane se tento subjekt údajů sám správcem zpracování osobních údajů týkajících se druhé osoby, jejíž hlas byl zaznamenán. K tomu dojde například v situaci, že subjekt údajů tento záznam bez dalšího zveřejní, a tedy rétorikou nařízení GDPR vlastně „určí účel a prostředky zpracování“.

O něco komplikovanější jsou pak situace, kdy spojení mezi osobními údaji a několika dotčenými osobami je pro správce nejasné, například v případě tzv. krádeže identity. V této souvislosti EDPB uvádí, že oběti by měly být poskytnuty informace o všech osobních údajích, které správce uchovává v souvislosti s jejich identitou (tedy do jisté míry identitou obou osob, neboť druhá osoba podvodně zneužívá identity jiné osoby a jedná jejím jménem), včetně těch, které byly shromážděny na základě jednání podvodníka. Jinými slovy, i poté, co se správce dozvěděl o krádeži identity, jsou osobní údaje spojeny s identitou oběti nebo s ní souvisejí, a proto představují osobní údaje subjektu údajů. Příklad č. 14: Pachatel podvodně zneužije identity jiné osoby, aby mohl hrát poker online. Pachatel platí online kasinu pomocí kreditní karty, kterou ukradl oběti. Když se oběť dozví o krádeži identity, požádá provozovatele online kasina, aby jí poskytl přístup k osobním údajům, které se jí týkají, a konkrétně k online hrám a informacím o kreditní kartě použité pachatelem. Existuje souvislost mezi shromážděnými údaji a obětí, protože byla zneužita její identita. Po odhalení podvodu jsou výše uvedené osobní údaje s ní stále spojeny z důvodu jejich obsahu (kreditní karta se jednoznačně týká oběti), účelu a účinku (informace o online hrách, které pachatel hrál, mohou být použity například k vystavení

[295] WP29. *Pokyny týkající se práva na přenositelnost údajů WP 242 rev.01*, přijaté dne 13. prosince 2016 naposledy revidované a přijaté dne 5. dubna 2017, s. 10. Dostupné zde: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-tykajici-se-prava-na-prenositelnost-udaju-v-cestine.pdf.

faktur oběti). Provozovatel online kasina by proto měl umožnit oběti přístup k výše uvedeným osobním údajům.[296]

Z hlediska práva na přístup může být závažným rizikem v současné době existující praxe neoprávněného využívání práva na přístup, odborně technicky nazvané jako tzv. *blagging*. Jedná se o kombinaci krádeže identity a nedostatečného zabezpečení zpracování ze strany správce, na jehož základě může třetí osoba předstírat nárok subjektu údajů a získat od správce soubor jeho zpracovávaných údajů. Jak píše prof. Polčák, to staví správce do nelehké pozice, kdy na jednu stranu musí poskytovat subjektům údajů na vyžádání jejich údaje a odpovídat za oprávněnost jejich požadavku, nesmí však vytvářet příliš obsáhlý identifikační profil subjektu údajů pouze za účelem verifikace jeho identity.[297]

Zajímavou otázkou, která byla dlouho sporná, je otázka poskytování tzv. přístupových logů (protokolů o přístupu zaměstnanců nebo jiných pověřených osob správce k osobním údajům určité osoby), resp. zdali mohou být tyto logy také předmětem práva na přístup podle článku 15 nařízení GDPR. Povinnost logování byla dokonce výslovně upravena v dřívějším zákoně č. 101/2000 Sb., o ochraně osobních údajů, a to konkrétně v § 13 odst. 4 písm. c) jako jedna z povinností správce a zpracovatele při zabezpečení osobních údajů. V zákoně o zpracování osobních údajů již sice výslovně uvedena není, lze ji ovšem dovodit z čl. 5 odst. 1 písm. f) a článku 32 nařízení GDPR jako součást bezpečnostních opatření, které by měl správce přijmout pro zajištění důvěrnosti a integrity zpracovávaných osobních údajů, jak ostatně potvrdil i Nejvyšší správní soud.[298] Také problematikou poskytování logů se zabýval EDPB a byla dokonce i součástí stížnosti podané českému dozorovému úřadu. EDPB je toho názoru, že tyto logy spadají do odpovědnosti správce a slouží spíše pro kontroly dozorových úřadů. Správce by proto měl zajistit, aby osoby jednající v rámci jeho pravomoci, které mají přístup k osobním údajům, nezpracovávaly osobní údaje jinak než na základě pokynů správce, jak je ostatně uvedeno i v článku 29 nařízení GDPR. Pokud však osoba zpracovává osobní údaje pro jiné účely, než jak vyplývá z pokynů správce, může se stát správcem tohoto zpracování a podléhat příp. správním sankcím vydaným dozorovými úřady. V současné době je tato otázka na unijní úrovni již vyřešená, jedná se o věc C-579/21 *Pankki S*. Nejdříve bylo v dané věci

[296] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 36.
[297] POLČÁK, Radim, MYŠKA, Matěj, HOSTAŠ, Petr, KASL, František, KYSELOVSKÁ, Tereza, LECHNER, Tomáš, LOUTOCKÝ, Pavel, MÍŠEK, Jakub, TOMÍŠEK, Jan, STUPKA, Václav a UŘIČAŘ, Miroslav. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. 656 s. Právní monografie. ISBN 978-80-7598-045-8.
[298] Rozsudek Nejvyššího správního soudu ze dne 26. 3. 2024, čj. 6 As 32/2023-40, bod 48.

vydáno stanovisko generálního advokáta[299], jehož závěr zněl tak, že subjektu údajů není přiznáno právo znát z informací, které má správce k dispozici (případně ze záznamů operací nebo operačních souborů), totožnost zaměstnance nebo zaměstnanců, kteří z pověření a podle pokynů správce nahlíželi do jeho osobních údajů. Podle generálního advokáta je důležité rozlišovat mezi informacemi, které představují osobní údaje, a informacemi, které pouze souvisejí s prováděným zpracováním (účel zpracování nebo kategorie zpracovávaných údajů). Informace v podobě logů se týkají pouze zpracování, a nikoli osobních údajů subjektu údajů, podle čl. 4 odst. 1 nařízení (EU) 2016/679. Kromě toho generální advokát konstatoval, že pokud zaměstnanec jedná na základě „přímého pověření" svého zaměstnavatele, neměl by být kvalifikován jako „příjemce" osobních údajů (podle čl. 15 odst. 1 písm. c) nařízení (EU) 2016/679), a proto jeho totožnost nemusí být sdělována subjektu údajů z důvodu transparentnosti.

Rozsudek Soudního dvora ve věci C-579/21 *Pankki S* je jedním ze stěžejních rozsudků k právu na přístup. Jde o rozsudek, který se zabývá nejen rozsahem práva na přístup, ale je ukázkou, jak Soudní dvůr přistupuje k tzv. vážení práv, konkrétně práva na přístup subjektu údajů s právem na ochranu soukromí a osobních údajů jiných osob (konkrétně zaměstnanců správce). Pan J. M. byl bývalý zaměstnanec a zákazník finské banky Pankki. Jednoho dne se dozvěděl, že někteří zaměstnanci banky několikrát nahlíželi do jeho osobních klientských údajů. Obrátil se proto na správce s žádostí o poskytnutí informací týkajících se těchto operací zpracování. Banka žádosti částečně vyhověla a poskytla některé podrobnosti o operacích nahlížení, odmítla však sdělit totožnost zaměstnanců (konkrétně tzv. přístupové logy, resp. protokolové soubory). Odmítnutí banka zdůvodnila právě ochranou osobních údajů svých zaměstnanců, což potvrdil i finský dozorový úřad. Pan J. M. se rozhodl obrátit na soud (správní soud pro východní Finsko), který položil Soudnímu dvoru několik otázek ohledně typu informací, které má subjekt údajů právo získat podle článku 15 nařízení.

Soudní dvůr v zásadě respektoval linii argumentace vytyčenou již ve stanovisku generálního advokáta. Soudní dvůr potvrdil široký rozsah práva na přístup. Článek 15 GDPR musí být vykládán s ohledem na kontext, jakož i cíle a účel nařízení. Ustanovení článku 15 musí být vykládáno v tom smyslu, že informace o operacích nahlížení do osobních údajů subjektu, které se týkají dat a účelů těchto operací, jsou informacemi, které má tento subjekt právo získat

[299] Stanovisko generálního advokáta Manuela Campos Sánchez-Bordony ze dne 15. prosince 2022, Pankki S, C-579/21, EU:C:2022:1001.

od správce. To znamená, že podle článku 15 sem spadají i protokolové soubory správce (logy), neboť jednak odhalují existenci zpracování údajů, jednak informují o četnosti a intenzitě operací nahlížení, a umožňují tak subjektu údajů ujistit se o tom, že prováděné zpracování je skutečně odůvodněno účely, které správce uvádí. Naproti tomu toto právo v sobě nezahrnuje právo na informace o totožnosti zaměstnanců uvedeného správce, kteří prováděli tyto operace z jeho pověření a v souladu s jeho pokyny, ledaže jsou tyto informace nezbytné k tomu, aby subjekt údajů mohl účinně vykonávat práva, která mu toto nařízení přiznává, a za podmínky, že jsou zohledněna práva a svobody těchto zaměstnanců. V této souvislosti Soudní dvůr také vyjasnil, že zaměstnanci správce nemohou být kvalifikováni jako „příjemci" údajů, pokud skutečně jednají v souladu s pokyny správce. Posléze už Soudní dvůr přistoupil k vážení práv. Podle něj je nutné najít rovnováhu mezi právem na přístup subjektu údajů a ochranou osobních údajů dalších osob. Správce by podle něj neměl v takovýchto situacích volit řešení obecného odmítnutí poskytnutí údajů. Zároveň by měl správce zvolit takové prostředky sdělování osobních údajů, které neporušují práva a svobody jiných osob. Pokud subjekt údajů pochybuje například o pravdivosti informací týkajících se účelu těchto nahlížení nebo má jiné pochybnosti o zákonnosti nahlížení a tím zdůvodňuje nezbytnost informování o totožnosti zaměstnanců správce, má v této souvislosti využít práva podat stížnost u dozorového úřadu na základě čl. 77 odst. 1 nařízení GDPR. Tento orgán pak může požádat správce, aby mu poskytl veškeré informace, které potřebuje k posouzení stížnosti.[300]

Dalším významným rozsudkem Soudního dvora, který se týká rozsahu práva na přístup, je rozsudek ve věci C-154/21 *Österreichische Post (Informations relatives aux destinataires de données personnelles)*[301]. Předmětem sporu byla otázka, zdali má subjekt údajů v rámci práva na přístup podle článku 15 také právo na sdělení totožnosti konkrétních příjemců, kterým byly jeho osobní údaje zpřístupněny. Otázka vyvstala ve sporu mezi fyzickou osobou a hlavním poskytovatelem poštovních a logistických služeb v Rakousku. Podnik odmítl osobě totožnost konkrétních příjemců sdělit, pouze obecně uvedl, že osobní údaje nabízí obchodním klientům pro marketingové účely. Žadatel se s odpovědí správce nespokojil a obrátil se na soud. Jak soud prvního stupně, tak odvolací soud daly za pravdu správci s tím, že nařízení přiznává správci možnost sdělit subjektu údajů pouze kategorie příjemců, aniž by musel jmenovitě uvádět

[300] Rozsudek ze dne 22. června 2023, Pankki S, C-579/21, EU:C:2023:501, zejména body 77 až 83.
[301] Rozsudek ze dne 12. ledna 2023, Österreichische Post (Informations relatives aux destinataires de données personnelles), C-154/21, EU:C:2023:3.

konkrétní příjemce. Žadatel se následně obrátil na Nejvyšší soud, který podal předběžnou otázku k Soudnímu dvoru EU.

Generální advokát Pitruzzella rozhodl, že právo na přístup podle čl. 15 odst. 1 písm. c) GDPR zastává funkční a pomocnou roli ve vztahu k výkonu ostatních práv subjektu údajů stanovených v GDPR. Z toho vyplývá, že aby mohl být zajištěn užitečný účinek nařízení GDPR musí být toto ustanovení vykládáno v tom smyslu, že právo na přístup k osobním údajům se musí v zásadě povinně vztahovat na možnost získat od správce informace o konkrétních příjemcích. Soudní dvůr se v zásadě ztotožnil s názorem generálního advokáta Pitruzzelly.[302] Úvodem s odkazem na svou předchozí judikaturu připomněl nutnost zohlednit kontextuální výklad, který zachovává užitečný účinek. Jazykový výklad je nedostačující, neboť pojmy „příjemci" a „kategorie příjemců" jsou v ustanovení použity neutrálně za sebou, aniž by mezi nimi bylo možné dovodit pořadí priority. Je tedy třeba použít také teleologický a systematický výklad. Článek 15 GDPR proto musí být vykládán s ohledem na kontext, jakož i cíle a účel nařízení. Vzhledem k tomu, že článek 15 stanoví skutečné právo na přístup ve prospěch subjektu údajů, znamená to, že je na subjektu údajů (a tedy nikoli na správci), aby si vybral mezi dvěma alternativami, které jsou v něm stanoveny. Dále, právo na přístup podle něj umožňuje účinný výkon práv subjektu údajů, neboť toto právo je nezbytné k tomu, aby subjekt údajů mohl případně uplatnit své právo na opravu, právo na výmaz, právo na omezení zpracování, jakož i právo na námitku proti zpracování svých údajů a právo na soudní ochranu pro případ utrpěné škody. Aby byl tedy zaručen užitečný účinek všech těchto uvedených práv, musí mít subjekt údajů zejména právo na sdělení totožnosti konkrétních příjemců. Konečně, odůvodnění svého výkladu Soudní dvůr nachází i v samotném znění článku 19 nařízení.[303] Na závěr Soudní dvůr uvedl, že právo na ochranu osobních údajů není absolutním právem a musí být posuzováno v souladu se zásadou proporcionality, což znamená, že správce může žádost o sdělení totožnosti konkrétních příjemců odmítnout ve dvou výjimečných případech. Jedná se zaprvé o situaci, kdy žádosti není možné vyhovět z materiálního hlediska (např. totožnost příjemců ještě není známá) a zadruhé o situaci, kdy jsou žádosti zjevně nedůvodné nebo nepřiměřené. Žadatel tedy byl se svým nárokem úspěšný.

[302] Stanovisko generálního advokáta Giovanniho Pitruzzelly ze dne 9. června 2022, Österreichische Post (Informations relatives aux destinataires de données personnelles), C-154/21, EU:C:2022:452.
[303] Článek 19 nařízení GDPR se týká oznamovací povinnosti správce ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování. V jeho druhé větě se píše o povinnosti správce informovat subjekt údajů o konkrétních příjemcích, pokud to subjekt požaduje.

5.2 Poskytnutí přístupu správcem

Cílem této části je přiblížit, jakým způsobem může správce žádosti o přístup řešit a zároveň uvést praktické příklady různých způsobů poskytnutí přístupu, jakož i význam čl. 12 odst. 1 nařízení GDPR ve vztahu k právu na přístup. Tato část by rovněž měla poskytnout určité zpřesnění ohledně toho, co je považováno za běžně používaný elektronický formulář, jakož i časové hledisko poskytnutí přístupu podle čl. 12 odst. 3 nařízení GDPR.

Z hlediska teorie práva je nařízení GDPR obecnou regulací, není příliš normativní v řešení, jak má správce poskytnout přístup k osobním údajům. Prof. Polčák[304] a JUDr. Míšek[305] hovoří dokonce o moderní regulaci, tzv. performativních pravidlech (*performance-based rules*), které umožňují svým adresátům, aby si sami zvolili, jak dosáhnout normotvůrcem předepsaného cíle. Tento regulatorní přístup zvolil evropský normotvůrce jako základní regulatorní způsob pro nařízení GDPR. Jedná se o regulatorní přístup, který se právě uplatňuje v právu informačních a komunikačních technologií, zejména v oblasti kybernetické bezpečnosti a ochraně osobních údajů[306]. Tento model nevychází z klasického dualismu – regulující a regulovaný subjekt, nýbrž z dualismu – stát a regulovaný subjekt v podobě tzv. definiční autority (pojem užívaný prof. Polčákem). Stát, resp. normotvůrce zde pouze obecně definuje povinnost v podobě teleologických norem, aniž by pravidla konkrétně definoval nebo dohlížel na jejich dodržování. Je pak na definičních autoritách, aby samy stanovily vlastní vnitřní normy v podobě interních vnitropodnikových směrnic nebo třeba smluvních ujednání (např. smlouva o poskytování služby). Ty pak také fakticky vykonávají kontrolu nad určitou oblastí, mají totiž nejlepší přehled o tom, jak se dané prostředí chová a jak dosáhnout jeho efektivní regulace. Základním předpokladem uplatnění tohoto modelu performativní regulace je, že zájmy státu i definiční autority musí být prakticky totožné. Jak píše prof. Polčák, nejen stát má totiž zájem na bezpečnosti dat a infrastruktur, nýbrž i ten, kdo je vlastní, spravuje nebo provozuje. Prof. Polčák obecně předpokládá použitelnost tohoto modelu v různých oblastech práva při splnění tří generických znaků: Zaprvé, jde o oblasti, v nichž má definiční autorita

[304] POLČÁK, Radim, MYŠKA, Matěj, HOSTAŠ, Petr, KASL, František, KYSELOVSKÁ, Tereza, LECHNER, Tomáš, LOUTOCKÝ, Pavel, MÍŠEK, Jakub, TOMÍŠEK, Jan, STUPKA, Václav a UŘIČAŘ, Miroslav. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. 656 s. Právní monografie. ISBN 978-80-7598-045-8.
[305] MÍŠEK, Jakub, 2020. *Moderní regulatorní metody ochrany osobních údajů*. 1. vydání Brno: Masarykova univerzita, 279 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia. ISBN 978-80-210-9736-0.
[306] Regulační metoda performativních pravidel se doposud uplatňovala především v silně technologicky determinovaných odvětvích, tj. např. letecké dopravě nebo kontrole emisí – viz např. COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, č. 50(3), s. 525. U of Penn, Inst for Law & Econ Research Paper No. 17-18. Dostupné z SSRN: https://ssrn.com/abstract=3014768. [cit. 2023-04-15].

vyšší úroveň znalostí regulovaného substrátu (personálního i technického) než stát. Zadruhé, v těchto oblastech platí, že definiční autorita může fakticky dosáhnout regulace snadněji než stát, protože má vyšší úroveň práv. A zatřetí, zájmy definiční autority a státu musí být v zásadě synergické. JUDr. Míšek ve své monografii přehledně shrnuje výhody i nevýhody tohoto regulatorního přístupu. Výhodou je především vysoká flexibilita a adaptabilita regulace a podpora inovací. Tento model umožňuje pružnost a schopnost se přizpůsobit novým technologickým a společenským změnám. Společnosti také mohou být více ochotné investovat do nových technologií. Osobně bych ještě doplnila mezi výhody zvýšení odpovědnosti (organizací a jednotlivců za jejich chování) a posílení práv jednotlivců (jednotlivci získávají větší kontrolu nad svými údaji). Nevýhodou jsou pak vyšší náklady a relativně vyšší administrativní zátěž definičních autorit. Performativní regulace může být složitá a nákladná na implementaci a dodržování, zejména pro menší organizace, které nemusí mít potřebné zdroje. Prof. Polčák k nevýhodám uvádí též nezvyklost pro regulované subjekty. K tomu bych připojila též vysoké riziko nejasností a různých interpretací.

Performativní pravidla v nařízení GDPR jsou dle JUDr. Míška vybudována na dvou základních kamenech: zásadě odpovědnosti správce (tzv. *accountability*), dle níž je správce údajů odpovědný za zpracování, které provádí, má proto přizpůsobit proces zpracování tak, aby odpovídal požadavkům nařízení a byl schopen tento stav prokázat. Druhým konceptem je pak „*přístup založený na riziku*“, správce musí provádět nezbytné hodnocení rizik, které zpracování údajů představuje pro práva a svobody subjektů údajů a dalších fyzických osob. Laicky řečeno, čím vyšší riziko zpracování představuje, tím vyšší nároky jsou na správce kladeny. Náročnost vyřizování žádostí práva na přístup do velké míry závisí na těchto faktorech: velikosti správce (resp. jeho organizace), komplexnosti operací zpracování, které správce provádí a množství správcem shromážděných informací o subjektu údajů. Dalšími faktory s významným vlivem jsou: počet subjektů údajů, kategorie zpracovávaných údajů, jakož i tok údajů v rámci různých organizací a případné předávání mezi nimi. Vyřizování žádostí práva na přístup tak bude složitější proces, pokud jsou i správcem prováděné operace zpracování údajů komplexnější. Vzhledem k rozdílům ve zpracování osobních údajů se může vhodný způsob poskytnutí přístupu odpovídajícím způsobem lišit.

Britský dozorový úřad ICO na svých internetových stránkách[307] píše, že se od správce očekává vynaložení rozumného a přiměřeného úsilí k nalezení a získání požadovaných informací pro odpověď subjektu údajů. Správce proto není povinen provádět vyhledávání, které by bylo neopodstatněné nebo nepřiměřené vzhledem k významu poskytování přístupu k informacím. V rámci posouzení, zda vyhledávání může být neopodstatněné nebo nepřiměřené, by měl správce zvážit: okolnosti žádosti (a), jakékoli obtíže spojené s nalezením informací (b) a základní povahu práva na přístup (c). Důkazní břemeno přitom leží na správci, který musí být schopen odůvodnit, proč je v konkrétním případě vyhledání informací neopodstatněné nebo nepřiměřené. ICO dále uvádí, že i v případě, kdy se vyhledání určitých informací pro správce jeví jako neopodstatněné nebo nepřiměřené, stále by se měl zabývat i dalšími informacemi, resp. údaji, které jsou předmětem žádosti o přístup. Měl by současně zvážit, zdali by vyhledání informací nepomohlo sdělení dalších skutečností od subjektu údajů, resp. další vyjasnění žádosti o přístup. Kromě toho, správce by měl mít vybudovaný systém pro shromažďování všech relevantních informací, které mají být poskytnuty subjektu údajů. Systém by měl být vytvořen tak, aby správce mohl efektivně vyhledávat a extrahovat požadované informace a v případě potřeby odstranit údaje třetích osob. ICO se dále zabývá situací, kdy je žádost vztažena na elektronickou formu, nicméně se tyto osobní údaje již v („živých“) elektronických systémech správce nenacházejí a nejsou tedy dostupné. Jedná se o situace, kdy správce údaje archivoval (a), údaje zkopíroval do souborů určených k zálohování dat (b) nebo údaje vymazal (c). ICO uznává, že proces přístupu k elektronicky archivovaným nebo zálohovaným údajům může být složitější než proces přístupu k „živým“ údajům. V tomto smyslu však neexistuje žádná „technologická výjimka“ z práva na přístup. Správce by měl mít vybudované postupy pro vyhledávání a získávání osobních údajů, které elektronicky archivoval nebo zálohoval. Lze očekávat, že vyhledávací mechanismy pro elektronické archivní a záložní systémy nebudou tak sofistikované jako mechanismy pro „živé“ elektronické systémy. Správce by však měl vynaložit stejné úsilí k nalezení informací pro reakci na žádost o přístup, jako by hledal archivované nebo zálohované údaje pro své vlastní účely. Ve vztahu k vymazaným údajům pak ICO uvádí, že požadavek na opětovné vytvoření osobních údajů v okamžiku, kdy je správce trvale ze svých systémů vyřadil, by byl neúměrným požadavkem kladeným na

[307] ICO (2022). *Right of access - How do we find and retrieve the relevant information?* Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/how-do-we-find-and-retrieve-the-relevant-information. [cit. 2023-04-15].

správce. Nelze po něm tedy požadovat, aby využil vysoce nákladných technických prostředků k rekonstituci údajů, aby mohl žádosti o přístup vyhovět.

Obecně platí, že subjekty údajů by měly mít přístup ke všem informacím, které o nich správce zpracovává. To znamená, že správce je povinen vyhledávat osobní údaje ve všech svých informačních systémech, ale nejen v nich, povinnost se uplatní také na další systémy, evidence či rejstříky (respektive i jiné podoby strukturování osobních údajů), ledaže by subjekt údajů výslovně svou žádost omezil například na konkrétní informační systém správce. Platí tedy, že i za předpokladu, že subjekt údajů svou žádost nijak nespecifikuje a jde tedy o žádost obecnou, má správce povinnost poskytnout veškeré informace a osobní údaje, nejedná-li se o zjevně nedůvodnou nebo nepřiměřenou žádost, což by musel správce prokázat. Správce by tedy u obecné žádosti měl vždy předpokládat, že subjekty údajů chtějí uplatnit své plné právo podle čl. 15 odst. 1 až 2 nařízení (EU) 2016/679. Tomu odpovídá i jednotný výklad EDPB v Pokynech k právu na přístup.

Co všechno musí vzít správce při takovém vyhledávání v potaz? A jak moc důkladně musí k takovému vyhledávání přistupovat? Správce by měl při vyhledávání v první řadě použít dostupné informace v organizaci, týkající se subjektu údajů, které pravděpodobně povedou ke shodám v systémech v závislosti na tom, jak jsou informace strukturovány. Pokud jsou například informace roztříděny v souborech v závislosti na jménu nebo referenčním čísle, mohlo by se vyhledávání omezit na tyto faktory. Pokud však struktura údajů závisí i na jiných faktorech, jako jsou například rodinné vztahy nebo profesní označení nebo jakýkoli druh přímých či nepřímých identifikátorů (např. číslo zákazníka, uživatelské jméno nebo IP adresy), musí být vyhledávání rozšířeno tak, aby zahrnovalo i tyto faktory, a to za předpokladu, že správce má rovněž tyto informace týkající se subjektu údajů nebo je o těchto informacích subjektem údajů informován. Správce však nesmí požadovat, aby subjekt údajů poskytl více informací, než je nezbytné k identifikaci subjektu údajů. Pokud správce používá pro své činnosti zpracování údajů zpracovatele, musí být vyhledávání přirozeně rozšířeno tak, aby zahrnovalo i osobní údaje zpracovávané zpracovatelem. V souladu s článkem 25 nařízení GDPR o záměrné a standardní ochraně údajů by správce (a všichni zpracovatelé, které používá) měli již mít rovněž zavedené funkce umožňující dodržování práv subjektů údajů. Tyto funkce by měly být zavedeny ještě před samotným počátkem operace zpracování. To v této souvislosti znamená, že by měly existovat vhodné způsoby, jak při vyřizování žádosti nalézt a získat

informace o subjektech údajů. Podle EDPB[308] je však třeba doplnit, že příliš extenzivní výklad by v tomto ohledu mohl vést k funkcím vyhledávání a získávání informací, které samy o sobě představují riziko pro soukromí subjektů údajů. Je proto důležité mít na paměti, že proces získávání údajů a informací by měl být rovněž navržen způsobem šetrným k ochraně osobních údajů, aby neohrožoval soukromí dalších osob, například zaměstnanců správce.

5.2.1 Způsoby poskytnutí přístupu

Způsoby poskytnutí přístupu jsem do značné míry popsala již v předchozí části 5.6 – Modality (způsoby) poskytnutí práva na přístup, z kontextuálního hlediska bych se k nim však ráda vrátila i v této části. Výše jsem již objasnila, že při podávání žádosti o přístup mají subjekty údajů právo obdržet kopii svých údajů, stejně jako, že právo na kopii je třeba chápat jako jeden ze způsobů poskytování přístupu k osobním údajům. Právo na kopii je zároveň považováno za hlavní způsob poskytování přístupu k osobním údajům.

