Západočeská univerzita v Plzni

Fakulta právnická

Rigorózní práce

Ochrana osobních údajů ve světle Nařízení Evropského parlamentu a Rady (EU) 2016/679

Mgr. Tereza Filipová

Plzeň

2018

Rigorózní řízení
Studijní obor: Právo Evropské unie

Katedra ústavního a evropského práva

Rigorózní práce

Ochrana osobních údajů ve světle Nařízení Evropského parlamentu a Rady (EU) 2016/679

Autor: Mgr. Tereza Filipová

Plzeň 2018

Čestné prohlášení

„Prohlašuji, že jsem tuto rigorózní práci zpracovala samostatně, a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala způsobem ve vědecké práci obvyklým.“

V Plzni dne…….

……..
Mgr. Tereza Filipová

Poděkování

Děkuji paní docentce JUDr. Monice Forejtové, Ph.D., za její vedení, ochotu, vstřícný přístup a cenné rady, které mi během zpracování práce věnovala v rámci přípravného kurzu k rigorózní práci. Mé poděkování patří také celé mé rodině za tvorbu potřebného zázemí při psaní práce.

Seznam použitých zkratek a pojmů

Nařízení, Obecné nařízení	Nařízení Evropského parlamentu a Rady (EU) 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 (obecné nařízení o ochraně osobních údajů)
v angl. znění GDPR	General Data Protection Regulation
Směrnice	Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
Trestní směrnice	Směrnice Evropského parlamentu a Rady (EU) 2016/680, 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
Zákon o ochraně osobních údajů	zákon č. 101/200 Sb., o ochraně osobních údajů a o změně některých zákonů
Adaptační zákon, prováděcí zákon	zákon o zpracování osobních údajů, zatím pouze jako vládní návrh, který dosud v České republice neprošel legislativním procesem – sněmovní tisk č. 138
Smlouvy	Smlouva o Evropské unii a Smlouva o fungování Evropské unie
Úřad	Úřad pro ochranu osobních údajů
Skupina WP29	Pracovní skupina ustavená na základě čl. 29 Směrnice, nyní Evropský sbor pro ochranu osobních údajů
DPIA	Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment)
DPO	Pověřenec pro ochranu osobních údajů (Data Protection Officer)

Obsah

1. Úvod

Osobní údaje každého z nás jsou denně zpracovávány mnoha institucemi a společnostmi, aniž si to často uvědomujeme. Přitom hodnota osobního údaje v moderní době stoupá, a s tím vyvstává nutnost jeho zvýšené ochrany. Současné technologie poskytují využívání a zpracování osobních údajů v nebývalém rozsahu, což souvisí zejména s rychlým rozšířením nových informačních technologií, automatizovaným zpracováním údajů, chytrých zařízení a aplikací, umožňujících nové způsoby systematického a potenciálně invazivního zpracování dat. Souvisí to jednak se snížením pořizovacích nákladů na tyto technologie a jednak se jedná o zcela nové techniky zpracování osobních údajů.

V poslední době se ukázalo, jak moc je ochrana osobních údajů významná, avšak ne všude ve světě samozřejmá. Jako odstrašující případ lze uvést nedávné spuštění kreditního systému hodnocení obyvatel v Číně, kteří jsou sledováni ve všech oblastech života, a to s využitím nejmodernějších technologií a umělé inteligence. Následně dochází ke zkombinování takto získaných osobních údajů. Získané záznamy jsou vyhodnocovány systémem, který zohledňuje chování v jednotlivých situacích. Tím vznikne komplexní hodnocení této osoby. Sledovanými aspekty jsou například obsah nákupů, interakce s jinými lidmi, zdravotní stav nebo dopravní přestupky. Chování vyhodnocené jako nežádoucí se následně promítne do negativního hodnocení osoby, což má za následek omezení jejího přístupu například ke vzdělání, koupi letenek nebo získání pasu. Čínská vláda předestírá, že systém vnese větší transparentnost do společnosti a odstraní některé její ekonomické či sociální neduhy. V současné době byla spuštěna pilotní verze systému, přičemž se předpokládá její plné využití do roku 2020. Nelze ale přehlížet, že se se jedná o zásah do jednoho ze základních práv více než 1,4 miliardy osob.[1]

Technologický vývoj jde kupředu mílovými kroky a právo je nuceno se tomuto jevu pružně přizpůsobovat. Dosavadní právní úprava tak sotva mohla postihnout veškeré aspekty ochrany takto získaných osobních údajů, když v době jejího vzniku mnohé technologie ještě neexistovaly. S rozvojem informačních technologií pak narůstá zvýšená potřeba tyto údaje chránit, neboť se stávají

[1] CHORZEMPA, Martin, Paul TRIOLO a Samm SACKS. China´s Social Credit System: A Mark of Progress or a Threat to Privacy?. *Peterson institute for international economics* [online]. [cit. 2018-11-12]. Dostupné z: https://piie.com/system/files/documents/pb18-14.pdf

zranitelnějšími a roste riziko jejich zneužití. Obecné nařízení reflektuje na zvýšenou potřebu ochrany osobních údajů. V případě, že by tato oblast nebyla regulována, velmi rychle by došlo k závažným zásahům do integrity práv jednotlivců. Vždyť právo na ochranu osobních údajů lze zařadit do základních lidských práv, zaručovaným nejen Listinou základních práv Evropské unie, ale také ústavními normami jednotlivých členských států. Dá se tedy říci, že ochrana osobních údajů tvoří spolu se samotným osobním údajem jednotný organismus, a není proto možné tyto dvě složky od sebe oddělovat.

Dosavadní právní úprava ochrany osobních údajů nebyla ze strany správců a zpracovatelů mnohdy plně respektována, což bylo jedním z důvodů, proč nedocházelo k efektivní aplikaci ochrany osobních údajů. Obecně nařízení klade důraz na vymahatelnost práv subjektů údajů a zároveň povinností správců a zpracovatelů, odpovědných za zpracování, a to zejména tím, že určuje náročnější pravidla pro zpracování a proaktivnější přístup správců. Základním východiskem je přitom skutečnost, že při poskytnutí osobních údajů subjektem údajů správci dochází pouze k jejich „propůjčení“ a vlastníkem stále zůstává subjekt údajů. Správce či zpracovatel tak k nakládání s osobními údaji musí přistupovat jako k půjčené věci a v této souvislosti s nimi i řádně hospodařit a ochraňovat je. Zároveň právo na ochranu osobních údajů není právem absolutním a musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy.[2]

Ačkoli je Obecné nařízení mnohdy nazýváno revolucí v ochraně osobních údajů, není to docela pravda. Elementární principy a zásady byly obsaženy již ve Směrnici. Obecné nařízení tuto problematiku nemění, naopak na ni navazuje, kombinuje osvědčené zásady práv na ochranu údajů s mírnou modernizací a zavádí některé nové instituty. V mnoha případech také dochází k odstranění právního vakua, kdy řešení některých otázek stálo pouze na právním výkladu jednotlivých ustanovení a nebylo zakotveno napřímo v právní normě. Obecné nařízení nepředstavuje zásadnější zvrat oblasti ochrany osobních údajů a v případě, že správci řádně dodržovali všechny principy a zásady, obsažené v současně účinném zákoně o ochraně osobních údajů, neměla by pro ně transformace na novou právní úpravu představovat větší potíže. Přesto vyvolává Obecné nařízení celou řadu obav ze strany správců, a to zejména s ohledem na vysoké sankce, které hrozí v případě jeho nedodržení.

[2] Bod 4 recitálu k Obecnému nařízení

Tato rigorózní práce si klade za cíl přiblížit jednotlivá práva subjektů údajů, analyzovat povinnosti správců a zpracovatelů a dále upozornit na některé zajímavé aspekty ve vztahu k dosavadní úpravě, a také k některým zahraničním úpravám. Autorka práce se pohybuje na poli advokacie a ve své praxi již řešila otázky implementace Obecného nařízení do činnosti obchodních společností a spolků a v práci se tak pokusí demonstrovat některé praktické dopady Obecného nařízení.

Rigorózní práce odpovídá právnímu stavu ke dni 15.11.2018

2. Evropsko-právní východiska ochrany osobních údajů

2.1 Důvody vedoucí ke změně právní úpravy

Jak již bylo v této práci zmíněno právo na ochranu soukromí, potažmo právo na ochranu osobních údajů můžeme nalézt v Listině základních práv a svobod Evropské unie[3], která říká, že *„každý má právo na ochranu osobních údajů, které se ho týkají“* a dále že *„tyto osobní 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.“* Již ze samotného znění Listiny tedy můžeme vyčíst některá práva subjektu údajů a povinnosti správců a zpracovatelů. Obecné nařízení tedy ze znění Listiny vychází a užívá v ní obsažené záruky jako základní kameny pro vymezení práv a povinností. V odůvodnění Obecného nařízení nacházíme hned několik odkazů na Listinu, které se mj. vymezují tak, že 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.[4] Listina zakotvuje základní práva a svobody při aplikaci norem evropského práva. Přiznání právní závaznosti je spojováno s Lisabonskou smlouvou, která přinesla změnu znění článku 6 Smlouvy o Evropské unii, kterým byla Listině přiznána právní závaznost. Evropská unie tak získala vlastní interní nástroj identifikace a ochrany lidských práv. Listina představuje základní katalog lidských práv, zahrnující také právo na ochranu osobních údajů. Jednotlivé postupy a nástroje vymáhání nalézáme jednak v Obecném nařízení a dále tuto oblast formují judikaturní závěry soudů.[5]

Dosavadní právní úprava ochrany osobních údajů na evropské úrovni byla doposud upravena Směrnicí Rady 95/46/ES o ochraně osobních údajů z roku

[3] Listina základních práv Evropské unie 2012/C 326/02

[4] Bod 4 Odůvodnění Obecného nařízení

[5] STEHLÍK, Václav, Ondrej HAMUĽÁK a Michal PETR. *Právo Evropské unie: ústavní základy a vnitřní trh*. Praha: Leges, 2017. Student (Leges). ISBN 978-80-7502-277-6., s. 149

1995. Tato směrnice byla doplněna rámcovým rozhodnutím Rady[6], které jako obecný nástroj na úrovni Unie upravovalo ochranu osobních údajů v oblasti policejní a justiční spolupráce v trestních věcech. Dosavadní Směrnice tak vznikla před více než dvaceti lety, kdy neexistovaly sociální sítě či cloudová úložiště a z tohoto důvodu nemohla taková právní úprava vedle pokračujícího technického pokroku obstát. Jedním z největších nedostatků Směrnice tedy byla zastaralost právní úpravy. Dalo by se říci, že možnost revize stávajícího právního rámce přímo vyplývá i z primárního práva, tedy již ze zmiňované Listiny základních práv Evropské unie.

2.2 Proces přijímání Obecného nařízení

V souladu s běžnou praxí Evropská rada vyzvala Komisi, aby zhodnotila fungování nástrojů Evropské unie pro ochranu osobních údajů. Návrhy možných řešení se objevily v tzv. Stockholmském programu,[7] který nastínil cíle souhrnného řešení problémů na poli svobody, bezpečnosti a práva. Následně v listopadu 2010 Komise ve svém sdělení uvedla, *že „pokud jde o základní právo na ochranu osobních údajů, potřebuje Evropská unie komplexnější a jednotnější politiku.“* Jako hlavní důvody změny právní úpravy zde byly zmiňovány zejména technologický rozvoj a nutnost zohlednit vývoj digitální ekonomiky na celém vnitřním trhu Evropské unie. Stejně jako u většiny významnějších revizí, proběhla i tentokrát veřejná konzultace, která probíhala více než dva roky a to ve dvou fázích. První fáze se zabývala právním rámcem pro základní právo ochrany osobních údajů a ve druhé se již jednalo o komplexnější přístup Komise k ochraně osobních údajů v Evropské unii. Evropský parlament schválil v rámci usnesení v červenci 2011 zprávu,[8] ve které podpořil činnost Komise k reformě rámce pro ochranu osobních údajů.[9]

Následně Rada Evropské unie přijala v únoru 2011 závěry, ve kterých podpořila snahu Komise o tuto reformu. Evropský hospodářský a sociální výbor

---

[6] Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech

[7] Stockholmský program: Otevřená a bezpečná Evropa, která slouží svým občanům a chrání je (2010/C 115/01). In: *Evropská rada* [online]. 2010 [cit. 2018-08-05]. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:FULL:CS:PDF

[8] European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025 (INI))

[9] KOMÍNKOVÁ, Magda. Jak vznikalo Nařízení o ochraně osobních údajů (GDPR)?. *Euroskop.cz* [online]. 2018, 27.3.2018 [cit. 2018-08-05]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/

obdobně podpořil cíl Komise sjednotit pravidla uplatňování právní úpravy. Většina zúčastněných stran během konzultací souhlasila se stávajícími pravidly, nicméně uvedla, že je potřeba reagovat na rychlý vývoj nových technologií a globalizaci. Kritika směřovala zejména na nejednotnost ze strany hospodářských subjektů a dále složitost pravidel týkajících se mezinárodního předávání osobních údajů. Komise po řadě jednání představila návrh o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Před konečným přijetím návrhu byl dokument v průběhu čtyř let několikrát projednáván v institucích Evropské unie. V průběhu června 2015 dosáhla Rada po mnoha kolech jednání obecného přístupu, tedy politické dohody[10], na jejímž základě mohla zahájit jednání s Parlamentem. Dohody mezi Radou, Parlamentem a Komisí bylo v rámci trialogu dosaženo 15. prosince 2015. Následně Coreper dne 18. prosince 2015 potvrdil kompromisní znění dohodnuté pro jednání s Parlamentem. Dle požadavků Evropské rady bylo dohody dosaženo do konce roku 2015. Na začátku dubna 2016 na základě doporučení Výboru pro občanské svobody, spravedlnost a vnitřní věci pro druhé čtení schválil Parlament postoj Rady v prvním čtení bez pozměňovacích návrhů. K finálnímu podpisu došlo 27. dubna 2016.[11] Z dlouhé přípravy Obecného nařízení a níže uvedeného vyplývá, o jak významný mezník v rámci evropské ochrany osobních údajů se jedná.

Z výsledků hlasování o přijetí Obecného nařízení vyplývá, že pro jeho přijetí hlasovaly všechny členské státy kromě Rakouska, své výhrady vyjádřilo pouze několik členských států včetně České republiky. Co se týká jejího postoje k Obecnému nařízení, vyjádřila se v průběhu jednání tak, že oceňuje vyřešení řady problematických otázek, například vztahu k platným dohodám nebo posílení vzájemné spolupráce mezi dozorovými úřady. Česká republika však vyjádřila pochybnosti nad uplatňováním Obecného nařízení, pokud jde o správce v zahraničí, přičemž v takovém případě podle ní nemusí být ochrana osobních údajů dostatečná. Doslova se vyjádřila tak, že *„by to mohlo vést k falešnému pocitu jistoty mezi evropskými občany.“* Dále vyjádřila politování nad tím, že se Obecné nařízení příliš řídí dosavadní Směrnicí. Například nebylo možné nahradit

[10] Ochrana údajů: Rada se dohodla na obecném přístupu. In: *Rada Evropské unie* [online]. 2015 [cit. 2018-08-05]. Dostupné z: http://www.consilium.europa.eu/cs/press/press-releases/2015/06/15/jha-data-protection/

[11] KOMÍNKOVÁ, Magda. Jak vznikalo Nařízení o ochraně osobních údajů (GDPR)?. *Euroskop.cz* [online]. 2018, 27.3.2018 [cit. 2018-08-05]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/

kazuistickou kategorii „citlivé osobní údaje“ systematičtějším využitím přístupu, který je založený na posouzení rizika, ačkoliv skutečná citlivost osobních údajů a z ní vyplývající potřeba ochrany se může lišit podle způsobu zpracování.[12]

Česká republika dále vyjádřila znepokojení nad horními limity sankcí v kombinaci s nejasně vymezeným okruhem přestupků, týkajících se porušení ochrany osobních údajů. Mimo to mají správní pokuty ještě větší vliv na malé a střední podniky, které jsou často hnací silou inovací, neboť se odkazuje na pevnou částku i na částku stanovenou na základě ekonomické síly, podle toho, která je vyšší. Česká republika také vyjádřila politování nad tím, že se ve větší míře neuplatnil přístup založený na riziku, a že některými požadavky se na správce a zpracovatele uvaluje nadměrná administrativní a jiná zátěž. Dále se Česká republika domnívá, že adaptační období je nepřiměřeně krátké, neboť je třeba vyhodnotit a v případě potřeby pozměnit mnoho právních předpisů.[13]

Pro zajímavost přehlasované Rakousko namítalo, že v konečné navrhované podobě Obecné nařízení nedosahuje stupně ochrany ani na úrovni původní Směrnice. K právní formě nařízení se vymezuje tak, že tato není zvolena vhodně, protože nedává státům prostor tyto nedostatky „vykompenzovat“ prostřednictvím vnitrostátních předpisů, neboť ty budou upravovat pouze dílčí otázky. Míří tak zřejmě k tomu, že pokud by byla dána tato možnost, Rakousko by si upravilo některé okruhy ochrany osobních údajů přísněji, a to s ohledem na dosavadní stav. Domnívá se, že Obecné nařízení neposkytuje takovou úroveň ochrany osobních údajů, jaká byla před přijetím Obecného nařízení v Rakousku v soukromém sektoru dostupná.[14]

2.3 Právní forma Obecného nařízení

V rámci této práce se jeví jako vhodné osvětlit právní formu Obecného nařízení. Nařízení řadíme do okruhu sekundárního práva Unie. Představuje závazný právní akt, který má obecnou působnost. Do jisté míry ho lze připodobnit k vnitrostátnímu zákonu parlamentu členského státu. Je adresováno neurčitému počtu adresátů a má právní závaznost erga omnes. Závaznost se vztahuje ke všem jeho ustanovením a je přímo zakázáno, aby národní předpisy členských zemí dle

[12] Odůvodnění hlasování 7920/1/16 REV 1 (Interinsitutcionální spis: 2012/0011 (COD)). In: *Rada Evropské unie* [online]. 7.11.2016 [cit. 2018-08-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CONSIL:ST_7920_2016_REV_1&from=EN

[13] Tamtéž

[14] Tamtéž

své potřeby jeho znění jakkoliv měnily nebo modifikovaly. Obecná závaznost spočívá zejména v tom, že všechny státní, správní orgány i soudy jsou povinny nařízení aplikovat přednostně před národním právem. Tím se projevuje jedna ze základních zásad evropského práva, kterou představuje princip přednosti a nadřazenosti.[15] Tento princip přitom nenajdeme v žádném psaném prameni evropského práva[16], ale vyplynul poprvé až ze zcela zásadního rozsudku Soudního dvora van Gend & Loos[17], kde soud konstatoval, že přistoupením k zakládacím smlouvám, které založily nový právní řád, v jehož prospěch členské státy v určitých oblastech omezily svou suverenitu, plyne přednost aplikace norem evropského práva před národní právní úpravou. Tento princip se přitom vztahuje nejen na členské státy, ale i na jeho státní příslušníky. Tímto krokem soud stanovil ještě jeden zcela stěžejní princip evropského práva, a to tzv. bezprostřední účinek norem evropského práva. Jeho smyslem je ochrana státních příslušníků před neplněním povinností členských států, které pro ně vyplývají z norem evropského práva, a to za předpokladu, kdy při postupu členského státu hrozí podstatné narušení účinnosti evropského práva. A s tím i to, že subjekt, který se cítí takovým postupem poškozen, má v takovém případě právo se dovolat napřímo právní normy, která existuje mimo rámec vnitrostátního práva. Jednotlivci se tak mohou dovolávat svých práv, vyplývajících z evropského práva přímo u národních soudů.[18]

V této souvislosti lze zmínit také rozsudek Costa proti E.N.E.L.[19], který formuloval zásadu aplikační přednosti evropského práva před právem členských států, přičemž důsledkem tohoto rozhodnutí je nemožnost použití národních právních předpisů, které nejsou v souladu s ustanoveními evropského práva, a to ani v případě, že právní předpis členského státu je novější než evropská norma. Soudní dvůr vyvodil obdobný závěr také v případě Internationale Handelsgesellschaft[20], kde se vyjádřil tak, že jednotnost a účinnost práva

---

[15] FOREJTOVÁ, Monika a Michaela TRONEČKOVÁ. *Evropské právo v praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. Monografie (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-301-8, s. 55

[16] Pozn. s výjimkou čl. 288 Smlouvy o fungování EU

[17] Rozsudek Evropského soudního dvora ze dne 5. února 1963 N.V. Algemene Transport- en Expeditie Onderneming van Gend & Loos proti Nederlandse administratie der belastingten, věc 26/62

[18] De BÚRCA, G., CRAIG, P. EU Law: Text, Cases, and Materials. Oxford: Oxford University Press, 2011, ISBN: 978-0-19-927389-8, s. 270

[19] Rozsudek Soudního dvora ze dne 15. července 1964 Flaminio Costa proti E.N.E.L., věc 6/64

[20] Rozsudek Soudního dvora ze dne 17. prosince 1970, Internationale Handelsgesellschaft GmbH proti Einfuhr- und Vorratsstelle für Getreide und Futtermittle, věc 11/70

Společenství by byla omezena, pokud by byly při posuzování platnosti aktů vydaných orgány Společenství používány pouze normy nebo zásady vnitrostátního práva. Podle tohoto rozhodnutí může být otázka týkající se případného zásahu do základních práv aktem orgánů Společenství posouzena toliko v rámci samotného práva Společenství. Zavedení zvláštních posuzovacích kritérií, podléhajícím právním předpisům nebo ústavnímu pořádku určitého členského státu, by mělo tím, že by poškozovalo materiální jednotu a účinnost práva Společenství, za následek narušení jednoty společného trhu a ohrožení soudržnosti Společenství.[21]

Pro úplnost lze v této věci zmínit ještě rozsudek Simmenthal SpA.,[22] který přímou použitelnost vykládá i v souvislosti s tím, že každý vnitrostátní soudce, rozhodující v rámci své pravomoci má povinnost plně aplikovat právo Unie a chránit práva jednotlivců tím, že nepoužije ustanovení vnitrostátního předpisu, které by bylo s právem Unie v rozporu.[23] Zároveň se vyslovuje k přímé použitelnosti ve vztahu k principu jednotnosti, který je rovněž zcela zásadní a byl jedním z hnacích motorů pro vytvoření Obecného nařízení.

Současná roztříštěnost právních úprav ochrany osobních údajů v jednotlivých členských státech Evropské unie totiž vytvářela překážky pro další ekonomický rozvoj. Dosavadní právní rámec, založený Směrnicí, přestal být pro účelnou ochranu osobních údajů dostačující, a to zejména s ohledem na její formu. Směrnice je jedním z právních aktů Evropské unie, jejímž hlavním účelem je harmonizovat právní řády jednotlivých členských států. Nestanovuje však práva a povinnosti členským státům napřímo, ale pouze udává cíl, kterého mají členské státy dosáhnout a zakotvit ho do svých vnitrostátních právních řádů. Úkolem členských států tedy bylo přijmout požadavky, určené Směrnicí, ale dosažení žádoucích výsledků zůstalo v dispozici států samotných. Vlastní právní úprava byla poté aplikována skrze vnitrostátní právní předpisy.[24] Naproti tomu nařízení žádnou takovou implementaci nepřepokládá a je přímo použitelné a závazné v celém svém rozsahu.

---

[21] FOREJTOVÁ, Monika a Michaela TRONEČKOVÁ. *Evropské právo v praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. Monografie (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-301-8, s. 31

[22] Rozsudek Soudního dvora ze dne 9. března 1978 Amministrazione delle Finanze dello Stato proti Simmenthal SpA., věc 106/77

[23] FOREJTOVÁ, Monika a Michaela TRONEČKOVÁ. *Evropské právo v praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. Monografie (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-301-8, s. 32

[24] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. *Právo Evropské unie*. Praha: Leges, 2013. Student (Leges). ISBN 978-80-87576-53-3, s. 110

Směrnice jsou problematické zejména proto, že se uplatňují zprostředkovaně a zastřeně za vnitrostátním právem, jejich vědomé zohlednění není samozřejmostí a jejich použití vyvolává obtíže. Složitost nakládání se směrnicemi nutně přináší chyby při jejich uplatnění. Často se pak směrnice neuplatní vůbec. Nejistota ohledně uplatnění směrnicového práva podrývá autoritu práva Evropské unie jako celku. Nařízení určená pro přímé uplatnění jsou podstatně jednodušším právním nástrojem. Nahrazování směrnic nařízeními může mít zřetelné přínosy i v podobě zmírnění zátěže národních parlamentů, neboť při přímé aplikovatelnosti nařízení není třeba vytvářet prováděcí předpisy. Nicméně je na tomto místě nutno připomenout, že i nařízení potřebují doprovod práva členských států, neboť bez něj je jejich aplikace složitější. Členské státy pravidelně musí svými zákony ustavit či pověřit úřady a další instituce pro uplatnění nařízení. Taková nařízení tedy mají částečně směrnicový charakter, který se v textaci nařízení projevuje například slovy „pokud členský stát nestanoví jinak, platí..“ [25] K tomuto typu Obecné nařízení patří, neboť, jak bude osvětleno v této práci, v určitých oblastech dává členským státům možnost, aby určitá hlediska upravily ve svých vnitrostátních právních řádech.

Pokud bychom tedy porovnali jednotlivé dosavadní vnitrostátní právní úpravy ochrany osobních údajů v členských státech, nalezli bychom celou řadu odlišností, což způsobovalo problémy zejména u podnikatelských subjektů, které podnikaly na území dvou a více členských států. Z tohoto důvodu vyvstávala nutnost studovat jednotlivé vnitrostátní předpisy a zpracování osobních údajů jim podřídit. S tím souvisí i poněkud heterogenní postup dozorových orgánů v jednotlivých členských státech, který rovněž není pro efektivní ochranu osobních údajů žádoucí. V případně jednotné právní úpravy dochází ke snazšímu sbližování národních ekonomik členských států a k postupnému vytvoření jednotného digitálního trhu. Bude plně respektován jeden ze základních cílů evropského práva, a to princip volného pohybu osob, zboží a služeb, se kterým je transfer osobních údajů neodmyslitelně spjat. Lze očekávat, že i společnosti, pocházející z mimoevropských zemí, získají snadnější přístup na evropský trh, což lze hodnotit opět pozitivně. Současně bude ponechán českému i evropskému digitálnímu průmyslu dostatečný prostor pro vývoj inovativních a inteligentních obchodních modelů, které z obchodního hlediska umožní vytvořit životaschopný

[25] KŘEPELKA, Filip. Nahrazování směrnic nařízeními (důvody, skutečnost, možnosti). In: *Právník*. 03/2017, s. 215, 222-223

potenciál již existujícího obrovského množství dat, a to za současného dodržení principů ochrany osobních údajů.

Obecné nařízení dopadá na všechny země Evropské unie, avšak za vhodnější je třeba považovat širší označení evropský prostor. Jeho účinnost totiž dopadá i na státy Evropského hospodářského prostoru – Island, Norsko a Lichtenštejnsko, kde bude Obecné nařízení aplikováno tehdy, jakmile dojde k jeho inkorporaci do Dohody o Evropském hospodářském prostoru. Do té doby bylo nutné, aby tyto státy upravily své vnitrostátní předpisy. Pro efektivnější aplikaci bylo předpokládáno, že k tomuto včlenění dojde k 25. květnu 2018, tedy ke dni účinnosti Obecného nařízení ve státech Evropské unie.[26] V době tvorby práce k inkorporaci do Dohody o Evropském hospodářském prostoru již došlo, byť s drobnějším zpožděním.[27]

Obecné nařízení představuje milník v oblasti ochrany osobních údajů nejen v evropském prostoru, ale je možno říci, že se jedná o mezník v celosvětovém kontextu. Jeho aplikace totiž v jistých případech může překročit hranice evropského prostoru, k čemuž dochází velmi často. Teritoriální působnost Obecného nařízení dopadá na správce a zpracovatele, kteří jsou usazeni na území evropského prostoru nebo zde mají provozovnu. Obecné nařízení tak reaguje na rozsudek Soudního dvora ve věci Google Spain proti Mario Costeja González,[28] který odstranil pochybnosti při aplikaci evropské ochrany osobních údajů v případě provozovny správce.[29] Pro zajímavost lze zmínit, že i vymezení pojmu „provozovna“ bylo v rámci judikatury soudního dvora již řešeno.[30]

---

[26] Incorporation of the GDPR into the EEA Agreement [online]. In: . 13.4.2018 [cit. 2018-08-01]. Dostupné z: http://www.efta.int/EEA/news/Incorporation-GDPR-EEA-Agreement-508041

[27] Decision of the European Economic Area Joint Committee No. 154/2018 of 6 July 2018 amending Annex XI (Electronic communication audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement (2018/1022)

[28] Rozsudek Soudního dvora EU ze dne 13. května 2014 ve věci Google Spain SL, Google Inc. proti Agencia Española De Protección de Datos (AEPD), Mario Costeja González, věc C-131/12

[29] V této věci šlo mj. o vyřešení předběžné otázky, zda se uplatní evropské právo ochrany osobních údajů (v tomto případě ještě Směrnice) za předpokladu, že internetový vyhledavač je provozován společností, která sídlí ve Spojených státech a ve Španělsku vystupuje pouze skrze svoji dceřinou společnost Google Spain, která se zabývá také reklamou na internetu. Soud konstatoval, že s ohledem na nutnost zajistit odpovídající úroveň ochrany se předmětné právo uplatní.

[30] Rozsudek Soudního dvora ze dne 1. října 2015 Weltimmo, s.r.o., proti Nemzeti Adatbéfrlmi és Információszabadság Hatóság, věc C-230/14, ve kterém bylo zmíněno, že pod pojmem provozovna se předpokládá efektivní a skutečný výkon činnosti prostřednictvím stálého zařízení, a že právní forma takové provozovny, ať jde o pobočku nebo dceřinou společnost s vlastní právní subjektivitou, není rozhodující. Pokud je stejný správce usazen na území několika členských států, musí zajistit, aby všechny provozovny plnily povinnosti stanovení

Druhý typ místní působnosti Obecného nařízení, představuje situace, kdy správce či zpracovatel sice nemá na území evropského prostoru provozovnu, ale zpracovává osobní údaje subjektů údajů, které se nacházejí na území evropského prostoru, a zároveň činnost zpracování souvisí s nabídkou zboží nebo služeb bez ohledu na to, zda je od subjektů údajů požadována nějaká platba. V krajním případě se tak pod regulaci Obecného nařízení dostává v podstatě každý, kdo provozuje webové stránky přístupné z evropského prostoru, a to jako provoz elektronické služby, která provádí sběr IP adres v přístupových protokolech či sledování návštěvníků stránek skrze soubory cookie, javascriptů nebo podobných technologií, neboť tyto činnosti lze podřadit pod zpracování osobních údajů.[31] Činnosti správce také můžou souviset s monitorováním subjektů údajů. V obou těchto případech je tak ochrana osobních údajů subjektů údajů zajištěna.

Teritoriální aplikace Obecného nařízení je významná i z toho důvodu, že chrání osobní údaje všech osob, které z tohoto prostoru pocházejí, tedy osobní údaje nejen občanů Evropské unie. S tím bezpochyby souvisí i zvýšení právní jistoty, neboť se tak správci a zpracovatelé osobních údajů nemohou vyhnout důsledkům Obecného nařízení tím, že by zpracovávali osobní údaje mimo evropský prostor. Obecné nařízení se také užije v případě aplikace právního řádu členského státu na základě mezinárodního práva veřejného.

Rychlý technický pokrok však nebyl jediným hnacím motorem k vytvoření Obecného nařízení. V českém právním řádu doposavad řešil ochranu osobních údajů zákon o ochraně osobních údajů. Prakticky tedy došlo k tomu, že Obecné nařízení nahradilo jednotlivé vnitrostátní právní předpisy členských států, za splnění principu aplikační přednosti evropského práva. Doposud účinná právní úprava ochrany osobních údajů, obsažená v zákoně o ochraně osobních údajů, tak byla nahrazena právy a povinnostmi, vyplývajícími z Obecného nařízení. Za účelem úpravy některých aspektů vyplývajících z Obecného nařízení bude přijat adaptační zákon, který nahradí stávající zákon o ochraně osobních údajů. Za určitých okolností totiž Obecné nařízení předpokládá vnitrostátní úpravu, kterou budou upravena některá hlediska, týkající se národního dozorového orgánu, vložení ustanovení, kterým se ruší a mění některé vnitrostátní předpisy s ohledem

vnitrostátními právními předpisy, které se vztahují na jejich činnost, zejména s cílem vyloučit jejich obcházení.

[31] FÄRBER, Claus Dr. European General Data Protection Regulation to Apply from May 2018. *McDermott Will & Emery* [online]. 2016 [cit. 2018-02-16]. Dostupné z: https://www.mwe.com/en/thought-leadership/publications/2016/06/european-general-data-protection-regulation

na přijetí Obecného nařízení, upřesnění okruhu správců s povinností jmenovat pověřence apod.[32] Jeho účelem tedy není duplikovat články Obecného nařízení, ale pouze upravit tu část, kde byla ponechána možnost vnitrostátní modifikace některých otázek. Jisté rozpaky budí načasování přijetí tohoto prováděcího předpisu, neboť v době tvorby této práce je již Obecné nařízení v účinnosti, zatímco prováděcí zákon účinnosti ještě nenabyl, k čemuž nedošlo ani ke dni uzavření této práce. Prováděcí zákon však ve svých závěrečných ustanoveních počítá s nabytím účinnosti již v den jeho vyhlášení.

Nelze však opomenout určitou problematičnost současné situace právní úpravy ochrany osobních údajů v České republice, neboť původní zákon o ochraně osobních údajů je stále platným a účinným právním předpisem. Ačkoli ze stanovisek Úřadu může současný stav působit tak, že Obecné nařízení tento zákon nahradilo bez dalšího na základě principu aplikační přednosti, nelze „starý zákon" zcela opomíjet, a to zejména s ohledem na souhrn otázek, jejichž úpravu přenechává Obecné nařízení vnitrostátním právním úpravám členských států. Do doby účinnosti prováděcího zákona tak bude Česká republika setrvávat v určité právní dvojkolejnosti. Česká republika zároveň patří k posledním státům evropského prostoru, které nemají účinný prováděcí zákon.[33]

[32] Základní příručka k GDPR. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-01-24]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=3938

[33] Jak ukazuje i mapka, která je přílohou č. 1 této práce

3. Pojem osobní údaj

V rámci zpracování této práce nelze vynechat osvětlení pojmu osobní údaj, který je základním kamenem celé práce, neboť se Obecné nařízení vztahuje pouze na zpracování informací, které lze označit právě za osobní údaje. Zpracování jiných informací o osobách, nespadá pod Obecné nařízení, jejich ochrana je umožněna skrze ustanovení v části občanského zákoníku, týkající se práva na ochranu osobnosti.

Pojem osobní údaj poprvé definovala Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. ledna 1981[34] jako *„každou informaci týkající se identifikované nebo identifikovatelné fyzické osoby (subjektu údajů)“*. Tato formulace přetrvala bez větších změn až do současné doby, kdy ji zákon o ochraně osobních údajů obsáhl a zpřesnil, tak, že *„osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“* [35] Obecné nařízení charakterizuje pojem osobní údaj velmi obdobně, zpřesňuje však způsob identifikace subjektu údajů, kterým může být navíc identifikační číslo, lokační údaj nebo síťový identifikátor. Jedná se o reakci na nedostatečnost stávající právní úpravy v souvislosti s již zmiňovaným technickým vývojem, kdy nastalé otázky musely být řešeny pouze judikaturně. Pod pojem osobní údaj tak spadá i dynamická IP adresa, neboť v případě, že uživatel dané internetové stránky odhalí během připojení svoji totožnost, může provozovatel stránky uživatele identifikovat spojením jeho jména s IP adresou jeho počítače.[36] Obecné nařízení tedy ponechává definici beze změny, rozšiřuje jen výčet identifikátorů, který má s ohledem na co nejširší ochranu osobního údaje jednotlivce charakter demonstrativního výčtu.

Pokud hovoříme o subjektu údajů, pak jím je fyzická osoba, které se osobní údaje týkají. Právnické osoby pod tuto ochranu nespadají. Přichází tedy

---

[34] Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 115/2001 Sb. m. s. ze dne 28. ledna 1981

[35] § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

[36] Rozsudek Soudního dvora ze dne 19. října 2016 Patrick Breyer proti Spolkové republice Německo, věc C-213/15

v úvahu otázka, zda se Obecné nařízení vztahuje taktéž na fyzické podnikající osoby. K této problematice se již v minulosti vyjádřil Ústavní soud, když konstatoval, že u fyzických podnikajících osob, je nutné za rozlišovací kritérium považovat právě podnikatelskou činnost, přičemž údaje o ní nepožívají ochrany osobních údajů.[37] Tento názor však byl postupem času překonán, neboť podnikatelská činnost je úzce spjata se soukromým životem dané osoby a je proto obtížné informace pocházející z obou těchto sféro od sebe oddělovat. V zájmu zachování základních principů Obecného nařízení tak převažuje nutnost přiznat stejnou míru ochrany všem údajům o fyzické osobě, byť některé souvisejí spíše s její ekonomickou činností. Shodně tomu bude i u fyzických osob, které zastupují právnickou osobu.