Za určitých okolností však může být vhodné, aby správce poskytl přístup jinými způsoby než poskytnutím kopie. Správce tak může poskytnout přístup i tzv. dočasným způsobem, a to například těmito způsoby: poskytnutím ústní informace; nahlížením do spisů; poskytnutím přístupu na místě nebo vzdáleného přístupu bez možnosti stahování. O těchto způsobech může správce uvažovat, pokud je to v zájmu subjektu údajů, nebo pokud o to subjekt údajů výslovně požádá. Poskytnutí přístupu na místě tak může být například vhodným počátečním opatřením, pokud správce zpracovává velké množství nedigitalizovaných údajů, aby subjekt údajů mohl být informován o tom, které osobní údaje jsou zpracovávány, a aby mohl učinit informované rozhodnutí o tom, jaké osobní údaje chce obdržet prostřednictvím kopie. Rozhodnutí o způsobu poskytnutí přístupu tedy spočívá na správci s tím, že by měl především zohlednit zájem subjektu údajů. Zde je ovšem důležité doplnit, že poskytnutí přístupu jinými způsoby, než je poskytnutí kopie, nezbavuje subjekty údajů práva na obdržení kopie, pokud o ni projeví zájem. Stejně tak považuji za nutné doplnit, že kopie je stále z hlediska praxe dozorových úřadů privilegovaným způsobem poskytnutí přístupu.

V praxi se český dozorový úřad často potýká s argumentací správců reagující na stížnosti proti nim podané v tomto smyslu: „*stěžovatel (subjekt údajů) nepožadoval poskytnutí kopie zpracovávaných osobních údajů*“, nebo že „*stěžovatel nepoužil ve své žádosti slovo kopie*

[308] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 41-42.

v rámci vymezení rozsahu své žádosti“. Argumentace správců se tedy soustředí na výklad pojmu „kopie“, na to, že požadavek kopie musí výslovně vyplývat z žádosti a především pak výklad prostého ustanovení čl. 15 odst. 3 nařízení GDPR, který v první větě stanoví pouze: „*Správce poskytne kopii zpracovávaných osobních údajů*.“ Podle mého názoru však nelze žádost subjektu údajů posuzovat příliš formalisticky, a to tak, aby byl subjekt údajů zbaven svých práv. Žádost je třeba posuzovat také materiálně, tj. pokud požadavek kopie jednoznačně vyplývá z obsahu jeho žádosti, je třeba právu na kopii vyhovět. Domnívám se tak, že jiný výklad, a to výklad v neprospěch subjektu údajů jde jednoznačně proti smyslu právní úpravy nařízení GDPR. Ani samotné ustanovení čl. 15 odst. 3 nařízení GDPR tedy nehovoří nic o tom, že by měl správce kopie poskytovat pouze na výslovnou žádost subjektu údajů, správce má dle ustanovení jasnou pozitivní povinnost jednat. Sice souhlasím, že poskytnutí kopie osobních údajů nemusí automaticky znamenat poskytnutí kopie dokumentu. Správce má většinou i jiné možnosti, jakými může přístup poskytnout, nicméně poskytnutí kopie dokumentu s osobními údaji je zpravidla i pro něj nejjednodušší cestou, která je pro subjekt údajů zároveň dostatečně srozumitelná a přehledná. Při zkoumání historického vývoje právní úpravy lze také zjistit, že jde o nejvýznamnější rozdíl ve srovnání s dřívějším ustanovením o právu na přístup podle směrnice 95/46. Tím, že správci mají povinnost poskytovat kopie, je fakticky posíleno právo subjektu údajů na přístup, protože již neumožňuje omezit rozsah tohoto práva tak, aby zahrnovalo pouze souhrn zpracovávaných osobních údajů. Recitál 63 nařízení GDPR hovoří například o možnosti správce „poskytnout dálkový přístup k bezpečnému systému, který by subjektu údajů umožnil přímý přístup k jeho osobním údajům.“

Ještě obecněji, pojem kopie a jeho výklad byly také předmětem řízení u Soudního dvora EU, jedná se o rozsudek ze dne 4. května 2023, *Österreichische Datenschutzbehörde*, C‑487/21. Případ se týkal obchodní poradenské agentury CRIF, poskytující informace o solventnosti třetích osob. Na ní se obrátil žadatel s žádostí o přístup podle článku 15 GDPR. Žadatel konkrétně požádal, aby mu byly „ve standardním technickém formátu“ poskytnuty kopie dokumentů, tedy všech e-mailů a výpisů z databází, které obsahují mimo jiné jeho osobní údaje. Společnost mu v odpovědi zaslala pouze souhrnný seznam zpracovávaných osobních údajů. Poté, co se nespokojený žadatel neúspěšně obrátil na rakouský dozorový úřad, podal žalobu k rakouskému Spolkovému správnímu soudu. Rakouský soud se nakonec obrátil na Soudní dvůr s žádostí o výklad klíčových pojmů (pojem „kopie“ a pojem „informace“ podle čl. 15 odst. 3) a vyjasnění vztahu mezi ustanoveními v rámci článku 15 nařízení.

Soudní dvůr sice potvrdil, že čl. 15 odst. 3 nařízení nezaručuje absolutní právo na pořízení kopií dokumentů. Současně ale konstatoval, že je třeba zohlednit obvyklý smysl tohoto pojmu, který označuje, ve světle teleologického výkladu, věrnou reprodukci nebo opis originálu, takže čistě obecný popis zpracovávaných údajů nebo odkaz na kategorie osobních údajů neodpovídá této definici. Z doslovné analýzy pak podle něj vyplývá, že ustanovení přiznává subjektu údajů právo získat věrnou reprodukci svých osobních údajů chápaných v širším smyslu, které jsou předmětem operací, jež je nutno kvalifikovat jako zpracování správcem. Z toho vyplývá, že kopie zpracovávaných osobních údajů, kterou správce musí podle čl. 15 odst. 3 první věty GDPR poskytnout, musí vykazovat všechny vlastnosti umožňující subjektu údajů účinně uplatňovat svá práva podle tohoto nařízení, a musí proto tyto údaje úplně a přesně reprodukovat. Za účelem zajištění toho, aby takto poskytnuté informace byly snadno pochopitelné, se totiž může jako nezbytná ukázat reprodukce výpisů z dokumentů či celých dokumentů nebo výpisů z databází, které obsahují mimo jiné zpracovávané osobní údaje, je-li uvedení zpracovávaných údajů do kontextu nezbytné pro zajištění jejich pochopitelnosti.[309] Soudní dvůr mimoto zdůraznil také význam práva na přístup, neboť slouží jednotlivcům jako prostředek k ověření přesnosti a zákonnosti zpracování jejich osobních údajů, což jim usnadňuje výkon dalších souvisejících práv, jako je oprava, výmaz nebo omezení zpracování. Ve vztahu k pojmu „informace“ podle čl. 15 odst. 3 dospěl Soudní dvůr k závěru, že vzhledem k tomu, že toto ustanovení nezakládá samostatné právo, je třeba pojem „informace“ chápat, že se vztahuje výhradně na osobní údaje, jejichž kopii je správce povinen poskytnout.

K široké interpretaci pojmu kopie, kterou zaujal Soudní dvůr EU ve výše uvedeném rozsudku, se ostatně přiklánějí i ostatní dozorové úřady, což se promítlo do Pokynů k právu na přístup[310]. Také zde se hovoří o tom, že pojem může zahrnovat různé druhy přístupu k osobním údajům, pokud je úplný (tj. zahrnuje všechny požadované osobní údaje) a subjekt údajů může tyto své údaje uchovávat. To znamená, že informace jsou subjektu údajů poskytnuty způsobem, který mu umožňuje uchovávat veškeré informace o sobě a vrátit se k nim.

Jak již bylo uvedeno dříve v této práci, je na správci, aby se v závislosti na dané situaci rozhodnul, jakým způsobem poskytne kopii zpracovávaných údajů spolu s doplňujícími informacemi. Může tak učinit např. e-mailem, poštou nebo použitím samoobslužného nástroje. Pokud subjekt údajů podává žádost elektronickými prostředky, a zároveň nepožaduje jinak,

[309] Rozsudek ze dne 4. května 2023, Österreichische Datenschutzbehörde, C-487/21, EU:C:2023:369, body 21, 28, 39 a 41.
[310] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 13-14.

informace by měly být poskytnuty v běžně používaném elektronickém formátu, jak je uvedeno v čl. 15 odst. 3 nařízení GDPR. Správce musí v každém případě zvážit vhodná technická a organizační opatření, včetně odpovídajícího šifrování (obzvláště v případě poskytování informací prostřednictvím e-mailu nebo online samoobslužných nástrojů). Pokyny také uvádějí, že v situaci, kdy správce zpracovává osobní údaje žadatele pouze v malém měřítku, kopie osobních údajů a doplňující informace by měly být v zásadě poskytnuty jednoduchým způsobem.

Jsou vhodnější manuální či automatizované postupy pro vyřizování žádostí o přístup? Na to nelze jednoznačně odpovědět. Jisté však je, že nařízení GDPR (technologicky neutrální), ani Pokyny k právu na přístup se nesnaží klást v této otázce správcům překážky. Správci, kteří zpracovávají velké množství údajů, se tak mohou při vyřizování žádostí o přístup spolehnout i na manuální postupy. Dozorové úřady si však jsou vědomy, že v dnešní době, obzvláště vzhledem k množství zpracovávaných údajů, může být pro správce mnohem výhodnější a efektivnější používat automatizované postupy pro vyřizování žádostí subjektů údajů. Typicky se jedná o správce, kteří obdrží velký počet žádostí. Pokyny proto výslovně zmiňují výhody samoobslužných nástrojů. Ty mohou usnadnit účinné a včasné vyřizování žádostí subjektů údajů o přístup a rovněž správci umožnit začlenit ověřovací mechanismus přímo v rámci tohoto nástroje. Zde je ovšem třeba zdůraznit, že samoobslužné nástroje by nikdy neměly omezovat rozsah získaných osobních údajů. Není-li možné poskytnout tímto způsobem všechny informace podle článku 15, je nutné poskytnout zbývající informace jiným způsobem. Správce skutečně může podle Pokynů tento typ nástrojů propagovat a preferovat. Je však třeba poznamenat, že správce musí rovněž vyřizovat i takové žádosti o přístup, které nejsou zasílány prostřednictvím tohoto zavedeného komunikačního kanálu.

5.2.2 Vhodná opatření pro poskytnutí přístupu

Článek 12 nařízení GDPR stanoví požadavky na poskytování přístupu, tj. pro poskytnutí potvrzení, osobních údajů a doplňujících informací podle článku 15, a upřesňuje rovněž formu, způsob a lhůtu ve vztahu k právu na přístup. Další požadavky jsou především rozvedeny v „Pokynech k transparentnosti skupiny WP 29“[311], pokud jde o článek 12, a to většinou ve vztahu k článkům 13 a 14, ale také ve vztahu k článku 15 a k transparentnosti obecně. To, co je

[311] WP29. *Pokyny k transparentnosti WP 260 rev.01*, přijaté dne 29. listopadu 2017 naposledy revidované a přijaté dne 11. dubna 2018. Strany 7–9. Dostupné z: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_cs.pdf.

v těchto pokynech upřesněno, se tak může často vztahovat i na poskytování přístupu podle článku 15 nařízení GDPR.

V čl. 12 odst. 1 nařízení GDPR se stanoví, že správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem veškerá sdělení o zpracování podle článku 15 za použití jasných a jednoduchých jazykových prostředků. Stručnost znamená, že správci údajů by informace, resp. sdělení měli předkládat efektivním a výstižným způsobem, aby se předešlo zahlcení subjektů údajů informacemi. Vhodné je, aby správci tyto informace jasně odlišili od jiných, s ochranou soukromí nesouvisejících informací, například od smluvních ustanovení nebo všeobecných podmínek. V souvislosti s přívlastkem „transparentní" lze zase odkázat na oblast spotřebitelské regulace. Jistý průnik spotřebitelské regulace a práva na ochranu osobních údajů představuje rozsudek Soudního dvora EU ze dne 28. 7. 2016, C-191/15 *Verein für Konsumenteninformation* (také nazývaný jako *Amazon EU Sarl*). V tomto rozsudku Soudní dvůr dovodil, že zneužívající charakter ujednání může vyplývat ze znění nesplňujícího požadavek použití jasného a srozumitelného jazyka. Tento požadavek navíc musí být podle Soudu s ohledem na nerovné postavení, ve kterém se nachází spotřebitel vůči obchodníkovi zejména z hlediska úrovně informovanosti, vykládán široce.[312]

Z obsahového hlediska transparentnosti se v online prostředí doporučuje použít vícevrstvá prohlášení/oznámení o ochraně soukromí, která subjektům údajů umožní přejít na konkrétní část prohlášení/oznámení o ochraně soukromí, o něž mají zájem a chtějí si je přečíst, aniž by museli procházet velké množství textu a vyhledávat v něm konkrétní témata. Srozumitelnost lze vyložit tak, že by informacím o zpracování měla porozumět i průměrná osoba v cílové skupině. Tento požadavek vlastně znamená, že by správce v souladu se zásadou odpovědnosti měl mít znalosti o lidech, o nichž shromažďuje informace, které může využít, aby určil, jakým jazykovým prostředkům daná cílová skupina pravděpodobně porozumí. Pokud jsou cílovou skupinou například pracující odborníci, lze u nich rozumně předpokládat vyšší úroveň porozumění, než pokud se budou shromažďovat osobní údaje dětí. Pod prvkem „snadné přístupnosti" se rozumí, že subjekt údajů by tyto informace neměl složitě dohledávat: mělo by být okamžité zřejmé, kde a jak se k informacím dostane, například přímým poskytnutím, uvedením odkazu, jasným nasměrováním na něj nebo formou odpovědi na otázku položenou přirozeným jazykem (například v online vícevrstvém prohlášení/oznámení ochraně soukromí,

[312] Rozsudek ze dne 28. července 2016, Verein für Konsumenteninformation, C-191/15, EU:C:2016:612, bod 68.

v často kladených otázkách, prostřednictvím kontextových vyskakovacích oken, která se aktivují, když subjekt údajů vyplňuje elektronický formulář nebo v interaktivním digitálním prostředí prostřednictvím chatbotového rozhraní atd. Požadavek jasných a jednoduchých jazykových prostředků zase značí, že informace by měly být poskytovány co nejjednodušším způsobem, bez použití složitých souvětí a jazykových struktur. Informace by neměly obsahovat příliš právních, technických výrazů nebo odborné terminologie. Za všech okolností musí být u zpracování vyjádřeny účely a právní základ zpracování. V následujícím příkladu uvedu příklady špatné a dobré praxe.

Příklady špatné praxe. V následujících větách nejsou dostatečně jasně vysvětleny účely zpracování:

- „*Vaše osobní údaje můžeme použit k vývoji nových služeb*“ (není jasné, o jaké služby se jedná a jak údaje pomohou k jejich vývoji);
- „*Vaše osobní údaje můžeme použít pro výzkumné účely*“ (není jasné, na jaký druh výzkumu se odkazuje); a
- „*Vaše osobní údaje můžeme použít pro nabízení personalizovaných služeb*“ (není jasné, v čem personalizace spočívá).

Příklady dobré praxe:

- „*Budeme uchovávat historii vašich nákupů a informace o dříve zakoupených výrobcích použijeme k tomu, abychom vám mohli doporučit další výrobky, o kterých se domníváme, že byste o ně mohli mít zájem*“ (je jasné, jaký typ údajů bude zpracován, že subjekt údajů bude předmětem cílených reklam na výrobky a že jejich data budou používána k těmto účelům);
- „*Budeme pro analytické účely uchovávat a analyzovat informace o vašich nedávných návštěvách našich internetových stránek a o tom, jak si prohlížíte jejich různé části, abychom věděli, jakým způsobem lidé naše internetové stránky používají a mohli zvýšit jejich intuitivnost*“ (je jasné, jaký typ údajů bude zpracován, i druh analýzy, kterou bude správce provádět); a
- „*Budeme uchovávat záznamy o článcích, na které jste na našich internetových stránkách klikli, a tyto informace použijeme pro cílenou reklamu na těchto internetových stránkách, tak aby souvisela s vašimi zájmy určenými na základě článků,*

které jste si přečetli“ (je jasné, v čem personalizace spočívá a jak byly zájmy přisouzené subjektu údajů určeny).[313]

V čl. 12 odst. 2 se stanoví, že správce usnadňuje subjektu údajů výkon práva na přístup. Ustanovení připomíná, že správci by neměli klást různé formální překážky pro výkon práv subjektů údajů podle článku 15.[314] Přesnější požadavky v tomto ohledu budou muset být posuzovány případ od případu. Při rozhodování o tom, která opatření jsou vhodná, musí správci vzít v úvahu všechny relevantní okolnosti, mimo jiné i množství zpracovávaných údajů, složitost jejich zpracování a znalosti o subjektech údajů.

V čl. 12 odst. 3 se dále píše, že správce poskytne subjektu údajů na žádost podle článku 15 informace o přijatých opatřeních. Pokyny k transparentnosti v souvislosti s články 13 a 14 objasňují pojem „poskytnout“. Tento výklad lze analogicky vztáhnout i k právu na přístup podle článku 15. Je to správce údajů, na němž spočívá povinnost aktivně jednat, předat dotčené informace subjektu údajů, nebo aktivně navést subjekt údajů k jejich umístění. To tedy znamená, že subjekt údajů nesmí být povinen aktivně vyhledávat informace uvedené v tomto článku 15, například v podmínkách použití internetových stránek nebo aplikace. Skupina WP29 (nyní EDPB) navíc doporučuje, aby veškeré informace určené subjektům údajů jim byly dostupné na jednom jediném místě nebo v jednom úplném dokumentu, ke kterému je snadný přístup, pokud si subjekt údajů chce přečíst veškeré informace.

5.2.3 Časové hledisko poskytnutí přístupu

Časové hledisko pro poskytování přístupu je předmětem úpravy v čl. 12 odst. 3 a 4 nařízení GDPR. Zde se vyžaduje, aby správce poskytl subjektu údajů informace o opatřeních přijatých v souvislosti s žádostí podle článku 15 bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. To znamená, že správce je povinen vyřídit žádost odpovědí, popřípadě přijmout odpovídající opatření ve lhůtě jednoho měsíce od obdržení žádosti. Ve stejné lhůtě je správce povinen informovat subjekt údajů v případě, že žádosti nevyhovuje. Lhůtu k vyřízení žádosti o přístup lze prodloužit nejvýše o dva měsíce s ohledem

[313] WP29. *Pokyny k transparentnosti WP 260 rev.01*, přijaté dne 29. listopadu 2017 naposledy revidované a přijaté dne 11. dubna 2018. Strany 9–10. Dostupné z: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_cs.pdf.
[314] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 430-448. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

na složitost a počet žádostí, za předpokladu, že byl subjekt údajů informován o důvodech tohoto odkladu do jednoho měsíce od obdržení žádosti. V souladu se zásadou odpovědnosti správce a jeho povinností usnadňovat výkon práv subjektů údajů by možnost prodloužení lhůty neměla být správcem používána svévolně, ale skutečně jen v odůvodněných případech, kdy mu nařízení GDPR dává celkem rozumnou možnost zohlednit například i vyšší počet nikoliv jednoduchých žádostí.[315] Tato povinnost informovat subjekt údajů o prodloužení lhůty a důvodech by neměla být zaměňována s informacemi, které musí být poskytnuty neprodleně, nejpozději však do jednoho měsíce, pokud správce na žádost nepřijme opatření, jak je podrobně uvedeno v čl. 12 odst. 4 nařízení GDPR.

Spojení „*bez zbytečného odkladu*“ je třeba vykládat tak, že správce reaguje rychle a měl by poskytnout informace podle článku 15 co nejdříve. To zároveň znamená, že pokud je možné požadované informace poskytnout v kratší lhůtě než jeden měsíc, měl by tak správce učinit. Z Pokynů EDPB zároveň vyplývá, že správce musí načasování odpovědi na žádost v některých situacích přizpůsobit době uchovávání, aby mohl poskytnout přístup. Logicky tedy platí, pokud správce obdrží žádost o přístup a zároveň zjistí, že doba uchovávání již uplynula, nemůže údaje nejprve vymazat, aby se vyhnul odpovědi na žádost o přístup, nýbrž naopak. Správce nejprve musí vyřídit žádost o přístup a informovat subjekt údajů (případně i přijmout nezbytná opatření, zaslat kopii údajů subjektu údajů apod.) a až poté přistoupit k výmazu údajů, které již překročily stanovenou dobu uchovávání.

Lhůta pro odpověď na žádost o přístup se počítá podle nařízení Rady (EHS, Euratom) č. 1182/71 ze dne 3. června 1971, kterým se určují pravidla pro lhůty, data a termíny. Pravidla počítání času se uplatní stejně jako dle českého práva, tj. odpovídají pravidlům v § 605 až 608 občanského zákoníku. Pokud poslední den časového období na vyřízení žádosti o přístup připadá na víkend nebo státní svátek, správce má čas na odpověď do následujícího pracovního dne. Lhůta začíná běžet okamžikem, kdy správce obdrží žádost podle článku 15, což znamená, že žádost je doručena správci prostřednictvím jednoho z jeho oficiálních komunikačních kanálů. V Pokynech EDPB se dokonce píše, že není nezbytné, aby si správce byl žádosti skutečně vědom („*It is not necessary that the controller is in fact aware of the request*“). Může ale dojít k situaci, kdy lhůtu bude třeba platně pozastavit (tzv. stavění lhůty), a to konkrétně, pokud bude doručena žádost imperfektní (např. správce si nebude jistý totožností osoby

[315] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 430-448. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

podávající žádost). V takovém případě, za předpokladu, že správce bez zbytečného odkladu požádá o další informace pro ověření totožnosti žadatele, dojde k stavění lhůty, a to dokud správce neobdrží potřebné informace od subjektu údajů. Totéž platí pro případy, kdy správce požádal subjekt údajů o upřesnění činností zpracování, jichž se žádost týká, jsou-li splněny podmínky stanovené v 63. bodě odůvodnění.[316] Příklad č. 15: Poté, co správce obdrží žádost od subjektu údajů, okamžitě zareaguje a požádá o další informace, které potřebuje k potvrzení totožnosti osoby, která žádost podala. Žadatel odpoví až o několik dní později a informace, které zašle za účelem ověření totožnosti, se nejeví jako dostatečné, což vyžaduje, aby správce požádal o další vysvětlení. Za této situace dojde k stavění lhůty, dokud správce neobdrží dostatek informací k ověření totožnosti subjektu údajů.

Pokud jde o možnost správce prodloužit lhůtu až o další dva měsíce, s přihlédnutím ke složitosti případu a počtu žádostí, je nutné k tomuto ustanovení přistupovat jako k výjimce z obecného pravidla, které by nemělo být nadužíváno. V Pokynech EDPB se píše, že pokud správce přistupuje často k prodlužování lhůty, může to indikovat potřebu, aby interně přehodnotil své obecné postupy pro vyřizování žádostí o přístup.

Nelze jednoznačně určit, v čem všem může spočívat „*složitost žádosti*". Záleží na konkrétních okolnostech každého případu. Mezi relevantní faktory nicméně patří například[317]:

– množství údajů zpracovávaných správcem,

– způsoby, jak jsou informace (resp. osobní údaje) u správce uloženy; zejména je třeba zohlednit, jak obtížné je získat tyto informace, například pokud jsou údaje zpracovávány různými útvary organizace a jak rychle jsou informace dostupné,

– potřebu editovat informace, pokud se použije výjimka, například informace týkající se jiných subjektů údajů nebo informace, které představují obchodní tajemství,

– potřebu zapojit zvláštní zdroje/ technologie k vyhledání potřebných informací (např. pokud subjekt údajů výslovně požaduje přístup k osobním údajům, které již správce trvale smazal v souladu se svými zásadami uchovávání, a jeho organizace nemá při běžném podnikání

[316] Bod 63 odůvodnění nařízení GDPR, poslední věta: „*Pokud správce zpracovává velké množství informací týkajících se subjektu údajů, měl by mít možnost před poskytnutím informací požádat subjekt údajů, aby konkrétně uvedl, kterých informací nebo činností zpracování se jeho žádost týká*."
[317] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 50-51.

přístup k technologii, která může obnovit trvale smazané soubory z počítačů a bude muset zaměstnat zvláštní IT odborníky),

– pokud se vyžaduje další práce s těmito informacemi, aby byly srozumitelné nebo další práce s těmito informacemi, aby byla současně chráněna práva třetích osob.[318]

I když žádost o přístup spadá do jednoho nebo více výše uvedených scénářů, musí správce údajů stále prokázat, proč nemůže vyhovět do jednoho kalendářního měsíce, a že je v konkrétním případě nezbytné jednostranné prodloužení lhůty. Zejména se doporučuje, aby správce údajů prodloužil lhůtu tak, aby reagoval co nejrychleji (např. 1,5 měsíce namísto dvou celých měsíců), aby splnil povinnost usnadnit výkon práv subjektů údajů. Subsidiárně může správce částečně vyhovět žádosti o přístup a současně požádat o více času v souvislosti s dílčími složitějšími otázkami, které se jí týkají. Pokyny EDPB v tomto smyslu doplňují, že pouhá skutečnost, že vyhovění žádosti by vyžadovalo větší úsilí, ještě neznamená, že žádost lze považovat za složitou, vyžadující prodloužení lhůty. Stejně tak skutečnost, že společnost obdrží velký počet žádostí, neznamená automatické prodloužení lhůty. Správce, a tím spíše takový správce, který zpracovává velké množství údajů, by měl mít zavedeny postupy a mechanismy, aby byl schopen vyřizovat žádosti ve standardní lhůtě za běžných okolností.[319]

5.3 Omezení práva na přístup

Jak již bylo na několika místech v této práci poukázáno, právo na přístup, obdobně jako i další práva subjektů údajů, nepatří mezi práva absolutní. Koneckonců, i samotná Listina základních práv EU, která byla zařazena mezi prameny primárního práva EU, a jež upravuje ochranu osobních údajů v samostatném článku 8, umožňuje omezení výkonu práv a svobod uznaných v Listině, konkrétně v článku 52, za předpokladu splnění několika podmínek. Především musí takové omezení respektovat podstatu práv a svobod. Právo na přístup podléhá omezením v několika ustanoveních nařízení GDPR. Jedná se zaprvé o omezení v čl. 15 odst. 4 nařízení GDPR (práva a svobody třetích osob) a zadruhé o omezení v čl. 12 odst. 5 nařízení

[318] DPC. Průvodce irského úřadu pro ochranu osobních údajů pro správce údajů – Žádosti subjektů údajů o přístup (originál: Subject Access Requests: A Data Controller's Guide), říjen 2022. Dostupné zde: https://www.dataprotection.ie/sites/default/files/uploads/2022-10/20221005%20Subject%20Access%20Requests%20A%20Data%20Controller%27s%20Guide.pdf. [cit. 2024-04-14].

[319] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 50-51.

GDPR (zjevně nedůvodné nebo zjevně nepřiměřené žádosti). Právo Unie nebo členského státu může navíc omezit právo na přístup v souladu s článkem 23 nařízení GDPR. To je pravděpodobně jedno z nejdůležitějších ustanovení nařízení, co se týče možností individuálních změn ze strany jednotlivých členských států EU. Ustanovení totiž umožňuje členským státům prostřednictvím jejich legislativních opatření omezit rozsah povinností a práv uvedených v článcích 12 až 22 a v článku 34 nařízení, jestliže takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti s cílem zajistit některý, v článku taxativně a obecně vymezený cíl. Přímo v nařízení GDPR (článek 23) je tedy zdůrazněna nutnost respektovat podstatu základních práv a svobod a princip proporcionality. Výjimky týkající se zpracování osobních údajů pro vědecké, historické nebo statistické účely nebo pro účely archivace ve veřejném zájmu mohou být odpovídajícím způsobem založeny na čl. 89 odst. 2 a čl. 89 odst. 3 nařízení GDPR, to je tedy dalším ustanovením upravujícím možné omezení práva na přístup. Nařízení GDPR zároveň upravuje výjimky pro zpracování prováděné pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu, a to konkrétně v čl. 85 odst. 2 nařízení GDPR. Mimo výše uvedených omezení, nařízení GDPR neumožňuje žádné další výjimky nebo odchylky z práva na přístup. Kromě toho není ani dovoleno omezit právo na přístup ve smlouvě mezi správcem a subjektem údajů.

Podle 63. bodu odůvodnění je právo na přístup uděleno subjektu údajů, aby byl informován o zpracování svých osobních údajů, tj. aby si byl vědom zákonnosti zpracování a mohl si toto zpracování ověřit. Právo na přístup mimo jiné umožňuje subjektu údajů v závislosti na okolnostech dosáhnout opravy, výmazu nebo omezení zpracování jeho osobních údajů, jak ostatně konstatoval již Soudní dvůr EU v rozsudku ve spojených věcech C-141/12 a C-372/12, *YS a další*[320]. Nařízení GDPR navíc nikde nestanoví povinnost subjektu údajů jeho žádost odůvodnit, je tedy na něm, zda tyto důvody uvede či nikoliv. Pokud jsou splněny požadavky článku 15 nařízení GDPR, měly by být důvody žádosti považovány za irelevantní.

5.3.1 Omezení právy třetích osob

Podle čl. 15 odst. 4 nařízení GDPR nesmějí být právem získat kopii nepříznivě dotčena práva a svobody jiných osob. Vysvětlení tohoto omezení je uvedeno v páté a šesté větě 63. bodu odůvodnění. Tímto právem by neměla být nepříznivě dotčena práva ani svobody ostatních,

[320] Rozsudek ze dne 17. července 2014, YS a další, spojené věci C-141/12 a C-372/12, EU:C:2014:2081.

například obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení. Mohou sem spadat informace, které tvoří jakési know-how správce či třetích osob, a souvisejí se zpracováním. Jedná se jen o příklady, v zásadě platí, že jakékoli právo nebo svoboda založené na právu Unie nebo členských států mohou být podstatou omezení v odstavci 4, včetně práva na ochranu osobních údajů jiné osoby nebo osobnostního práva jiné osoby či ochrany důvěrnosti komunikace. Zde bych ráda upozornila na početnou judikaturu Evropského soudu pro lidská práva, rozvíjející koncept ochrany soukromí a ochrany důvěrnosti komunikace. Podle Pokynů EDPB je nicméně důležité si uvědomit, že ne každý zájem automaticky zakládá omezení podle odstavce 4. Například ekonomické zájmy společnosti, pokud se nejedná o obchodní tajemství, duševní vlastnictví nebo jiná chráněná práva, by se neměly brát v úvahu při uplatňování čl. 15 odst. 4. Výsledkem těchto úvah správce by nemělo být celkové odepření poskytnutí všech informací, pokud lze alespoň některé informace subjektu údajů poskytnout.

Omezení v odstavci 4 se vzhledem ke svému zařazení vztahuje pouze na samotnou kopii osobních údajů, nikoliv na další informace poskytované podle čl. 15 odstavce 1 písm. a) až h) nařízení GDPR. V tomto smyslu Pokyny EDPB nicméně doplňují, že omezení v odstavci 4 sice výslovně hovoří o právu získat kopii, nicméně z logiky věci by se sem měly řadit i jiné způsoby poskytování přístupu k údajům. Kopie je zde uvedena z důvodu, že se jedná o hlavní a nejčastější způsob poskytování přístupu ke zpracovávaným údajům. Práva a svobody jiných osob by tedy měla být zohledněna i v případě poskytování přístupu ke zpracovávaným údajům jiným způsobem než kopií (kupříkladu poskytnutím přístupu subjektu údajů na místě nebo poskytnutím vzdáleného přístupu).[321] Je na správci, aby byl schopen nepříznivé dotčení práv a svobod jiných osob prokázat, pouze obecné obavy nestačí. Důsledky ustanovení čl. 15 odst. 4 by měly být spíše v tom, že správce omezí pokud možno rozsah předávaných údajů subjektu údajů či subjekt údajů speciálně poučí o omezení v nakládání s nimi, přičemž subjekt údajů by měl tato omezení dodržovat tehdy, pokud to nebude bránit účelu článku 15, tedy zejména užití předávaných údajů k ochraně jeho práv. „*Jinými osobami*“ je nutné rozumět osoby odlišné od subjektu údajů, tedy i správce, který údaje shromažďuje, případně i zpracovatele.[322] Pokud by chtěl evropský normotvůrce vyloučit z ochrany správce a zpracovatele, jistě by použil výraz

[321] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 52-53.
[322] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 474-491. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

„*třetí strana*“ namísto výrazu „*jiná osoba*“. Pokud jde o to, komu je odstavec 4 určen, tedy kdo je vlastně adresátem této normy, doktrína se domnívá, že by se mělo jednat jak o správce, který údaje předává a může tak omezit rozsah příslušného datového souboru, tak o subjekt údajů, který údaje obdrží a který je například nemůže bez dalšího předat vůči konkurenčnímu správci či s nimi nakládat jiným právem zakázaným způsobem.[323] Tento výklad se zdá být i dle mínění autorky rozumný. Jestliže správce situaci vyhodnotí tak, že subjektu údajů nelze poskytnout úplný přístup v důsledku omezení podle čl. 15 odst. 4 nařízení GDPR, musí nicméně subjekt údajů bezodkladně a nejpozději do jednoho měsíce informovat o důvodech tohoto postupu (čl. 12 odst. 4 nařízení GDPR). Správce dále musí v tomto odůvodnění odkázat na konkrétní okolnosti a umožnit subjektům údajů posoudit, zda budou chtít proti tomuto postupu přijmout opatření. Správce musí zejména subjekt údajů poučit o možnosti podat stížnost u dozorového úřadu (článek 77 nařízení GDPR) a žádat o soudní ochranu (článek 79 nařízení GDPR).

Pokud jde o odůvodnění omezení práva na přístup, lze jej nalézt nejen v již zmíněném recitálu 63, ale v základní rovině i v recitálu 4 nařízení GDPR. Recitál 4 zdůrazňuje, že ani právo na ochranu osobních údajů není absolutním právem a je tedy třeba, aby výkon práva na přístup byl v rovnováze s ostatními základními právy v souladu se zásadou proporcionality. Správce by tedy měl provést základní posouzení o třech krocích. V prvním kroku musí odhalit a prokázat, zda by vyhovění žádosti mělo negativní dopady na práva a svobody ostatních osob. Správce by tak měl zvážit zájmy všech dotčených osob s přihlédnutím ke konkrétním okolnostem případu, a zejména k pravděpodobnosti a závažnosti rizik, která při sdělování údajů představují. V rámci druhého kroku by se měl správce pokusit uvést do souladu („smířit“) proti sobě stojící práva, například zavedením vhodných opatření ke zmírnění rizika pro práva a svobody jiných osob. Jak již bylo uvedeno dříve, omezení by pokud možno nemělo vést k úplnému odmítnutí poskytnutí jakýchkoliv kopií údajů, a tedy odepření práva subjektu údajů na přístup k jeho osobním údajům, ale kupříkladu znečitelnění části záznamu, rozmazáním části údajů jiných osob apod. Není-li však možné nalézt smírné řešení, musí správce ve třetím kroku rozhodnout, které z protichůdných práv a svobod nakonec převáží.[324] Ve vztahu k omezení vyplývajícímu z článku 52 Listiny základních práv EU lze zmínit především jeho odstavec 1, který stanoví požadavek, aby každé omezení výkonu práv a svobod bylo stanoveno zákonem, respektovalo podstatu těchto práv a svobod a zároveň dodržovalo zásadu proporcionality. Dalším výkladovým nástrojem pro vyjasnění ustanovení Listiny jsou vysvětlení vyhotovená

[323] Tamtéž.
[324] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 53-54.

pod vedením prezídia Evropského konventu. Podle nich je účelem článku 52 stanovit rozsah práv a zásad obsažených v Listině a stanovit pravidla pro jejich výklad. Odstavec 1 se pak zabývá omezením práv a jeho znění je založeno na judikatuře Soudního dvora EU. Zde se odkazuje na rozsudek Soudního dvora EU ve věci C-292/97, *Karlsson a další*: *„V judikatuře Soudního dvora je jasně stanoveno, že na výkon základních práv je možné uvalit omezení, mimo jiné v rámci společné organizace trhu, pokud tato omezení skutečně odpovídají cílům obecného zájmu sledovaným Společenstvím a nepředstavují vzhledem ke sledovanému cíli nepřiměřené a neopodstatněné omezování ohrožující samu podstatu těchto práv*“.[325] Odkaz na obecné zájmy uznávané Unií zahrnuje jak cíle uvedené v článku 3 SEU, tak další zájmy chráněné zvláštními ustanoveními Smluv, jako čl. 4 odst. 1 SEU, čl. 35 odst. 3 SFEU a články 36 a 346 uvedené smlouvy.[326]

Pokyny EDPB uvádějí několik příkladů k posouzení správce, zdali přistoupit k omezení práva na přístup, či právu vyhovět v plném rozsahu. Příklad č. 16: Správcem je maloobchodník, který nabízí svým zákazníkům možnost objednávat produkty prostřednictvím zvláštní linky provozované jeho zákaznickou službou. Za účelem prokázání obchodních transakcí správce uchovává záznamy hovorů v souladu s přísnými požadavky platných právních předpisů. Zákazník požádá o kopii hovoru, který vedl s pracovníkem zákaznické služby. V první fázi správce žádost analyzuje a zjistí, že záznam obsahuje osobní údaje, které se rovněž týkají někoho jiného, konkrétně pracovníka zákaznické služby. Ve druhé fázi musí správce za účelem posouzení, zda by poskytnutí kopie ovlivnilo práva a svobody jiných osob, vyvážit protichůdné zájmy, zejména s ohledem na pravděpodobnost a závažnost možných rizik pro práva a svobody jeho pracovníka, která existují v okamžiku předávání záznamu zákazníkovi. Správce dospěje k závěru, že osobní údaje týkající se pracovníka zákaznických služeb jsou v záznamech velmi omezené, jedná se totiž pouze o osobní údaje v podobě jeho hlasu. Správce navíc konstatuje, že pracovník na základě záznamu není snadno identifikovatelný. Kromě toho je obsah hovoru profesní povahy a subjekt údajů byl účastníkem tohoto hovoru. Na základě výše uvedených okolností správce objektivně vyhodnotil situaci, že právem na přístup nejsou nepříznivě dotčena práva a svobody pracovníka zákaznické služby, a správce proto může subjektu údajů poskytnout úplný záznam, včetně těch částí, které se týkají pracovníka zákaznické služby.

[325] Rozsudek ze dne 13. dubna 2000, Karlsson a další, C-292/97, EU:C:2000:202, bod 45.
[326] Evropský konvent. Vysvětlení prezídia Evropského konventu k Listině základních práv EU. Úřední věstník Evropské unie C 303/17 - 14.12.2007. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:CS:PDF. [cit. 2024-04-14].

Příklad č. 17: Hráč X je registrován jako uživatel na herní platformě Y (dále jako „společnost Y“). Jednoho dne je hráč X informován o omezení svého online účtu. Vzhledem k tomu, že se nemůže přihlásit, požádá správce o přístup ke všem osobním údajům, které se ho týkají. Kromě toho žádá hráč X o sdělení informací týkajících se důvodů omezení jeho přístupu k účtu. Společnost Y, jakožto správce online herní platformy, u níž byla žádost podána, informuje uživatele ve všeobecných obchodních podmínkách dostupných na jejích internetových stránkách, že jakýkoli druh podvádění (zejména používáním softwaru třetích stran) bude mít za následek dočasný nebo trvalý zákaz užívání její herní platformy. Společnost Y rovněž informuje uživatele ve svých zásadách ochrany soukromí o zpracování osobních údajů za účelem odhalování herních podvodů v souladu s požadavky stanovenými v článku 13 nařízení GDPR. Po obdržení žádosti hráče X o přístup by společnost Y měla tomuto hráči poskytnout kopii osobních údajů o něm zpracovávaných. Pokud jde o sdělení informací týkajících se důvodů omezení účtu, měla by společnost Y potvrdit hráči X, že se rozhodla omezit přístup hráče X k online hrám z důvodu, že se dopustil jednoho nebo opakovaných herních podvodů, které jsou v rozporu s všeobecnými podmínkami používání. Kromě informací poskytnutých o zpracování za účelem odhalování herních podvodů by společnost Y měla hráči X poskytnout přístup k informacím, které o herních podvodech hráče X uložila, a které vedly k omezení jeho přístupu. Společnost Y by měla hráči X zejména poskytnout informace, které vedly k omezení jeho účtu (např. přehled protokolů, tzv. logů; datum a čas, kdy se hráč dopustil podvádění; detekce softwaru třetí strany;…), aby si subjekt údajů (tj. hráč X) mohl ověřit, že zpracování údajů bylo přesné. Podle čl. 15 odst. 4 a 63. bodu odůvodnění nařízení GDPR však společnost Y není povinna odhalit žádnou část technického fungování softwaru proti podvodům, i když se tyto informace týkají hráče X, pokud je lze považovat za obchodní tajemství. Nezbytné vyvážení zájmů podle čl. 15 odst. 4 GDPR bude mít za následek, že obchodní tajemství společnosti Y vyloučí zpřístupnění těchto osobních údajů, protože znalost technického fungování softwaru proti podvodům by mohla uživateli rovněž umožnit obejít budoucí odhalení podvodů nebo odhalení jiných zneužití.[327]

5.3.2 Omezení v podobě zjevně nedůvodné nebo nepřiměřené žádosti

Aby nebyla práva subjektů údajů zneužívána a nepředstavovala neúměrnou zátěž pro správce, má správce podle čl. 12 odst. 5 nařízení GDPR možnost odmítnout nebo zpoplatnit ty

[327] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 55-57.

žádosti, o nichž vyhodnotí, že jsou zjevně nedůvodné nebo nepřiměřené. Tyto pojmy je třeba vykládat restriktivně, neboť nesmí být oslabovány zásady transparentnosti a bezplatnosti práv subjektů údajů. Správce musí být schopen doložit, proč se domnívá, že žádost je zjevně nedůvodná nebo nepřiměřená, a odůvodnit to ve sdělení, kterým žadatele informuje o odmítnutí žádosti nebo o vyhovění žádosti s uložením administrativního poplatku. Správce zároveň musí být schopen na požádání vysvětlit tyto důvody příslušnému dozorovému úřadu. Každá žádost by proto měla být posuzována případ od případu v kontextu, v němž je podána. Důsledky zjevně nedůvodné nebo nepřiměřené žádosti o právo na přístup mohou být tedy následující: správce se buď rozhodne účtovat přiměřený poplatek (s přihlédnutím k administrativním nákladům na poskytnutí informací nebo sdělení či provedení požadovaného úkonu), nebo odmítne žádosti vyhovět. Správce není podle EDPB primárně povinen účtovat tento přiměřený poplatek před tím, než odmítne žádost vyřídit. Správce nicméně nemá úplnou volnost při výběru mezi těmito dvěma možnostmi, musí učinit odpovídající rozhodnutí v závislosti na konkrétních okolnostech. U zjevně nedůvodných žádostí si lze jen stěží představit, že by účtování přiměřeného poplatku bylo vhodným opatřením, naopak, v případě nepřiměřených žádostí bude často právě nejvhodnějším opatřením, v souladu se zásadou transparentnosti, sloužícím jako kompenzace za administrativní náklady, které opakované žádosti způsobují. EDPB určitě správcům doporučuje, aby vždy před účtováním přiměřeného poplatku na základě čl. 12 odst. 5 nařízení GDPR subjektům údajů sdělili, že tak hodlají učinit. Subjektům údajů tak dají dostatečný prostor se rozhodnout, zda žádost ponechat či stáhnout, aby se vyhnuli zpoplatnění.

Kdy lze žádost považovat za „zjevně nedůvodnou“? Žádost o právo na přístup je zjevně nedůvodná, pokud nejsou při uplatňování objektivního přístupu jasně a zjevně splněny požadavky článku 15 nařízení GDPR. Pokyny EDPB nicméně připomínají, že existuje jen velmi omezený prostor pro použití této výjimky, pokud jde o žádosti o právo na přístup. Subjekt údajů totiž nemusí důvodnost své žádosti o právo na přístup nijak dokládat. Za zjevně nedůvodné by mohly být považovány žádosti např. v případě, že jsou zcela nesrozumitelné a nelze ani výkladem posoudit, o co se subjektu údajů jedná, případně žádosti, které podává neoprávněná osoba, která neprokáže svou totožnost. Pokyny EDPB v této souvislosti nicméně uvádějí, že žádosti, které vůbec nespadají do oblasti působnosti nařízení GDPR, nebo zjevně nejsou předmětem zpracování konkrétního správce, by pravděpodobně neměly být vyhodnoceny jako „zjevně nedůvodné“. Správce v těchto případech žádostem vyhovět ani fakticky nemůže, nelze to však odůvodnit výjimkou podle čl. 12 odst. 5 nařízení GDPR. Správce by dále neměl mít za to, že žádost je zjevně nedůvodná, protože subjekt údajů již dříve u správce podal žádosti, které

byly zjevně nedůvodné nebo nepřiměřené nebo pokud žádost obsahuje subjektivní či nevhodný jazyk.

A jaké jsou situace, kdy lze žádost považovat za „zjevně nepřiměřenou“? Za zjevně nepřiměřené mohou být žádosti považovány zejména tehdy, pokud se opakují nebo je jich velký počet. Také zde je správce povinen nepřiměřenost prokázat, přičemž samo nařízení GDPR nabízí jako příklad nepřiměřenosti opakující se žádosti, jak ostatně vystihuje anglický a francouzský výraz „*excessive*“ či německý výraz „*exzessiven*“, aniž by však nařízení GDPR nějak upřesnilo takovou přemíru žádostí nebo definovalo výraz „nepřiměřený“. Zvolená formulace v nařízení GDPR ale jasně ukazuje, že i jiné důvody mohou naplnit znaky této nepřiměřenosti. V této souvislosti je nutno doplnit, že samo nařízení GDPR (v čl. 15 odst. 3, pokud jde o právo na kopii) předpokládá možnost, že subjekt údajů podá u správce více než jednu žádost. Posouzení „nepřiměřenosti“ proto závisí na analýze provedené správcem a na specifikách odvětví, v němž daný správce působí. Správce zároveň musí posoudit, zda byla překročena hranice přiměřených intervalů, či nikoli. O tom ostatně hovoří i bod 63 odůvodnění nařízení: *„(Subjekt údajů) měl by moci toto právo snadno a v přiměřených odstupech uplatňovat…“* Správce zkrátka musí pečlivě zohlednit konkrétní okolnosti u každého případu.

Pokud se žádost překrývá s předchozí žádostí, lze překrývající se žádost obecně považovat za nepřiměřenou, pokud a do té míry, co se týká přesně stejných údajů nebo činností zpracování. Skutečnost, že by správci zabralo obrovské množství času a úsilí poskytnout informace nebo kopii subjektu údajů, nemůže sama o sobě učinit žádost nepřiměřenou. Jak již bylo uvedeno, důvodem vyhodnocení žádosti jako nepřiměřené, mohou být i jiné důvody, než pouze opakující se povaha žádosti. Patří sem případy zneužití práva na přístup podle nařízení GDPR, což znamená případy, kdy subjekty údajů využívají práva na přístup s jediným záměrem způsobit správci škodu nebo újmu. Zneužívající úmysl, a na jeho základě vyhodnocení žádosti jako nepřiměřené, může být například v těchto situacích: a) forma nátlaku ze strany subjektu údajů – subjekt údajů podá žádost, ale zároveň nabídne její stažení výměnou za nějakou formu výhody od správce nebo b) šikana ze strany subjektu údajů – subjekt údajů přehlcuje správce pouze s úmyslem obtěžovat jej nebo jeho zaměstnance, aby paralyzoval jeho činnost. Při rozhodování, zda uplynula přiměřená doba od poskytnutí informací na předchozí žádost, by správce měl s ohledem na přiměřená očekávání subjektu údajů zvážit podle Pokynů EDPB zejména tyto faktory:

A) je zpracování osobních údajů prováděno v rámci hlavní činnosti správce (*as part of its core activity processes*)?;

B) frekvence změny údajů datového souboru – jak často se údaje mění, jak moc je pravděpodobné, že by se informace mezi žádostmi změnily? Pokud datový soubor zjevně není předmětem jiného zpracování než uložení a subjekt údajů si je toho vědom, typicky z důvodu podání předchozí žádosti o právo na přístup, může to být indicií pro posouzení žádosti jako nepřiměřené;

C) povaha údajů – to by mohlo zahrnovat například, zda se jedná o zvláštní kategorii údajů (citlivé údaje) či nikoliv;

D) účely zpracování – mezi ně může patřit, zda je pravděpodobné, že zpracování způsobí žadateli újmu (škodu), pokud bude zveřejněno;

E) zda se následné žádosti týkají stejného typu informací nebo činností zpracování, nebo odlišných.

Také specifika odvětví hrají důležitou roli, neboť lze očekávat vyšší frekvenci změny datového souboru v případě sociálních sítí (Facebook, LinkedIn, Twitter atd.) než například v případě registrů – katastru nemovitostí nebo (centrálních) obchodních rejstříků. Obecně lze říci, že čím častěji dochází ke změnám v datových souborech a databázích správce, tím častěji mohou subjekty údajů žádat o přístup, aniž by byly jejich žádosti nepřiměřené. Za určitých okolností ale může být i druhá žádost téhož subjektu údajů považována za „žádost opakující se povahy“. Příklad č. 18: (truhlář): Subjekt údajů podává každé dva měsíce žádost o přístup k truhláři, který pro něj vyrobil stůl. Truhlář na první žádost odpověděl úplně. Při rozhodování o tom, zda uplynul přiměřený interval, je třeba vzít v úvahu, že truhlář zpracovává a shromažďuje osobní údaje pouze příležitostně, nikoli v rámci své hlavní činnosti, a ještě méně pravděpodobné je, že by často poskytoval služby stejnému subjektu údajů. V tomto případě truhlář poskytl subjektu údajů pouze jednu službu, tudíž není pravděpodobné, že by v datovém souboru týkajícím se subjektu údajů došlo ke změnám. Vzhledem k povaze a množství zpracovávaných osobních údajů lze rizika spojená se zpracováním považovat za nízká, dále účel zpracování (fakturační účel a vedení evidence pro plnění právních povinností – daňové povinnosti) pravděpodobně nezpůsobí subjektu údajů újmu. Žádost se navíc týká stejných informací jako poslední žádost. Takové žádosti lze proto v důsledku považovat za nepřiměřené, a to z důvodu jejich opakující se povahy. Příklad č. 19 (platforma sociální sítě): Platforma sociální sítě, jejíž hlavní činností je shromažďování a/nebo zpracování osobních údajů subjektu údajů, provádí rozsáhlé komplexní a nepřetržité činnosti zpracování. Subjekt údajů, který využívá služeb platformy, podává žádosti o přístup každé tři měsíce. V tomto případě jsou ale

změny osobních údajů týkajících se subjektu údajů velmi pravděpodobně časté, správce navíc zpracovává širokou množinu shromažďovaných údajů, které zahrnují i odvozené citlivé osobní údaje (např. údaje o politických názorech, náboženském vyznání, etnickém původu) zpracovávané za účelem zobrazení relevantního obsahu a uživatelů sítě subjektu údajů. Za těchto okolností nelze žádosti o přístup podané každé tři měsíce v zásadě považovat za nepřiměřené z důvodu opakování.

Tyto příklady z dílny EDPB jsou tedy poměrně jasné, poukážu ale na případ, kdy situace může být sporná. Příklad č. 20 (úvěrové agentury): Podobně jako v případě sociálních sítí nelze vyloučit, že ke změnám relevantních údajů uchovávaných úvěrovými agenturami bude docházet v relativně krátkých intervalech. To vyplývá z mnoha faktorů, kterých si subjekt údajů jako osoba, jež není součástí interních procesů, obvykle není vzhledem ke složitosti obchodního modelu vědoma. Odpověď na otázku, které typy údajů byly shromážděny pro výpočet hodnoty úvěrového skóre správcem a které jsou v současné době do tohoto výpočtu zahrnuty, proto může poskytnout pouze samotná úvěrová agentura. Kromě toho může mít zpracování údajů prostřednictvím úvěrových agentur a výsledná bodová hodnota důvěryhodnosti žadatele dalekosáhlé důsledky pro subjekt údajů s ohledem na zamýšlená právní jednání, jako je uzavírání kupních, nájemních nebo leasingových smluv. Obecně nelze určit žádný konkrétní interval, v němž by podání další žádosti o přístup mohlo být považováno za nepřiměřené podle čl. 12 odst. 5 nařízení GDPR. Je spíše nutné celkové zvážení okolností konkrétního případu. Vzhledem k významu zpracování údajů pro realitu každodenního života subjektů údajů však lze předpokládat, že jednoroční interval bude v každém případě příliš velký na to, aby bylo možné žádost považovat za nepřiměřenou. Pokud je žádost podána ve velmi krátkém intervalu, mělo by být rozhodující, zda má subjekt údajů oprávněný důvod předpokládat, že se informace nebo zpracování od jeho poslední žádosti změnily. Jestliže subjekt údajů provedl v mezičase finanční transakci, například si vzal úvěr, měl by být oprávněn požádat o přístup k informacím o úvěru, i když taková žádost byla podána a zodpovězena krátce předtím.[328]

5.3.3 Omezení některých práv a povinností podle článku 23 nařízení GDPR

Článek 23 nařízení GDPR má za cíl vymezit úpravu práva na ochranu osobních údajů v poměru k jiným právům či veřejným zájmům. Právo na ochranu osobních údajů je totiž

[328] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023, s. 57-58.

nutné vyvažovat proporcionálně s těmito jinými právy či veřejnými zájmy. Článek 23 tedy představuje omezení, které lze vztáhnout na práva a povinnosti vymezené v čl. 5, 12 až 22 a 34 nařízení GDPR. Dále je důležité zmínit i bod 73 odůvodnění nařízení GDPR, podle něhož by omezení měla být v souladu s požadavky stanovenými v Listině základních práv EU a Evropské úmluvě o ochraně lidských práv a základních svobod. Zároveň bude nezbytné zajistit soulad s jinými lidskoprávními předpisy a ústavním pořádkem daného členského státu. EDPB považuje tuto problematiku za důležitou, o čemž svědčí i to, že právě k těmto omezením podle článku 23 vydal zvlášť pokyny s podrobným vysvětlením.[329] Podle těchto Pokynů musí být dány jasné důvody pro uplatnění omezení podle článku 23. Aby byla omezení v souladu s právem, musí být stanovena v legislativním opatření členského státu nebo Evropské unie, musí se týkat omezeného počtu práv subjektů údajů a/nebo povinností správce údajů, které jsou uvedeny v článku 23 nařízení GDPR, musí respektovat podstatu dotčených základních práv a svobod, představovat nezbytné a přiměřené opatření v demokratické společnosti a zajišťovat jeden ze zájmů uvedených v čl. 23 odst. 1 nařízení GDPR. Ustanovení čl. 23 odst. 1 nařízení GDPR uvádí taxativní výčet těchto cílů, resp. zájmů, kterých je celkem 10. Tyto zájmy jsou pravděpodobně záměrně formulovány poměrně široce, aby bylo členským státům i EU umožněno zajistit ochranu jejich zájmů pomocí omezení. To ovšem neznamená možnost nepřiměřeného omezování ochrany osobních údajů, vždy musí být splněny výše uvedené požadavky.