Pro určení zda jde o osobní údaj či nikoliv je nutné posoudit vztah dané informace ke konkrétní identifikované nebo identifikovatelné osobě. Za osobní údaj můžeme tedy považovat jakoukoliv informaci, která vykazuje přiřaditelnost ke konkrétní osobě. V dané situaci pak není rozhodné, která forma byla pro zachycení této informace zvolena, zda elektronická, písemná, zvuková, fotografická apod. Při určení, zda se jedná o osobní údaj, můžeme vycházet z hodnocení pracovní skupiny WP29, která pod pojem osobní údaj podřadila informace vztahující se k soukromému a rodinnému životu jednotlivce, informace o jakémkoli druhu činnosti, kterou se jednotlivec zabývá, například informace o jeho pracovních vztazích nebo ekonomickém či společenském chování. Není přitom rozhodné, v jakém postavení se pak tato osoba nachází, např. v pozici zaměstnance, zákazníka, pacienta apod. Nezávisí ani na tom, zda uvedená informace je či není pravdivá. Pravidla ochrany osobních údajů dávají možnost ochrany i takových údajů, u nichž počítají i s tou možností, že dané informace nejsou pravdivé nebo ne zcela prokázané.[38]

Základní definice užívá ve vztahu k osobnímu údaji pojem identifikovaná či identifikovatelná fyzická osoba. Elementární rozdíl mezi oběma pojmy lze spatřovat v tom, zda je možné danou osobu identifikovat přímo či nepřímo. Obecné nařízení přitom výslovně osvětluje pouze pojem identifikovatelná osoba. Pro zdůraznění rozdílu je však na místě vymezit i pojem identifikovaná osoba.

---

[37] Nález Ústavního soudu ze dne 9. března 2004, sp. zn. Pl. ÚS 38/02

[38] *Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data* [online]. 20.6.2007, (01248/07/EN) [cit. 2018-02-03]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Z pohledu správce se jedná o takovou osobu, kterou může od ostatních osob odlišit napřímo, a to za využití údajů, které má sám k dispozici, bez použití jiných databází. Rozsah údajů, postačujících k identifikaci takové osoby však záleží na konkrétním případu. Zejména se bude jednat o situace, kdy posuzujeme subjekt údajů, nacházející se v úzce věcně či místně vymezeném prostoru. Typický příklad představuje subjekt údajů, žijící na malém městě, kde kombinace místa bydliště a jeho jména vytváří natolik jednoznačnou identifikaci této osoby, že není třeba využít jeho další osobní údaje. Stejně tomu bude například v případě zaměstnanců malé společnosti. Z technického pohledu tvoří prokazatelné identifikátory například rodné číslo nebo označení datové schránky.

Pro jednoznačné rozlišení identifikovatelné osoby musí správce využít kromě jemu dostupných údajů i údaje vedlejší, bez kterých není možné danou osobu rozlišit napřímo. Tyto vedlejší údaje přitom může získat například z vlastních databází, zpracovávajících osobní údaje za jiným účelem, nebo využije osobních údajů dostupných ve veřejných rejstřících. Při aplikaci právní úpravy ochrany osobních údajů však není až tak rozhodující, zda se jedná o identifikaci přímou či nepřímou, podstatná je možnost odlišení jednotlivce od jiných osob.

3.1 Zvláštní kategorie osobních údajů

Vedle „základního“ okruhu osobních údajů rozlišuje Obecné nařízení i tzv. zvláštní kategorii osobních údajů. Dosavadní právní úprava vykládá tuto podmnožinu osobních údajů obdobně, s tím, že ji nazývá pojmem citlivý údaj. Protože se jedná o termín přiléhavější a v našem právním řádu vžitý, lze předpokládat, že se bude pro tuto skupinu osobních údajů neformálně užívat i nadále. Na rozdíl od běžných informací o fyzických osobách jsou tyto osobní údaje zvláštní tím, že vypovídají o skutečnostech mnohem více invazivních a do soukromí dotčených osob mnohem více zasahujících, než zpracování jiných údajů. Z tohoto důvodu může zpracování z jejich samotné povahy vážně ohrozit základní právo subjektů na soukromí. Pro zpracování informací zvláštní povahy je stanoven přísnější režim, který se týká zejména účelů zpracování takových informací. Obecně je možné říci, že oprávnění ke zpracování této skupiny údajů je užší a omezuje se převážně na specifické situace. Zvláštní charakter zpracovávaných údajů by však pro daného správce či zpracovatele měl být hlavním korektivem při úvahách o tom, jaká je zapotřebí přijmout opatření k zabezpečení dat. Pro tyto situace se stanovují zvláštní právní důvody pro

zpracování takových údajů.[39] Jedná se zejména o výslovný souhlas, veřejný zájem nebo údaje výslovně zveřejněné subjektem údajů. Zvýšená ochrana se rovněž projevuje v souvislosti se sankčními ustanoveními Obecného nařízení a nutností zvýšeného zabezpečení takových údajů. Více o tomto tématu autorka zmiňuje ve čtvrté kapitole práce.

Za zvláštní kategorii považuje Obecné nařízení údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, dále pak také informace týkající se zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Obecné nařízení také nově neřadí do zvláštní kategorie osobních údajů údaj o národnostním původu a naopak rozšiřuje tuto kategorii vedle údaje o sexuálním životě fyzické osoby i o údaj o sexuální orientaci fyzické osoby. V komparaci se Směrnicí přibyly do zvláštní kategorie údajů také genetické a biometrické údaje. U těchto údajů však musí být splněna podmínka zpracování za účelem jedinečné identifikace fyzické osoby. Do zvláštní kategorie osobních údajů se tyto údaje budou řadit pouze tehdy, jestliže budou zpracovávány technickými prostředky nebo systémy umožňujícími identifikaci člověka. Český zákon o ochraně osobních údajů tyto informace do definice začlenil již v minulosti, a proto z tohoto pohledu nedochází k žádné změně. Výčet těchto údajů nápadně připomíná diskriminační důvody, vymezené v antidiskriminačním zákoně. Nejedná se o náhodu, neboť i ten vychází ze stejných základů unijního práva, konkrétně se jedná o výčet diskriminačních důvodů, uvedených v čl. 19 Smlouvy o fungování Evropské unie.

3.1.1 Osobní údaje týkající se rozsudků v trestních věcech a trestných činů

Komparací stávající právní úpravy a Obecného nařízení dojdeme k závěru, že údaje, týkající se rozsudků v trestních věcech a trestných činů nyní nespadají do zvláštní kategorie osobních údajů, ačkoli je zákon o ochraně osobních údajů řadil přímo mezi citlivé údaje. Neznamená to však, že by zákonodárce ochranu tohoto „citlivého“ osobního údaje opomněl. Obecné nařízení na ni odkazuje v samostatném článku, ačkoli není do taxativního výčtu zvláštní kategorie

[39] *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 60

osobních údajů zařazena, a dále ji upravuje speciální trestní směrnice.[40] V průběhu času se informace o trestné činnosti jako citlivého údaje v naší právní úpravě střídavě rozšiřovala a zužovala. Do dosavadního zákona o ochraně osobních údajů ho přinesl zákon č. 439/2004 Sb., tzv. euronovela, neboť před její účinností byl za citlivý údaj o osobě považován jakýkoli údaj o trestné činnosti osoby. Euronovelou se tato kategorie vymezila pouze na údaj o odsouzení za trestný čin, čímž došlo k zpřesnění do té doby neurčitého pojmu „údaj o trestné činnosti“. Současné pojetí pojmu tak vyznívá velmi úzce, neboť za citlivý údaj je považována pouze informace o odsouzení za trestný čin. Nezabývá se dalšími informacemi, týkajícími se například zastavení trestního stíhání podle § 307 trestního řádu nebo o narovnání dle § 309 trestního řádu.[41] Podle Obecného nařízení dochází opět k rozšíření, protože se tento přísnější režim vztahuje na zpracování jakýchkoliv osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření. Nový právní rámec tak bude zahrnovat i další informace o trestné činnosti osoby, zmíněné výše.

Nejasná může být výkladová situace s ohledem na údaj o bezúhonnosti dané osoby. S přihlédnutím k výkladu pojmu osobní údaj a elementárním důvodům zvýšené ochrany zvláštní kategorie osobních údajů, lze vyvodit závěr, že informace o bezúhonnosti do této kategorie nepatří. Podstatné hledisko představuje možnost zásahu nebo ohrožení soukromí dotčené osoby. Údaj o bezúhonnosti, tedy informace vypovídající o neexistujícím odsouzení, však žádné takové riziko nepředstavuje. Je-li však údaj o trestné činnosti dané osoby pozitivní, ať už z jakéhokoli důvodu, bude tato informace požívat ochrany dle zvláštní kategorie ochrany osobních údajů.[42]

Protože se jedná o oblast natolik specifickou a rozsáhlou, Obecné nařízení ji neupravuje a za účelem ošetření této problematiky, byla vytvořena samostatná trestní směrnice, která nese společné zásady a principy jako Obecné nařízení. Tato směrnice upravuje specifickou povahu policejní a justiční spolupráce v trestněprávních věcech a obsahuje zvláštní pravidla pro ochranu osobních údajů

---

[40] 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

[41] *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 60

[42] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě. Komentář*. Leges, 2018. ISBN 978-80-7502-288-2, s . 134

a jejich volný pohyb. Týká se jak přeshraničního, tak vnitrostátního zpracování osobních údajů příslušnými orgány členských států za účelem vymáhání práva, pod které se řadí prevence, vyšetřování, odhalování a stíhání trestných činů, anebo výkonu trestů jakož i ochrana a předcházení ohrožení veřejné bezpečnosti. Za cíl si stanovuje chránit právo jednotlivců na ochranu vlastních údajů a zároveň zaručit vysokou úroveň veřejné bezpečnosti. Nevztahuje se naopak na zpracování osobních údajů prováděné při výkonu činností, které nespadají do oblasti působnosti práva Unie či zpracování prováděné orgány, institucemi a jinými subjekty Unie. Trestněprávní směrnice nahrazuje již zmiňované Rámcové rozhodnutí Rady[43], které se věnovalo pouze zpracování osobních údajů přenesených nebo uveřejněných mezi členskými státy navzájem.[44] Protože však jde o směrnici, bude nutné její provedení, a to zejména novelami příslušných zákonů.[45]

[43] Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech

[44] VARVAŘOVSKÝ, Petr a Libor ZBOŘIL. Trestněprávní směrnice jako doplnění obecného nařízení na ochranu osobních údajů. *E-pravo.cz* [online]. 9.8.2018 [cit. 2018-08-20]. Dostupné z: https://www.epravo.cz/top/clanky/trestnepravni-smernice-jako-doplneni-obecneho-narizeni-na-ochranu-osobnich-udaju-108013.html

[45] Například zákona č. 273/2008 Sb., o Policii České republiky

4. Zpracování osobních údajů

4.1 Základní principy

Aby bylo možné hovořit o zpracování osobních údajů ve smyslu Obecného nařízení, je nutné definovat také pojem zpracování, který je nedílně propojen se samotným pojmem osobní údaj. K tomu, abychom mohli bez dalšího přistoupit k aplikaci Obecného nařízení, je tedy potřeba, aby se jednalo o osobní údaj jako předmět, se kterým je nakládáno a aby toto nakládání bylo natolik kvalifikovanou činností, kterou lze považovat za zpracování osobních údajů. Obě podmínky přitom musí být splněny kumulativně. Za zpracování osobních údajů pak není možné považovat jakoukoliv činnost nebo nakládání s osobními údaji. Obecné nařízení definuje pojem zpracování osobních údajů jako jakoukoliv operaci nebo soubor operací s osobními údaji, která je prováděna s osobními údaji nebo soubory osobních údajů s 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. Zmíněná definice se tak příliš neliší od dosavadní právní úpravy, kdy Obecné nařízení blíže specifikuje kvalifikované činnosti, spadající pod zpracování osobních údajů. Výčet kvalifikovaných činností je přitom demonstrativní, dává adresátovi právní normy alespoň základní představu o tom, které činnosti lze považovat zpracování osobních údajů.[46]

Obecné nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Uvedené vymezení záměrně vyznívá technologicky neutrálně právě s ohledem na to, aby zahrnulo co největší množství technologií, zpracovávajících osobní údaje, a to se zřetelem i na jejich budoucí vývoj. Velice často ale dochází k situaci, kdy jsou osobní údaje z nějakého důvodu zpracovávány pouze manuálně. V takovém případě se Obecné nařízení užije všude tam, kde jsou osobní údaje obsaženy v nějaké evidenci, nebo do ní mají být zařazeny. Osobní údaje požívají ochrany Obecného nařízení tehdy, jestliže jsou systematicky uspořádány podle daných

[46] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3, s. 55

kritérií nebo podle specifického klíče, a to i v případě, že nejsou pevně spjaty s elektronickým médiem a existují pouze v papírové podobě. Pokud není splněno hledisko evidence, neznamená to, že by tyto údaje nebyly nikterak chráněny. Paušálně je možné říci, že na zpracování osobních údajů, nespadajících pod ochranu Obecného nařízení, se nadále vztáhnou ustanovení občanského zákoníku, týkající se ochrany osobnosti, popřípadě se použijí další speciální právní předpisy, zabývající se ochranou obchodního tajemství, smluvní povinnosti mlčenlivosti nebo ochrany bankovního tajemství.[47]

Samo Obecné nařízení pak ze zpracování osobních údajů vyjímá ty činnosti, které nespadají do oblasti působnosti práva Evropské unie a činnosti vykonávané členskými státy, které lze podřadit pod společnou zahraniční a bezpečnostní politiku členských států. Zpracováním osobních údajů ve smyslu Obecného nařízení není ani takové zpracování, které provádí fyzická osoba v průběhu výlučně osobních či domácích činností. Z působnosti Obecného nařízení jsou vyňaty i činnosti prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Jak již bylo v této práci řečeno, takové zpracování je sice vyňato z působnosti Obecného nařízení, ale je upraveno v samostatné trestní směrnici.

4.2 Vztah správce a zpracovatele

Právní úprava umožňuje, aby na místo správce prováděla operace s osobními údaji subjektů i osoba od správce odlišná – zpracovatel. Tím může být fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje namísto správce. Zpracovatel nemusí provádět zpracování od začátku do konce, tedy veškeré operace, ale může provádět jen některou či některé činnosti související se zpracováním. Nemusí jít tedy vždy o subjekt, který osobní údaje shromáždil.[48]

Tak jako existuje celá řada právních titulů zpracování jako takového, vyvstává povinnost doložit právní důvod zpracování u zpracovatele pro správce, a tedy doložení původu zpracovatelského vztahu mezi těmito subjekty. V praxi bude nejčastěji docházet k využití osoby zpracovatele na základě smluvního

[47] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 66

[48] Důvodová zpráva k zákonu č. 101/2000 Sb., Sněmovní tisk 374/0

vztahu mezi správcem a zpracovatelem, a to na základě zpracovatelské smlouvy.[49] Typickým příkladem takového zpracovatelského vztahu je zpracování mezd účetní kanceláří pro zaměstnavatele, které jsou předány osobní údaje zaměstnanců dané společnosti za účelem zpracování mezd. Zpracovatelská smlouva musí mít písemnou formu, přičemž za akceptovatelnou lze považovat i elektronickou formu. Správce by měl pečlivě zvážit výběr zpracovatele, zejména s ohledem na dostatečnou odbornost a využít ke zpracování pouze takového zpracovatele, který je schopen zajistit uspokojivou záruku zavedení vhodných technických a organizačních opatření tak, aby zpracování probíhalo zcela v souladu s Obecným nařízením, jako by je prováděl sám správce. Obecné nařízení totiž přičítá správci objektivní odpovědnost za porušení, neboť se jedná o osoby určující zpracování osobních údajů. Není však vyloučen regresní nárok správce vůči zpracovateli.

Z tohoto důvodu je proto velmi důležité dostatečně určitě vymezit vzájemný vztah zpracovatelskou smlouvou. Obecně lze říci, že taková smlouva by měla obsahovat předmět, rozsah, povahu a účel zpracování, kategorii zpracovávaných osobních údajů a míru citlivosti, dobu zpracování, kategorie subjektu údajů a vzájemná práva a povinnosti zpracovatele a správce. Z praktického hlediska by autorka práce doporučila zařadit do těchto smluv také ustanovení, ukládající zpracovateli povinnost průběžně vyhodnocovat stav technických organizačních opatření k zabezpečení osobních údajů, posuzování vlivu zpracování na ochranu osobních údajů, povinnost být správci nápomocen zejména s ohledem na právo subjektu na výmaz či ohlašování porušení zabezpečení. Za velmi vhodné se jeví také stanovit povinnost zpracovatele umožnění provádění inspekcí a auditů ze strany správce a neméně důležité zavedení povinnosti mlčenlivosti pro všechny zaměstnance zpracovatele, kteří přicházejí do styku s údaji, poskytnutými správcem. Zpracování osobních údajů pro správce však může provádět i více zpracovatelů. Správce by při tom však měl zvážit, zda dokáže zajistit dodržování souladu s Obecným nařízením i v případě takového řetězení zpracovatelů. První zpracovatel může do zpracování zapojit další zpracovatele, avšak vždy s předchozím souhlasem správce. S přihlédnutím ke všem specifikům daného případu si autorka práce dovoluje doporučit, aby toto

[49] V cizích zdrojích označovaná jako data processing agreement

povolení mělo vždy konkrétní podobu pro specifickou fyzickou nebo právnickou osobu.[50]

Z pohledu zpracovatele je potřeba se zaměřit na to, aby byly ve smlouvě přesně specifikovány pokyny správce a s nimi spojené operace zpracovatele, které je oprávněn s osobními údaji provádět. Zpracovatel vystupuje v podřízeném postavení vůči správci a vyvstává mu povinnost osobní údaje zpracovávat pouze k účelu, k jakému mu byly svěřeny, a jen v souladu s pokyny správce. Za předpokladu, že by zpracovatel tyto pokyny nedodržel nebo překročil rozsah zpracování, se vystavuje riziku, že sám určí účel a prostředky zpracování a v daném okamžiku se stane správcem s vyvozením veškerých odpovědnostních důsledků s tímto souvisejících. V případě, že už jsou takové zpracovatelské smlouvy již uzavřeny, lze doporučit provedení revizí tak, aby bylo možné doložit soulad s Obecným nařízením.

Závěrem této podkapitoly lze zmínit, že zpracovatelská smlouva není jediným právním důvodem vztahu zpracovatele a správce. Právním základem může být i jiný právní akt, ačkoli se z hlediska četnosti se bude jednat bezpochyby o menšinové množství případů. Tímto jiným právním aktem může být zákon nebo podzákonný předpis, který pověří specifický subjekt zpracováním osobních údajů, např. Správa základních registrů je jako zpracovatel pověřena zpracováním osobních údajů, pocházejících ze základních registrů na základě zákona č. 11/2009 Sb., o základních registrech, přičemž správcem je v tomto případě Ministerstvo vnitra.[51] Budou-li v této práci popisovány povinnosti správce, uplatní se podle dané situace přiměřeně také na zpracovatele.

4.3 Zásady zpracování osobních údajů

Základními východisky ochrany osobních údajů představuje soubor základních zásad osobních údajů, které v sobě zároveň zahrnují elementární povinnosti správců a zpracovatelů osobních údajů. Mezi tyto zásady, které společně vytváří základy pro ochranu osobních údajů, se řadí zákonnost, korektnost, transparentnost, omezení účelu, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost. Soubor těchto zásad je přímo uveden v čl. 5 odst. 1 Obecného nařízení, přičemž všechna další ustanovení v něm obsažená

[50] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě. Komentář*. Leges, 2018. ISBN 978-80-7502-288-2, s . 240-244

[51] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 276

s nimi musí být v souladu. Správce také nese důkazní břemeno při jejich dodržování.

4.3.1 Zásada zákonnosti zpracování

Jednou z hlavních zásad zpracování osobních údajů je zákonnost jako hlavní předpoklad toho, aby bylo možné považovat zpracování osobních údajů za legální. Právní důvod zpracování totiž představuje možnost tyto osobní údaje vůbec zpracovávat. Správce může osobní údaje zpracovávat pouze na základě nějakého legitimního důvodu, přičemž tyto jsou obsaženy v čl. 6 odst. 1 Obecného nařízení. Zároveň musí dojít k naplnění podmínky, že zpracování osobních údajů dochází nejen v souladu s Obecným nařízením, ale také s právním řádem jako takovým. Zpracování se totiž děje vždy za nějakým účelem a právní důvod musí daný účel pokrývat. Právních důvodů zpracování může existovat i více, správce by však měl vzít v potaz, zda nakládání s osobními údaji s důvody zpracování plně koresponduje, resp. zda tento důvod pokrývá všechny operace správce, které s údaji provádí.

V průběhu času však může dojít k situaci, kdy správci odpadne jeden právní důvod ke zpracování osobních údajů subjektu. Za daného stavu musí posoudit, zda pro okruh údajů, které o subjektu zpracovává, postačuje jiný právní důvod. V opačném případě správci vyplývá povinnost, takové údaje o subjektu zlikvidovat. Může nastat i situace, kdy správce nikdy neměl legitimní právní důvod osobní údaje subjektu zpracovávat, a poté lze hovořit o nelegálním zpracování.

4.3.1.1 Souhlas se zpracováním osobních údajů

V dosavadní právní úpravě byl institut souhlasu se zpracováním osobních údajů dlouhodobě zakotven, ale v praxi často zcela nesprávně využíván. Podle dosavadního zákona o ochraně osobních údajů byl souhlas subjektu údajů se zpracováním jeho osobních údajů považován za nadřazený, ačkoli všechny právní důvody zpracování jsou na stejné úrovni a nelze některý z nich nad ostatní vyvyšovat, přičemž rovnost zůstala samozřejmě zachována i v Obecném nařízení. Zákon o ochraně osobních údajů stanovuje, že správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů a dále následoval výčet právních důvodů, pro které správce souhlas subjektu údajů nepotřebuje. Poněkud nešťastná formulace, uvedená v zákoně o ochraně osobních údajů, tak vedla k tomu, že

mnozí správci považovali za hlavní právní důvod zpracování osobních údajů právě souhlas subjektu údajů. Zároveň souhlas subjektu údajů jako jediný z právních důvodů zpracování předpokládá aktivní jednání subjektu údajů, tedy faktické udělení souhlasu se zpracováním údajů pro jeden nebo více účelů zpracování. Tím se také odlišuje od skupiny ostatních právních důvodů zpracování, neboť pro samotný souhlas není v Obecném nařízení explicitně přiřazen účel zpracování, a subjekt údajů ho uděluje pro konkrétní záměr správci.[52]

Souhlas se zpracováním osobních údajů je přesně definován Obecným nařízením jako jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením svolení ke zpracování svých osobních údajů. Tento právní důvod představuje spíše doplňkovou možnost k získání právního důvodu správci, který z Obecného nařízení přímo nevyplývá a správci tak nesvědčí právní důvod osobní údaje zpracovávat. Společně však musí být splněna podmínka, že i takový „dodatečný" právní důvod není v rozporu s Obecným nařízením nebo s ustanovením jiného zákona.[53]

Primární podstatou souhlasu se zpracováním osobních údajů je jeho svobodné a dobrovolné poskytnutí ze strany subjektu údajů. Subjekt není vázán žádnou povinností souhlas udělit a nemůže být za jeho neposkytnutí nijak postižen. Pro zhodnocení výše zmíněného kritéria je třeba posoudit, zda byl souhlas poskytnut skutečně svobodně a zda nebyla vůle subjektu při jeho udělení ovlivněna do té míry, že bychom nemohli hovořit o úmyslu subjektu údajů tento souhlas fakticky udělit. Jedná o častou nesprávnou praxi ze strany správců, kteří podmiňují poskytnutí produktu nebo služby subjektu údajů teprve tehdy, až jim udělí souhlas se zpracováním dalších osobních údajů, bezprostředně nepotřebným k plnění smlouvy, ke kterému mají zákonný právní titul. Mnohdy se souhlas objevuje na stránkách internetových obchodů, kde subjekt údajů nemůže dokončit objednávku zboží nebo služeb, aniž by zaškrtl políčko souhlasu se zpracováním osobních údajů. Souhlas se zpracováním osobních údajů nemůže a nesmí být podmínkou, která by sama o sobě v případě jeho neudělení znemožňovala

[52] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3, s. 67

[53] HORKÁ, Nikola. Souhlas se zpracováním osobních údajů ve světle nové legislativy. *E-pravo.cz*[online]. 2018, , 1-3 [cit. 2018-02-19]. Dostupné z: https://www.epravo.cz/top/clanky/souhlas-se-zpracovanim-osobnich-udaju-ve-svetle-nove-legislativy-106991.html

uzavření smluvního vztahu. Jedná se o zcela typický případ, kdy souhlas není udělen svobodně. Pokud naopak správce podmíní například získání slevy z ceny produktu nebo služby poskytnutím souhlasu se zpracováním osobních údajů nad rámec těch, které potřebuje k plnění smlouvy, nejedná se o porušení povinnosti správce. Subjekt údajů má v daném případě možnost se rozhodnout, zda tyto údaje poskytne či nikoliv, plnění smlouvy jako celku však tomuto souhlasu není podmíněno.[54]

Velmi často k tomuto problému dochází také v případě tzv. formulářových smluv, kde tvoří neoddělitelnou součást smlouvy obchodní podmínky, ve kterých je již včleněn souhlas subjektu údajů s poskytnutím osobních údajů nad rámec smlouvy. Subjekt údajů nemá operativní prostor pro to, aby mohl o podobě smlouvy diskutovat a tento souhlas po vlastním uvážení neposkytnout. Dostává se tak do situace výběru, zda podepíše smlouvu jako celek v pro něj nevýhodném znění, či se rozhodne souhlas neposkytnout, čímž nezíská danou službu nebo produkt. Udělení souhlasu se zpracováním osobních údajů má mít podobu aktivního jednání subjektu údajů, nikoli vyjádření nesouhlasu s předpokládaným souhlasem. Souhlas se zpracováním osobních údajů je projevem vůle subjektu údajů, tedy jednostranným právním jednáním, a nikoli dvoustrannou smlouvou mezi správcem a subjektem údajů. Uvedená situace nesplňuje i další kritérium udělení souhlasu, a to podmínku jeho odlišitelnosti. Je-li souhlas obsažen v obchodních podmínkách nebo jiném jednolitém textu, subjekt údajů nemusí být schopen ho od ostatního textu dostatečně odlišit a uvědomit si vážnost a možné důsledky, které vzniknou jeho poskytnutím. Aby mohl správce, který osobní údaje subjektu získal tímto způsobem, tyto i nadále zpracovávat, bude muset získat nový souhlas subjektu údajů, neboť dosavadní pozbývá platnosti. Uvedenou problematiku řešilo již výkladové stanovisko Úřadu pro ochranu osobních údajů, které však právě s ohledem na laxní přístup mnohých správců, nebylo v praxi vždy respektováno. [55]

Neméně důležitou povinností správce představuje doložení udělení souhlasu ze strany subjektu údajů. Například u elektronického získání souhlasu může mít později správce obtíže jeho získání prokázat. Zcela jednoznačně pak lze

---

[54] EßER, Martin, Philipp KRAMER a Kai VON LEWINSKI. *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze: Kommentar*. 5. Auflage. Carl Heymanns Verlag, 2017. ISBN 978-3-452-28841-7, s. 128-129

[55] Stanovisko Úřadu pro ochranu osobních údajů č. 2/2011, ve znění aktualizované verze z února 2014

říci, že správce by měl využít písemnou formu udělení souhlasu, právě s ohledem na to, že bude moci být v budoucnu vyzván, aby souhlas doložil. Subjekt údajů může svůj souhlas dát správci i ústně, avšak tento souhlas by měl být opět se souhlasem subjektu údajů zároveň nahrán pomocí audiozáznamu. Správce by měl být schopen prokázat vazbu mezi subjektem a uděleným souhlasem. Zároveň to ale neznamená, že by správce měl k doložení souhlasu shromažďovat více informací, než je nutné.[56]

Součástí souhlasu musí být i informace pro subjekt údajů, obsahující totožnost správce, účel zpracování, rozsah zpracovávaných osobních údajů a informace o tom, že subjekt údajů může svůj souhlas odvolat. Souhlas se uděluje vždy konkrétnímu správci nebo okruhu správců, s jejichž výčtem musí mít subjekt údajů možnost se seznámit. Z hlediska množství informací, které je správce povinen subjektu údajů poskytnout, lze doporučit, aby správci souhlas koncipovali jako samostatný dokument, čímž jednak splní podmínku oddělitelnosti a jednak veškeré informace o poskytnutém souhlasu budou vyjádřeny v jednotné formě. Subjektu údajů náleží právo udělený souhlas odvolat, přičemž toto odvolání nemá retroaktivní účinky, ale platí pouze do budoucna. O tomto právu musí být při udělení souhlasu poučen. Vhodné je souhlas doplnit také dobou, na kterou se souhlas uděluje, neboť Obecné nařízení žádný konkrétní časový úsek nestanovuje. Pracovní skupina WP29 doporučila jako vhodnou praxi souhlas po určité době obnovovat, kdy se opětovně poskytnou všechny informaci subjektu znovu.[57]

Autorka práce se však domnívá, že toto řešení není příliš šťastné, neboť uvedený postup by vyžadoval rozšíření administrativního aparátu správců, který by jednak musel „hlídat“ všechny souhlasy s ohledem na dobu, na kterou byly poskytnuty, a jednak řešit každý jednotlivý případ neobnovení souhlasu na další období ze strany subjektu údajů a nepřiměřeně tak správce zatížil plněním povinností z toho vyplývajících. Účelnější a pro správce efektivnější řešení představuje dostatečně jasně informovat subjekt údajů při prvním udělení souhlasu o jeho právech, zejména o právu souhlas odvolat, a nechat si udělit souhlas na dobu neurčitou, popř. po dobu trvání věrnostního programu, využívání služby apod. Ačkoli subjekt údajů požívá ochrany slabší smluvní strany, nelze

[56] *Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679*[online]. 28.11.2017, (17/EN/WP259) [cit. 2018-02-03]. Dostupné z: ec.europa.eu/newsroom/just/document.cfm?doc_id=48849, s. 19

[57] Tamtéž, s. 20

toto právo vykládat natolik extenzivně, že by se správce musel po nějaké době znovu „ubezpečovat“, zda udělený souhlas platí a zda má subjekt údajů nadále zájem takový souhlas poskytnout. A to i s ohledem na skutečnost, že po celou dobu trvání souhlasu náleží subjektu právo udělený souhlas odvolat.

Zejména důležitou informaci představuje účel a rozsah zpracování osobních údajů, se kterými má subjekt možnost se dopředu seznámit a předem svůj souhlas zvážit. Uvedením této informace dává správce určitou míru právní jistoty i sám pro sebe. V případě, že subjekt svůj souhlas jako takový či jen pro určitý účel zpracování odvolá, a zároveň nemůže správce poskytnuté osobní údaje zpracovávat na základě jiného právního důvodu, vzniká mu povinnost takové údaje zlikvidovat. Správným vymezením a formulací při udělení souhlasu tak může správce předejít mnoha komplikacím, které by v budoucnu mohly vzniknout. [58]

4.3.1.2 Další právní důvody zpracování osobních údajů

U dalších právních důvodů zpracování můžeme pozorovat zásadní rozdíl proti udělení souhlasu ze strany subjektu údajů, a to z hlediska projevu vůle subjektu údajů. Zatímco u právního důvodu poskytnutého souhlasu se vyžaduje aktivní jednání a přímý úmysl subjektu své osobní údaje poskytnout, u dalších právních důvodů zůstává subjekt pasivní a jeho osobní údaje jsou zpracovávány na základě zákonných právních důvodů. Je však třeba zmínit, že absence souhlasu subjektu údajů automaticky neznamená libovůli správce ve vztahu k rozsahu účelu zpracování a ani jeho povinnost případně prokázat, že ten který osobní údaj byl nezbytný pro konkrétní účel zpracování.

Jedním z nejčastějších právních důvodů zpracování představuje plnění ze smlouvy, který zároveň úzce souvisí se zásadou minimalizace údajů. Příkladem může být situace zákazníka, který si objedná oblečení skrze internetový obchod. Pro plnění smlouvy je z hlediska nutných údajů obhajitelné, požaduje-li prodejce od zákazníka jméno, příjmení, adresu, telefon a emailovou adresu, a to pro účely doručení zboží. Prodejce k uskutečnění nákupu nepotřebuje znát například datum narození kupujícího, neboť pro samotné plnění smlouvy to není podstatné. Dalším

[58] Article 29 Data Protection Working Party: Opinion 15/2011 on the definition of consent [online]. 13.6.2011, (01197/11/EN) [cit. 2018-02-03]. Dostupné z: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1308, s. 9-10, 13

právními důvody zpracování jsou plnění zákonem stanovené povinnosti, ochrana životně důležitých zájmů subjektu údajů a plnění úkolu ve veřejném zájmu nebo výkonu veřejné moci. V mnoha případech se zmíněné právní důvody zpracování prolínají a záleží tak na správci, aby správně stanovil, kterým právním důvodem danou kategorii zpracovávaných osobních údajů pokryje, nebo aby si se zpracováním nad rámec opatřil souhlas subjektu údajů. Správcem v dané situaci bude nejčastěji správní orgán např. finanční správy, obec, samosprávná komora aj.

Z hlediska interpretace nejzajímavějším a zároveň posledním zákonným důvodem jsou oprávněné zájmy správce. Jedná se po souhlasu se zpracováním osobních údajů o další velmi diskutovaný právní důvod zpracování, zejména s ohledem na skutečnou oprávněnost zájmu na straně správce. Ten totiž osobní údaje zpracovávat nemůže, pokud nad oprávněným zájmem převáží zájmy nebo základní práva a svobody subjektu údajů, jejichž osobní údaje mají být zpracovány. Důležité bude pro správce správně a dostatečně určitě charakterizovat oprávněnost zájmu, která se zároveň promítá do praktických stránek, neboť může přicházet v úvahu provedení testu proporcionality oprávněného zájmu správce na straně jedné a zájmů subjektu údajů na straně druhé. Dalším hlediskem je posouzení souladnosti oprávněného zájmu jak s ustanoveními Obecného nařízení, tak s právním řádem jako takovým. Typickým příkladem tohoto právního důvodu je využití kamerového zařízení v prostorách správce, kterým sleduje prostory prodejny, do které přicházejí zákazníci a další osoby, postavení do role subjektu údajů, jejichž obraz je kamerami snímán. Uvedené jednání chrání majetek správce i zákazníky v prodejně a zároveň nedosahuje takové intenzity zásahu do soukromí subjektu, že lze předpokládat správcův úspěch v testu proporcionality z pohledu oprávněnosti.[59] Za vhodné se jeví doplnit, aby správce zákazníky přicházející do obchodu na tuto skutečnost upozornil, typicky například viditelným vylepením upozornění, že prostor, do kterého zákazníci vstupují, je monitorován kamerovým systémem. Této problematice autorka vyčlenila speciální kapitolu 9.2.

4.3.1.3 Právní důvody zpracování zvláštní kategorie osobních údajů

V této práci již byla vymezena zvláštní kategorie osobních údajů, se kterou se pojí i speciální zpracování této skupiny osobních údajů. Základním rysem kategorie je negativní vymezení jejich zpracování, a to, že jejich zpracování je

[59] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 134-135

obecně zakázáno. V případě, že správce takové údaje potřebuje zpracovávat, musí právní důvod zpracování spadat pod jednu z výjimek obsažených v čl. 9 odst. 2 Obecného nařízení. Přestože se tedy fakticky jedná spíše o výjimky, jsou v této kapitole pojmenovány jako právní důvody zpracování citlivých údajů. Jak už vyplývá z jejich samotného výčtu, Obecné nařízení předpokládá úzkou propojenost s vnitrostátními právními předpisy, v českém právním prostředí např. se zákonem o ochraně veřejného zdraví, zákonem o pojistném na všeobecné zdravotní pojištění nebo zákonem o archivnictví a spisové službě. Tyto vnitrostátní právní předpisy podrobněji upravují právní důvody, které správce opravňují ke zpracování citlivých údajů.