Článek 23 odst. 2 nařízení GDPR pak stanoví prostřednictvím demonstrativního výčtu, že každé legislativní opatření by mělo být odůvodněno z hlediska účelu a kategorie zpracování, kategorie osobních údajů, rozsahu zavedených omezení, záruk proti zneužití údajů nebo protiprávnímu přístupu k nim či jejich protiprávnímu předání. Legislativní omezení by dále mělo uvést správce či kategorie správců, stanovit dobu uložení a rizika z hlediska práv a svobod subjektů údajů. Subjekty údajů kromě toho musí být informovány o daném omezení, pokud toto informování nemůže být na újmu účelu omezení. Z výše uvedených Pokynů[330]lze k tomu doplnit, že důvod pro omezení by měl být v souladu s bodem 8 odůvodnění nařízení GDPR srozumitelný pro osoby, na něž se vztahuje. To zahrnuje zejména jasné pochopení toho, jak a kdy se omezení může uplatnit. Například, vnitrostátní právní předpisy týkající se prevence a

[329] EDPB. *Pokyny 10/2020 týkající se omezení podle článku 23 GDPR*, verze 2.1, přijaté dne 13. října 2021, s. 6. Dostupné zde: https://www.edpb.europa.eu/system/files/2023-07/edpb_guidelines202010_on_art23_adopted_after_consultation_cs.pdf.
[330] EDPB. *Pokyny 10/2020 týkající se omezení podle článku 23 GDPR*, verze 2.1, přijaté dne 13. října 2021, s. 12 až 15. Dostupné zde: https://www.edpb.europa.eu/system/files/2023-07/edpb_guidelines202010_on_art23_adopted_after_consultation_cs.pdf.

vyšetřování porušování etických pravidel regulovaných povolání by mohly stanovit, že pokud může zveřejnění skutečnosti, že určitá osoba je vyšetřována pro závažné porušení, poškodit účel vyšetřování, informace nemusí být po omezenou dobu subjektu údajů zpřístupněny. Dále například ve správním vyšetřování, zejména v jeho předběžné fázi, může správce údajů rozhodnout, že v daný okamžik informace o důvodu omezení neposkytne – je-li toto omezení zákonné a v konkrétním případě nezbytně nutné k prevenci újmy na účelu omezení. Subjekt údajů by pak měl obdržet zvláštní oznámení o ochraně údajů v pozdější fázi, ačkoli je stále možné, že některá práva zůstanou nadále omezována, například právo na přístup k informacím o zahájení vyšetřování nebo k tvrzením potenciálních obětí obtěžování. Otázkou výjimek a omezení se také zabýval mnohokrát i Soudní dvůr EU, ačkoli většinou ještě v rámci působnosti dřívější směrnice 95/46. Jako příklad lze uvést již zmíněný rozsudek *YS a další* ve spojených věcech C-141/12 a C-372/12.[331] V tomto rozsudku se Soudní dvůr zabýval rozsahem práva na přístup, pojmem „osobní údaje" i právě otázkou omezení (dříve upravenou v článku 13 směrnice 95/46). V tomto rozsudku Soudní dvůr sice rozhodl, že „*údaje, které se týkají žadatele o povolení k pobytu uvedené ve správním dokumentu, který obsahuje důvody, které úředník uvádí na podporu návrhu rozhodnutí, jehož vypracováním byl pověřen v rámci řízení, které předchází přijetí rozhodnutí týkajícího se žádosti o takové povolení, a případně údaje uvedené v právním rozboru, který je v tomto dokumentu obsažen, představují osobní údaje ve smyslu tohoto ustanovení; takto však nelze kvalifikovat uvedený rozbor jako takový*." Podle Soudu totiž právní rozbor nepředstavuje informaci týkající se žadatele o povolení k pobytu, ale nanejvýš informaci týkající se posouzení a použití tohoto práva příslušným orgánem na situaci tohoto žadatele. Žadatel tedy nemá automaticky přístup k tomuto dokumentu jako celku.

Rozsahem informační povinnosti správce a podmínkami výjimek a omezení se Soudní dvůr EU dále zabýval v rozsudku *Bara a další* ve věci C-201/14.[332] V tomto rozsudku byly osobní údaje předány mezi dvěma vnitrostátními orgány (daňovým a zdravotním), ale subjekty údajů nebyly o předání a dalším použití údajů informovány. Soudní dvůr EU zvažoval, zda se na tento případ může vztahovat výjimka uvedená v článku 13 směrnice 95/46 (dnes tomu odpovídá právě článek 23 nařízení GDPR týkající se zájmu členského státu, pokud jde o rozpočtovou a daňovou oblast). Soud rozhodl, že se úřady nemohou této výjimky dovolávat, protože nebyla stanovena legislativním opatřením, ale protokolem, který nebyl předmětem úředního zveřejnění. V souvislosti s informační povinností se Soudní dvůr EU zabýval dále

[331] Rozsudek ze dne 17. července 2014, YS a další, spojené věci C-141/12 a C-372/12, EU:C:2014:2081.
[332] Rozsudek ze dne 1. října 2015, Bara a další, C-201/14, EU:C:2015:638.

rozsahem výjimky týkající se trestního práva a jiného vymáhání práva. Ve věci *IPI*[333] Soud rozhodl, že profesní organizace a soukromí detektivové nepodléhají povinnosti informovat subjekt údajů, protože jejich vyšetřování a oznamování porušení pravidel odpovídá zájmu v podobě „předcházení trestným činům a jejich vyšetřování, odhalování a stíhání nebo nedodržování deontologických pravidel pro regulovaná povolání“. Pokud se tedy členský stát rozhodl výjimku zavést do vnitrostátního práva, pak se jí profesní organizace a soukromí detektivové mohou dovolávat a povinnost informovat subjekt údajů se na ně nevztahuje.

Pokud jde o právo na přístup (a ostatně i další práva subjektu údajů), EDPB připomíná, že správci by měli omezení zrušit, jakmile pominou okolnosti, které je odůvodňují. Pokud by správce neumožnil subjektu údajů výkon jeho práv poté, co bylo omezení zrušeno, může se subjekt údajů v souladu s čl. 57 odst. 1 písm. f) obrátit na dozorový úřad a podat na správce stížnost. Omezení může mít různé podoby, ovšem nikdy nemůže dojít k obecnému pozastavení všech práv. Legislativní opatření stanovující omezení podle článku 23 GDPR, mohou rovněž stanovit opožděný výkon tohoto práva, částečný výkon tohoto práva nebo jeho omezení na určité kategorie údajů, nebo že právo lze vykonávat nepřímo prostřednictvím nezávislého dozorového úřadu.

5.3.4 Omezení upravená v zákoně o zpracování osobních údajů

Česká republika přijala na základě uvedeného článku 23 nařízení GDPR výjimky z aplikace některých ustanovení nařízení. Jedná se o ustanovení § 11 (Omezení některých práv a povinností) a ustanovení § 12 (Výjimka z povinnosti oznámení porušení zabezpečení osobních údajů subjektu údajů) zákona o zpracování osobních údajů.

[333] Rozsudek ze dne 7. listopadu 2013, IPI, C-473/12, EU:C:2013:715.

Ustanovení § 11 tohoto zákona[334] upravuje podmínky omezení výkonu práv subjektů údajů uvedených v čl. 12 až 22 a v jim odpovídajícím rozsahu též čl. 5 nařízení GDPR.[335] Tyto podmínky omezení jsou koncipovány obecně, že se práva subjektů údajů přiměřeně omezí nebo se jejich provedení odloží. Podle důvodové zprávy k adaptačnímu předpisu zde zákonodárce předpokládal, že konkrétní omezení práv subjektů údajů bude stanoveno primárně zvláštními právními předpisy upravujícími konkrétní oblast zpracování osobních údajů. Ustanovení § 11 tohoto zákona tak bylo koncipováno jako ustanovení subsidiární povahy ke zvláštním právním předpisům a lze jej využít pouze v případě, že konkrétní řešení střetu práva na ochranu osobních údajů a chráněného zájmu není upraveno zvláštním předpisem. Ustanovení § 11 ovšem dle názoru autorky neodpovídá smyslu nařízení GDPR. Je totiž koncipováno velmi široce, úvahu ohledně aplikace výjimky nechává v zásadě na správci, neboť odstavec 1 obsahuje pouze dovětek, „*je-li to nezbytné a svým rozsahem přiměřené k zajištění chráněného zájmu uvedeného v § 6 odst. 2 (pozn. autorky: tohoto zákona)*.“ Pojem „chráněný zájem“ je definován v § 6 odstavci 2 taxativním výčtem. Jedná se o zájmy, které lze shrnout pod pojmy jako zajištění obrany a bezpečnosti země, veřejný pořádek, hospodářské a finanční zájmy země, ochrana nezávislosti justice, odhalování protiprávního jednání a ochrana a obhajoba práv a povinností osob. Správce tedy v zásadě provádí subjektivní rozhodování, neboť ustanovení § 11 nijak neupravuje ani předchozí kontrolu ze strany dozorového úřadu, ani oznámení subjektům údajů. Lze tedy mít legitimní obavy z případného nadužívání ze strany správců či zpracovatelů a z netransparentnosti takového postupu. Jediným kontrolním opatřením před nepřiměřeným postupem správce nebo zpracovatele je zavedení oznamovací povinnosti správce nebo zpracovatele vůči dozorovému úřadu, které je obsaženo v odstavci 2 tohoto ustanovení. Zde je vyjádřen požadavek na správce, aby v oznámení dozorovému úřadu uvedl alespoň v relevantním rozsahu skutečnosti demonstrativně uvedené v čl. 23 odst. 2 nařízení

[334] § 11 – Omezení některých práv a povinností
(1) „Nestanoví-li jiný právní předpis jinak, čl. 12 až 22 a v jim odpovídajícím rozsahu též článek 5 nařízení Evropského parlamentu a Rady (EU) 2016/679 se použijí přiměřeně nebo se splnění povinností správce nebo zpracovatele nebo uplatnění práva subjektu údajů stanovených těmito články odloží, je-li to nezbytné a svým rozsahem přiměřené k zajištění chráněného zájmu uvedeného v § 6 odst. 2.
(2) Omezení některých práv nebo povinností podle odstavce 1 správce nebo zpracovatel bez zbytečného odkladu oznámí Úřadu, přitom uvede v přiměřeném rozsahu skutečnosti podle čl. 23 odst. 2 nařízení Evropského Parlamentu a Rady (EU) 2016/679; to neplatí pro soudy provádějící zpracování osobních údajů podle čl. 55 odst. 3 nařízení Evropského Parlamentu a Rady (EU) 2016/679.“
[335] UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, s. 618-628. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-04-14].

GDPR.[336] Bližší úprava pravomocí dozorového úřadu či jeho postupu po obdržení takového oznámení podle § 11 odst. 2 však absentuje. Autorka je tak toho názoru, že toto ustanovení není z hlediska požadavků nařízení GDPR dostačující.

Ustanovení § 12 zákona o zpracování osobních údajů se týká omezení oznamovací povinnosti správce vůči subjektům údajů v případě porušení zabezpečení osobních údajů. Nařízení GDPR totiž obecně upravuje ve stanovených případech, kdy musí být porušení zabezpečení osobních údajů nahlášeno dozorovému úřadu (článek 33) a oznámeno subjektům údajů (článek 34). Pokud je totiž porušení zabezpečení osobních údajů vyhodnoceno jako vysoce rizikové pro práva a svobody fyzických osob, musí být porušení zabezpečení oznámeno i subjektům údajů. Výjimky z povinnosti správce oznamovat případy porušení dotčeným subjektům údajů jsou v první řadě upraveny v samotném nařízení GDPR v čl. 34 odst. 3. Správce jednak nemusí oznamovat porušení zabezpečení v případě, že osobní údaje nelze přiřadit ke konkrétním osobám, např. prostřednictvím přijatého opatření šifrování. Oznámení se dále nevyžaduje, pokud byla správcem přijata následná opatření zajišťující, že se vysoké riziko neprojeví. Poslední liberační důvod tvoří okolnost, že by oznámení porušení zabezpečení osobních údajů vyžadovalo nepřiměřené úsilí ze strany správce. Nařízení GDPR k tomuto poslednímu liberačnímu důvodu ovšem doplňuje požadavek, že v takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření. Zákon o zpracování osobních údajů tak doplňuje v již zmíněném ustanovení § 12 výjimky stanovené nařízením GDPR. Ustanovení § 12 umožňuje omezit či odložit oznámení porušení zabezpečení osobních údajů subjektům údajů, aby se zamezilo negativním důsledkům pro chráněné zájmy, jak jsou uvedeny v § 6 odst. 2 zákona o zpracování osobních údajů. Podle důvodové zprávy je smyslem tohoto omezení předejít negativnímu důsledku bezodkladného oznamování, jako je vyvolání paniky, ohrožení veřejného pořádku, narušení činnosti státních orgánů atd. Zárukou proti nadužívání tohoto ustanovení je oznamování postupu správce dozorovému úřadu za podmínek vysvětlených u ustanovení § 11.[337]

Výše komentovaná ustanovení § 11 a 12 zákona o zpracování osobních údajů byla přijata na základě článku 23 nařízení GDPR, tedy základního ustanovení upravujícího omezení, resp. výjimky z práv a povinností stanovených nařízením GDPR. Na tomto místě je ale třeba

[336] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABARTA, Petr, KAŠPÁRKOVÁ, Kateřina, 2019. *Zákon o zpracování osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR. 1. vydání, 212 s. ISBN 978-80-7598-467-8.
[337] Vláda. Důvodová zpráva k zákonu č. 110/2019 Sb. o zpracování osobních údajů, č. 110/2019 Dz.

podotknout, že zákon o zpracování osobních údajů obsahuje pro práva subjektů údajů (v našem případě konkrétně právo na přístup) i další výjimky na několika místech. Tyto výjimky zde stručně shrnu. Jedná se zaprvé o ustanovení § 16 zákona, které upravuje zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely. Toto ustanovení je reakcí na článek 89 nařízení GDPR, který členským státům umožňuje stanovit některé odchylky od standardního režimu v případě zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely. Právo subjektů údajů na přístup, na opravu, na omezení zpracování, jakož i právo vznést námitku proti zpracování může být omezeno nebo odloženo za předpokladu nezbytnosti a přiměřenosti pro splnění daných účelů. Základním korektivem je tedy posouzení nezbytnosti a přiměřenosti, což znamená, že správce či zpracovatel by tedy měl práva subjektů údajů omezovat pouze v takové míře, aby byl schopen efektivně provést historický či vědecký výzkum, případně statistickou činnost. V odstavci 3 je navíc výslovně zmíněno omezení práva subjektu údajů na přístup k osobním údajům u vědeckého výzkumu, pokud by poskytnutí informací vyžadovalo nepřiměřené úsilí ze strany správce nebo zpracovatele. Důvodem této výjimky je dle zákonodárce náročnost administrace tohoto práva u vědeckého výzkumu a snaha o zachování efektivity vědeckého výzkumu.[338]

Zadruhé sem spadá ustanovení § 19 zákona, které se týká tzv. novinářské výjimky. Ustanovení umožňuje správcům výjimky z povinností dle nařízení GDPR u zpracování pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu. Účelem je ochrana zdroje a obsahu informací, typicky spojená právě s výkonem novinářské profese. V odstavci 2 je opět výslovně omezeno právo na přístup dle článku 15 nařízení GDPR v případě probíhajícího zpracování osobních údajů. Probíhajícím zpracováním se přitom rozumí zpracování osobních údajů před jejich zveřejněním. Zákon zároveň připouští, aby správce omezil právo na přístup, pokud by výkon tohoto práva ze strany subjektu údajů ohrozil nebo zmařil účel zpracování nebo pokud by jeho vypořádání neúměrně zatížilo správce.

Zatřetí se jedná o ustanovení § 23 zákona, které obecně upravuje výjimky z povinností správců při zpracováních osobních údajů pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu. Na základě tohoto ustanovení je možné omezit či odložit výkon některých práv subjektů údajů (včetně práva na přístup) a povinností správce, jsou-li splněny kumulativně dvě podmínky, a sice a) takový postup je potřebný ke splnění účelu

[338] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABARTA, Petr, KAŠPÁRKOVÁ, Kateřina, 2019. *Zákon o zpracování osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR. 1. vydání, 212 s. ISBN 978-80-7598-467-8.

zpracování uvedeného v § 17 odst. 1; a zároveň b) tento postup nepovede k vysokému riziku pro zájmy subjektu údajů. Jedná se o velmi obecně koncipované ustanovení, nelze ovšem opomenout, že novináři nemohou této výjimky zneužívat, což vyplývá již ze samotné podstaty požadavku proporcionality, uvedeném právě v § 17 odst. 1 zákona. Vzhledem k obecnosti ustanovení lze očekávat v budoucnu jeho upřesnění prostřednictvím judikatury. Za možný problematický fakt ovšem považuji, že zákon o zpracování osobních údajů nijak neupravuje, jak se má v této situaci správce vypořádat s žádostí subjektu údajů o přístup.

Začtvrté a naposledy je třeba zmínit ustanovení § 28 zákona. Toto ustanovení upravuje právo na přístup k osobním údajům v režimu trestněprávní směrnice, tedy jedná se o implementaci článků 14 a 15 směrnice 2016/680. Také zde platí, že smyslem je, aby subjekt údajů získal informace o tom, zda spravující orgán zpracovává jeho osobní údaje či nikoliv. V odstavci 1 jsou dále vyjmenovány informace, na které má subjekt údajů nárok v případě, že spravující orgán o něm skutečně osobní údaje zpracovává. Patří sem informace o účelu zpracování, zákonných podkladech pro toto zpracování, příjemcích či jejich kategorií, předpokládané době uchování osobních údajů nebo způsobu jejího určení, poučení o právu na opravu, omezení zpracování nebo výmaz osobních údajů a zdroji těchto údajů. Následující odstavce (především odstavec 2) poté upravují omezení práva subjektu údajů na přístup. V odstavci 2 je uvedeno, že žádosti subjektu údajů na přístup k osobním údajům může spravující orgán nevyhovět nebo jí vyhovět pouze omezeně, pokud jsou naplněny legitimní důvody taxativně zde vyjmenované. Také tyto důvody jsou stanoveny velmi široce. V první řadě sem patří předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti státu nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, jakož i pátrání po osobách a věcech. Dalšími důvody jsou vedení řízení o přestupku či kázeňském přestupku, dále ochrana utajovaných informací nebo ohrožení oprávněných zájmů třetí osoby. Vzhledem ke specifičnosti těchto zákonných zájmů (důvodů), myslí zákon v odstavci 3 i na to, že je třeba upravit informační povinnost vůči subjektům údajů, pokud by vyhovění žádosti či pouhé sdělení o nevyhovění žádosti mohlo ohrozit plnění úkolů spravujícího orgánu. V takovém případě musí spravující orgán informovat subjekty údajů stejně jako ty žadatele, jejichž osobní údaje nezpracovává. Z důvodů zajištění následné zpětné kontroly je pak v odstavci 4 stanoveno, že spravující orgán je povinen vést o odmítnutí žádosti a důvodech odmítnutí po dobu nejméně 3 let dokumentaci. Tato dokumentace by měla být v případě potřeby zpřístupněna dozorovému úřadu.

6. Uplatňování práva na přístup v praxi

V této práci jsem se snažila podrobit právo na přístup podrobnějšímu zkoumání z různých úhlů, mapovat jeho historické kořeny, právně-teoretický základ, účel, význam ve společnosti, strukturu, konkrétní příklady z praxe i z judikatury, vztah k ostatním právům subjektů údajů i dalším blízkým samostatným pojmům (soukromí, přístup k informacím), včetně praktických doporučení ohledně podávání žádostí o přístup (pro subjekty údajů) i jejich vyřizování (pro správce). Domnívám se však, že pro ucelené povědomí je potřeba i ověřit, jakým způsobem funguje právo na přístup v praxi; jestli je skutečně subjekty údajů uplatňováno a především účinně dodržováno ze strany správců. Nabízí se také otázka, jak moc je ochrana prostřednictvím práva na přístup účinná? Těmto otázkám bych se proto ráda věnovala v této poslední části.

6.1 Obecné zhodnocení evropské regulace

Uznávaný odborník na ochranu osobních údajů, profesor Kuner, patřil současně mezi velké kritiky evropského systému ochrany osobních údajů reprezentovaného směrnicí, kde vycházel z argumentů právní filozofie. Prof. Kuner ve své studii[339] konkrétně navázal na starší diskusi mezi H. L. A. Hartem a L. Fullerem o přednostech právního pozitivismu (jehož zastáncem byl Hart) oproti přednostem teorie přirozeného práva (kterou naopak prosazoval Fuller). Oba vědci totiž předkládali zásadní otázky o povaze práva, charakteristikách úspěšného a účinného právního řádu a úloze vymáhání práva při zajišťování jeho správného fungování. Právě tyto otázky si prof. Kuner kladl v souvislosti s evropským právem na ochranu údajů, a dospěl k závěru, že je příliš obsáhlý, komplikovaný, byrokratický, ne příliš jasný z hlediska cílů a stále více zastaralý ve srovnání s moderními trendy regulatorní praxe.[340] Po vzoru Fullerova konceptu vnitřní morálky práva, který vychází z osmi klíčových selhání práva, konstruoval i prof. Kuner pět základních problémů evropského systému ochrany osobních údajů: 1) Chybějící pravidla, která by upravovala každodenní situace; 2) Nedostatečná publicita a sdělování relevantních pravidel; 3) Nejasná pravidla (zde uvádí jako podskupiny a) nedostatek právně závazných rozhodnutí soudů a regulatorních orgánů a nadměrné spoléhání se na

[339] KUNER, Christopher, 2008. *The 'Internal Morality' of European Data Protection Law*. Online. Roč. 2008, s. 10-19. Dostupné z: SSRN: https://ssrn.com/abstract=1443797. [cit. 2024-08-24].
[340] MATEJKA, Ján, 2013. 4. Právní regulace ochrany soukromí, její limity a možnosti. In: MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, s. 57-156. ISBN 978-80-904248-7-6.

nezávazné prameny práva; b) spoléhání se na obecné právní zásady, které nejsou výslovně uvedeny v platných právních předpisech); 4) Vzájemně si odporující pravidla a 5) Neshoda mezi pravidly a jejich uplatňováním v praxi. Navzdory své kritice nicméně prof. Kuner obecně považoval evropský systém ochrany osobních údajů za evropský úspěch, který předběhl svou dobu a od té doby se rozšířil po celém světě. Směrnice 95/46 o ochraně údajů však byla přijata těsně před internetovou revolucí a globalizací zpracování údajů, a proto vyžadovala revizi a úpravu, aby si zachovala svou vnitřní soudržnost, a tím i svou účinnost, ve vztahu k úřadům, správcům a jednotlivcům.

V tomto smyslu je třeba doplnit, že kritika prof. Kunera byla poplatná své době, směrnice 95/46 byla skutečně v mnoha ohledech problematická a nedostatečná. Uvedenými problémy nařízení GDPR netrpí (snad až na výjimky – stále lze pozorovat nejasnost některých pravidel), domnívám se dokonce, že od té doby urazila Evropská unie obrovský kus cesty. Hlavním cílem nařízení GDPR bylo odstranit roztříštěný přístup k ochraně údajů a zajistit větší ochranu subjektům údajů. To se mu podle mého názoru z větší části podařilo, i když roztříštěnost částečně přetrvává, a to zejména v případech, kdy mají členské státy možnost nařízení GDPR vnitrostátně upřesnit.

Nařízení GDPR od doby své účinnosti již prošlo dvojí revizí, či přesněji řečeno hodnocením, které vydala Evropská komise jako součást svého závazku pravidelně přezkoumávat účinnost tohoto předpisu. První zpráva Komise z června 2020 potvrdila, že nařízení GDPR přineslo vysokou úroveň ochrany osobních údajů v EU, ale zdůraznila také potřebu zjednodušení a zlepšení v některých oblastech, jako jsou práva subjektů údajů nebo přeshraniční spolupráce nebo dokončení harmonizace odvětvových právních předpisů s nařízením GDPR.[341] V červenci 2024 pak byla vydána Druhé zpráva Komise o uplatňování obecného nařízení o ochraně osobních údajů.[342] Jak lze z této nedávno vydané Druhé zprávy zjistit, stále přetrvává celá řada dílčích problémů, identifikovaných zúčastněnými stranami. Zpráva uvádí některé příklady: a) rozdílné výklady klíčových pojmů v oblasti ochrany údajů ze strany dozorových úřadů; b) odlišné názory na to, zda je subjekt správcem nebo zpracovatelem; c) značné rozdíly ve vnitrostátních správních a procesních postupech a d) v

[341] Evropská komise 2020. *SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ Ochrana osobních údajů jakožto pilíř posílení postavení občanů a přístup EU k digitální transformaci – dva roky uplatňování obecného nařízení o ochraně údajů*, COM/2020/264 final, 24. června 2020. Dostupné zde: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52020DC0264. [cit. 2024-09-25].

[342] Evropská komise 2024. *SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ: Druhá zpráva o uplatňování obecného nařízení o ochraně osobních údajů*, COM/2024/357 final, 25. července 2024. Dostupné zde: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52024DC0357. [cit. 2024-09-25].

některých případech se dozorové úřady neřídí pokyny EDPB nebo na vnitrostátní úrovni zveřejňují pokyny, které jsou v rozporu s pokyny EDPB. Pokud jde o body za a) a za d), domnívám se z vlastní zkušenosti, že dozorové úřady podnikají reálné kroky k tomu, aby tyto problémy řešily, především intenzivnější spoluprací mezi sebou a koordinovanými postupy. Bod za b) je tak trochu nevděčným problémem, otázka určení hlavního odpovědného subjektu je totiž velmi komplikovaná i v jiných oblastech právní regulace. V oblasti ochrany osobních údajů navíc skutečně záleží na okolnostech a kontextu konkrétního zpracování, nelze tedy univerzálně určit typové oblasti zpracování, kde bude určitý subjekt vždy v pozici správce. Bod za c) je tak podle mého názoru asi nejpalčivějším problémem současnosti. V duchu zásady procesní autonomie a s ohledem na odlišnosti vnitrostátních procesních předpisů postupují dozorové úřady v procesních otázkách mnohdy různě. To by mělo představovat pro státy (především pak pro legislativní útvary) výzvu pro budoucí řešení. Evropská komise sice představila v červenci 2023 návrh tzv. „procesního nařízení“[343], tento návrh se nicméně zabývá pouze přeshraničním prosazováním nařízení GDPR, tudíž neřeší problémy, které konkrétně vyplývají z nedostatečné adaptace nařízení GDPR do vnitrostátních právních řádů, což je podle mě konkrétně problém pro ČR. Komise chce podporovat a sledovat provádění nařízení GDPR i nadále, další zprávu tak lze očekávat v roce 2028.

6.2 Unijní poznatky ohledně uplatňování práva na přístup

Vzhledem k tomu, že uplynulo již 6 let od účinnosti nařízení GDPR, je namístě také ohlédnutí nad uplatňováním tohoto nařízení, konkrétně ve vztahu k právům subjektů údajů. Důležité poznatky předkládá právě zmíněná Druhá zpráva Komise o uplatňování obecného nařízení o ochraně osobních údajů[344], která zároveň přináší shrnutí mnoha aktérů.

Tato Druhá zpráva Komise se na nemalém prostoru věnuje právům subjektů údajů a k tomu poskytuje i zajímavou statistiku.[345] Vyplývá z ní, že jednotlivci jsou stále více

[343] Dne 4. 7. 2023 představila Evropská komise Návrh Nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679 („Procesní nařízení“). Cílem je překonat významné rozdíly ve vnitrostátních správních postupech a výkladech pojmů v rámci mechanismu spolupráce podle nařízení GDPR. Dne 13. 6. 2024 se Rada Evropské unie dohodla na společném postoji – přijala obecný přístup. Evropská komise, 2023. *Návrh Nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679 („Procesní nařízení“)*, COM/2023/348 final, 4. července 2023. Dostupné zde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0348. [cit. 2024-09-25].

[344] Evropská komise 2024. *SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ: Druhá zpráva o uplatňování obecného nařízení o ochraně osobních údajů*, COM/2024/357 final, 25. července 2024. Dostupné zde: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52024DC0357. [cit. 2024-09-25].