Některé speciální právní důvody nápadně připomínají základní výčet primárních právních důvodů zpracovaní, obsažených v čl. 6 odst. 1, není tomu však náhodou, neboť správce potřebuje ke zpracování citlivých údajů s ohledem na důvěrnost informací zároveň splnit i některý z primárních důvodů zpracování. Pro účely srovnání například v případě výslovného souhlasu ke zpracování již nepostačuje konkludentní projev vůle subjektu údajů jako právní důvod zpracování, ale tento musí být vyjádřen zcela jednoznačně, například zatržením zaškrtávacího pole nebo jinou zcela explicitní formou. U plnění povinností a výkonu práv v oblasti ochrany důležitých zájmů subjektu údajů se stírá základní právní důvod zpracování a dále se rozšiřuje na situace ochrany i jiných osob, přičemž musí být zároveň splněna podmínka, že subjekt údajů není fyzicky způsobilý udělit svůj souhlas sám. V daném případě se pak kumulativní splnění primárního důvodu zdá až nadbytečné, neboť definice podle čl. 9 odst. 2 Obecného nařízení ji obsahuje nad rámec základní definice ve „zpřísněné“ podobě. Podobná situace je i u důvodů veřejného zájmu v oblasti veřejného zdraví, kde již samotný veřejný zájem vyplývá přímo z názvu právního důvodu. Přestože uvedená podmínka splnění i základního právního důvodu může vyznívat jako nadbytečná, v mnohých případech se jeví jako zásadní. Pro účely vědeckého výzkumu bude správce potřebovat ještě předchozí souhlas podle čl. 6 odst. 1 písm. a) Obecného nařízení, při sčítání obyvatelstva převáží povaha zpracování ve veřejném zájmu podle písm. e) apod. Závěrem této kapitoly je třeba říci, že splnění podmínky zpracování zvláštní kategorie osobních údajů nezbavuje správce povinnosti si zajistit elementární právní důvod zpracování podle čl. 6

odst. 1 Obecného nařízení, kdy si zákonodárce klade za cíl zajištění vyšších nároků na zajištění zpracování a s tím související ochrany citlivých údajů.[60]

4.3.2 Zásada korektnosti a transparentnosti

Správce by měl rovněž zachovávat korektnost a transparentnost, aby subjekt údajů měl nejen při poskytnutí osobních údajů, ale i po celou dobu, co jsou jeho osobní údaje zpracovávány, přehled nad rozsahem zpracování a měl nad touto činností kontrolu. S tím souvisí celá řada informačních povinností ze strany správce, zejména o hloubce zpracování osobních údajů nebo informování subjektu o závažných porušeních zabezpečení osobních údajů. Správce nesmí vůči subjektu údajů zastírat účel, pro který jsou osobní údaje zpracovávány. Přitom by měl dbát na ohleduplnost vůči subjektu údajů tak, aby zohlednil jeho subjektivní očekávání ohledně míry zpracování. Takové subjektivní očekávání se pak může zcela rozcházet s realitou, neboť např. běžní uživatelé internetu často ani netuší a nerozpoznají, jaké všechny údaje jsou o nich shromážděny, bez jejich aktivního přispění. Mělo by tedy dojít k nastolení rovnováhy mezi ochranou subjektu osobních údajů a zároveň efektivním využití dat pro správce.[61]

Na zásadu korektnosti bezprostředně navazuje zásada transparentnosti, neboť všechny informace směřující od správce k subjektu údajů přitom musí být předány v jednoduché, srozumitelné a snadno přístupné podobně, subjekt údajů musí být ze strany správce poučen o svých právech, možných rizicích zpracování i všech dotčených osobách, které mohou s jeho osobními údaji přijít do kontaktu. V určitých situacích, zejména z právního důvodu zpracování na smluvním základě také záleží na subjektu údajů, které své osobní údaje správci poskytne.

4.3.3 Zásada omezení účelu

Tato zásada úzce souvisí se zásadou zákonnosti. Každé zpracování osobních údajů činí správce s nějakým účelem a každý účel musí být podložen zákonným důvodem zpracování. Správce například uzavře se subjektem údajů smlouvu o koupi zboží skrze internetový eshop. Po dodání zboží ze strany subjektu údajů správci odpadá právní důvod zpracování za účelem plnění

---

[60] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě. Komentář*. Leges, 2018. ISBN 978-80-7502-288-2, s .79

[61] CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law 2016* [online]. 2016, 3-4 [cit. 2018-02-27]. Dostupné z: http://data-reuse.eu/wp-content/uploads/2016/01/International-Data-Privacy-Law-2016-Custers.pdf

smlouvy, může ale dále zpracovávat tyto údaje pro splnění povinné archivace, tedy ze zákonného důvodu. S osobními údaji pak může činit pouze takové operace, odpovídající tomuto právnímu důvodu. Pro správce se může jevit jako výhodné využít získané údaje o subjektu údajů i jiným způsobem, například pro marketingové účely, na základě čehož si při tvorbě objednávky zboží vyžádá souhlas subjektu údajů se zpracováním pro tento účel. Po splnění předmětu smlouvy mu tak zůstane kromě zákonného důvodu archivace i právní titul k marketingovým účelům. Podstatou této zásady tedy je, aby osobní údaje subjektu údajů mohly být zpracovány výhradně pro účel, k jakému byly získány a tomu musí odpovídat právní důvod správce k jejich zpracování.[62]

4.3.4 Zásada minimalizace údajů

Zásada minimalizace vychází z principu proporcionality a zároveň úzce souvisí se zásadou zákonnosti a omezení účelu. Zpracovávané údaje musí být přiměřené relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který mají být zpracovávány. Okruh informací tak musí být omezen na nutnou míru, odpovídající sledovanému účelu. Správce by se tak měl ujistit, že nemá o subjektu více informací, než kolik jich potřebuje pro splnění daného účelu, popř. zda tyto informace podřadí pod jiný účel zpracování. Základní otázkou pro správce je proč uvedené osobní údaje drží a k čemu je používá. Obvykle správce data zpracovává po určitých kategoriích nebo celcích. Například zaměstnavatel pro účely pracovní smlouvy nepotřebuje od zaměstnance znát údaje o rodinném stavu nebo pro určité pracovní pozice informace o zdravotním stavu.[63]

4.3.5 Zásada přesnosti

Další neméně důležitou zásadu představuje přesnost zpracovávání údajů, která opět velmi úzce souvisí se zásadou omezení účelu. Zpracovávané údaje lze považovat za nepřesné, jestliže jsou nesprávné nebo zavádějící ve vztahu k faktické skutečnosti a z tohoto důvodu nekorespondují s účelem zpracování. Správci vyplývá povinnost informace průběžně aktualizovat zejména tam, kde na přesnosti a aktuálnosti závisí další okolnosti, což může mít vliv na důsledky zpracování. Zaměstnavatel by si měl pro určité pozice zajistit přesně informace o

---

[62] EßER, Martin, Philipp KRAMER a Kai VON LEWINSKI. *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze: Kommentar*. 5. Auflage. Carl Heymanns Verlag, 2017. ISBN 978-3-452-28841-7, s.199-200

[63] Tamtéž, s. 208

dosaženém vzdělání nebo kvalifikaci zaměstnance. Typicky se bude jednat o řidičské oprávnění řidičů, kde se jeví jako zcela nezbytné v průběhu trvání pracovního poměru řidiče zkoumat, zda mu potřebné oprávnění nebylo odejmuto. Problematickou otázkou může být technická proveditelnost zajištění přesnosti údajů. Naopak v některých případech se může udržitelnost aktuálnosti dat jevit jako nežádoucí, zejména tam, kde jsou osobní údaje uchovávány ze statistických, archivačních nebo vědeckých důvodů.[64]

4.3.6 Zásada omezení uložení

Zásada omezení uložení je rovněž velmi úzce propojena se zásadou omezení účelu, neboť délka doby uchování osobních údajů závisí na účelu, pro který byly tyto údaje získány. Obecné nařízení nestanovuje žádnou minimální či maximální dobu, po kterou můžou být osobní údaje zpracovávány. Správce by měl provést revizi okruhu zpracovávaných informací a u každé kategorie určit po jak dlouhou dobu mají být uchovávány. Nežádoucí situace může nastat tehdy, jestliže správce uchovává údaje déle, než je nezbytně nutné, s čímž souvisí zajištění likvidace údajů, které už nejsou potřeba.[65] Typickým příkladem je sledování prodejny kamerovým systémem, kde po určité době odpadá další důvod jejich uchování, např. z důvodu ochrany majetku a možného zaznamenání krádeže v prodejně není nutné, aby správce jako provozovatel prodejny uchovával kamerové záznamy v řádu let. U některých kategorií informací by z hlediska jejich charakteru bylo naopak nežádoucí, kdyby byly zlikvidovány předčasně. Delší dobu uchování vyžadují informace zpracovávané pro archivní účely. V některých případech se pak osobní údaje uchovávají po neomezeně dlouhou dobu.

4.3.7 Zásada integrity a důvěrnosti

Každý správce by měl revidovat úroveň zabezpečení jím zpracovávaných kategorií osobních údajů tak, aby bylo možné odstranit případné nedostatky v této oblasti, přičemž by tak měl činit průběžně. Správce je povinen zajistit bezpečnost uchovávaných dat, aby nemohlo dojít k jejich neoprávněnému či protiprávnímu zpracování, jejich náhodné ztrátě, zničení nebo poškození. Úložiště by zároveň mělo být celistvé a natolik technicky vyspělé, aby odpovídalo postupnému

[64] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4, s. 63-64

[65] Tamtéž, s. 67-68

technologickému pokroku a dokázalo tak vzdorovat jeho možnému prolomení. Uvedenou problematiku již řeší zákon o kybernetické bezpečnosti, který stanovuje správcům zpracovávajícím údaje v rámci kybernetického prostředí, soubor bezpečnostních opatření, kterými mají bezpečnost údajů zajistit.[66] Obecné nařízení ukládá správci zavedení vhodných technických a organizačních opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Přitom je potřeba zajistit ochranu napříč všemi technologiemi a úložišti dat, nejen těch v kybernetickém prostoru, přestože se skrze tento zdroj uchovává a zpracovává nejvíce informací.

4.4 Ochrana osobních údajů dítěte v Obecném nařízení

Jak již bylo v této práci zmíněno, subjekt údajů požívá zvýšené ochrany slabší strany, neboť se předpokládá, že nemá nebo nemusí mít dostatek znalostí, týkajících se nakládání s jeho osobními údaji ani celkovými dopady zpracování. U dětí to platí obzvlášť, a proto kromě zvýšené ochrany zpracování osobních údajů, přiřadil zákonodárce rovněž zvýšenou ochranu zpracování osobních dat dítěte jako takové, neboť dítě si tím spíše nemůže dostatečně uvědomovat důsledky poskytnutí svých osobních údajů a jejich dalšího nakládání s nimi. Autorka ponechává stranou opět nešťastně zvolený český předklad Nařízení, který za dítě považuje všechny osoby mladší 18 let, ačkoli z pohledu například trestně právního by mělo terminologicky rozlišovat mezi dítětem a osobou mladistvou, popř. užít souhrnný pojem mládež. Pro účely této práce a zamezení dalších nejasností bude dále užíváno terminologie Nařízení, tj. užití pojmu dítě pro všechny osoby mladší 18 let.

Uvedená zvýšená ochrana však nepokrývá všechny případy zpracování osobních údajů dítěte, ale pouze takové, ke kterým dochází v souvislosti se službami informační společnosti přímo dítěti. V této souvislosti se jeví jako vhodné definovat pojem služby informačních společností, kterou se rozumí jakákoli služba informační společnosti, tj. každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb. Přitom se může jednat o službu poskytnutou na dálku bez současné přítomnosti stran nebo službu poskytnutou elektronicky, která je odeslaná z výchozího do cílového místa

[66] § 5 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

pomocí elektronického zařízení nebo službu poskytovanou na individuální žádost příjemce služeb.[67]

Obecné nařízení stanovuje podmínky pro využití služeb informační společnosti dítětem mladším 16 let, které k využití služeb potřebuje vyjádření souhlasu nebo schválení osobou, která za dítě zodpovídá, nejčastěji tedy zákonným zástupcem. Bude tedy na správci, aby si technicky zajistil a později mohl doložit, že za dítě udělila souhlas skutečně taková osoba, což může být často problematické. Vhodným doporučeným řešením situace je na straně správce označit, že uvedená služba může být využívána pouze osobami staršími 16 let, čímž se zbaví nutnosti později souhlas u mladších osob prokazovat.[68]

Obecné nařízení dává členských státům možnost věkovou hranici snížit až na 13 let, a to skrze prováděcí vnitrostátní právní předpis. Tato možnost vyvolala napříč Evropskou unií, ale i v České republice celou řadu diskuzí. Připravovaný adaptační zákon o ochraně osobních údajů počítá se snížením věkové hranice na 15 let. Ministerstvo vnitra, coby předkladatel návrhu zákona, navrhovalo snížení dokonce na 13 let. Dostalo se tak do rozporu s Radou vlády pro vědu a výzkum a některými dalšími rozporovateli, neboť ti požadovali zachování věkové hranice 16 let, popř. by souhlasili s jejím maximálním snížením na 15 let, s odkazem na § 35 či 37 občanského zákoníku.[69] Argumentovali zejména nedostatečnou volní a mravní vyspělostí třináctiletých dětí. Ministerstvo vnitra však odkázalo na to, že tato věková hranice v praxi bez problému obstála např. v USA a rovněž byla podle v té době aktuálních informací odsouhlasena v dalších 8 státech Evropské unie, např. v severských státech. Předkladatel návrhu zákona má za nepřiměřené, aby dítě mladší, avšak blízké věku 16ti let, potřebovalo souhlas svých zákonných zástupců např. k instalaci nebo využívání komunikační aplikace nebo sociální sítě. Zároveň Ministerstvo dodává, že takové dítě je již mnohdy trestně odpovědné, může legálně pracovat a poznamenalo, že i civilní soudy ve věcech péče o dítě berou v potaz názor dítěte staršího 12ti let.[70]

---

[67] Pojem služba informační společnosti blíže vymezuje Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti

[68] Consultation: Children and the GDPR guidance. *Infomration Commisssioner´s Office* [online]. 2017 [cit. 2018-02-23]. Dostupné z: https://ico.org.uk/about-the.../children-and-the-gdpr-guidance, s. 29

[69] Zákon č. 89/2012 Sb., občanský zákoník

[70] Předkládací zpráva návrhu zákona o zpracování osobních údajů a Vypořádání připomínek k návrhu zákona o zpracování osobních údajů. *Ministerstvo vnitra* [online]. 2017 [cit. 2018-02-22]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

Ačkoli Obecné nařízení umožňuje snížit věkovou hranici pro platné on-line souhlasy na 13 let, přestože samo stanovuje subsidiární hranici 16 let, je nutné vzít v úvahu problémy a rizika hrozící v souvislosti s užitím informačních technologií, zejména co se týká nelegálního obsahu, kyberšikany apod. Současně nelze odhlédnout od reálného života společnosti, kdy děti běžně užívají mobilní telefony a zasílají textové zprávy, takže omezování například emailových služeb, sociálních sítí nebo podobných způsobů komunikace se v některých situacích může stát snadno nepřiměřeným. Je-li dítě daného věku způsobilé k udělení souhlasu, mělo by být zároveň způsobilé i k jeho odvolání, případně k uplatnění dalších práv – např. práva na výmaz.[71]

Autorka práce se názorově ztotožňuje s tímto výkladem, tedy je pro snížení věkové hranice na 15 let, avšak má za to, že daná možnost členských států upravit danou oblast rozdílně vytváří překážky pro sjednocení právní úpravy a vystupuje proti smyslu Obecného nařízení jako celku. Například pro provozovatele sociálních sítí vyvstane opět nutnost zkoumat jednotlivé vnitrostátní právní předpisy, aby bylo možné zjistit, od kolika let si dítě může založit svůj účet samo a v kterých státech ve stejném věku bude potřebovat souhlas zákonného zástupce. Lze zmínit, že Úřad pro ochranu osobních údajů neměl k určení věkové hranice žádných připomínek.

[71] Důvodová zpráva k § 7 vládního návrhu zákona o zpracování osobních údajů cit. dne 20.6.2018, s. 61-62

5. Práva subjektů údajů

Obecné nařízení charakterizuje ucelený soubor práv subjektů údajů. Práva subjektů údajů představují neoddělitelnou součást ochrany osobních údajů v případech, kdy dochází k jejich zpracování, neboť subjekt údajů vystupuje ve vzájemném vztahu se správcem jako slabší strana. Často totiž dochází k tomu, že subjekt údajů nemá možnost ovlivnit, zda jeho osobní údaje budou zpracovány či nikoliv. Musí tak požívat speciální ochrany, kterou mu zaručuje ucelený katalog práv subjektů údajů, charakterizovaných v této kapitole.

Vymezení práv subjektů údajů samozřejmě není novinkou, práva subjektů údajů při zpracování obsahovala už Směrnice a tato práva byla transponována i do zákona o ochraně osobních údajů. Obecné nařízení si klade za cíl práva subjektů údajů posílit, což byl také jeden z hlavních důvodů jeho přijetí. Zavádí do praxe několik novinek v této oblasti, například zcela nové právo na přenositelnost.

5.1 Právo na informace

5.1.1 Transparentnost poskytnutí informace

Subjekt údajů vystupuje vůči správci ve slabším postavení, na což Obecné nařízení reflektuje hned na několika místech svého znění. Tato skutečnost se projevuje možná nejvíce u poskytování informační povinnosti správce vůči subjektu údajů. Stanovuje správci povinnost splnit tuto informační povinnost vůči subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků. Cílem tohoto ustanovení je, aby subjekt údajů byl zcela obeznámen se způsoby zpracování svých osobních údajů, a aby byl schopen porozumět sdělení správce. Představuje tak podstatnou podmínku efektivní ochrany osobních údajů zejména proto, že na základě uvedených informací se subjekt údajů může sám na ochraně svých osobních údajů podílet. Tedy v prvé řadě se svobodně rozhodnout, zda za daných podmínek své osobní údaje poskytne či se domáhat nápravy, nejsou-li jeho osobní údaje zpracovávány v souladu s právní úpravou. V případě, že informační povinnost není splněna ze strany správce řádně, může to mít vliv i na platnost souhlasu se zpracováním osobních údajů, neboť projev vůle subjektu údajů se zpracováním může být považován za zcela legitimně udělený pouze tehdy, pokud byly subjektu údajů předem dány veškeré relevantní informace,

týkající se zamýšleného zpracování osobních údajů a je mu tak umožněno se svobodně a vědomě rozhodnout, zda se souhlas se zpracováním svých osobních údajů za těchto podmínek udělí. V případě, že jsou informace poskytnuty úplně, avšak ne zcela srozumitelnou formou, může být situace ze strany dozorového úřadu posouzena tak, jako by informační povinnost správce nebyla řádně splněna.[72]

Povinnost plnění informační povinnosti transparentní formou se přitom uplatňuje při všech situacích, kdy správce nějakým způsobem informuje subjekt údajů. Jedná se o například o situaci, kdy správce získá osobní údaje od subjektu údajů pro účely plnění obchodního závazku včetně případu získání souhlasu nebo při plnění oznamovací povinnosti v případě bezpečnostního incidentu. Srozumitelnost poskytované informace lze zajistit nejen volbou jednoduchých formulací sdělení, ale také vhodným grafickým zpracováním textu. Za vhodné se jeví také užití FAQ, tedy zpracovaní problematiky do otázek a odpovědí či využití hypertextových odkazů například v zápatí emailu, obsahující odkaz na informační povinnost na internetových stránkách. Správce by měl být schopen věrohodným způsobem prokázat, že informační povinnost splnil, jakým způsobem a popřípadě jaká opatření přijal, což souvisí se zásadou odpovědnosti správce.

Informace a sdělení poskytuje správce písemně či jinými prostředky. Typicky se tak děje skrze elektronická média, ať už prostřednictvím emailu či mobilní síť, přičemž za vhodnou formu je rovněž považováno splnění informační povinnosti skrze webové stránky správce.[73] Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby. Tedy je to právě subjekt údajů, kdo volí způsob komunikace se správcem, například položí-li dotaz v oblasti ochrany osobních údajů písemnou formou, měla by být i odpověď od správce v písemné podobě.

5.1.2 Splnění informační povinnosti podle původu osobních údajů

Podle původu můžeme osobní údaje rozdělit na dvě kategorie, a to na ty, které byly získány přímo od subjektu údajů a na ty, které se ke správci dostaly jiným způsobem. Za situace, kdy osobní údaje poskytuje správci subjekt údajů

[72] Rozhodnutí Úřadu pro ochranu osobních údajů č.j. 26/05/SŘ- OSČ, č.j. 50/05/SŘ-OSČ, č.j. 70/05/SŘ-OSČ. Úřad *pro ochranu osobních údajů* [online]. 2013 [cit. 2018-08-11]. Dostupné z: https://www.uoou.cz/k-plneni-informacni-povinnosti/d-1596

[73] Výslovně se o tomto vyslovuje také vládní návrh prováděcího zákona v § 17 odst. 1

sám, například typicky za účelem plnění smlouvy, musí již v okamžiku získání těchto údajů správce poskytnout subjektu údajů určitý okruh povinně sdělovaných informací. Jedná se o totožnost a kontaktní údaje správce nebo jeho případného zástupce, byl-li ustanoven pověřenec, pak i jeho kontaktní údaje. Dále musí správce sdělit informace o účelech zpracování a v případě, že je právním titulem zpracování oprávněný zájem správce, tento rovněž odůvodnit. Za předpokladu, že správce předává tyto údaje dalším osobám, typicky zpracovateli na základě zpracovatelské smlouvy, je povinen uvést tohoto příjemce a není-li možné tuto osobu konkretizovat, pak alespoň kategorii takových příjemců. Má-li správce v úmyslu předávat osobní údaje do zemí mimo evropský prostor, pak musí uvést tuto skutečnost v rámci splnění informační povinnosti, a to společně s uvedením garancí o odpovídající ochraně, například na základě rozhodnutí Evropské komise či vhodných záruk. Je také nutné připomenout, že v tomto případě není vyžadováno aktivní sdělení ze strany subjektu údajů. Tyto údaje mohou být získány od subjektu údajů bez jeho aktivního přičinění. V případě, že je to nezbytné pro zajištění spravedlivého a transparentního zpracování, je nad rámec výše uvedeného správce povinen poskytnout také údaje o době, po kterou budou osobní údaje zpracovávány. Neví-li správce přesně, pak lze tento časový úsek vymezit například dobou trvání smlouvy.[74]

Poměrně široce Obecné nařízení vymezuje splnění informační povinnosti na úseku poučení subjektu údajů o jeho právech, zejména také o možnosti odvolat souhlas, je-li tento právním titulem ke zpracování nebo právo podat stížnost u dozorového orgánu. Dále by měl subjekt údajů informovat o tom, že poskytování osobních údajů představuje zákonný či smluvní požadavek a případně také skutečnost, že dochází k automatizovanému rozhodování, včetně profilování. Pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než pro který byly shromážděny, poskytne subjektu údajů ještě před tímto dalším zpracováním informace. Výjimka ze splnění informační povinnosti se uplatní tehdy, jestliže subjekt údajů již byl v minulosti řádně poučen.

Druhou kategorii poskytování informací subjektu údajů představuje situace, kdy osobní údaje nebyly získány přímo od subjektu údajů, ale například od jiného správce či z veřejného rejstříku. Nad výše zmíněný okruh poskytovaných informací musí správce sdělit i kategorie dotčených osobních

[74] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě. Komentář*. Leges, 2018. ISBN 978-80-7502-288-2, s . 158-159

údajů, tedy například i to, zda se jedná o zpracování zvláštní kategorie osobních údajů. Pokud se jedná o splnění informační povinnosti, je-li to nezbytné pro zajištění spravedlivého a transparentního zpracování, nad výše uvedené okruhy poskytovaných informací, uvede správce rovněž zdroj, ze kterého osobní údaje pocházejí, popřípadě, zda je získal z veřejných zdrojů. Návrh prováděcího zákona také počítá s tím, že správce může při zpracování osobních údajů pro novinářské, akademické, umělecké či literární účely odložit nebo odepřít subjektu údajů sdělit zdroj, ze kterého osobní údaje pocházejí, je-li to potřebné k ochraně zdroje a obsahu informací. [75]

V kategorii osobních údajů získaných odjinud než od subjektu údajů se také liší časový horizont poskytnutí takových informací. Informační povinnost musí správce v tomto případě splnit v přiměřené lhůtě po získání osobních údajů, nejpozději však do jednoho měsíce s ohledem na konkrétní okolnosti. V případě, že dochází ke komunikaci se subjektem údajů, pak nejpozději v okamžiku první komunikace a v případě, že jsou tyto osobní údaje zpřístupněny jinému příjemci, pak při prvním zpřístupnění.

Správce není povinen poučovat subjekt údajů v případě, že subjekt údajů těmito informacemi již disponuje a správce informační povinnost v úplném rozsahu splnil. Dále tehdy, pokud by to bylo nemožné nebo by to vyžadovalo nepřiměřené úsilí, to platí zejména v případě zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Správce také nemusí plnit informační povinnost, pokud osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství. Posledním případem je získávání či zpřístupnění výslovně stanovené právem Unie či členského státu, včetně zákonné povinnosti mlčenlivosti.

Platí při tom zásada, že správce či zpracovatel by měl výkon práv subjektů údajů usnadňovat, nikoli ztěžovat. Například údaje správce by měly být snadno dostupné, při komunikaci se subjektem údajů by měl volit srozumitelnou formu a podobně.

5.2 Právo na přístup k osobním údajům

Subjekt údajů má právo po správci žádat informaci, zda zpracovává jeho osobní údaje a v případě kladné odpovědi má povinnost sdělit rozsah

[75] § 18 odst. 1 vládního návrhu prováděcího zákona, sněmovní tisk č. 138

zpracovávaných osobních údajů – zejména účelu zpracování, kategorie dotčených osobních údajů, příjemců, zdroji, informaci, zda dochází k automatizovanému zpracování, plánované doby zpracování a poučení o právech subjektu údajů podobně jako tomu bylo u vymezení informační povinnosti. Jedná se tak o právo subjektu údajů, které vzniká až na základě jeho aktivního podnětu, nicméně správce si pro tyto případy musí připravit vhodné zázemí. To se děje zejména tím, že si v rámci záznamů o činnostech zpracování stanoví okruh zpracovávaných osobních údajů a také všechny oblasti, ve kterých tyto osobní údaje zpracovává. Jakmile tedy subjekt údajů uplatní své právo na přístup, správce má již přesnou představu, kde všude se osobní údaje v rámci jeho vnitřních postupů zpracování nacházejí. Vhodné je také si dopředu stanovit jak bude postupováno, až některý subjekt údajů své právo uplatní, tedy proškolit zaměstnance o tom, jak postupovat nebo vytvořit formuláře pro příjem žádostí subjektů údajů. Právo na přístup se přitom vztahuje i na zpracování osobních údajů, které proběhlo v minulosti s ohledem na posouzení procesu zákonnosti zpracování osobních údajů. Měl by však být brán zřetel na zátěž, kterou taková rešerše v mnohých případech správci přináší.[76]

5.2.1 Žádosti subjektů údajů

Součástí práva na přístup je také právo subjektu údajů podávat ke správci či jeho pověřenci žádosti. Ty se budou v praxi nejčastěji týkat žádosti o poskytnutí informace o zpracovávaných osobních údajích. Pravidla pro vyřizování žádostí uvedená v této podkapitole, lze nicméně zobecnit pro všechny typy žádostí ze strany subjektů údajů, ať už se bude jednat o žádost o přenesení osobních údajů či o jejich výmaz. Poskytnutí informací musí proběhnout bezplatně – typicky podle článků 13 a 14 Obecného nařízení, v případě, že se jedná o první kopii.[77]

Jak již bylo v této kapitole řečeno, způsob komunikace se správcem obvykle určuje subjekt údajů, a to i v oblasti podávání žádosti. Správce by měl odpověď zaslat ve stejné formě, v jaké ji obdržel – listinná podoba, skrze datovou schránku, email a podobně. Právě s ohledem na ochranu osobních údajů by měl správce bezpečně identifikovat žádající subjekt, a to právě s ohledem na ochranu osobních údajů. Rovněž tím předchází možné budoucí důkazní tíži na své straně.

[76] Rozsudek Soudního dvora ze dne 7. května 2009 College van burgmester en wethouders van Rotterdam v. M.E.E. Rijkeboer, věc C-553/07

[77] PAAL, Boris a Daniel PAULY. *Datenschutz-Grundverordnung: Beck´sche Kompakt-Kommentare*. C.H. Beck, 2017. ISBN 978-3-406-69570-4, s. 196-197

Měl by si tedy prověřit totožnost osoby, která projevila vůli takovou žádost zaslat. To může v praxi činit potíže, proto lze doporučit správcům, aby si zajistili vhodný způsob ověření, například požádat subjekt údajů o zaslání žádosti se zaručeným podpisem a podobně. Subjekt údajů je sice tím, kdo určuje způsob komunikace, nicméně správce může vhodným způsobem navést subjekt údajů k jemu nejpřijatelnější formě komunikace – například na svých webových stránkách připravit speciální formulář.

Vyjádření k žádosti subjektu údajů musí správce zaslat bez zbytečného odkladu, nejpozději však do jednoho měsíce ode dne obdržení žádosti. Buď této žádosti vyhoví a splní požadavek subjektu údajů bez dalšího nebo může žádost odmítnout s tím, že je povinen subjekt údajů informovat o důvodech odmítnutí. Například proto, že žadatelem je třetí osoba, která nemá právo tyto informace požadovat či je žádost zcela nesrozumitelná. Za vhodnější se v takovém případě jeví vyzvat subjekt údajů k doplnění žádosti, stejně tak jako v případě nedostatečné identifikace subjektu údajů. Stejně by měl správce postupovat také tehdy, jestliže je od počátku jasné, že s pořízením odpovědi na žádost vzniknou neúměrně vysoké náklady nebo se nejedná o první žádost subjektu údajů za poslední dobu. Správce by si měl v takovém případě nechat od subjektu údajů předem odsouhlasit, zda je srozuměn s výší daného poplatku.

Z praxe časté jsou rovněž případy, kdy si zpracování odpovědi na danou žádost může vyžádat delší časový úsek. Na tyto případy Obecné nařízení pamatuje a udává správcům možnost lhůtu prodloužit o další dva měsíce. Avšak i v tomto případě by měl subjekt údajů obdržet informaci o prodloužení lhůty s řádným odůvodněním. Posoudí-li správce žádost jako neodůvodněnou, pak by ji měl zamítnout ve lhůtě jednoho měsíce a tuto lhůtu dále neprodlužovat.
Správcům lze doporučit, aby vedli dokumentaci podaných žádostí a odpovědí na ně a aby zavedli interní postupy tak, aby bylo účinným způsobem a včas na žádosti reagováno.

5.3 Právo na opravu a doplnění

Jedna ze zásad, která tvoří součást Obecného nařízení, je zásada přesnosti. Aby bylo zpracování osobních údajů efektivní, musí být zpracovávané osobní údaje udržovány v aktuální podobě. S tím souvisí i právo subjektu údajů, aby správce bez zbytečného odkladu opravil nepřesné údaje, či aby tyto osobní údaje doplnil. Na druhé straně je i ve správcově zájmu, aby zpracovával přesné a

kompletní údaje. Může tak s ohledem na účely zpracování požádat subjekt údajů o kontrolu aktuálnosti jeho osobních údajů, například v rámci přihlašovací aplikace na stránkách správce či v rámci emailu. Právo na opravu je výslovně zakotveno již Listinou základních práv a svobod Evropské unie.[78]

5.4 Právo na výmaz

Jinak zvané také jako „právo být zapomenut“ představuje další, nikoli však nové právo subjektu údajů, které bylo obsaženo rovněž v dosavadní právní úpravě. Významným okamžikem bylo v této souvislosti uznání existence práva na výmaz po zveřejnění rozsudku ve věci Google Spain[79], který vymezil právo jednotlivce požadovat po správci opravu, výmaz zejména v případě, že se jedná o nepřesné nebo neúplné údaje a dále právo vznášet proti tomuto zpracování námitky z důvodu posouzení oprávněného zájmu správce.[80] V této souvislosti je však potřeba rozlišit, zda se jedná o situaci, kdy správce je povinen osobní údaje vymazat ze své vlastní povinnosti – například ztratil-li právní titul ke zpracování určitého okruhu osobních údajů nebo údajů jako celku, nebo je povinen údaje vymazat na základě žádosti subjektu údajů, kterému se věnuje tato podkapitola. Prostá žádost subjektu údajů k výmazu ze strany správce však nestačí, a to zejména s ohledem na celý systém a fungování zpracování osobních údajů. V daném případě musí být splněn některý z důvodů pro výmaz na žádost subjektu údajů, uvedený v Obecném nařízení, například když subjekt odvolá udělený souhlas a správce nemá jiný právní důvod pro zpracování osobních údajů.

Jak již bylo zmíněno, výmaz by měl za určitých okolností provést sám správce při plnění základních zásad Obecného nařízení, nicméně může dojít k tomu, že správce je měl vymazat z vlastní iniciativy, ale z nějakého důvodu tak neučinil, k čemuž dochází typicky tehdy, když správce zpracovává osobní údaje protiprávně, tj. bez právního titulu zpracování nebo již osobní údaje, které byly shromážděny pro určitý účel, nejsou potřebné.

---

[78] BUCHNER, Benedikt a Jürgen KÜHLING. *DS-GVO Datenschutz-Grundverordnung: Kommentar*. C. H. Beck, 2017. ISBN 978-3-406-70212-9, s. 399-400

[79] Rozsudek Soudního dvora EU ze dne 13. května 2014 ve věci Google Spain SL, Google Inc. proti Agencia Española De Protección de Datos (AEPD), Mario Costeja González, věc C-131/12

[80] Article 29 Data Protection Working Party: Guidelines on the implementatiion of the court of justice of the European union judgment on „Google Spain and inc v. Agencia Espanola de Protección de datos (AEPD(and Mario Costeja González“ [online].26.11.2014, (14/EN; WP225) [cit. 2018-09-5]. Dostupné z: http://www.dataprotection.ro/servlet/ViewDocument?id=1080

Při uplatnění práva na výmaz se více než kde jinde uplatňuje princip proporcionality v souvislosti s posouzením zájmu subjektu údajů, jehož údaje jsou zpracovávány, ve vztahu k zájmu správce, nebo veřejnému zájmu. Ochrana práv subjektů údajů tak nemůže být bezbřehá a vždy bude v daném případě potřeba zkoumat, zda za určitých okolností není subjekt údajů povinen toto zpracování strpět.

Obecné nařízení stanovuje z uplatnění práva na výmaz výjimky, neboť v určitých situacích i přes existenci práva subjektu údajů na výmaz převažuje veřejný zájem – například při ochraně veřejného zdraví, při výkonu práva na svobodu projevu a práva na informace, pro účely archivace ve veřejném zájmu nebo pro účely vědeckého a historického výzkumu. V tomto smyslu je zajímavým případem zpracování osobních údajů, pocházejících z veřejných rejstříků. V této souvislosti již Soudní dvůr řešil předběžnou otázku ve věci možnosti výmazu údajů o osobě z veřejných rejstříků, kdy se přiklonil k názoru, že veřejný zájem na zachování právní jistoty, vyplývající z úplnosti údajů ve veřejných rejstřících, převládá nad právem subjektu údajů tyto údaje vymazat.[81]

Zvláštní výjimkou je také uchování údajů pro účely určení, výkonu nebo obhajobu právních nároků správce, který však bude muset v odpovědi na žádost subjektu údajů dostatečně odůvodnit, zejména s ohledem na zásadu nezbytnosti a minimalizace údajů. Cíle veřejného zájmu mohou platně odůvodnit zasahování do soukromí jednotlivce pouze tehdy, je-li to stanoveno zákonem a není-li to nepřiměřené vzhledem ke sledovanému cíli. Vždy musí dojít k posouzení nezbytnosti a k aplikaci výjimek přistoupit tehdy, jestliže daného cíle není možné dosáhnout jinak než zpracováním předmětných osobních údajů. Tento obecný princip se přitom uplatní nejen u práva na výmaz, ale všude tam, kde se posuzuje veřejný zájem ve vztahu ke zpracování.[82]

Právo na výmaz má však širší dopady. Správce, který zveřejnil osobní údaje za současného splnění podmínek, podmiňujících povinnost správce takové údaje vymazat, musí o žádosti subjektu údajů na jejich výmaz informovat další správce, kteří tyto osobní údaje zpracovávají. Z pochopitelných důvodů se jedná pouze o prostou povinnost tyto správce informovat, nikoli o povinnost na jejich

---

[81] Rozsudek Soudního dvora ze dne 9. března 2017 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatore Mannimu, věc C-398/15

[82] Rozsudek Soudního dvora ze dne 20. května 2003 Österreichischer Rundfunk aj., spojené věci C-465/00, C-38/01 a C-139/01 (Urteil des Gerichtshofes vom 20. Mai 2003, Österreichischer Rundfunk und andere, Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01)

straně výmaz zajistit. Pouhá informace o žádosti o výmaz však nezakládá jiným správcům bez dalšího povinnost tyto údaje vymazat, jelikož mohou disponovat vlastním právním titulem pro zpracování. Pokud tedy správce takovou informaci dostane, měl by s ní nakládat tak, jako by jej o výmaz požádal sám subjekt údajů, a v dané konkrétní situaci posoudí, zda jsou v jeho případě splněny podmínky pro výmaz či nikoli.[83]

5.5 Právo na omezení zpracování

Právo na omezení zpracování představuje další právo subjektu údajů, které vzniká až na základě iniciace z jeho strany, typicky skrze podání žádosti. Způsob podání žádosti i reakce správce probíhá stejně, jako tomu bylo u podání žádosti na výmaz osobních údajů. Předpokladem pro uplatnění práva na omezení zpracování může být situace, kdy správce řeší požadavek subjektu údajů, a do doby vyřešení omezí zpracování údajů, kterých se žádost týká – typicky když subjekt údajů požádal o ověření přesnosti zpracovávaných údajů nebo když správce vyřizuje podanou námitku subjektu údajů. V mezidobí se zpracování omezí, což prakticky znamená, že s těmito osobními údaji nebudou prováděny žádné operace zpracování, vyjma uložení těchto údajů. Naproti tomu zcela vyloučen je výmaz osobních údajů, který představuje rovněž operaci zpracování a se kterým souvisí i další dvě podmínky omezení zpracování. V obou případech by správce mohl údaje vymazat. Obecné nařízení v této souvislosti popisuje případ, kdy je zjištěno, že správce zpracovával osobní údaje v rozporu se zákonem, ale subjekt si výmaz z nějakého důvodu nepřeje, zároveň však souhlasí s omezením zpracování. Posledním případem, kdy může dojít k omezení zpracování, je situace, kdy správce osobní údaje již nepotřebuje, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků.