[345] Statistika v této zprávě například uvádí, že celkem 72 % respondentů v EU uvedlo, že o nařízení GDPR slyšelo, z toho 40 % ví, o co se jedná.

obeznámeni se svými právy podle nařízení GDPR a aktivně je uplatňují, což je jednoznačně pozitivní. V praxi dozorových úřadů se to taktéž projevuje v rychlém a výrazném nárůstu počtu stížností.[346] Kritický pohled ovšem zazněl ze strany Agentury pro základní práva FRA[347], která konstatovala, že ačkoli se povědomí o ochraně údajů mezi širokou veřejností zvýšilo, porozumění ochraně údajů je stále nedostatečné, o čemž svědčí velký počet banálních nebo neopodstatněných stížností. Kromě toho je podle agentury FRA podáváno jen velmi málo stížností týkajících se zpracování citlivých údajů nebo zneužití osobních údajů v oblasti digitálních technologií. Ve zprávě Komise se nadto uvádí, že podle informací samotných správců je právo na přístup (podle článku 15 nařízení GDPR) nejčastěji uplatňovaným právem subjektů údajů a zároveň právem, které představuje pro správce největší výzvu. Ačkoli sbor EDPB přijal v roce 2022 pokyny k tomuto právu, správci nadále hlásí problémy, například ve vztahu k výkladu pojmu „nedůvodné nebo nepřiměřené žádosti“. Dalším problémem, který ve zprávě Komise správci identifikovali, je vysoký počet žádostí, které jsou podávány za účelem nesouvisejícím s ochranou údajů, například za účelem shromažďování důkazů pro soudní řízení. V tomto smyslu je ale nutné doplnit, že podle nedávného rozsudku Soudního dvora EU[348], nejsou důvody žádosti subjektu údajů o přístup k osobním údajům relevantní (to ostatně bylo podrobně rozebráno i v této práci). Organizace občanské společnosti kromě toho upozorňují, že odpovědi na žádosti o přístup jsou často opožděné nebo neúplné („základní informace“ jsou někdy považovány za „obchodní tajemství“ nebo za „důvěrné“) nebo dokonce někdy zcela chybí, přičemž obdržené údaje nejsou vždy v čitelném formátu. Mnoho stížností na GDPR se týká zejména toho, že správci neodpovídají na žádosti o přístup, vyřizování těchto stížností dozorovými úřady může být rovněž pomalé a trvat až několik let. Orgány veřejné moci zase uvádějí potíže při vzájemném ovlivňování práva na přístup a pravidel pro přístup veřejnosti k dokumentům. S ohledem na tyto okolnosti se tak sbor EDPB rozhodl v únoru 2024 zahájit společnou koordinovanou dozorovou akci (tzv *CEF*, *Coordinated Enforcement Framework*) se zaměřením na implementaci práva na přístup.[349] K této akci se rozhodl připojit v polovině března 2024 také český Úřad pro ochranu osobních údajů. Ten píše na svých stránkách, že se

[346] Jak vyplývá například z Výroční zprávy Úřadu pro ochranu osobních údajů za rok 2023, počet přijatých podnětů a stížností za rok 2023 byl rekordní, celkem 2322. ÚOOÚ. Výroční zpráva ÚOOÚ za rok 2023. Online. Dostupné z: https://uoou.gov.cz/media/vyrocni-zpravy/vz2023-elektronicka-verze.pdf. [cit. 2024-09-25].
[347] FRA. *Report – GDPR in practice – Experiences of data protection authorities*. 11. června 2024. Dostupné zde: https://fra.europa.eu/cs/publication/2024/gdpr-experiences-data-protection-authorities. [cit. 2024-09-25].
[348] Rozsudek ze dne 26. října 2023, FT (Copies du dossier médical), C-307/22, EU:C:2023:811.
[349] EDPB. 28. 2. 2024. CEF 2024: Launch of coordinated enforcement on the right of access (CEF 2024: Zahájení společné koordinované dozorové akce k právu na přístup). Bližší informace dostupné zde: https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_cs. [cit. 2024-09-25].

společné koordinované akce EDPB na úrovni celého EHP má zúčastnit celkem 31 dozorových úřadů, a to včetně 7 německých úřadů pro ochranu osobních údajů.

Zajímavý je pohled na uplatňování práva na přístup z pozice správců v soukromém podnikovém sektoru, který podle mého názoru je třeba na tomto místě více rozvést. Cenným zdrojem je v tomto případě Zpráva expertní skupiny mnoha zúčastněných stran k hodnocení nařízení (EU) 2016/679 z června 2024[350]. Jak již bylo uvedeno výše, kde píšu o zprávě Komise, podle podnikového sektoru je právo na přístup zdaleka nejvyužívanějším právem. Zástupci odvětví pojišťovnictví uvedli, že v některých společnostech se množství žádostí o přístup zvýšilo třikrát až pětkrát, někde dokonce až desetkrát. Jeden člen působící jako právní poradce a několik členů z řad podniků se domnívá, že právo na přístup je příliš obsáhlé a podrobné, zejména v případě nadměrného počtu žádostí, kdy subjekt údajů žádá o přístup ke všem zpracovávaným osobním údajům. Z tohoto důvodu někteří z těchto členů vysvětlují, že významným problémem je neexistence zásady proporcionality při vyřizování žádostí o přístup. Členové proto vyzývají k většímu vyjasnění rozsahu použitelnosti práva na přístup, zejména v některých specifických souvislostech, jako je pracovněprávní vztah nebo vyřizování stížností centrem zákaznické podpory. Další obava, kterou vyjádřilo několik členů z řad podniků, spočívá v tom, že právo na přístup je často uplatňováno zneužívajícím způsobem, což může představovat značnou zátěž pro organizační zdroje. Je tomu tak proto, že převažujícím motivačním faktorem pro výkon práva na přístup není podle nich ochrana osobních údajů, ale jiné účely, jako je potřeba získat informace v souvislosti se zaměstnáním, shromáždit důkazy pro stížnosti nebo soudní řízení. Podle jejich názoru široký výklad práva na přístup zastávaný Soudním dvorem EU může vést ke značné zátěži pro správce. Kromě toho někteří členové požadují podrobnější upřesnění, co představuje nedůvodnou nebo nepřiměřenou žádost o přístup. Ze strany některých podniků v odvětví bankovnictví a pojišťovnictví zase zaznívají názory, že stále existuje právní nejistota ohledně výkladu práva na získání kopie, a požadují bližší upřesnění, že nemusí nutně zahrnovat vydání kopií dokumentů, v nichž se údaje nacházejí. Ve vztahu k pokynům EDPB k právu na přístup vyjadřují podniky spíše odměřený postoj, domnívají se, že EDPB zvolilo až příliš normativní přístup, který může znamenat riziko pro potřebnou flexibilitu správců a může vést k obtížnějšímu vyřizování žádostí o přístup bez jasného přínosu pro subjekty údajů.

[350] E03537 – Multistakeholder expert group to support the application of Regulation (EU) 2016/679. *Report from Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679*, Ref. Ares(2024)4222971, 10. června 2024. Dostupné zde: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=54422&fromExpertGroups=3537. [cit. 2024-09-25].

6.3 Nedostatky ve vztahu k právu na přístup (z hlediska normativní úpravy i *soft law*)

Článek 15 nařízení GDPR je svou strukturou poměrně jednoduchým a stručným ustanovením o čtyřech odstavcích. Na tomto místě bych ráda indikovala některé problematické body, které bohužel nejsou řešeny ani v nařízení, ani v příslušných pokynech k právu na přístup.

Předně, nikde není obsaženo podrobnější vysvětlení, kdy lze žádosti považovat za zjevně nedůvodné nebo nepřiměřené, což může představovat značnou právní nejistotu pro správce i subjekty údajů. Zde je možné nicméně vyjít alespoň z doporučení ICO[351], které upozorňuje na faktory, které by měl správce údajů zohlednit při posuzování důvodnosti a přiměřenosti vyhledávání osobních údajů. Správce by tak měl zvážit: okolnosti žádosti (a), jakékoli obtíže spojené s nalezením informací (b) a základní povahu práva na přístup (c). V tomto smyslu by bylo také vhodné povzbuzovat správce k transparentnosti, aby na stránce informující o právu na přístup bylo umístěno oznámení subjektu údajů s nezbytnými informacemi o možnosti vzniku administrativních nákladů na kopie nebo nedůvodné a nepřiměřené žádosti, informovat subjekty o tom, jaké administrativní náklady by mohly být započteny do poplatku apod. Druhým problémem, na nějž upozorňují zejména správci, je absence možnosti správců zohlednit v rámci procesu posuzování žádosti práva na přístup zásadu proporcionality. Zásada proporcionality přitom hraje významnou úlohu, jde o obecnou zásadu práva EU a je výslovně stanovena v čl. 5 odst. 4 SEU. Jak jsem již uváděla výše, také z judikatury Soudního dvora EU (konkrétně rozsudku *Rijkeboer*[352]) vyplývá, že je třeba zajistit spravedlivou rovnováhu jednak mezi zájmem subjektu údajů na ochraně jeho soukromí (a jeho právem na přístup) a jednak zátěží, kterou pro správce představuje jeho povinnost tyto informace uchovávat. Je tedy nutné tento rozpor objasnit v tom smyslu, že zásada proporcionality by měla být uplatňována, i když s určitými omezeními. Dalším problémem je, že článek 15 ve svém výčtu poskytovaných informací na základě práva na přístup vůbec nezahrnuje informaci o právním základu pro zpracování údajů. Subjekt údajů tak má možnost se o právním základu zpracování dozvědět pouze na základě *privacy policy* daného správce (resp. plnění jeho informační povinnosti dle článku 13 nebo 14 nařízení). To rozhodně nepřispívá k posílení transparentnosti. Domnívám se, že poskytnutí konkrétního právního základu použitého pro každý účel a kategorii údajů by

[351] ICO (2022). *Right of access - How do we find and retrieve the relevant information?* Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/how-do-we-find-and-retrieve-the-relevant-information. [cit. 2024-09-25].
[352] Rozsudek ze dne 7. května 2009, Rijkeboer, C-553/07, EU:C:2009:293.

mělo být pro správce povinné i při individualizovaném poskytování práva na přístup.[353] Právo na přístup musí subjektu údajů umožnit ověřit, zda jsou jeho osobní údaje zpracovávány zákonným způsobem (na základě řádného právního základu), a že správce má povinnost prokázat soulad se zásadou zákonnosti. Bez znalosti právního základu zpracování by navíc subjekty údajů v některých případech nebyly schopny posoudit, jaká práva subjektu údajů mohou uplatnit, neboť některá z těchto práv závisí právě na použitelném právním základu.

Z hlediska zabezpečení, nařízení i pokyny na několika místech upozorňují na význam vhodných technických opatření, vč. šifrování, nerozvíjejí však podrobněji, jak by měly standardy šifrování vypadat. Otázka šifrování, pseudonymizace, anonymizace a zajištění zabezpečení údajů jako celku je navíc řešena především z hlediska uchovávání údajů, a nikoli pro případy vyřizování žádostí o přístup, tj. zasílání samotných údajů správci subjektům údajů. Jak nařízení, tak pokyny také zdůrazňují význam zvláštní ochrany dětí a zranitelných osob (např. důchodci, osoby se zdravotním postižením). Neuvádí ovšem příklady, jakým způsobem tyto osoby chránit. To může být obzvláště rizikové, zejména s ohledem na rozmáhající se praktiky tzv. *dark patterns*, tedy různých klamavých forem uživatelských rozhraní v online prostředí. V tomto smyslu francouzský CNIL vyzývá k využívání takového webdesignu a architektury webových stránek, které budou směřovat k efektivní a jasné komunikaci s dětmi. CNIL podporuje používání různých ikon, obrázků, videí, barevných schémat a dalších nástrojů, stejně jako procesů, které dětem umožní dostatečnou autonomii při nakládání s jejich údaji online.[354] Zejména pokyny mohly být podle mého názoru také podrobnější, pokud jde o meze práva na přístup spočívající v právech a svobodách jiných osob (čl. 15 odst. 4 nařízení GDPR). EDPB mohlo poskytnout správcům konkrétnější postup (například v podobě seznamu jednotlivých procesních kroků, které by měli podniknout) v případě kolize práva na soukromí více osob. Také v tomto případě se lze inspirovat britským ICO.[355] Ten, stručně řečeno, navrhuje tzv. tříkrokový test: 1) pokusit se najít způsob, jak zpřístupnit údaje vynecháním osobních údajů třetí osoby; 2) pokud se předchozí krok ukáže jako nemožný, pokusit se získat platný souhlas třetí osoby; 3) pokud souhlas nelze získat, měl by správce zvážit, zda je rozumné

[353] AUSLOOS, Jef, VEALE, Michael and MAHIEU René, 2019. Getting Data Subject Rights Right. Online. *JIPITEC.* December 2019, 10 (2019) 283, s. 27 (283-309). Dostupné z SSRN: https://ssrn.com/abstract=3544173. [cit. 2024-09-25].

[354] CNIL (2021). *Recommandation 6: Renforcer l'Information et les Droits des Mineurs par le Design* (Doporučení č. 6: Posílit informovanost a práva nezletilých prostřednictvím designu). Dostupné z: https://www.cnil.fr/fr/recommandation-6-renforcer-linformation-et-les-droits-des-mineurs-par-le-design. [cit. 2024-09-25].

[355] ICO (2022). *Right of access - What should we do if the request involves information about other individuals?* Dostupné z: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/information-about-other-individuals. [cit. 2024-09-25].

poskytnout informace bez souhlasu dotčené třetí osoby. Správce by tak měl poskytnout údaje subjektu údajů v co největším rozsahu a případně vysvětlit, že některé údaje poskytnout nelze z důvodu zásahu do práv třetích stran. Pokyny dále uvádějí formát PDF jako vhodný pro poskytování kopie s osobními údaji, ačkoli, jak uvádí odborníci, jde pouze o formát vhodný k tisku, nikoli však k analýze dat. Bylo by vhodnější proto poskytovat informace v otevřeném formátu, který je strojově i lidsky čitelný, jako je třeba XML.[356] Konečně, nařízení ani pokyny neřeší otázku, zda v případě, že správce nerespektuje právo na přístup (případně se dopustí prodlení), má subjekt údajů právo požadovat náhradu újmy podle článku 82 nařízení GDPR. Konkrétně v tomto ohledu Vrchní zemský soud ve Vídni[357] rozhodl, že opožděná odpověď může vést k nehmotné újmě, což potvrdil i Nejvyšší soud Rakouska[358]. Na základě toho by pak subjekt údajů mohl právem požadovat odškodnění. Na druhou stranu Okresní soud v Bonnu ve dvou případech[359] rozhodl, že subjekty údajů mají nárok na odškodnění pouze v případě, že dojde k porušení při zpracování, přičemž tvrdí, že opožděná odpověď na právo na přístup není porušením nařízení vyplývajícím ze samotného zpracování.[360] Podobná názorová linie přetrvává prozatím v aktuální judikatuře německých soudů (např. rozsudek zemského soudu v Kolíně nad Rýnem[361]). V tomto případě zemský soud zamítl nárok na náhradu újmy, protože prodlení a tím i porušení článků 15 a 12 odst. 3 GDPR samo o sobě nepostačuje k uplatnění nároku na náhradu újmy (resp. neznamená to, že by osoba dotčená porušením GDPR, které pro ni mělo negativní důsledky, byla osvobozena od povinnosti prokázat, že tyto důsledky představují nemajetkovou újmu ve smyslu článku 82 tohoto nařízení).

Úprava je možná až příliš obecná a celou řadu problematických aspektů neřeší. Na druhou stranu je také pravda, že přílišná kazuistika by učinila úpravu mnohem méně srozumitelnou,

---

[356] AUSLOOS, Jef, VEALE, Michael and MAHIEU René, 2019. Getting Data Subject Rights Right. Online. *JIPITEC.* December 2019, 10 (2019) 283, s. 27 (283-309). Dostupné z SSRN: https://ssrn.com/abstract=3544173. [cit. 2024-09-25].

[357] Vrchní zemský soud ve Vídni. Oberlandesgericht Wien. (2020). 11 R 153/20f, 154/20b. Dostupné z: https://noyb.eu/sites/default/files/2020-12/BVI-209_geschw%C3%A4rzt.pdf.

[358] Nejvyšší soud Rakouska. OGH. (23. 6. 2021). Rozsudek 6Ob56/21k. Dostupné z: https://1url.cz/Q1R4r.

[359] Zemský soud v Bonnu. Landgericht Bonn (1. 7. 2021). Rozsudky 15 O 372/20 a 15 O 355/20. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Text=15%20O%20372/20. https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Bonn&Datum=01.07.2021&Aktenzeichen=15%20O%20355/20.

[360] Reuschlaw. *Recent case law on the right of access in accordance with Article 15 of the GDPR.* 10. srpen 2021. Dostupné z: https://www.reuschlaw.de/en/news/recent-case-law-on-the-right-of-access-in-accordance-with-article-15-of-the-gdpr/. [cit. 2024-09-25].

[361] Zemský soud v Kolíně nad Rýnem. Landgericht Köln (19. 4. 2024). Rozsudek 12 S 4/23. Dostupné z: https://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2024/12_S_4_23_Urteil_20240419.html.
De Lege Data. 24. září 2024. *Landgericht Köln: die bloße verspätete Auskunft stellt keinen Schaden im Rahmen des Art. 82 DSGVO dar* (Zemský soud v Kolíně nad Rýnem: pouhé prodlení s poskytnutím informací nepředstavuje újmu ve smyslu čl. 82 GDPR). Dostupné z: https://www.delegedata.de/2024/09/landgericht-koeln-die-blosse-verspaetete-auskunft-stellt-keinen-schaden-im-rahmen-des-art-82-dsgvo-dar/. [cit. 2024-09-25].

což je z hlediska subjektů údajů i správců nežádoucí. Lze ovšem konstatovat, že EDPB se mohlo v pokynech věnovat podrobněji celé řadě otázek.

6.4 Poznatky z právně-empirických studií ohledně uplatňování práva na přístup

Pro získání skutečně podrobné představy, jakým způsobem funguje právo na přístup v praxi, je nicméně potřeba získat relevantní data na základě výzkumu. Vyšla jsem z dvou právně-empirických studií akademických pracovníků z Belgie a Nizozemska, kterou provedli v letech 2020 a 2022 Pierre Dewitte a Jef Ausloos[362], jejichž některé výsledky bych zde ráda prezentovala a následně analyzovala. Podle těchto autorů mělo být cílem jejich empirických studií shromáždit kvantitativní a kvalitativní zjištění o tom, jak vybraní poskytovatelé online služeb plní své povinnosti v oblasti transparentnosti a jak v praxi odpovídají na žádosti o přístup.

Ze studií provedených v letech 2020 a 2022 tak hned na začátku vyplynulo, že stále 6 % (2020) a 4 % (2022) správců vůbec neuvádí, jak mohou subjekty údajů vykonávat svá práva, a to navzdory povinnosti správce usnadnit výkon práva na přístup stanovené v čl. 12 odst. 2 nařízení GDPR. Z hlediska formy žádosti o přístup, které sami správci navrhli k uplatnění práva na přístup, převládaly v obou případech email a zvláštní kontaktní formulář (Obr. 1). Ukázalo se, že poměrně velká část správců, a sice 25 % (2020) a 28 % (2022) vůbec nenabízela neregistrovaným uživatelům možnost podat žádost o přístup pomocí prostředků, které byly za tímto účelem speciálně vytvořeny, a to zejména proto, že tento proces vyžadoval použití kontaktního formuláře nebo nástroje, který byl k dispozici pouze přihlášeným uživatelům. To lze považovat za omezení použitelnosti článku 15, které jde proti smyslu ustanovení (ověřit používání osobních údajů a nikoli vyžadovat další údaje, které nejsou nezbytné). V této souvislosti byly v průběhu studií identifikovány také další problémy, např. zvláštní kontaktní formulář nebyl jednoduše dohledatelný, nýbrž dostupný až po zadání do vyhledávače Google; mnohdy chybělo uvedení kontaktních emailových adres; jindy zase správci využívali služeb třetích stran, které pro vyřizování žádostí vyčlenily použití zvláštních platforem, a které ovšem po uživatelích vyžadovaly množství nadbytečných informací. Co naopak autoři studie ocenili,

[362] DEWITTE, Pierre a AUSLOOS, Jef, 2024. Chronicling GDPR Transparency Rights in Practice: The Good, the Bad and the Challenges Ahead. Online. *International Data Privacy Law*. May 2024, Volume 14, Issue 2, s. 28 (106–133). Dostupné z: https://doi.org/10.1093/idpl/ipad026. [cit. 2024-09-01].

je to, že v případě provedených studií nezaznamenali ani jeden případ, kdy by správce požadoval odůvodnění nebo měl výhrady k podané žádosti bez odůvodnění. Z hlediska procesu vyřizování žádostí vyplynulo, že správci zpravidla nejsou schopni poskytnout vyčerpávající uspokojivou odpověď napoprvé (Obr. 2: v roce 2020 ani jeden správce, v roce 2022 pouze 7 %). V naprosté většině případů tak byla nutná nějaká forma interakce se správcem a zasílání upomínek, celkem bylo nutné zaslat alespoň jednu upomínku ve 20 % případů (2020) a 16 % případů (2022) před získáním první věcné odpovědi. Zásadním problémem je ovšem výsledek, kdy 10 % (2020) a 15 % správců (2022) neposkytlo vůbec žádnou odpověď, a to i přes opakované upomínky (také Obr. 2). Z hlediska této práce považuji za zajímavý také ukazatel, že 7 % (2020) a 3 % správců (2022) výslovně požadovalo pro vyřízení žádosti o přístup zaslání skenu průkazu totožnosti subjektu údajů.

Ve vztahu k procesu vyřízení odpovědi si správci obecně počínali výrazně lépe v pozdější studii z roku 2022. I přesto ale bylo identifikováno několik problémů, například v některých případech bylo zapotřebí až 4 upomínek, než správce reagoval na žádost; jindy zase uživatelé obdrželi nefunkční URL adresy pro stažení kopie s jejich údaji; v některých případech byl uživatelům uzavřen jejich požadavek („ticket“) ihned po obdržení první věcné odpovědi od správce, aniž by měli možnost na něj navázat a museli tak založit nový (tím vzniká riziko, že správce bude tento požadavek považovat za žádost o další kopii ve smyslu čl. 15 odst. 3, za kterou by si případně mohl naúčtovat poplatek). Účastníci také často považovali proces za příliš chaotický a zdlouhavý, v některých případech došlo i k bezdůvodnému pozastavení jejich účtu bez předchozího upozornění; jindy zase upozornili na fakt, že bohužel první kontakt navázali nikoli s právníkem či odborným týmem, ale s neproškolenými členy zákaznického servisu. Z hlediska míry spokojenosti uživatelů s konečnou odpovědí (Obr. 3) si správci významně polepšili, 55 % uživatelů bylo spokojeno či velmi spokojeno (2022), oproti 33 % (2020). V otázce dodržení lhůty (mezi první žádostí a konečnou odpovědí) si ovšem správci příliš dobře nevedli, studie prokázala (Obr. 4), že 51 % (2020) a 77 % správců (2022) nedodrželo jednoměsíční lhůtu stanovenou v čl. 12 odst. 3 nařízení GDPR. Z hlediska množství a kvality informací poskytnutých v odpovědích jsou závěry smíšené. Správci si sice skóre v tomto ohledu vylepšili v pozdější studii, na druhou stranu se obecně ukázalo, že je zapotřebí vysoká míra aktivity uživatele. Studie například odhalila, že v roce 2020 správci stále neposkytovali adekvátní informace o konkrétních účelech zpracování, kategoriích zpracovávaných osobních údajů, době či kritériích uchovávání nebo kategoriích příjemců (Obr. 5). Zde je ovšem třeba poznamenat, že lze vidět podstatné zlepšení v pozdější studii z roku 2022 (také Obr. 5).

Obdobně, podstatný rozdíl ukazují i výsledky v informování uživatelů o jejich dalších právech jako subjektů údajů (Obr. 6), zatímco v roce 2020 tak správci plnili průměrně kolem 40 %, v roce 2022 to bylo již nad 70 % a v některých případech i docela výrazně.

Jakým způsobem interpretovat výsledky těchto studií? Obecně z nich vyplynulo, že ačkoli došlo k výraznému zlepšení způsobu, jakým poskytovatelé online služeb jako správci zpracovávají žádosti o přístup, stále přetrvávají problémy, přičemž mezi ty nejpalčivější patří: časté poskytování šablonovitých odpovědí, přílišná rutinizace procesu, spíše obecná než konkrétní povaha poskytování informací a nedodržování standardní měsíční lhůty. Pokud jde o prvně zmíněný problém, a sice poskytování šablonovitých odpovědí, tak doplním, že řada správců se bohužel snaží si proces vyřizování odpovědí usnadnit a ve velké míře jej automatizovat, což však není vždy ku prospěchu subjektům údajů. Odpovědi jsou mnohdy nedostatečně individualizovány, správci někdy pouze rutinně kopírují texty ze zásad ochrany údajů. Navíc i samotné podání žádostí správci v mnoha případech podmiňují předchozí registrací, což je podle mého názoru nedůvodné omezování rozsahu práva na přístup. Domnívám se, že také časové hledisko dodržování lhůt představuje oblast, kde je velký prostor ke zlepšení. Na druhou stranu, z hlediska vývoje dodržování práva na přístup je podle mého názoru pozitivní, že se v naprosté většině zkoumaných bodů správci zlepšili. Výsledky studií ukázaly, že i když musí být subjekty údajů aktivně zapojeni a v některých případech své žádosti správcům upomínat, jsou s obdrženými odpověďmi poměrně spokojení. Je tedy patrné, že se správci na tento proces připravili a snaží se profesionalizovat, často vytvářejí nové interní postupy a technické nástroje (např. funkce pro stahování kopií údajů). Toto shrnutí bych nicméně uzavřela tím, že je potřeba na těchto procesech stále pracovat. Stále je bohužel dost oblastí, kde mají správci co vylepšovat.

Závěr

Cílem této práce bylo zpracovat právo subjektů údajů na přístup k osobním údajům podle článku 15 nařízení GDPR na unijní úrovni. Jejím smyslem bylo podat relativně ucelený pohled (byť nikoli vyčerpávající) na různé aspekty související s tímto právem. Tyto aspekty byly zkoumány prostřednictvím následujících **výzkumných otázek či spíše okruhů**. V rámci **prvního okruhu** jsem zkoumala význam a účel práva na přístup, vztah práva na přístup k ostatním právům a základní rozdíly oproti právu být informován podle článků 13 a 14 nařízení GDPR. Význam práva na přístup tkví zejména v posílení postavení subjektů údajů. Slouží ke zmírnění nerovnováhy moci mezi subjekty údajů a správci a je tak dle mého názoru jedinečným a nezastupitelným nástrojem umožňujícím subjektům údajů získat zpět kontrolu nad vlastními osobními údaji. S tím úzce souvisí dvě hlavní funkce, a to posílení transparentnosti činnosti správce a usnadnění kontroly subjektu údajů nad jeho údaji. Od toho se odvíjí také účel práva na přístup – jako kontrolní oprávnění umožnit jednotlivci ověřit zákonnost zpracování jeho osobních údajů. Z judikatury Soudního dvora EU navíc vyplývá, že odůvodnění žádosti práva na přístup není po subjektu údajů požadováno, může tak právo na přístup uplatnit i pro účely, které přímo nesouvisejí s ochranou údajů nebo které budou dokonce použity v právních postupech směřujících proti správci. Vztah práva na přístup k ostatním právům subjektů údajů se na první pohled odráží i v systematice nařízení GDPR. Právo na přístup je uvedeno na prvním místě pod článkem 15 a po něm následují ostatní práva subjektů údajů. Je tak sledován logický postup, jakým mohou být práva subjektů údajů uplatňována. Z judikatury Soudního dvora EU dokonce vyplývá, že právo na přístup je nezbytné pro výkon dalších práv subjektů údajů. To bych možná jen lehce poupravila, nezbytnost je ve většině případech dána, až na výjimky, kdy těmito údaji již subjekt údajů disponuje a může tak účinně vykonávat další práva. Na rozdíl od práva být informován podle článků 13 a 14 nařízení GDPR, které je rozhodující ve fázi před zahájením zpracování údajů, se právo na přístup uplatňuje v dalších fázích zpracování údajů. Subjekt údajů tak prostřednictvím práva na přístup získá informace o zpracování v jeho průběhu. Dalším rozdílem je, že toto právo vyžaduje aktivní přístup ze strany subjektu údajů. Konečně, od práva na přístup se očekává, že se subjektu údajů dostane podrobnějších a strukturovanějších informací, konkrétně „šitých na míru“ jeho osobě.