Obecné nařízení definuje situace, při kterých musí dojít ze strany správce k omezení zpracování, a to za předpokladu, že se neuplatní některá z výjimek, které představuje souhlas subjektu údajů, určení, výkon nebo obhajoba právních nároků, důvody ochrany práv jiné fyzické či právnické osoby nebo z důvodu důležitého veřejného zájmu Unie nebo některého členského státu. Omezení zpracování končí tehdy, jestliže pominou důvody, na základě kterých správce zpracování omezil. Aby mohl být výkon práv subjektů údajů řádný a zpracování osobních údajů probíhalo efektivně, vzniká správci informační povinnost vůči

[83] NULÍČEK, Michal. Právo být zapomenut. *Bulletin advokacie*. 2017(06).

všem příjemcům, kterým osobní údaje zpřístupnil, a to nejen ve vztahu k uplatnění práva na omezení zpracování, ale i v rámci uplatňování práva na výmaz či opravu.

5.6 Právo na přenositelnost údajů

Toto právo představuje zásadní novinku, která v dosavadní právní úpravě neměla ekvivalent. Do Obecného nařízení bylo vloženo ve snaze podpořit volný pohyb osobních dat v evropském prostoru, zejména k usnadnění přechodu mezi různými poskytovateli služeb a zároveň zvýšit soutěživost mezi správci. Právo na přenositelnost obsahuje dvě práva současně. Subjekt údajů má právo získat osobní údaje, které se ho týkají, a které správci poskytl, a to ve strukturovaném, běžně používaném a strojově čitelném formátu a zároveň právo tyto údaje předat jinému správci. Pokud je to technicky proveditelné, má subjekt údajů právo na to, aby jeho osobní údaje byly předány přímo jedním správcem druhému správci.

První zmíněné právo se velmi podobá právu na přístup, které již bylo v této kapitole popsáno, v této souvislosti však nejde jen o sdělení okruhu zpracovávaných údajů, ale o jejich faktické zpřístupnění, a to ve stanovené podobě. Právo na přenositelnost tak doplňuje právo na přístup, kdy dává subjektům údajů snadný způsob, jak mohou spravovat a znovu využívat osobní údaje. Rozsah osobních údajů takto poskytnutých je však užší, neboť je možné poskytnout jen ty osobní údaje, které se přímo týkají subjektu údajů a zároveň které subjekt údajů poskytl správci.

Druhá část zahrnuje právo takové osobní údaje převést od jednoho správce ke druhému, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Přínosem je zejména posílení pozice spotřebitele, který není vázán např. na aktuálního poskytovatele služeb a dochází ke kontrolovanému a zabezpečenému způsobu přenosu na základě iniciace ze strany subjektu údajů. Správce uskutečňující transfer přitom není a z logiky věci ani nemůže být odpovědný za nakládání s předanými osobními údaji ze strany přijímacího správce. Zejména s ohledem na to, že na rozdíl od poskytnutí osobních údajů zpracovateli, tuto osobu nevybírá, volí ji subjektu údajů, a proto tato odpovědnost tíhne na tomto správci. Přenositelnost údajů nezakládá automaticky možnost správci dané údaje vymazat a nemá rovněž vliv na původní lhůtu pro uchování dat, předaných podle práva na přenositelnost. Subjekt údajů může svá práva uplatnit kdykoli po celou dobu zpracování. Stejně tak, chce-li subjekt údajů uplatnit právo na výmaz,

nemůže správce argumentovat právem na přenositelnost jako důvodem pro odložení nebo odmítnutí požadovanému výmazu. Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen. Zároveň výkonem práva na přenositelnost nesmí být nepříznivě dotčena práva třetích osob.[84]

V neposlední řadě je třeba zmínit, že podmínky pro uplatnění práva na přenositelnost budou splněny tehdy, jestliže se jedná o zpracování prováděné automatizovanými prostředky, netýká se tedy např. papírových kartoték, neboť jeho naplnění by pro správce představovalo neúměrnou zátěž a mnohdy by bylo až nemožné.[85] Současně k výkonu práva na přenositelnost dochází tehdy, jestliže je zpracování založeno na uděleném „prostém" souhlasu ke zpracování osobních údajů či výslovném souhlasu se zpracováním zvláštní kategorie osobních údajů, a nebo je zpracování nezbytné pro splnění smlouvy.

Ačkoliv se jeví, že právo na přenositelnost představuje pro subjekt údajů pouze samé výhody, může tomu být i naopak, protože výkon práva na přenositelnost pro něj může představovat značné riziko, zejména s ohledem na to, že dostává do svého zařízení, leckdy pouze ledabyle či vůbec chráněného, lehce zpracovatelné agregované údaje o své osobě. Bylo by proto vhodné, aby správci při využití práva na přenositelnost současně informovali subjekt údajů o možných rizicích, které z něj pro něj plynou, a doporučili zvýšenou míru opatrnosti při nakládání se souborem obsahujícím stažené údaje.[86]

5.7 Právo vznést námitku proti zpracování

Zejména v situacích, kdy subjekt údajů nemá možnost ovlivnit, zda jeho údaje budou zpracovány, mu dává Obecné nařízení do rukou nástroj v podobě práva vznést proti tomuto zpracování námitku. Je tedy patrné, že podání námitky se bude vztahovat na úzký okruh aktivně legitimovaných subjektů údajů, a to ve vztahu k právnímu titulu zpracování správce.

V případě, že je právním titulem oprávněný zájem nebo plnění úkolu na základě oprávněného zájmu či plnění výkonu veřejné moci, je povinen provést tzv. balanční test, na základě kterého bude tento zájem posouzen v porovnání se

---

[84] *Article 29 Data Protection Working Party: Guidelines on the right to data portability*[online].13.12.2016, (16/EN; WP 242 rev. 01) [cit. 2018-09-05]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099, s. 5,6,7

[85] Tamtéž, s. 8

[86] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3, s. 139-140

zájmy subjektu údajů. Jestliže má subjekt údajů za to, že v daném případě jeho zájem převažuje, může podat proti takovému zpracování námitky. Vyřízení námitek má pravidla velmi obdobná jako při podání žádosti ze strany subjektu údajů, které již v byly v této práci blíže rozvedeny. Během vyřizování námitky musí správce zpracování omezit, tedy osobní údaje budou pouze uloženy u správce. Pokud po posouzení daného případu dojde správce k závěru, že jeho oprávněný zájem převažuje nad zájmy subjektu údajů, musí tento závěr dostatečně odůvodnit a v každém případě nese důkazní břemeno takové oprávněnosti.

Druhý typ námitek představuje námitka proti zpracování pro účely přímého marketingu. Vznese-li subjekt údajů námitku, musí správce přestat osobní údaje pro tento účel zpracovávat bez dalšího. V obou výše zmíněných případech však správce musí subjekt údajů výslovně upozornit na právo podat námitku a to tak, aby toto upozornění bylo uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.

Třetí typ námitek se uplatní v případě, že zpracování probíhá pro účely vědeckého nebo historického výzkumu či pro statistické účely. Posuzovanými hledisky bude na jedné straně zájem subjektu údajů nezpracovávat jeho osobní údaje k tomuto účelu, proti veřejnému zájmu na straně druhé se současným posouzením nezbytnosti takového zpracování.

5.8 Práva subjektu údajů v souvislosti s automatizovaným zpracováním

Jak již bylo v této práci zmíněno, automatizované zpracování představuje soubor takových operací, které jsou prováděny pouze technologickými prostředky bez zásahu člověka, a zároveň mají zásadní dopady do života subjektu údajů. Z tohoto důvodu stanovuje Obecné nařízení soubor ochranných opatření, spočívajících například ve splnění informační povinnosti nebo povinnosti provést analýzu DPIA. Nad to dává Obecné nařízení subjektu údajů možnost, aby nebyl předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracovaní, včetně profilování. V této souvislosti uvádí Obecné nařízení dovětek „výhradně“ tedy takové automatizované zpracování, které probíhá jako rozhodovací proces zcela bez lidského vlivu. Dopady na subjekt údajů přitom mohou být dvojí typu, a to buď právní např. přiznání či odmítnutí určité zákonem garantované sociální dávky, nebo neprávní účinky spočívající zejména v

dotěrnosti postupů profilování v souvislosti s cílenou reklamou. Například osoba ve finančních potížích vystavená inzerátům on-line hazardu, která je pobízena těchto nabídek využít, přičemž není vyloučena možnost, že tím zapříčiní další dluh.[87]

Toto automatizované individuální rozhodování má de facto podobu všeobecného zákazu, tak jako tomu bylo dle předchozí právní úpravy. Pokud není splněna některá z výjimek, pak správce nemůže zpracovávat údaje způsobem, popsaným v tomto článku Obecného nařízení. První výjimku představuje situace, kdy je takové zpracování nezbytné k uzavření nebo plnění smlouvy – typicky například v bankovním sektoru při vyřizování úvěru.

Druhou výjimkou z generálního zákazu představuje povolení založené právem Unie nebo členského státu, přičemž do této kategorie může spadat použití pro účely monitorování a prevence podvodů a daňových úniků nebo zajištění bezpečnosti a spolehlivosti služby poskytované správcem.[88]

Poslední výjimku tvoří souhlas subjektu údajů, a to v podobě výslovného prohlášení. Samozřejmostí ze strany správce by pak mělo být splnění obecných podmínek pro udělení souhlasu se zvýšeným důrazem na dostatečné informování subjektu údajů, zahrnující poučení o druhu činnosti s vysvětlením významu a předpokládaných důsledků zpracování, ale také schopnost udělený souhlas doložit. Zákonodárce si byl vědom rizik, které automatizované zpracování pro subjekt údajů přináší, zejména v případě udělení souhlasu nebo při plnění smlouvy, a proto správci nad rámec výše zmíněného ukládá správci v těchto dvou případech provést vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů. Toto opatření zahrnuje minimálně právo obdržet lidský zásah ze strany správce, právo vyjádřit svůj názor a právo napadnout takové rozhodnutí. Sem se dle recitálu řadí s ohledem na konkrétní okolnosti daného zpracování zavedení vhodných matematických nebo statistických postupů profilování, zavedení technických a organizačních opatření, která zajistí opravu faktorů vedoucích k nepřesnosti osobních údajů a minimalizaci rizika chyb. K automatizovanému rozhodování a profilování založeného na zvláštních kategoriích osobních údajů se recitál vymezuje tak, že by mělo být povoleno

---

[87] *Article 29 Data Protection Working Party:* Guidelines on Automated individual decision-making and Profiling for purposes of Regulation 2016/679 [online].3.10.2017, (17/EN; WP251) [cit. 2018-09-17]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=47742, s. 9-11

[88] Bod 71 recitálu Obecného nařízení

pouze za určitých podmínek. Tím je jednak výslovný souhlas nebo je takové automatizované rozhodování nezbytné z důvodu významného veřejného zájmu na základě práva Evropské unie nebo členského státu, a které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních lidských práv a zájmů subjektu údajů.[89]

5.8 Omezení práv a povinností

Článek 23 Obecného nařízení je pravděpodobně jedním z nejdůležitějších ustanovení, co se týče individuálních úprav a změn na úrovni jednotlivých členských států. Těm totiž umožňuje přijmout celou škálu výjimek z práv a povinností stanovených Obecným nařízením. Cílem tohoto článku je umožnit úpravu práva osobních údajů v poměru k jiným právům či veřejným zájmům. Jakkoliv je právo na ochranu osobních údajů podstatné, stále je nutné proporcionálně vyvažovat neméně důležitými zájmy, zejména s těmi veřejnými. Takové omezení lze vztáhnout na práva a povinnosti vymezené v článcích 5, 12 až 22 a 34 Obecného nařízení. Tyto výjimky je možné uplatnit v právu Evropské unie i v právních řádech členských států skrze legislativního opatření.[90] Taková omezení předpokládá zákon o zpracování osobních údajů zejména v souvislosti se zajištěním obranných a bezpečnostních zájmů České republiky, přecházení, vyhledávání nebo odhalování trestné činnosti, zajištění veřejného pořádku nebo jiného důležitého cíle obecného veřejného zájmu Evropské unie v oblasti měnové, daňové či v oblasti veřejného zdraví. Dále předpokládá omezení některých práv a povinností v souvislosti s ochranou nezávislosti soudů a soudců nebo dohledové, kontrolní či regulační funkce spojené s výkonem veřejné moci.[91]

---

[89] Bod 71 recitálu Obecného nařízení

[90] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 264-265

[91] § 11 vládního návrhu zákona o zpracování osobních údajů cit. dne 18.9.2018, sněmovní tisk č. 138

6. Povinnosti správce

V této práci byla dosud detailně popisována role subjektů údajů, tedy fyzických osob, jejichž osobní údaje jsou zpracovávány. Pokud hovoříme o zpracování osobních údajů, pak neméně důležitým subjektem je správce, který určuje účel a prostředky zpracování, tedy provádí zpracování a odpovídá za něj. Správci a rovněž také zpracovateli vyplývá z Obecného nařízení celá řada povinností, souvisejících s nakládání s osobními údaji. Mnoho z těchto povinností bylo zmíněno již v předchozí kapitole, kde na jedné straně je dáno právo subjektu údajů a na druhé straně povinnost správce či zpracovatele výkon tohoto práva zajistit.

6.1 Odpovědnost správce

Jedním ze základních principů Obecného nařízení je princip odpovědnosti správce. Ten se projevuje jednak v povinnosti doložit soulad zpracování osobních údajů s Obecným nařízením a jednak s povinností být tento soulad schopen prokázat. První hledisko zahrnuje zejména povinnost s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavést vhodná technická a organizační opatření, aby byl správce schopen doložit, že zpracování je prováděno v souladu s Obecným nařízením. Protože vymezení technických procesů zajištění tohoto souladu by již přesáhlo právní hledisko zpracování této práce, odkazuje autorka pro orientaci v této problematice na stanovisko pracovní skupiny WP29 v oblasti cloud computingu[92], které i přes specifické pojetí poskytování cloudových služeb dobře poslouží pro vymezení základního rámce technických a organizačních předpokladů k zajištění souladu zpracování.

Z právního pohledu důležitější představuje druhé hledisko principu odpovědnosti správce, spočívající v povinnosti doložit soulad zpracování. Vyvstává tak potřeba vést pečlivou dokumentaci po celou dobu zpracování osobních údajů, která správci umožní i s odstupem času prokázat soulad zpracování, v určitých případech také po skončení zpracování. Jak již bylo

[92] *Article 29 Data Protection Working Party: Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing*[online]. 22.9.2015, (2588/15/EN; WP232) [cit. 2018-05-05]. Dostupné z: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

zmíněno, zpracování podrobné dokumentace by nemělo být činností jednorázovou, ale tato činnost by měla probíhat kontinuálně, přičemž by mělo docházet k aktualizaci vedené dokumentace. „Důkazním materiálem“ správce jsou zejména záznamy o činnostech zpracování, dále k tomuto účelu poslouží zápisy o školení zaměstnanců, o způsobu nakládání s osobními údaji a jejich zabezpečení včetně uložených pokynů zaměstnancům, rozhodnutí vedení organizace o zpracování osobních údajů, dokumentace zabezpečení a evidence případů jeho prolomení, určení cílů a prostředků zpracování. Z dokumentace by mělo být patrno, jaké cíle byly v oblasti ochrany osobních údajů uvnitř organizace vytyčeny a jakým způsobem probíhá kontrola jejich dodržování. Toto zhodnocení je možné zahrnout i do tzv. GAP analýzy,[93] která je vhodná pro určení strategie dosažení souladu zpracování s využitím zhodnocení nesrovnalostí mezi stanovenými cíly a dosaženými výsledky.

Správcům lze doporučit, aby vedená dokumentace byla vedena srozumitelnou formou tak, aby i osoba stojící mimo danou organizaci byla schopna analyzovat a zhodnotit probíhající procesy zpracování osobních údajů uvnitř organizace, a to zejména s ohledem na možnost kontroly ze strany dozorového orgánu, který bude doložení souladu posuzovat. Závěrem této podkapitoly je třeba zmínit, že udržování souladnosti zpracování s Obecným nařízením a schopnost tento soulad doložit trvá po celou dobu „životnosti“ osobních údajů a představuje kontinuální proces zpracování osobních údajů správcem nebo zpracovatelem.

6.1.1 Záznamy o činnostech zpracování

Základním rámcem pro doložení souladu zpracování mimo obecné vedení dokumentace je povinnost vést záznamy o zpracování osobních údajů. Jedná se o zcela novou povinnost správců a zpracovatelů. Na rozdíl od výše popisovaných způsobů vedení dokumentace, které popisují konkrétní operace a postupy v rámci organizace, přináší záznamy o činnostech zpracování vymezení primárního rámce zpracování osobních údajů. Jedná se například o jméno a kontaktní údaje správce, účely zpracování, popis kategorií subjektů údajů a kategorií zpracovávaných osobních údajů, kategorie příjemců, kterým budou osobní údaje zpřístupněny,

[93] Modelový příklad užití GAP analýzy v oblasti ochrany osobních údajů http://www.powysthb.wales.nhs.uk/sitesplus/documents/1145/IMT%26G_Item_3.6_GDPR_Appendix%202.pdf

informace o případném předání osobních údajů do třetích zemí, plánované lhůty pro výmaz jednotlivých kategorií údajů nebo obecný popis technických a organizačních bezpečnostních opatření. Podle rozsahu zmocnění správce je k sestavení záznamů o činnostech zpracování povinen také zpracovatel. Uvedené záznamy se vyhotovují písemně, přičemž akceptovatelná je také elektronická forma. Obecné nařízení ukládá povinnost takové záznamy vést a dále stanovuje povinnost na požádání předložit tyto záznamy dozorovému úřadu.