Druhý okruh se týkal struktury článku 15 nařízení GDPR a zejména vyjasnění práva na kopii, zahrnutém v čl. 15 odst. 3 nařízení GDPR. Je to samostatné právo subjektu údajů, stojící vedle práva na přístup, nebo se jedná o jednu z komponent, příp. modalit práva na přístup? Právo na kopii není dalším samostatným právem subjektu údajů, ale způsobem

(modalitou) poskytnutí přístupu k údajům, což ostatně opět potvrdila judikatura Soudního dvora EU. Právo na kopii tak znamená, že subjektu údajů musí být poskytnuta věrná a srozumitelná reprodukce všech jeho osobních údajů. To může zahrnovat, pokud je to nezbytné pro ochranu jeho práv a zájmů, kopie výpisů z dokumentů, celých dokumentů nebo výpisů z databází.

V rámci **třetího okruhu** výzkumné otázky bylo zkoumáno, zdali je normativní úprava práva na přístup v článku 15 nařízení GDPR dostatečná. V této souvislosti byla také zkoumána vhodnost úpravy v unijních aktech *soft law* (zejména Pokynů k právu na přístup[363]). Dospěla jsem k závěru, že normativní úprava článku 15 nařízení je celkově dostatečná, s jednou výhradou. Čl. 15 odst. 1 měl v rámci výčtu podle mého názoru také zahrnovat kategorii informace o právním základu. Jde o informaci naprosto stěžejní pro uplatnění některých práv subjektů údajů (konkrétně právo na přenositelnost a právo vznést námitku). Obecně mám tedy za to, že úprava dostatečná je, neboť poskytuje subjektům údajů široké právo na přístup ke svým osobním údajům, včetně informací o účelu zpracování, kategoriích osobních údajů a případných příjemcích těchto údajů. Jak EDPB, tak Soudní dvůr EU se často vyjadřují k povaze práva na přístup – právo na přístup by mělo být podle nich interpretováno široce, aby subjekty údajů měly snadný přístup ke svým údajům, s čímž souhlasím. Místy se objevují názory, že současná právní úprava může být pro některé subjekty příliš obecná nebo ne zcela srozumitelná, domnívám se, že cesta ovšem nevede přes další technické zatěžování tohoto ustanovení. Pokud jde o úpravu obsaženou v pokynech EDPB (tedy unijním *soft law*), myslím si, že jde obecně o správný počin, jeho užitečnost se ostatně projevila již u předchozích aktů EDPB či WP29. Bohužel ale podle mého názoru EDPB plně nevyužilo svůj potenciál. Pokyny celou řadu oblastí neřeší nebo řeší pouze velmi povrchně. Lépe tak mohla být vysvětlena například zásada proporcionality, resp. jak mohou správci zajistit spravedlivou rovnováhu mezi zájmem subjektu údajů (a jeho právem na přístup) a zátěží, kterou to pro správce představuje; dále rozsah práva na přístup; meze práva na přístup spočívající v právech a svobodách jiných osob; otázky ohledně formátu kopie; ochrana dětí a dalších zranitelných osob; otázka šifrování apod. Určité nejasnosti tedy přetrvávají a vyvěrají zejména z praktické implementace práva na přístup.

Čtvrtý okruh pak mířil na otázky, do jaké míry představuje právo na přístup k vlastním údajům skutečné posílení práv subjektů údajů? Jaké je jeho využití v praxi? Je ochrana prostřednictvím práva na přístup účinná? Tyto otázky vyžadují hlubší zamyšlení. Jsou tedy

[363] EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023.

práva subjektů údajů v čele s právem na přístup dostatečně vhodným mechanismem k posílení kontroly subjektů údajů nad jejich osobními údaji v ekonomice založené na datech? Helena U. Vrabec ve své monografii k *Právům subjektů údajů podle GDPR*[364] je k otázce účinnosti kontrolních práv subjektů údajů velice kritická, hovoří o nich jako o nedokonalém prostředku individuální kontroly nad osobními údaji, které nedokáže účinně plnit své úkoly. Jako řešení nabízí alternativní (sebe)regulační přístupy, které se opírají o (1) technologická řešení a (2) právní ustanovení v oblasti práva na ochranu údajů i mimo ni.

V rámci první skupiny má na mysli především větší zapojení technologie umělé inteligence, která například může zlepšit poznávací schopnosti subjektů údajů, rozebrat klíčové aspekty zásad ochrany osobních údajů, příp. zajistit jejich vizualizaci prostřednictvím online platformy, která umožňuje trojrozměrné znázornění datových toků. Pro zaručení práva na přístup se vkládají naděje do vývoje v oblasti blockchainu, pro uplatnění práva na výmaz zase do softwaru, který sám zajistí, že informace budou po určité době vymazány (v jisté podobě implementoval Google u služby Gmail). A konečně, technologie může pomoci integrovat všechna práva subjektu údajů do „panelu ochrany osobních údajů“, rozhraní poskytujícího uživatelům přístup k informacím o osobních údajích a konfiguraci nastavení ochrany osobních údajů. Ukázkovým příkladem takového panelu je projekt MyData[365], který zahájila finská vláda. Jeho cílem je poskytnout jednotlivcům praktické prostředky pro přístup, získávání a používání souborů údajů obsahujících jejich osobní údaje z různých zdrojů, včetně dopravních údajů, telekomunikačních údajů, lékařských záznamů, finančních informací a údajů získaných z různých online služeb. Většina technologických řešení ovšem zatím není dokonalá, např. blockchain sice posiluje právo na přístup tím, že zajišťuje subjektům údajů přístup k úplnému řetězci transakcí, ale je, zatím ve své veřejné verzi, překážkou pro výkon práva na výmaz. Pokud jde o druhou jmenovanou skupinu právních řešení, Helena U. Vrabec hovoří o holistickém přístupu k GDPR, který by využíval právní nástroje a regulační strategie i z jiných oblastí, než je právo na ochranu údajů. Konkrétně uvádí právo na ochranu spotřebitele, právo hospodářské soutěže a regulaci umělé inteligence.

---

[364] VRABEC, Helena U., 2021. 9.2 The way forward for data subject rights. In: *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*. Oxford University Press, s. 227-236. Online. ISBN 9780191904851. Dostupné z: https://doi.org/https://doi.org/10.1093/oso/9780198868422.001.0001. [cit. 2024-08-29].

[365] Antti Poikola, Kai Kuikkaniemi, and Harri Honko, '*MyData: A Nordic Model for Human-centered Personal Data Management and Processing*' (2014). Dostupné z: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=ibid. [cit. 2024-09-04].

Navzdory obecně širokému přijetí práva na přístup jako mechanismu posílení postavení subjektu údajů, ne všichni vědci tento názor podporují[366]. Například Koops[367] tvrdí, že práva subjektu údajů jsou teoretická a v praxi nemají význam, a proto nemohou jednotlivcům poskytnout skutečnou kontrolu nad jejich osobními údaji. Domnívá se, že ani úspěšné příklady uplatňování práv subjektů údajů zřejmě nenaznačují účinnou kontrolu subjektů údajů nad zpracováním jejich údajů. Uvádí také, že složitost pravidel ochrany údajů umocňuje problém s dodržováním předpisů ze strany správců. Proto je podle Koopse „informační sebeurčení nevymahatelné". Lazaro a Le Métayer[368] zastávají rovněž skeptický přístup k tomu, zda práva subjektů údajů mohou fungovat jako mechanismus posílení postavení subjektu údajů. Naznačují, že předpoklad, podle něhož právo na ochranu údajů zajišťuje „kontrolu", vyplývá z chybného pohledu na teorie ochrany soukromí a údajů. Cormack[369] nejenže zpochybňuje praktický význam práva na přístup, nýbrž dokonce se ptá, zda toto právo nepředstavuje potenciální hrozbu pro soukromí (myšleno zejména zpřístupnění neoprávněným třetím osobám). Jeho zkoumání využívání práva na přístup naznačuje, že přínos zpřístupnění osobních údajů subjektům údajů je v praxi mnohem menší, než se doufalo. Domnívá se, že pro transparentnost je důležitější vědět, jak jsou informace zpracovávány, než skutečné hodnoty, kterých se to týká. Přístup subjektu se navíc podle něj zřídkakdy používá k zajištění přesnosti informací a vzhledem k rozsahu zpracování osobních údajů může být nepraktický. Účinnějším prostředkem je tak dle něj například pravomoc soudu nařídit zveřejnění údajů, zároveň může poskytovat lepší ochranu soukromí.

Domnívám se, že právo na přístup je dostatečně vhodným mechanismem k posílení kontroly subjektů údajů nad jejich osobními údaji a nařízení GDPR tak vnímám (i přes jeho nedostatky) převážně pozitivně. S Helenou D. Vrabec souhlasím, že by bylo vhodné komplementárně k nařízení GDPR doplnit i další alternativní řešení, ať již technická či právní. Ostatně se domnívám, že se tak již děje, nařízení GDPR nepůsobí izolovaně, tvorbu nařízení

[366] QUEZADA-TAVÁREZ, Katherine, 2021. Impact of the Right of Access on the Balance between Security and Fundamental Right: Informational Power as a Tool to Watch the Watchers. Online. *European Data Protection Law Review*. 2021, Volume 7, Issue 1, s. 15 (59–73). Dostupné z: https://doi.org/10.21552/edpl/2021/1/9. [cit. 2024-09-01].
[367] KOOPS, Bert-Jaap, 2014. The Trouble with European Data Protection Law. Online. *International Data Privacy Law.* October 2014, Volume 4, Issue 4, s. 12 (250–261). Dostupné z: https://doi.org/10.1093/idpl/ipu023. [cit. 2024-09-01].
[368] LAZARO, Christophe a LE MÉTAYER, Daniel, 2015. Control over personal data: True remedy or fairytale? Online. *SCRIPTed.* June 2015, Volume 12, Issue 1, s. 32. Dostupné z: https://doi.org/10.2966/scrip.120115.3. [cit. 2024-09-01].
[369] CORMACK, Andrew, 2016. Is the Subject Access Right Now Too Great a Threat to Privacy. Online. *European Data Protection Law Review*. 2016, Volume 2, No. 1, s. 13 (15–27). Dostupné z: https://doi.org/10.21552/EDPL/2016/1/5. [cit. 2024-09-01].

GDPR výrazně formovala regulace v oblasti ochrany spotřebitele (např. v rámci požadavků na transparentnost a informační povinnosti správce). Také samotná EU přijala řadu iniciativ, z nichž některé doplňují nařízení GDPR nebo upřesňují, jak by mělo být uplatňováno ve specifických oblastech, namátkou uvedu nařízení o digitálních službách[370], nařízení o digitálních trzích[371], akt o umělé inteligenci[372], nařízení o politické reklamě[373] nebo nařízení o evropské digitální identitě[374]. Nařízení GDPR tvoří základní kámen politiky EU v digitální oblasti. Lze si ovšem klást otázku, zda nařízení GDPR dokáže vhodně reagovat na některé v praxi existující obchodní modely (například model *Consent or Pay* od společnosti Meta Platforms). Společnost Meta Platforms totiž ode dne 30. října 2023 uvedla, že zavádí placenou verzi svých produktů Facebook a Instagram bez reklam uživatelům, kteří nechtějí udělit souhlas s používáním svých údajů a cílenou reklamou. De facto tak uživatelům nabídla pouze dvě možnosti: zaplatit za službu bez sledování nebo udělit souhlas se zpracováním svých osobních údajů včetně cílené reklamy. To vyvolalo značnou vlnu kritiky, jak ze strany jednotlivých dozorových úřadů, tak evropského regulátora (EDPB). Konkrétně to vyvolalo obavy nejen z hlediska ochrany údajů, ale i spotřebitelského práva, práva hospodářské soutěže nebo nařízení o digitálních trzích.

Pokud jde o využití práva na přístup v praxi, z empirických studií Pierre Dewitta a Jefa Ausloose vyplynulo, že uplatňování nařízení GDPR podnítilo prudký nárůst žádostí o právo na přístup, což zmíněné statistiky dokládají. Článek 15 se tak díky své funkční jednoduchosti stal jedním z nejvýznamnějších nástrojů, které jednotlivcům umožňují sledovat složité digitální infrastruktury a odhalovat neprůhledné praktiky v oblasti údajů. Ukázalo se, že je užitečný pro mnoho různých skupin osob při sledování různých účelů (přes běžné uživatele online služeb, zaměstnance v různých oblastech průmyslu, až po akademické výzkumné pracovníky). Jeho univerzálnost, která byla dříve často kritizovaná, bývá dnes uznávána jako jeho hlavní

[370] Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách).
[371] Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích).
[372] Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).
[373] Nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy.
[374] Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu.

přednost.[375] Význam práva na přístup se odráží i v proměně postoje správců a postupném zlepšování jejich interních procesů vyřizování práv subjektů údajů. To však neznamená, že právo na přístup funguje bezchybně nebo že není možné žádné zlepšení. Stále lze pozorovat velké mezery při vyřizování těchto žádostí o přístup. Zaprvé, žádosti jsou nedostatečně individualizovány, správci někdy pouze kopírují texty ze zásad ochrany údajů. Zadruhé, správci stále často nedodržují řádně lhůty. A zatřetí, mnohdy je potřeba správce na tyto žádosti často upomínat. Navíc, je potřeba určitě razantně odmítat pokusy o nepřiměřené omezování, resp. oslabování práva na přístup, které se čas od času stále objevují ze strany správců. Dodržování práva na přístup totiž může být ve výsledku pozitivní pro všechny zapojené strany. Zaprvé, umožní nejen ochranu subjektům údajů, ale může také zlepšit postavení správce, resp. zlepšit jeho vztah se zákazníky, příp. zaměstnanci, vybudovat jejich důvěru ke správci. Ve výsledku může také posílit reputaci správce jako etického a spolehlivého správce, což může představovat konkurenční výhodu. Zadruhé, požadavky práva na přístup nutí samotného správce k lepší organizaci a evidenci osobních údajů, což může vést ke zlepšení interních procesů a kvality dat. A zatřetí, nelze zapomínat ani na to, že řádné zabezpečení procesů práva na přístup znamená pro správce i minimalizaci rizika stížností a právních sporů, čímž předchází potenciálním nákladům spojeným s právním řízením a případnými sankcemi.

Úvahy bych tak zakončila s opatrnou, ale stále optimistickou nadějí. I přes výše zmíněné kritické hlasy se domnívám, že si právo na přístup a další práva subjektů údajů své postavení obhájí. Práva subjektů údajů jsou nedílnou součástí základního práva na ochranu údajů zakotveného v Listině základních práv Evropské unie. Ochrana prostřednictvím práva na přístup je účinná, neboť právo na přístup je základem pro dosažení účinné a úplné ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů. Účinný výkon ostatních práv tedy do určité míry závisí na právu na přístup.[376]

[375] DEWITTE, Pierre a AUSLOOS, Jef, 2024. Chronicling GDPR Transparency Rights in Practice: The Good, the Bad and the Challenges Ahead. Online. *International Data Privacy Law*. May 2024, Volume 14, Issue 2, s. 28 (106–133). Dostupné z: https://doi.org/10.1093/idpl/ipad026. [cit. 2024-09-01].

[376] AUSLOOS, Jef, VEALE, Michael and MAHIEU René, 2019. Getting Data Subject Rights Right. Online. *JIPITEC*. December 2019, 10 (2019) 283, s. 27 (283-309). Dostupné z SSRN: https://ssrn.com/abstract=3544173. [cit. 2024-09-25].

Seznam zkratek

akt o umělé inteligenci	Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)
AML	Anti-Money-Laundering (Boj proti praní špinavých peněz nebo financování terorismu)
CNIL	Commission Nationale de l'Informatique et des Libertés
ČR	Česká republika
DPC	Data Protection Commission
DPIA	Posouzení vlivu na ochranu osobních údajů
EDPB	Evropský sbor pro ochranu osobních údajů
EDPS	Evropský inspektor ochrany údajů
EFSA	Evropský úřad pro bezpečnost potravin
EHS	Evropské hospodářské společenství
ES	Evropské společenství
ESLP	Evropský soud pro lidská práva
EU	Evropská unie
EUDPR	Nařízení Evropského parlamentu a Rady (EU) 2018/1725 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES
EÚLP	Evropská úmluva o ochraně lidských práv
EURATOM	Evropské společenství pro atomovou energii
FRA	European Union Agency for Fundamental Rights (Agentura Evropské unie pro základní práva)
GDPR (nařízení 2016/679)	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
ICCPR	Mezinárodní pakt o občanských a politických právech
ICO	Information Commissioner's Office
Komise	Evropská komise
Listina	Listina základních práv Evropské unie
nařízení č. 45/2001	Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů
nařízení č. 1049/2001	Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise
nařízení o digitálních službách	Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách)
nařízení o digitálních trzích	Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním

	odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích)
nařízení o evropské digitální identitě	Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu
nařízení o politické reklamě	Nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy
OECD	Organizace pro hospodářskou spolupráci a rozvoj
OSN	Organizace spojených národů
Parlament	Evropský parlament
Rada	Rada EU
SDEU	Soudní dvůr Evropské unie
SEU	Smlouva o Evropské unii
SFEU	Smlouva o fungování Evropské unie
směrnice 95/46	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
trestněprávní směrnice (směrnice 2016/680)	Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV
Úmluva č. 108	Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (vyhlášená pod č. 115/2001 Sb. m. s.)
ÚOOÚ (Úřad)	Úřad pro ochranu osobních údajů
WP29	Article 29 – Data Protection Working Party
zákon o ochraně osobních údajů	Zákon č. 101/2000 Sb., o ochraně osobních údajů
zákon o zpracování osobních údajů	Zákon č. 110/2019 Sb. o zpracování osobních údajů

Seznam použitých zdrojů

1. Seznam použité literatury

AUSLOOS, Jef a DEWITTE, Pierre, 2018. Shattering One-Way Mirrors. Data Subject Access Rights in Practice. Online. *International Data Privacy Law*. March 2018, Volume 8, Issue 1, s. 25 (4–28). Dostupné z: https://doi.org/10.1093/idpl/ipy001. [cit. 2024-07-12].

AUSLOOS, Jef, VEALE, Michael and MAHIEU René, 2019. Getting Data Subject Rights Right. Online. *JIPITEC.* December 2019, 10 (2019) 283, s. 27 (283-309). Dostupné z SSRN: https://ssrn.com/abstract=3544173. [cit. 2024-09-25].

BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*. Praha: Leges, 2010, s. 79-80. ISBN 978-80-87212-42-4.

BOBEK, Michal, 2016. Výzkum v Právu: Reklama na Nike anebo kvantová fyzika? Online. *Jurisprudence*. November 26, 2016, No. 6, 2016, s. 8 (3-10), Dostupné z: https://ssrn.com/abstract=2875982. [cit. 2024-09-25].

CAREY, Peter, 2018. *Data Protection: A Practical Guide to UK and EU law*. Oxford University Press. Fifth edition, 410 s. ISBN 978-0-19-881541-9.

COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, č. 50(3), s. 525. U of Penn, Inst for Law & Econ Research Paper No. 17-18. Dostupné z SSRN: https://ssrn.com/abstract=3014768. [cit. 2023-04-15].

Collectif Dalloz, 2023. *Code de la protection des données personnelles 2024, annoté et commenté,* 1994 s., 6. vydání (z 11/2023). Online. Dalloz. ISBN 978-22-4723-215-4. Dostupné z: databáze Dalloz. [cit. 2024-04-14].

CORMACK, Andrew, 2016. Is the Subject Access Right Now Too Great a Threat to Privacy. Online. *European Data Protection Law Review*. 2016, Volume 2, No. 1, s. 13 (15–27). Dostupné z: https://doi.org/10.21552/EDPL/2016/1/5. [cit. 2024-09-01].

DEWITTE, Pierre a AUSLOOS, Jef, 2024. Chronicling GDPR Transparency Rights in Practice: The Good, the Bad and the Challenges Ahead. Online. *International Data Privacy Law*. May 2024, Volume 14, Issue 2, s. 28 (106–133). Dostupné z: https://doi.org/10.1093/idpl/ipad026. [cit. 2024-09-01].

DOCKSEY, Christopher, 2016. Four fundamental rights: finding the balance. Online. *International Data Privacy Law*. August 2016, Volume 6, Issue 3, s. 15 (195–209). Dostupné z: https://doi.org/10.1093/idpl/ipw014. [cit. 2024-04-14].

GALETTA, Antonella, DE HERT, Paul, L'HOIRY, Xavier and NORRIS, Clive, 2017. *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*. Law, Governance and Technology Series, vol 34. Springer Cham, 511 s. Online. ISBN 978-3-319-47573-8. Dostupné z: https://doi.org/10.1007/978-3-319-47573-8_15. [cit. 2022-03-07].

GASSER, Urs, 2015. Interoperability in the digital ecosystem. Online. *ITU – 15th Global Symposium for Regulators (GSR15)*. Roč. 2015, s. 33. Dostupné z: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/Discussion paper_interoperability.pdf. [cit. 2024-04-14].

HOLLEAUX, André, Conseiller d'État. Komentář k „*La Loi Du 6 Janvier 1978 Sur l'informatique et Les Libertés*“. Online. 181/31. La Revue administrative. 1978.

HORNUNG Gerrit, SCHNABEL Christoph, 2009. Data protection in Germany I: The population census decision and the right to informational self-determination. Online. *Computer Law & Security Review*. November 2008, Volume 25, Issue 1, s. 5 (84-88). ISSN 0267-3649. Dostupné z: https://doi.org/10.1016/j.clsr.2008.11.002. [cit. 2022-03-07].

KIESOW CORTEZ, Elif, 2021. *Data Protection Around the World: Privacy Laws in Action*. T.M.C. Asser Press The Hague, 279 s. Online. ISBN 978-94-6265-407-5. Dostupné z: https://doi.org/10.1007/978-94-6265-407-5. [cit. 2024-09-25].

KOOPS, Bert-Jaap, 2014. The Trouble with European Data Protection Law. Online. *International Data Privacy Law.* October 2014, Volume 4, Issue 4, s. 12 (250–261). Dostupné z: https://doi.org/10.1093/idpl/ipu023. [cit. 2024-09-01].

KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene, 2022. *Research Handbook on EU Data Protection Law*. Cheltenham, UK: Edward Elgar Publishing, 672 s. Online. ISBN 9781800371682. Dostupné z: https://doi.org/10.4337/9781800371682.

KOVÁČOVÁ, Lucia; NECHVÁTALOVÁ, Lucie a VÝBORNÝ, Štěpán, 2013. *Ochrana soukromí versus svoboda projevu médií*. Online. Spisy Právnické fakulty MU, Řada teoretická, Ed. S, 442. Brno: Masarykova univerzita, Právnická fakulta. ISBN 978-80-210-6521-5. Dostupné z: https://science.law.muni.cz/knihy/monografie/Ochrana_soukromi_vs_svoboda_projevu_medii.pdf. [cit. 2024-08-03].

KRATOCHVÍL, Jan; KMEC, Jiří; KOSAŘ, David; BOBEK, Michal, 2012. Online. *Evropská úmluva o lidských právech*. Praha: C. H. Beck, 1687 s. ISBN 978-80-7400-365-3. Dostupné z: databáze Beck online. [cit. 2024-07-20].

KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. *Zákon o ochraně osobních údajů*. 1. vydání. Online. Praha: C. H. Beck, 536 s. ISBN 978-80-7179-226-0. Dostupné z: databáze Beck online. [cit. 2022-03-07].

KUGLER, Tobias a RÜCKER, Daniel, 2018. *New European General Data Protection Regulation: A Practitioner's Guide*. Hart/Nomos, Bloomsbury Collections, 285 s. First edition. Online. ISBN 978-1-5099-2059-4 Dostupné z: https://doi.org/10.5040/9781509920594. [cit. 2024-09-25].

KÜHN, Zdeněk, 2017. Transformace pojmu soukromí na počátku třetího milénia. Online. *Jurisprudence*. Roč. 2017, roč. 26, č. 2, s. 3-11. ISSN 1802-3843. Dostupné z: databáze ASPI. [cit. 2024-08-18].

KUNER, Christopher, 2008. *The 'Internal Morality' of European Data Protection Law*. Online. Roč. 2008, s. 10-19. Dostupné z: SSRN: https://ssrn.com/abstract=1443797. [cit. 2024-08-24].

KUNER, Christopher; BYGRAVE, Lee A a DOCKSEY, Christopher, 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*, 1488 s. Online. Oxford University Press. ISBN 9780191932267. Dostupné z: https://doi.org/10.1093/oso/9780198826491.001.0001. [cit. 2024-04-14].

LAZARO, Christophe a LE MÉTAYER, Daniel, 2015. Control over personal data: True remedy or fairytale? Online. *SCRIPTed.* June 2015, Volume 12, Issue 1, s. 32. Dostupné z: https://doi.org/10.2966/scrip.120115.3. [cit. 2024-09-01].

LIPANOVÁ, Kateřina, 2020. K zásadní změně Úmluvy Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva č. 108). Online. *Jurisprudence*. 2020, Roč. 29, Č. 4, s. 10 (35-44). ISSN 1802-3843. Dostupné z: https://www.jurisprudence.cz/cz/casopis/k-zasadni-zmene-umluvy-rady-evropy-o-ochrane-osob-se-zretelem-na-automatizovane-zpracovani-osobnich-dat.m-443.html. [cit. 2024-09-25].

MAHIEU, René L.P. a AUSLOOS, Jef, 2020. Harnessing the collective potential of GDPR access rights: towards an ecology of transparency. Online. *Internet Policy Review*. Roč. 2020. Dostupné z: https://policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487. [cit. 2024-06-23].

MAHIEU, René L.P., ASGHARI, Hadi a VAN EETEN, Michel, 2018. Collectively Exercising the Right of Access: Individual Effort, Societal Effect. Online. *Internet Policy Review*. Roč. 2018, č. 7(3). Dostupné z: https://doi.org/10.14763/2018.3.927. [cit. 2024-06-23].

MATEJKA, Ján, 2013. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 260 s. ISBN 978-80-904248-7-6.

MÍŠEK, Jakub, 2020. *Moderní regulatorní metody ochrany osobních údajů*. 1. vydání Brno: Masarykova univerzita, 279 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia. ISBN 978-80-210-9736-0.

MORÁVEK, Jakub a BURIAN, David, 2012. *Předávání osobních údajů do zahraničí: česká a evropská právní úprava, otázky a odpovědi*. Praha: Linde, 263 s. ISBN 978-80-7201-878-9.

NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABARTA, Petr, KAŠPÁRKOVÁ, Kateřina, 2019. *Zákon o zpracování osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR. 1. vydání, 212 s. ISBN 978-80-7598-467-8.

NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan, 2018. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer, 2. vydání, 580 s. ISBN 978-80-7598-068-7.

PATTYNOVÁ, Jana; SUCHÁNKOVÁ, Lenka; ČERNÝ, Jiří a RŮŽIČKA, Miroslav, 2019. *Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář*. 2. vydání. Praha: Leges, 752 s. ISBN 978-80-7502-396-4.

POKORNÁ, Andrea, DVOŘÁKOVÁ, Helena, 2020. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer ČR, 352 s. ISBN 978-80-7598-309-1.

POLČÁK, Radim, MYŠKA, Matěj, HOSTAŠ, Petr, KASL, František, KYSELOVSKÁ, Tereza, LECHNER, Tomáš, LOUTOCKÝ, Pavel, MÍŠEK, Jakub, TOMÍŠEK, Jan, STUPKA, Václav a UŘIČAŘ, Miroslav. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. 656 s. Právní monografie. ISBN 978-80-7598-045-8.

POULLET, Yves, 2019. *La vie privée à l'heure de la société du numérique*. 1ère éd. Bruxelles: Larcier, 190 s. ISBN 9782807911079.

PURTOVA, Nadezhda, 2018. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. Online. *Law, Innovation and Technology*. Roč. 2018, č. 10(1), s. 35. Dostupné z: https://doi.org/10.1080/17579961.2018.1452176. [cit. 2024-07-12].

QUEZADA-TAVÁREZ, Katherine, 2021. Impact of the Right of Access on the Balance between Security and Fundamental Right: Informational Power as a Tool to Watch the Watchers. Online. *European Data Protection Law Review*. 2021, Volume 7, Issue 1, s. 15 (59–73). Dostupné z: https://doi.org/10.21552/edpl/2021/1/9. [cit. 2024-09-01].

QUINN, Brendan, 2021. *Data Protection Implementation Guide: A Legal, Risk and Technology Framework for GDPR*. Wolters Kluwer, 384 s. Online. ISBN 978-9403529004. Dostupné z: Kluwer Law International. [cit. 2024-08-24].

UŘIČAŘ, Miroslav a RÁMIŠ, Vladan a kol., 2021. *Obecné nařízení o ochraně osobních údajů. Komentář*, 1414 s. 1. vydání. Online. Praha: C. H. Beck. ISBN 978-80-7400-815-3. Dostupné z: databáze Beck online. [cit. 2024-07-16].

VANBERG, Aysem Diker a ÜNVER, Mehmet Bilal, 2017. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? Online. *European Journal of Law and Technology*. Roč. 2017, č. Vol 8, No 1. Dostupné z: https://www.ejlt.org/index.php/ejlt/article/view/546/726. [cit. 2024-04-14].

VOIGT, Paul a VON DEM BUSSCHE, Axel, 2017. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 383 s. Online. ISBN 978-3-319-57959-7. Dostupné z: https://doi.org/10.1007/978-3-319-57959-7. [cit. 2024-09-04].

VRABEC, Helena U., 2021. *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*. Oxford University Press, 288 s. Online. ISBN 9780191904851. Dostupné z: https://doi.org/https://doi.org/10.1093/oso/9780198868422.001.0001. [cit. 2024-08-29].

ZUBOFF, Shoshana, 2022. Věk kapitalismu dohledu: Boj o budoucnost lidstva u nové hranice moci. Argo, 728 s. ISBN 978-80-257-3936-5.

ŽŮREK, JUDr. Jiří. *Praktický průvodce GDPR (včetně rozhodovací praxe ÚOOÚ)* [online]. 2021 [cit. 2024-07-16].

2. Seznam použitých internetových zdrojů

Aktuální přehled států, které ratifikovaly Protokol k Úmluvě 108+ je k dispozici zde: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223. [cit. 2024-08-03].

Antti Poikola, Kai Kuikkaniemi, and Harri Honko, '*MyData: A Nordic Model for Human-centered Personal Data Management and Processing*' (2014). Dostupné z: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=ibid. [cit. 2024-09-04].

Bits of Freedom. Projekt *My Data Done Right*. Dostupné z: https://www.mydatadoneright.eu/. [cit. 2024-06-23].

BRAUCHART, Nina Maria. Master's Thesis. LLM Law and Technology, Tilburg University, June 2019. *The constitutional right to personal data protection in the face of automated decision-making. A comparison between France and Germany*, str. 24-25. [cit. 2022-03-07].

CNIL (září 2023). *Le droit d'accès: connaître les données qu'un organisme détient sur vous* (Právo na přístup: zjistěte, jaké údaje o vás organizace uchovává). Dostupné zde: https://www.cnil.fr/fr/comprendre-mes-droits/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous. [cit. 2024-04-14].

CNIL (2021). *Recommandation 6: Renforcer l'Information et les Droits des Mineurs par le Design* (Doporučení č. 6: Posílit informovanost a práva nezletilých prostřednictvím designu). Dostupné z: https://www.cnil.fr/fr/recommandation-6-renforcer-linformation-et-les-droits-des-mineurs-par-le-design. [cit. 2024-09-25].

CNIL, 2017. *'Comment Permettre à l'Homme de Garder La Main? Les Enjeux Éthiques Des Algorithmes et de l'Intelligence Artificielle'* (Jak umožnit lidem udržet si kontrolu? Etické výzvy algoritmů a umělé inteligence). Dostupné zde: https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de. [cit. 2022-03-07].

CNIL, 2014. Metodika francouzského dozorového úřadu CNIL k chytrému měření. *Pack de conformité – les Compteurs Communicants*. Online. Dostupné z: https://www.cnil.fr/sites/cnil/files/typo/document/Pack_de_Conformite_COMPTEURS_COMMUNICANTS.pdf. [cit. 2024-04-14].

Conseil d'Etat. *Etude Annuelle 2014 Du Conseil d'État – Le Numérique et Les Droits Fondamentaux* (La Documentation française 2014). 8. září 2014, str. 337. Dostupné zde: https://www.conseil-etat.fr/publications-colloques/etudes/le-numerique-et-les-droits-fondamentaux. [cit. 2022-03-07].

De Lege Data. 24. září 2024. *Landgericht Köln: die bloße verspätete Auskunft stellt keinen Schaden im Rahmen des Art. 82 DSGVO dar* (Zemský soud v Kolíně nad Rýnem: pouhé prodlení s poskytnutím informací nepředstavuje újmu ve smyslu čl. 82 GDPR). Dostupné z: https://www.delegedata.de/2024/09/landgericht-koeln-die-blosse-verspaetete-auskunft-stellt-keinen-schaden-im-rahmen-des-art-82-dsgvo-dar/. [cit. 2024-09-25].

DPC (říjen 2022). *Subject Access Requests: A Data Controller's Guide* (Žádosti subjektu údajů o přístup: Průvodce pro správce údajů). Dostupné zde: https://www.dataprotection.ie/sites/default/files/uploads/2022-10/20221005%20Subject%20Access%20Requests%20A%20Data%20Controller%27s%20Guide.pdf. [cit. 2024-04-14].

DPC (2020). Výroční zpráva irského dozorového úřadu DPC. *Data Protection Commission's Annual Report 2020* [online]. 98 s. Dostupné z: https://www.dataprotection.ie/sites/default/files/uploads/2021-02/DPC%202020%20Annual%20Report%20%28English%29.pdf. [cit. 2022-03-07].

E03537 – Multistakeholder expert group to support the application of Regulation (EU) 2016/679. *Report from Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679*, Ref. Ares(2024)4222971, 10. června 2024. Dostupné zde: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=54422&fromExpertGroups=3537. [cit. 2024-09-25].

EDPB. 28. 2. 2024. *CEF 2024: Launch of coordinated enforcement on the right of access* (CEF 2024: Zahájení společné koordinované dozorové akce k právu na přístup). Dostupné zde: https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_cs. [cit. 2024-09-25].

EDPB. 21. 1. 2019. *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. Dostupné z: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. [cit. 2024-06-23].

Internetové stránky EDPB. Dokumenty v rámci veřejné konzultace k Pokynům k právu na přístup. Dostupné z: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en. [cit. 2024-04-14].

EDPB. Dopis EDPB Evropskému parlamentu, Radě a Evropské komisi ze dne 28. března 2023 ke sdílení údajů pro účely boje proti praní peněz a financování terorismu s ohledem na mandát Rady k jednání. Dostupné zde: https://www.edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0018_aml_cft_council_en.pdf. [cit. 2024-08-24].

EDPB. Dopis EDPB adresovaný Evropské komisi ze dne 12. května 2022, navazující na legislativní balíček čtyř legislativních návrhů AML přijatý Evropskou komisí dne 20. července 2021, jehož cílem je posílit opatření EU v oblasti boje proti praní peněz a financování terorismu. Dostupné zde: https://www.edpb.europa.eu/system/files/2022-05/edpb_letter_out2022-0035_aml_cft_proposal_ec_en.pdf. [cit. 2024-08-24].

EDPS. Stanovisko evropského inspektora ochrany údajů 12/2021 ze dne 22. září 2021 k balíčku legislativních návrhů týkajících se boje proti praní peněz a financování terorismu (AML/CFT). Dostupné zde: https://www.edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf. [cit. 2024-08-24].

EC Communication 2010: *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, 4 November 2010. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF. [cit. 2022-03-07].

EC Report 2003: *Report from the Commission: First report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, 15 May 2003. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF.

Evropská komise 2024. *Sdělení Komise Evropskému parlamentu a Radě: Druhá zpráva o uplatňování obecného nařízení o ochraně osobních údajů*, COM/2024/357 final, 25. července 2024. Dostupné zde: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52024DC0357. [cit. 2024-09-25].

Evropská komise 2020. *Sdělení Komise Evropskému parlamentu a Radě: Ochrana osobních údajů jakožto pilíř posílení postavení občanů a přístup EU k digitální transformaci – dva roky uplatňování obecného nařízení o ochraně údajů*, COM/2020/264 final, 24. června 2020. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52020DC0264. [cit. 2024-09-25].

Evropský konvent. Vysvětlení prezídia Evropského konventu k Listině základních práv EU. Úřední věstník Evropské unie C 303/17 - 14.12.2007. Dostupné z: https://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:CS:PDF. [cit. 2024-04-14].

FRA. *Report – GDPR in practice – Experiences of data protection authorities*. 11. června 2024. Dostupné zde: https://fra.europa.eu/cs/publication/2024/gdpr-experiences-data-protection-authorities. [cit. 2024-09-25].

FRA. *Vysvětlení Agentury FRA k jednotlivým ustanovením Listiny základních práv Evropské unie*. Dostupné zde: https://fra.europa.eu/cs/eu-charter/. [cit. 2024-07-16].

HÄUSELMANN, Andreas, 2023. *The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber*. Online. European Law Blog. Dostupné z: https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/. [cit. 2024-06-23].

HUSTINX, Peter. Speeches and Articles EDPS. *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. Červenec 2013. Dostupné z: https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en. [cit. 2024-07-12].

ICO (2022). *Right of access - How do we find and retrieve the relevant information?* Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/how-do-we-find-and-retrieve-the-relevant-information. [cit. 2023-04-15].

ICO (2022). *Right of access - What should we do if the request involves information about other individuals?* Dostupné z: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/information-about-other-individuals. [cit. 2024-09-25].

ICO. Výroční zpráva britského dozorového úřadu ICO. *Information Commissioner's Annual Report and Financial Statements* 2020-21 [online]. Červenec 2021, 138 s. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf. [cit. 2022-03-07].

NOYB. *Your right of Access (Article 15).* Dostupné z: https://noyb.eu/en/your-right-access-article-15. [cit. 2024-06-23].

Reuschlaw. *Recent case law on the right of access in accordance with Article 15 of the GDPR.* 10. srpen 2021. Dostupné z: https://www.reuschlaw.de/en/news/recent-case-law-on-the-right-of-access-in-accordance-with-article-15-of-the-gdpr/. [cit. 2024-09-25].

ÚOOÚ. Výroční zpráva ÚOOÚ za rok 2023. Online. Dostupné z: https://uoou.gov.cz/media/vyrocni-zpravy/vz2023-elektronicka-verze.pdf. [cit. 2024-09-25].

ÚOOÚ. Základní příručka ÚOOÚ k ochraně údajů. Online. Dostupné z: https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju. [online]. [cit. 2024-04-14].

3. Seznam použitých právních předpisů a jiných právních dokumentů

Zákon č. 110/2019 Sb. o zpracování osobních údajů.

Důvodová zpráva k zákonu č. 110/2019 Sb. o zpracování osobních údajů.

Zákon č. 257/2016 Sb., o spotřebitelském úvěru.

Zákon č. 89/2012 Sb., občanský zákoník.

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

Zákon č. 101/2000 Sb., o ochraně osobních údajů.

Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).

Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu.

Nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy.

Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách).

Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích).

Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.

Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Evropská komise 2023. *Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679 („Procesní nařízení“)*, COM/2023/348 final, 4. července 2023. Dostupné zde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0348. [cit. 2024-09-25].

Evropská komise 2012. *Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů),* COM/2012/011 final, 25. ledna 2012. Dostupné zde: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A52012PC0011.

EDPB. *Guidelines 01/2022 on data subject rights – Right of access*, version 2.0, Adopted on 28 March 2023. Dostupné z: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.

EDPB. *Pokyny 10/2020 týkající se omezení podle článku 23 GDPR*, verze 2.1, přijaté dne 13. října 2021. Dostupné zde: https://www.edpb.europa.eu/system/files/2023-07/edpb_guidelines202010_on_art23_adopted_after_consultation_cs.pdf.

EDPB. *Pokyny 07/2020 k pojmům správce a zpracovatele v GDPR*. Verze 2.0. Přijato dne 7. července 2021. Dostupné zde: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_cs.pdf.

EDPB. *Pokyny č. 5/2019 ke kritériím práva být zapomenut v případech vyhledávačů podle nařízení GDPR*, verze 2.0, přijaté dne 7. července 2020. Dostupné zde: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_cs.pdf.

EDPB. *Guidelines 03/2019 on processing of personal data through video devices*, version 2.0, Adopted on 29 January 2020. Dostupné zde: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

WP29. *Pokyny k transparentnosti WP 260 rev.01*, přijaté dne 29. listopadu 2017 naposledy revidované a přijaté dne 11. dubna 2018, dostupné zde: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_cs.pdf.

WP29. *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258,* Adopted on 29 November 2017. Dostupné zde: https://ec.europa.eu/newsroom/article29/items/610178/en.

WP29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 (WP 251 rev.01)*, přijaté dne 3. října 2017, naposledy revidované a přijaté dne 6. února 2018. Dostupné zde: https://ec.europa.eu/newsroom/article29/items/612053.

WP29. *Pokyny týkající se práva na přenositelnost údajů WP 242 rev.01*, přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017, dostupné zde: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-tykajici-se-prava-na-prenositelnost-udaju-v-cestine.pdf.

WP29. *Stanovisko č. 5/2014 k technikám anonymizace (WP216),* přijaté dne 10. dubna 2014, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

WP29. *Stanovisko č. 12/2011 k inteligentnímu měření (WP183)*, přijaté dne 4. dubna 2011, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_cs.pdf.

WP29. *Stanovisko č. 1/2010 (WP169) k pojmům „správce" a „zpracovatel"*, přijaté dne 16. února 2010, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_cs.pdf.

WP29. *Stanovisko č. 4/2007 (WP136) k pojmu osobní údaje*, přijaté dne 20. června 2007, dostupné zde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf.

OECD. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (23rd September, 1980). OECD Publishing, Paris. Dostupné z: https://doi.org/10.1787/9789264196391-en. [cit. 2024-09-25].
OSN. Rezoluce Valného shromáždění ze dne 18. prosince 2013 č. 68/167. Právo na soukromí v digitálním věku. Dostupné z: https://digitallibrary.un.org/record/764407?v=pdf. [cit. 2024-09-27].

OSN. Rezoluce Valného shromáždění ze dne 18. prosince 2014 č. 69/166. Právo na soukromí v digitálním věku. Dostupné z: https://documents.un.org/doc/undoc/gen/n14/707/03/pdf/n1470703.pdf. [cit. 2024-09-27].

Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (tzv. Úmluva 108, vyhlášená pod č. 115/2001 Sb. m. s.).

Důvodová zpráva k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat (*Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*). Dostupné z: https://rm.coe.int/16800ca434. [cit. 2024-09-01].

Důvodová zpráva k Úmluvě 108+ (*Explanatory Report)*, dostupné zde: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. [cit. 2024-09-01].

Modernizovaná Úmluva 108: novinky v kostce (*The modernised Convention 108: novelties in a nutshell*). Dostupné z: https://rm.coe.int/16808accf8. [cit. 2024-09-01].

(Francouzský) Code monétaire et financier (Měnový a finanční zákoník z 16. prosince 1999). Dostupné zde: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043332956. [cit. 2024-08-24].

(Francouzský) Code pénal (Trestní zákoník z 22. července 1992). Dostupné zde: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719?init=true&page=1&query=code+p%C3%A9nal&searchField=ALL&tab_selection=all. [cit. 2024-08-24].

(Francouzský) Code civil (Občanský zákoník z 21. března 1804). Dostupné zde: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070721/. [cit. 2024-08-24].

(Francouzský) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Zákon č. 78-17 ze dne 6. ledna 1978 o informačních technologiích, souborech a svobodách). Dostupné zde: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/. [cit. 2024-08-24].

(Francouzský) Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens (Zákon č. 70-643 ze dne 17. července 1970 o posílení záruky individuálních práv občanů). Dostupné zde: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000693897. [cit. 2024-08-24].

(Německý) Bundesdatenschutzgesetz. Federální zákon o ochraně osobních údajů z 27. ledna 1977. Dostupné zde: https://offenegesetze.de/veroeffentlichung/bgbl1/1977/7#page=1. [cit. 2024-08-24].

(Německý) Datenschutzgesetz. Zákon o ochraně osobních údajů vydaný ve spolkové zemi Hesensko v roce 1970. Dostupné zde: https://starweb.hessen.de/cache/GVBL/1970/00041.pdf. [cit. 2024-08-24].

(Německý) Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten. Zákon o sledování výnosů ze závažné trestné činnosti. Dostupné zde: https://www.gesetze-im-internet.de/gwg_2017/BJNR182210017.html. [cit. 2024-08-24].

(Německý) Registermodernisierungsgesetz. Zákon o zavedení a používání identifikačního čísla ve veřejné správě a o změně některých zákonů (zákon o modernizaci rejstříků – RegMoG), dostupné zde: https://www.gesetze-im-internet.de/regmog/BJNR059100021.html. [cit. 2024-08-24].

Důvodová zpráva k německému zákonu o sledování výnosů ze závažné trestné činnosti. Dostupná zde: https://dserver.bundestag.de/btd/18/115/1811555.pdf. [cit. 2024-08-24].

(Švédský) Datalagen. Zákon o datech č. 289 z 11. května 1973. Dostupné zde: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289/. [cit. 2024-08-24].

UK Data Protection Act z roku 2018. Dostupné zde: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. [cit. 2024-08-24].

UK Data Protection Act z roku 1998. Dostupné zde: https://www.legislation.gov.uk/ukpga/1998/29/contents/enacted. [cit. 2024-08-24].

UK Data Protection Act z roku 1984. Dostupné zde: https://www.legislation.gov.uk/ukpga/1984/35/enacted. [cit. 2024-08-24].

UK. European Union (Withdrawal) Act z roku 2018. Dostupné zde: https://www.legislation.gov.uk/ukpga/2018/16/contents. [cit. 2024-08-24].

4. Seznam použité judikatury

Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17.

Nález Ústavního soudu ze dne 3. 4. 2018, sp. zn. IV. ÚS 1200/16.

Nález Ústavního soudu ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16

Rozsudek Nejvyššího správního soudu ze dne 26. 3. 2024, čj. 6 As 32/2023-40.

Rozsudek Nejvyššího správního soudu ze dne 13. 8. 2020, č. j. 1 As 387/2019-56.

Rozsudek Soudního dvora ze dne 7. března 2024, Endemol Shine Finland, C-740/22, EU:C:2024:216.

Rozsudek Soudního dvora ze dne 7. března 2024, IAB Europe, C-604/22, EU:C:2024:214.

Rozsudek Soudního dvora ze dne 7. prosince 2023, SCHUFA Holding (Scoring), C-634/21, EU:C:2023:957.

Rozsudek Soudního dvora ze dne 9. listopadu 2023, Gesamtverband Autoteile-Handel (Přístup k informacím o vozidlech), C-319/22, EU:C:2023:837.

Rozsudek Soudního dvora ze dne 26. října 2023, FT (Copies du dossier médical), C-307/22, EU:C:2023:811.

Rozsudek Soudního dvora ze dne 4. července 2023, Meta Platforms a další (Všeobecné podmínky používání sociální sítě), C-252/21, EU:C:2023:537.

Rozsudek Soudního dvora ze dne 22. června 2023, Pankki S, C-579/21, EU:C:2023:501.

Rozsudek Soudního dvora ze dne 4. května 2023, Bundesrepublik Deutschland, C-60/22, EU:C:2023:373.

Rozsudek Soudního dvora ze dne 4. května 2023, Österreichische Datenschutzbehörde, C-487/21, EU:C:2023:369.

Rozsudek Soudního dvora ze dne 12. ledna 2023, Österreichische Post (Informations relatives aux destinataires de données personnelles), C-154/21, EU:C:2023:3.

Rozsudek Soudního dvora ze dne 6. října 2020, La Quadrature du Net a další, spojené věci C-511/18, C-512/18 a C-520/18, EU:C:2020:791.

Rozsudek Soudního dvora ze dne 1. října 2019, Planet49, C-673/17, EU:C:2019:801.

Rozsudek Soudního dvora ze dne 24. září 2019, GC a další, C-136/17, EU:C:2019:773.

Rozsudek Soudního dvora ze dne 29. července 2019, Fashion ID, C-40/17, EU:C:2019:629.

Rozsudek Soudního dvora ze dne 14. února 2019, Buivids, C-345/17, EU:C:2019:122.

Rozsudek Soudního dvora ze dne 10. července 2018, Jehovan todistajat, C-25/17, EU:C:2018:551.

Rozsudek Soudního dvora ze dne 5. června 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388.

Rozsudek Soudního dvora ze dne 20. prosince 2017, Nowak, C-434/16, EU:C:2017:994.

Rozsudek Soudního dvora ze dne 27. září 2017, Puškár, C-73/16, EU:C:2017:725.

Rozsudek Soudního dvora ze dne 9. března 2017, Manni, C-398/15, EU:C:2017:197.

Rozsudek Soudního dvora ze dne 21. prosince 2016, Tele2 Sverige, spojené věci C-203/15 a C-698/15, EU:C:2016:970.

Rozsudek Soudního dvora ze dne 19. října 2016, Breyer, C-582/14, EU:C:2016:779.

Rozsudek Soudního dvora ze dne 28. července 2016, Verein für Konsumenteninformation, C-191/15, EU:C:2016:612.

Rozsudek Soudního dvora ze dne 6. října 2015, Schrems, C-362/14, EU:C:2015:650.

Rozsudek Soudního dvora ze dne 1. října 2015, Weltimmo, C-230/14, EU:C:2015:639.

Rozsudek Soudního dvora ze dne 1. října 2015, Bara a další, C-201/14, EU:C:2015:638.

Rozsudek Soudního dvora ze dne 16. července 2015, ClientEarth a PAN Europe v. EFSA, C-615/13 P, EU:C:2015:489.

Rozsudek Soudního dvora ze dne 11. prosince 2014, Ryneš, C-212/13, EU:C:2014:2428.

Rozsudek Soudního dvora ze dne 17. července 2014, YS a další, spojené věci C-141/12 a C-372/12, EU:C:2014:2081.

Rozsudek Soudního dvora ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317.

Rozsudek Soudního dvora ze dne 8. dubna 2014, Digital Rights Ireland a Seitlinger a další, spojené věci C-293/12 a C-594/12, EU:C:2014:238.

Rozsudek Soudního dvora ze dne 12. prosince 2013, X, C-486/12, EU:C:2013:836.

Rozsudek Soudního dvora ze dne 7. listopadu 2013, IPI, C-473/12, EU:C:2013:715.

Rozsudek Soudního dvora ze dne 17. října 2013, Schwarz, C-291/12, EU:C:2013:670.

Rozsudek Soudního dvora ze dne 19. dubna 2012, Bonnier Audio a další, C-461/10, EU:C:2012:219.

Rozsudek Soudního dvora ze dne 9. listopadu 2010, Volker und Markus Schecke a Eifert, spojené věci C-92/09 a C-93/09, EU:C:2010:662.

Rozsudek Soudního dvora ze dne 6. července 2010, Komise v. Bavarian Lager, C-28/08 P, EU:C:2010:378.

Rozsudek Soudního dvora ze dne 7. května 2009, Rijkeboer, C-553/07, EU:C:2009:293.

Rozsudek Soudního dvora ze dne 16. prosince 2008, Satakunnan Markkinapörssi a Satamedia, C-73/07, EU:C:2008:727.

Rozsudek Soudního dvora ze dne 6. listopadu 2003, Lindqvist, C-101/01, EU:C:2003:596.

Rozsudek Soudního dvora ze dne 20. května 2003, Österreichischer Rundfunk a další, spojené věci C-465/00, C-138/01 a C-139/01, EU:C:2003:294.

Rozsudek Soudního dvora ze dne 13. dubna 2000, Karlsson a další, C-292/97, EU:C:2000:202.

Usnesení Soudního dvora ze dne 27. května 2024, Addiko Bank, C-312/23, EU:C:2024:458.

Posudek 1/15 Soudního dvora (velkého senátu) k návrhu dohody mezi EU a Kanadou o předávání údajů jmenné evidence cestujících ze dne 26. července 2017, EU:C:2017:592.

Stanovisko generálního advokáta Manuela Campos Sánchez-Bordony ze dne 15. prosince 2022, Pankki S, C-579/21, EU:C:2022:1001.

Stanovisko generálního advokáta Giovanniho Pitruzzelly ze dne 9. června 2022, Österreichische Post (Informations relatives aux destinataires de données personnelles), C-154/21, EU:C:2022:452.

Stanovisko generálního advokáta Pedra Cruz Villalóna ze dne 9. července 2015, Bara, C-201/14, EU:C:2015:461.

Stanovisko generální advokátky Eleanor Sharpston ze dne 12. prosince 2013, YS a další, spojené věci C-141/12 a C-372/12, EU:C:2013:838.

Rozsudek velkého senátu ESLP ze dne 25. května 2021 Big Brother Watch a ostatní proti Spojenému království (stížnosti č. 58170/13, 62322/14 a 24960/15).

Rozsudek velkého senátu ESLP ze dne 25. května 2021 Centrum för rättvisa proti Švédsku (stížnost č. 35252/08).

Rozsudek prvního senátu ESLP ze dne 13. února 2020 Trajkovski a Chipovski proti Severní Makedonii (stížnosti č. 53205/13 a 63320/13).

Rozsudek pátého senátu ESLP ze dne 22. června 2017 Aycaguer proti Francii (stížnost č. 8806/12).

Rozsudek velkého senátu ESLP ze dne 8. listopadu 2016 Magyar Helsinki Bizottság proti Maďarsku (stížnost č. 18030/11).

Rozsudek velkého senátu ESLP ze dne 4. prosince 2015 Roman Zakharov proti Rusku (stížnost č. 47143/06).

Rozsudek pátého senátu ESLP ze dne 18. dubna 2013 M. K. proti Francii (stížnost č. 19522/09).

Rozsudek třetího senátu ESLP ze dne 27. října 2009 Haralambie proti Rumunsku (stížnost č. 21737/03).

Rozsudek velkého senátu ESLP ze dne 4. prosince 2008 S. a Marper proti Spojenému království (stížnosti č. 30562/04 a 30566/04).

Rozsudek čtvrtého senátu ESLP ze dne 17. července 2008 I proti Finsku (stížnost č. 20511/03).

Rozsudek velkého senátu ESLP ze dne 13. února 2003 Odièvre proti Francii (stížnost č. 42326/98).

Rozsudek druhého senátu ESLP ze dne 24. září 2002 M.G. proti Spojenému království (stížnost č. 39393/98).

Rozsudek druhého senátu ESLP ze dne 16. dubna 2002 Société Colas Est a další proti Francii (stížnost č. 37971/97).

Rozsudek velkého senátu ESLP ze dne 4. května 2000 Rotaru proti Rumunsku (stížnost č. 28341/95).

Rozsudek velkého senátu ESLP ze dne 16. února 2000 Amann proti Švýcarsku (stížnost č. 27798/95).

Rozsudek ESLP ze dne 25. února 1997 Z proti Finsku (stížnost č. 22009/93).

Rozsudek ESLP ze dne 24. dubna 1990 Huvig proti Francii (stížnost č. 11105/84).

Rozsudek ESLP ze dne 24. dubna 1990 Kruslin proti Francii (stížnost č. 11801/85).

Rozsudek velkého senátu ESLP ze dne 7. července 1989 Gaskin proti Spojenému království (stížnost č. 10454/83).

Rozsudek ESLP ze dne 26. března 1987 Leander proti Švédsku (stížnost č. 9248/81).

Rozsudek ESLP ze dne 2. srpna 1984 Malone proti Spojenému království (stížnost č. 8691/79).

Rozsudek ESLP ze dne 6. září 1978 Klass a ostatní proti Německu (stížnost č. 5029/71).

Bundesverfassungsgericht. BVerfG. Rozsudek prvního senátu Ústavního soudu ze dne 15. prosince 1983 – 1 BvR 209/83; BVerfGE 65, 1 (1983). Dostupné z: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html;jsessionid=32644501620FBA0356ACCB64EA7006A5.internet962.

Bundesverfassungsgericht. BVerfG (16. 7. 1969). Beschluss des Ersten Senats vom 16 Juli 1969 – 1 BvL19/63 (*Mikrozenzus*). Dostupné z: https://openjur.de/u/183523.html.

Zemský soud v Kolíně nad Rýnem. Landgericht Köln (19. 4. 2024). Rozsudek 12 S 4/23. Dostupné z: https://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2024/12_S_4_23_Urteil_20240419.html.

Zemský soud v Bonnu. Landgericht Bonn (1. 7. 2021). Rozsudek 15 O 372/20. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Text=15%20O%20372/20.

Zemský soud v Bonnu. Landgericht Bonn (1. 7. 2021). Rozsudek 15 O 355/20. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Bonn&Datum=01.07.2021&Aktenzeichen=15%20O%20355/20.

Conseil constitutionnel. Nález Ústavního soudu č. 2012-652 ze dne 22. 3. 2012. Dostupné zde: https://www.conseil-constitutionnel.fr/decision/2012/2012652DC.htm. [cit. 2022-03-07].

Conseil constitutionnel. Nález Ústavního soudu č. 2004-504 ze dne 12. 8. 2004. Dostupné zde: https://www.conseil-constitutionnel.fr/decision/2004/2004504DC.htm. [cit. 2022-03-07].

Conseil constitutionnel. Nález Ústavního soudu č. 99-422 ze dne 21. 12. 1999. Dostupné zde: https://www.conseil-constitutionnel.fr/decision/1999/99422DC.htm. [cit. 2022-03-07].

Nejvyšší soud Rakouska. OGH. (23. 6. 2021). Rozsudek 6Ob56/21k. Dostupné z: https://1url.cz/Q1R4r.

Vrchní zemský soud ve Vídni. Oberlandesgericht Wien. (2020). 11 R 153/20f, 154/20b. Dostupné z: https://noyb.eu/sites/default/files/2020-12/BVI-209_geschw%C3%A4rzt.pdf.

5. Seznam ostatních zdrojů

FRA. *Handbook on European data protection law.* [online]. Vydání z roku 2018. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-9491-901-4. Dostupné z: doi: 10.2811/343461. [cit. 2024-07-12].

ICO (listopad 2022). *How to deal with Subject Access Requests*. (Video britského dozorového úřadu – Jak vyřizovat žádosti o přístup k informacím). Dostupné zde: https://www.youtube.com/watch?v=WY98d-wUn5w. [cit. 2024-04-14].

Rozhovor s Shoshanou Zuboff na Radiu Wave ze dne 10. dubna 2023, podcast Vlna, *Soukromí, jak jsme ho znali ještě na přelomu tisíciletí, přestalo existovat*, upozorňuje vědkyně Shoshana Zuboff. Dostupné z: https://wave.rozhlas.cz/soukromi-jak-jsme-ho-znali-jeste-na-prelomu-tisicileti-prestalo-existovat-8966958. [cit. 2024-08-17].

Seznam příloh

1. **Příloha č. 1: Tabulka – Srovnání konkrétních složek práva na přístup podle směrnice 95/46 a nařízení GDPR**

2. **Příloha č. 2: Grafy – Právně-empirické studie Pierre Dewitta a Jefa Ausloose z let 2020 a 2022**

Příloha č. 1: Tabulka – Srovnání konkrétních složek práva na přístup podle směrnice 95/46 a nařízení GDPR

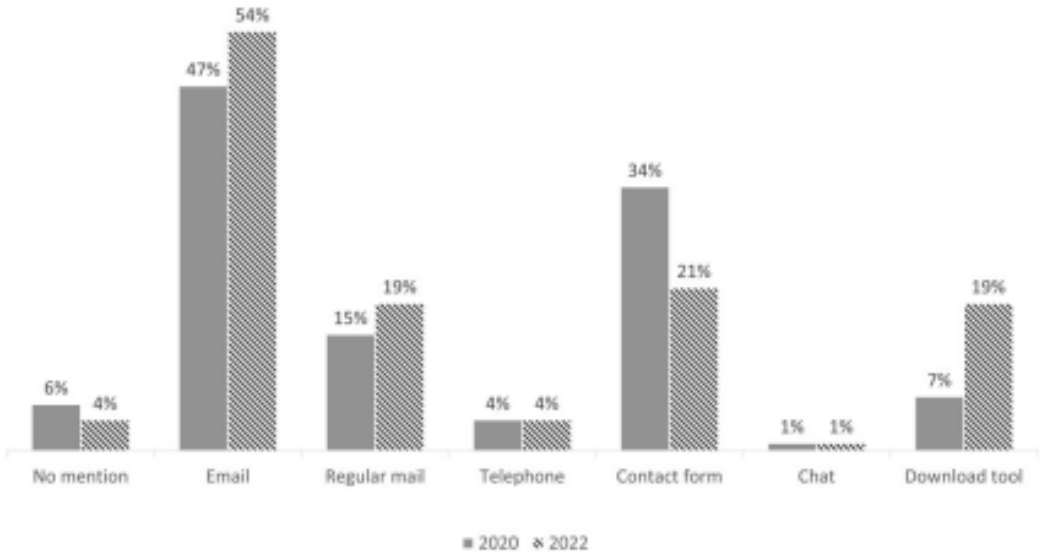
	Směrnice 95/46	GDPR
Poplatek	Čl. 12 písm. a): **bez [...] nadměrných [...] nákladů.**	Rec. 59; čl. 12 odst. 5: získání přístupu musí být **bezplatné**, se **dvěma výjimkami:** – Čl. 12 odst. 5 písm. a): možnost správců uložit přiměřený poplatek, pokud jsou žádosti zjevně nedůvodné nebo nepřiměřené; – Čl. 15 odst. 3: možnost správců uložit přiměřený poplatek za další požadované kopie.
Lhůta	Čl. 12 písm. a): **bez [...] prodlení.**	Rec. 59; čl. 12 odst. 3 až 4: bez ohledu na to, zda správce hodlá přijmout opatření, či nikoli, odpovědět subjektu údajů **bez zbytečného odkladu** a v každém případě **do jednoho měsíce od obdržení žádosti**. Možnost prodloužení této lhůty o **další dva měsíce**, v případě potřeby a s ohledem na složitost a počet žádostí.
Forma (žádost)	*Směrnice neobsahuje*	Rec. 59: správci by měli poskytnout prostředky pro podávání žádostí **elektronicky**, zejména pokud jsou osobní údaje zpracovávány elektronickými prostředky.
Forma (odpověď)	*Směrnice neobsahuje*	Rec. 63; čl. 12 odst. 1: informace se poskytují **písemně** nebo **jinými prostředky**, včetně ve vhodných případech **v elektronické formě**. Pokud je to možné, měl by být umožněn **přímý dálkový přístup** do zabezpečeného systému. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty **ústně**, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.
Srozumitelnost	Čl.12 písm. a) druhá odrážka: ve **srozumitelné formě**.	Rec. 58; čl. 12 odst. 1: **stručným, transparentním, srozumitelným** a **snadno přístupným** způsobem za použití **jasných a jednoduchých jazykových prostředků**, zejména v případě informací určených konkrétně **dítěti**.
Ověřování totožnosti	*Směrnice neobsahuje*	Rec. 64; čl. 12 odst. 6: správce **může** požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů a **měl by** k tomu využít všech vhodných opatření, zejména v souvislosti s on-line službami a síťovými identifikátory.
Omezení	Rec. 43; čl. 13 odst.1: členské státy mohou přijmout **legislativní opatření** s cílem omezit rozsah povinností a práv uvedených v **čl. 6 odst. 1, v článku 10, v čl. 11 odst. 1 a v článcích 12 a 21**, pokud toto omezení představuje **opatření nezbytné** pro zajištění: (viz výčet v čl. 13 odst. 1 písm. a) až g)). Čl. 13 odst. 2: s výhradou **přiměřených právních ochranných opatření** mohou členské státy, pokud **prokazatelně neexistuje nebezpečí narušení soukromí subjektu údajů**, omezit **legislativním opatřením**	Rec. 73; čl. 23 odst. 1 až 2: Právo Unie nebo členského státu může prostřednictvím **legislativního opatření** omezit rozsah **povinností a práv stanovených v článcích 12 až 22**, jestliže takové omezení **respektuje podstatu základních práv a svobod** a **představuje nezbytné a přiměřené opatření v demokratické společnosti** s cílem zajistit: (viz výčet v čl. 23 odst. 1. písm. a-j)). Tato opatření musí obsahovat **konkrétní ustanovení** alespoň, je-li to relevantní, pokud jde o: (viz výčet v čl. 23 odst. 2 písm. a-h)). Rec. 153; čl. 85 odst. 2: pro zpracování **pro novinářské účely nebo pro účely akademického,**

	práva uvedená v článku 12, jsou-li údaje zpracovávány **výlučně pro účely vědeckého výzkumu nebo jsou-li uchovávány formou osobních záznamů po dobu nepřesahující období nezbytné pro vypracování statistik.**	**uměleckého či literárního projevu** členské státy stanoví odchylky a výjimky z kapitoly III (práva subjektu údajů), pokud je to nutné **k uvedení práva na ochranu osobních údajů do souladu se svobodou projevu a informací.** Rec. 156; čl. 89 odst. 2: jsou-li osobní údaje zpracovány **pro účely vědeckého či historického výzkumu nebo pro statistické účely**, může právo Unie nebo členského státu stanovit odchylky od práv uvedených v článcích 15, 16, 18 a 21, s výhradou **podmínek a záruk uvedených v čl. 89 odst. 1**, pokud je **pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění zvláštních účelů,** a tyto odchylky jsou **pro splnění těchto účelů nezbytné.**

Zdroj: DEWITTE, Pierre a AUSLOOS, Jef, 2018. Shattering one-way mirrors–data subject access rights in practice. Online. *International Data Privacy Law.* 2018, Volume 8, Issue 1, s. 25 (4–28). Dostupné z: https://doi.org/10.1093/idpl/ipy001. [cit. 2024-09-25].

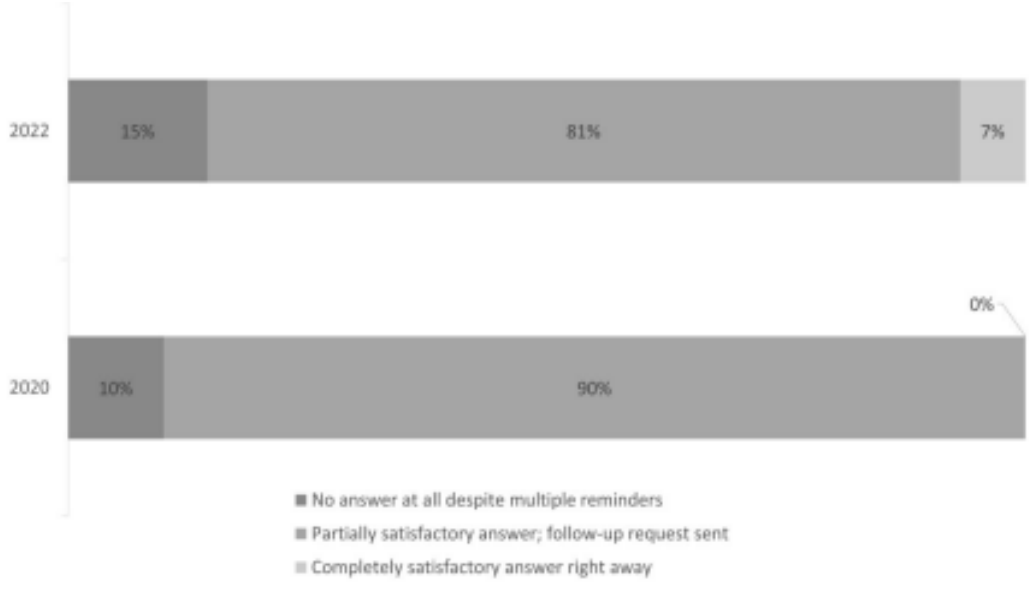
Příloha č. 2: Grafy – Právně-empirické studie Pierre Dewitta a Jefa Ausloose z let 2020 a 2022

Obr. 1 – Způsoby uváděné správci v zásadách ochrany údajů k uplatnění práva na přístup



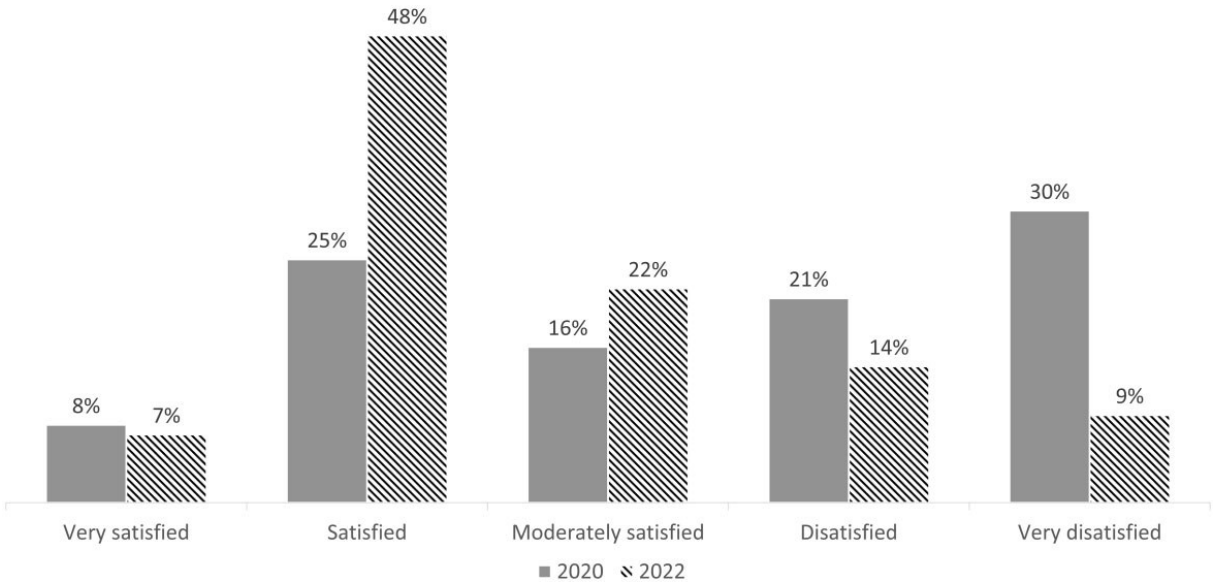
Zdroj: DEWITTE, Pierre a AUSLOOS, Jef, 2024. Chronicling GDPR Transparency Rights in Practice: The Good, the Bad and the Challenges Ahead. Online. *International Data Privacy Law*. May 2024, Volume 14, Issue 2, s. 28 (106–133). Dostupné z: https://doi.org/10.1093/idpl/ipad026. [cit. 2024-09-25].

Obr. 2 – Proces vyřizování žádostí o přístup, přehled typů obdržených odpovědí



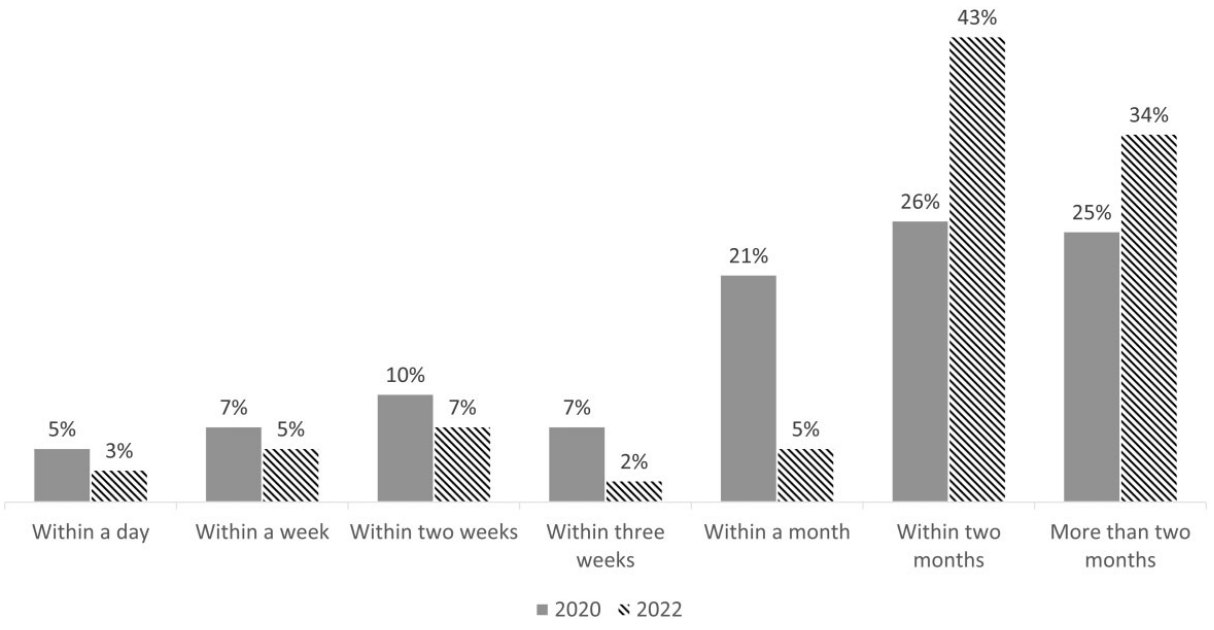
Zdroj: Tamtéž

Obr. 3 – Míra spokojenosti uživatelů s konečnou odpovědí



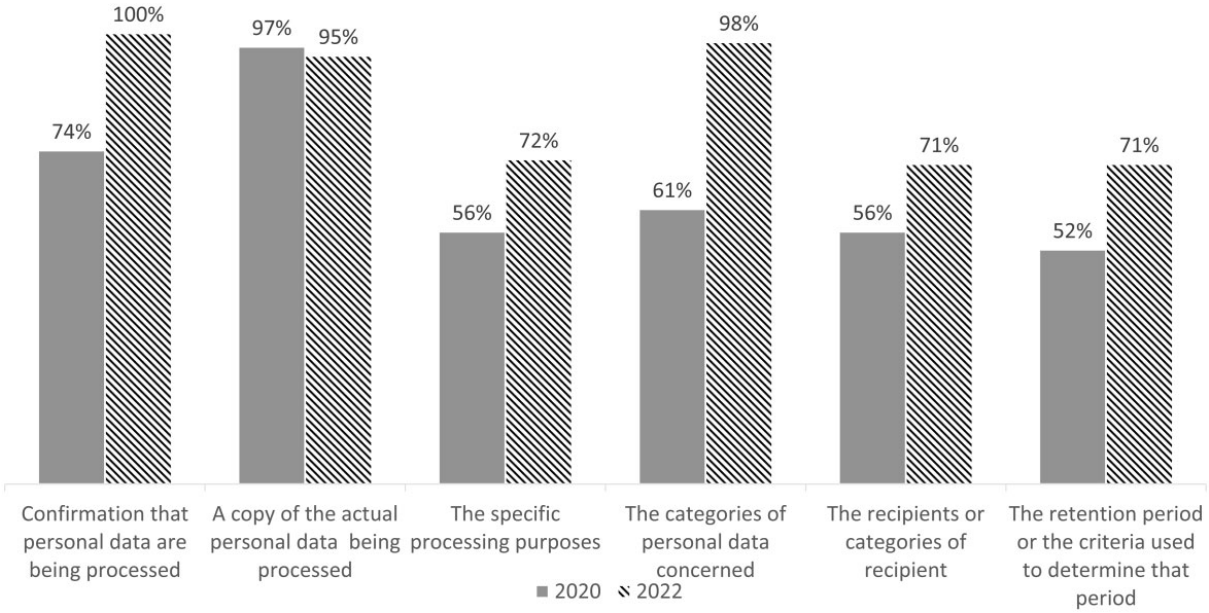
Zdroj: Tamtéž

Obr. 4 – Lhůta mezi první žádostí a konečnou odpovědí



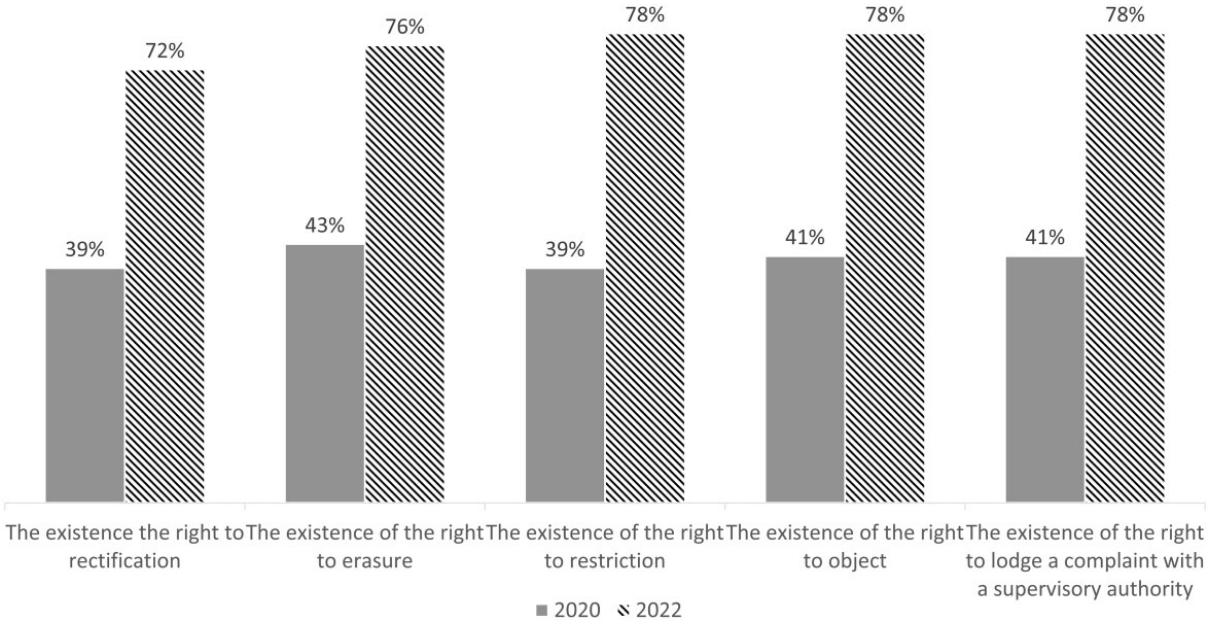
Zdroj: Tamtéž

Obr. 5 – Informace uvedené v závěrečné odpovědi



Zdroj: Tamtéž

Obr. 6 – Informace o dalších právech subjektů údajů uvedené v závěrečné odpovědi



Zdroj: Tamtéž

Ochrana osobních údajů v EU – práva subjektů údajů se zaměřením na právo na přístup

Abstrakt

Tato práce se zabývá problematikou práv subjektů údajů se zaměřením na právo na přístup. Účelem práce je komplexně uchopit a zpracovat právo subjektů údajů na přístup k osobním údajům podle článku 15 nařízení GDPR na úrovni EU. Právo na přístup jako jedno z kontrolních oprávnění totiž představuje klíčový prvek při posilování kontroly uživatelů nad jejich osobními údaji. Toto právo opravňuje subjekt údajů získat informace o tom, zda jsou jeho osobní údaje zpracovávány, a pokud ano, získat přístup ke svým osobním údajům, včetně dalších informací o zpracování údajů. Práce je rozdělena celkem na šest částí. V první části je zkoumán právní rámec, kontext a historické prameny práva na přístup. V rámci této části jsou taktéž analyzovány pojmy: právo na ochranu osobních údajů a právo na soukromí a jejich proměnlivost v čase, na kterou má nepochybně vliv i rozvoj technologií. V druhé části je vysvětlena základní terminologie ochrany osobních údajů, včetně základních zásad zpracování. Porozumění základních pojmů je klíčové pro správnou aplikaci nařízení GDPR. Třetí část práce se věnuje jednotlivým právům subjektů údajů. Zvláštní pozornost je pochopitelně věnována právu subjektů údajů na přístup. Autorka zdůrazňuje jeho postavení v právním řádu, jeho vztah k ostatním právům subjektů údajů, podobnosti a odlišnosti těchto práv. Následující části (čtvrtá a pátá) se pak zabývají již samotným právem na přístup a tvoří základní stavební kámen této práce, k čemuž autorka uvádí i jednotlivé příklady z praxe dozorových úřadů, EDPB a *case law* Soudního dvora EU i vnitrostátních soudů. Část čtvrtá podrobně analyzuje právně-teoretický základ práva na přístup; jeho genezi, včetně komparativního exkurzu; účel; význam; obecné principy a strukturu. V rámci této části se autorka zabývá také metodickým doporučením, jakým způsobem lze podávat žádosti o právo na přístup a jak lze tyto žádosti vyřizovat. Část pátá více upřesňuje rozsah práva na přístup a podrobně rozebírá jeho meze. Poslední část (část šestá) se soustřeďuje na uplatňování práva na přístup v praxi, zahrnuje obecné zhodnocení evropské regulace (včetně unijního zhodnocení), autorka kromě toho také představuje úvahy nad některými normativními nedostatky a interpretuje poznatky z provedených empirických studií k právu na přístup.

Klíčová slova: právo na přístup, GDPR, subjekt údajů

Data protection in the EU – data subjects' rights with a focus on the right of access

Abstract

This thesis addresses the issue of data subjects' rights, focusing on the right of access. The purpose of the thesis is to provide a complex understanding and elaboration of the right of access to personal data of data subjects under Article 15 of the GDPR at the EU level. The right of access as one of the control rights is a key element in strengthening users' control over their personal data. This right entitles the data subject to obtain information on whether his or her personal data is being processed and, if so, to access his or her personal data, including further information on the processing of the data. The thesis is divided into six parts. The first part examines the legal framework, context and historical sources of the right of access. Within this part, the concepts of the right to data protection and the right to privacy are also analysed, as well as their variability over time, which is undoubtedly also influenced by the development of technology. The second part explains the basic terminology of data protection, including the essential principles of processing. Understanding the basic concepts is crucial for the correct application of the GDPR. The third part of the thesis focuses on the individual rights of data subjects. Special emphasis is of course given to the right of access of data subjects. The author underlines its position in the legal order, its relation to other data subjects' rights, similarities and differences of these rights. The following parts (fourth and fifth) deal with the right of access itself and form the cornerstone of this thesis, for which the author also provides individual examples from the practice of supervisory authorities, the EDPB and the *case law* of the CJEU and national courts. Part four analyses in detail the legal-theoretical basis of the right of access; its genesis, including a comparative excursus; purpose; meaning; general principles and structure. Within this part, the author also discusses methodological guidance on how to make requests for the right of access and how such requests can be dealt with. Part five further clarifies the scope of the right of access and discusses its limits in detail. The last part (part six) focuses on the application of the right of access in practice, covering a general assessment of the European regulation (including the EU evaluation); in addition, the author also presents reflections on some normative deficiencies and interprets the findings of empirical studies conducted on the right of access.

Key words: right of access, GDPR, data subject