Ne každý správce je však povinen tyto záznamy vést. Z působnosti Obecného nařízení jsou vyloučení správci a zpracovatelé, kteří mají méně než 250 zaměstnanců. Naopak bez ohledu na počet zaměstnanců jsou povinni tyto záznamy vést ti správci či zpracovatelé, kteří provádějí takový druh zpracování, který pravděpodobně představuje riziko pro práva a svobody subjektů, není příležitostný nebo zahrnuje zpracování zvláštní kategorie údajů či zahrnuje osobní údaje, vztahující se k rozsudkům v trestních věcech. Pro účely možné kontroly ze strany dozorového účelu lze však doporučit všem správcům a zpracovatelům, aby si alespoň základní záznamy o činnostech zpracování vytvořili, neboť se jedná o splnění základního principu odpovědnosti, zmíněného výše, tedy aby byl správce schopen doložit soulad zpracování s Obecným nařízením. Článek 30 Obecného nařízení tak může posloužit jako soubor základních otázek, které by si měl každý správce či zpracovatel položit v rámci prvotní analýzy stavu zpracování osobních údajů. Uvedené kategorie již byly v obdobném znění uvedeny v zákoně o ochraně osobních údajů jako součást souboru sdělovaných informací dozorovému úřadu v rámci splnění oznamovací povinnosti zpracování.[94]

6.1.2 Kodexy chování a vydávání osvědčení

V souvislosti s povinností správce či zpracovatele prokázat soulad dodržování principů a zásad Obecného nařízení přichází v úvahu další z variant prokázání tohoto souladu. Jak je patrné, jedná se o volitelnou variantu ověření uplatňování Obecného nařízení, nikoli povinnost správce či zpracovatele. Správce by měl v této souvislosti zvážit všechna specifika jeho zpracování a rozhodnout se, zda přistoupí k dodržování stanoveného kodexu chování. V prvé řadě posouzení je třeba si položit základní otázku, zda se správce či zpracovatel řadí k určitému odvětví či oboru, pro který byl kodex vytvořen. Vytváření kodexů cílí

[94] § 16 zákona č. 101/2000 Sb., zákona o ochraně osobních údajů a o změně některých zákonů

především na skupiny mikropodniků, malých a středních podniků. V podstatě se jedná o správce a zpracovatele stejného typu, například banky, cestovní kanceláře, lékaře a podobně. Hlavním účelem kodexů je nalézt optimální cestu prokázání souladu v rámci specifik jednotlivých odvětví. V další fázi posouzení přichází na řadu zvážení výhod a nevýhod, které správci přistoupení k dodržování kodexu chování přináší. Jak již bylo v této kapitole zmíněno, hlavním účelem vytváření kodexů a výhodou, která z nich plyne, je zejména prokázání souladnosti dodržování Obecného nařízení vůči dozorovému úřadu. Může docházet k nejasnostem, jak v rámci daného odvětví splnit soulad s dodržováním Obecného nařízení. Kodex chování obsahuje souhrn mechanismů, jak tohoto souladu dosáhnout, což může být pro správce, který by tohoto chtěl docílit sám, mnohdy náročné, neboť k tomuto nemusí mít dostatečné množství zkušeností a nemusí podchytit všechna úskalí, které zpracování přináší. Tím, že kodexy podléhají přísnému procesu schvalování a jsou vypracovány odborníky v tomto oboru, přistoupením k dodržování kodexu tato starost správci odpadá.[95]

Další výhodou, kterou kodexy chování přináší, představuje usnadnění výběru zpracovatele pro správce. Již samotné přistoupení k dodržování kodexu chování zpracovatelem presumuje dostatečné technické a organizační zabezpečení zpracování osobních údajů na jeho straně, které by mělo být při výběru pro správce prioritou. Například v případě výběru zpracovatele pro účely zpracování účetnictví a daní, může být pro správce průkazným ukazatelem toho, že zpracovatel bude splňovat stanovená kritéria zabezpečení.

Připojení se ke kodexu chování také usnadňuje proces předávání osobních údajů do zemí mimo evropský prostor, neboť přistoupení k danému kodexu vylučuje povinnost správce k tomuto získat povolení dozorového úřadu. To však za předpokladu, že správce či zpracovatel přijme ve třetí zemi taková opatření, která zaručí odpovídající úroveň ochrany osobních údajů. Více prostoru je tomuto tématu věnováno v kapitole, zabývající se předání osobních údajů do třetích zemí a mezinárodním organizacím.

V neposlední řadě může mít přistoupení ke kodexu chování pozitivní vliv na způsob a výši uložené sankce v případě nedodržení souladu zpracování s Obecným nařízením. Přistoupení k dodržování kodexu chování přináší i negativum v podobě dalšího kontrolujícího v podobě akreditovaného subjektu,

[95] Kodexy chování. In: *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 2018-07-07]. Dostupné z: https://www.uoou.cz/kodexy-chovani/d-29493/p1=3938

kterému se správce či zpracovatel musí podřídit. Výkon jeho činnosti spočívá zejména v kontrole dodržování kodexu chování na straně jednotlivých správců či zpracovatelů, kteří k jeho dodržování přistoupili. Dále řeší stížnosti na porušování kodexu, pozastavení členství ve skupině správců či zpracovatelů, kteří ke kodexu přistoupili nebo jejich úplné vyloučení.

Akreditovaný subjekt musí být nezávislý, nesmí dojít k tomu, že by byl ovlivňován některým správcem či zpracovatelem, dále u něj musí být zcela vyloučen střet zájmů. Jak již z názvu vyplývá, jedná se o subjekt akreditovaný, který splňuje akreditační kritéria stanovená dozorovým úřadem, spočívající ve splnění dostatečné úrovně odborných znalostí. Akreditaci subjektů pro jednotlivá odvětví předává dozorový úřad ke schválení Evropskému sboru pro ochranu osobních údajů, a to za účelem splnění principu jednotnosti tak, aby byly dopady Obecného nařízení regulovány ve všech zemích evropského prostoru stejně. Obecné nařízení také výslovně vylučuje monitorování souladu dodržování kodexu chování u orgánů veřejné moci a veřejných subjektů. V neposlední řadě je třeba zmínit, že funkce akreditovaného subjektu nikterak neomezuje ani nenahrazuje výkon kontroly ze strany dozorového úřadu.[96]

K dalším způsobům prokázání souladu zpracování s Obecným nařízením představuje získání osvědčení, popřípadě pečeti či známky. Opět se jedná o jednu z dobrovolných variant prokázání souladu. Osvědčení vydané v souladu s Obecným nařízením může usnadnit nákup produktů nebo služeb, pokud se daný správce či zpracovatel tímto certifikátem prokáže. Může přitom vystupovat jako výrobce, prodejce nebo poskytovatel služeb, a osvědčením dokládat, že při správném nastavení parametrů produktů nebo služby je tento produkt nebo služba v souladu s Obecným nařízením. Tento „certifikát“ ochrany osobních údajů může mít také podobu známky či pečeti, který může vypadat podobně jako certifikát ochrany původu či biokvality, který se objevuje na obalech potravin. Osvědčení tedy na první pohled může vypadat podobně jako přijatý kodex chování, liší se však tím, že na rozdíl od kodexu prostupuje jednotlivými odvětvími a slouží spíše k ověření věrohodnosti správce. Další rozdíl od kodexu chování představuje omezená platnost osvědčení, a to na dobu maximálně tří let s tím, že jeho

[96] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě. Komentář*. Leges, 2018. ISBN 978-80-7502-288-2, s. 313-314

prodloužení není vyloučeno. Lze shrnout, že osvědčení přináší srovnatelné výhody i nevýhody jako přijetí kodexu chování. [97]

Obecné nařízení vyžaduje, aby členské státy určily, zda bude subjekty, které budou certifikovat splnění požadavků různých pečetí, známek a certifikátů ochrany soukromí akreditovat dozorový úřad, v České republice tedy Úřad pro ochranu osobních údajů nebo specializovaný akreditační orgán. Návrh zákona o zpracování osobních údajů ke dni uzávěrky zpracování této práce počítá s variantou, že by akreditaci subjektů vydávání osvědčení prováděl vnitrostátní akreditační orgán[98], a to Český institut pro akreditaci, o.p.s.[99]

6.1.3 Spolupráce s dozorovým úřadem

K dalším povinnostem správce či zpracovatele nově přibyla povinnost součinnosti s dozorovým úřadem. Nejedná se pouze o povinnost předložit na vyžádání záznamy o činnostech zpracování dle předchozí podkapitoly, ale poskytnutí komplexní součinnosti při spolupráci s dozorovým úřadem, typicky při provádění kontrol ze strany dozorového úřadu v rámci povolovacího řízení, řešení situací porušení zabezpečení apod. Součinnost si lze představit zejména v poskytnutí potřebné dokumentace, umožnění kontroly v prostorách podniku nebo organizace či ke sdělení podrobností o doložení souladu zpracování. V případě, že správce tuto součinnost dobrovolně neposkytne, vystavuje se ze strany dozorového úřadu sankci za nesplnění povinnosti.

Na tomto místě se jeví jako vhodné zmínit situace, kdy správce provádí přeshraniční zpracování osobních údajů, které probíhá ve více státech evropského prostoru nebo probíhá v jednom státě, ale budou jím dotčeny subjekty údajů v dalším státě. Podle současně účinného zákona o ochraně osobních údajů je správce povinen komunikovat ve stejné míře s dozorovými úřady ze všech dotčených států, tedy v zásadě musí notifikovat zpracování ve všech dotčených státech. Obecné nařízení přináší zjednodušení celého procesu, kdy pro správce provádějícího příhraniční zpracování je příslušný pouze jeden úřad, a to příslušný

---

[97] *Article 29 Working Party: Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679* [online].6.2.2018, (18/EN) [cit. 2018-07-07]. Dostupné z: ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877, s. 9

[98] Důvodová zpráva k § 15 vládního návrhu zákona o zpracování osobních údajů cit. dne 7.7.2018, s. 68

[99] Zákon o zpracování osobních údajů v § 15 výslovně neříká, že příslušným akreditačním orgánem je Český institut pro akreditaci. o.p.s., ale činí tak odkazem na zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů ve znění pozdějších předpisů

vedoucí dozorový úřad podle sídla jeho hlavní provozovny. Popisovaný mechanismus zpracování s přeshraničním prvkem se neuplatní, je-li zpracování nezbytné pro plnění právní povinnosti nebo pokud správce plní úkol ve veřejném zájmu.[100]

6.2 Přístup založený na riziku a zabezpečení osobních údajů

Princip odpovědnosti správce úzce souvisí s dalším důležitým principem zpracování osobních údajů, kterým je princip založený na riziku[101], nahrazující dosavadní institut oznamovací povinnosti. Ten ukládal správcům osobních údajů písemně oznámit svůj záměr ještě před započetím samotného zpracování Úřadu pro ochranu osobních údajů.[102] Tento krok měl minimalizovat zahájení zpracování osobních údajů, které by mohlo porušovat právní předpisy či mohlo být v rozporu se zásadami ochrany osobních údajů. Možné hrozby tak doposud posuzoval dozorový úřad, kde byla zkoumána všechna rizika zásahu do práv a svobod fyzických osob, jejichž osobní údaje měly být zpracovány. S účinností Obecného nařízení přechází povinnost zhodnocení rizik z velké části z Úřadu na správce.[103]

Obecné nařízení rozlišuje tři typy rizik podle míry závažnosti negativních důsledků na subjekty údajů, a to nízké, standardní a vysoké riziko. Z pohledu správce je toto rozlišení významné zejména s ohledem na zajištění technických a organizačních postupů při zpracování a dále možnou aplikaci dalších úkolů správce. Podstata principu spočívá v povinnosti správce vzít od počátku v potaz povahu, rozsah, kontext a účel zpracování s cílem zajistit soulad s Obecným nařízením. Správce by měl předem analyzovat možná rizika, která mohou mít vliv na práva a svobody fyzických osob a tomu přizpůsobit zabezpečení zpracovávaných údajů. Tzv. „standardní riziko“ znamená alespoň možnost vzniku negativních důsledků zpracování. Je-li vyhodnocena vysoká míra rizika, vyvstávají správci další povinnosti, mezi které patří například povinnost provést předchozí konzultace s dozorovým úřadem nebo v případě porušení zabezpečení

[100] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 416

[101] V cizích zdrojích označovaný anglickou zkratkou RBA – risk based approach

[102] § 16 zákona č. 101/2000 Sb., zákona o ochraně osobních údajů a o změně některých zákonů

[103] Sdělení ÚOOÚ k přístupu založenému na riziku. Úřad pro ochranu osobních údajů [online]. 2017 [cit. 2018-02-27]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=26872

informovat kromě dozorového úřadu i subjekt údajů. Nízká míra rizika naopak tuto oznamovací povinnost vylučuje zcela.[104]

Míra rizika přitom vyplývá z možnosti hrozby, která může v souvislosti se zpracováním osobních údajů nastat a s ní souvisejícími důsledky pro subjekty údajů, o jejichž osobní údaje se jedná. Zároveň je potřeba vyhodnotit kompromis mezi možnou hrozbou a tím, co zpracování osobních údajů přináší, nebo je-li v daném případě dokonce nezbytné – typicky u právního důvodu zpracování ze zákona. Vždy by však mělo platit, že možné riziko musí být menší než výsledek zpracování osobních údajů. K vyrovnání případné nerovnováhy může přispět i sám správce, a to zejména rozšířením instrumentů ochrany zabezpečení. Správce by měl v prvé řadě identifikovat hrozby spojené se zpracováním a charakterizovat potenciální újmu, která by subjektům údajů mohla vzniknout. Na základě prvotní analýzy se často na první pohled jeví situace tak, že největší míra rizika hrozí tzv. „zvenčí" organizace, např. napadením systému a následné krádeže dat, prolomení bezpečnostních hesel apod. Mnohdy se však riziko skrývá uvnitř organizace. Jedná se například o nedostatečné proškolení zaměstnanců v oblasti ochrany osobních údajů a následné pochybení či nezákonné zpracování osobních údajů, pro které nemá správce právní důvod, shromažďování většího okruhu osobních údajů či uchovávání osobních údajů po dobu delší, než je pro daný účel nutné.[105]

V další fázi přichází na řadu zhodnocení pravděpodobnosti vzniku dané hrozby, tedy možnost jejího uskutečnění, v jejímž důsledku by subjektům údajů vznikla hrozba. Při hodnocení závažnosti potenciální újmy se užije stejných kritérií, která vyvozují míru rizik v daném případě. Za hodnotící kritérium lze považovat zejména citlivost osobních údajů, objem zpracovávaných dat, zranitelnost subjektů údajů – např. zda jsou zpracovávány i osobní údaje dětí a možný dopad újmy do života subjektů údajů. V provedené analýze rizik a rozboru jejich dopadů se bude odrážet i případný postup ze strany dozorového orgánu, který bude posuzovat, zda vůbec toto zhodnocení před samotným zpracováním proběhlo a posoudí míru uvědomění správce o možnosti vzniku rizika, což může

[104] MALDOFF, Gabriel. The Risk-Based Approach in the GDPR: Interpretation and Implications. *IAPP Westin Fellow* [online]. **2017** [cit. 2018-02-27]. Dostupné z: https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf

[105] CNIL. Methodology for Privacy Risk Management: How to implement the Data Protection Act, s. 9-10 [online]. [cit. 2018-02-27]. Dostupné z: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

mít v případě nedodržení zabezpečení ochrany osobních údajů pozitivní vliv při ukládání sankce.

6.2.1 Některé využitelné nástroje zabezpečení

Vhodné se tedy jeví zmínit nástroje, kterých může správce využít, aby tato rizika minimalizoval. Jedná se o jisté bezpečnostní prvky, které mohou v určitých případech správci zlepšit jeho postavení v případě úniku těchto údajů. Záměrem autorky není vyjmenovat všechny instrumenty, které má správce k dispozici, aby rizikům předešel, neboť to by mohlo být předmětem práce technického oboru. Zabezpečení u každého správce probíhá zcela individuálně se zohledněním všech skutečností jako je hloubka nebo účel zpracování. Cílem je nastínit některé specifické právně-technické instrumenty, sloužící k zabezpečení osobních údajů.

Jednou z technik zabezpečení osobních údajů, kterou mohou správci zároveň předejít pozdějším problémům, je pseudonymizace. Tou se rozumí zpracování osobních údajů tak, že již nemohou být přiřazeny ke konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny k identifikované či identifikovatelné osobě. Účelem tohoto nástroje je snížení identifikace subjektu údajů, a to za současné možnosti dalšího využití těchto dat, např. analýzu. Osobní údaje tak zůstávají zachovány, pouze jsou některé údaje nebo znaky skryty tak, že nadále není možné bez použití dalších dodatečných informací subjekt údajů rozpoznat.

Další pomůcku zabezpečení představuje šifrování dat. Do úložiště, kde jsou data uložena, typicky například na disku počítače, není možné se dostat bez zadání „šifry“ typicky hesla nebo otisku prstu. Uložené osobní údaje jsou tak chráněny v případě ztráty kontroly nad jejich úložištěm, kdy není možné se k těmto datům dostat. Šifrování může být účinné pouze tehdy, pokud je heslo dostatečně silné a dochází k jeho průběžným obměnám, typicky například při personálních změnách ve společnosti. Šifrování se užívá buď pro celá úložiště, nebo jen pro nějakou část zpracování osobních údajů.

V určitých případech užitečným nástrojem může být i tzv. tokenizace. Jedná se o proces, kdy jsou osobní údaje, zejména z kreditní karty a další údaje, nahrazeny náhodně generovaným tokenem, který představuje prostý číselný řetězec. K tomuto dojde ještě před tím, než jsou osobní data zpracovávána nebo

uložena třetími subjekty, jako jsou banky, koncoví obchodníci nebo provozovatelé cloudových úložišť. Originální identifikovatelné údaje jsou uloženy u speciálního subjektu a tento je jediný schopen „spárovat“ token a původní data a tím výrazně zvyšuje bezpečnost a ochranu dat před jejich zneužitím.[106]

Zejména při uplatnění práv ze strany subjektů údajů se uplatní procesy autentizace a autorizace, aby bylo možné bezpečně identifikovat žádající subjekt, typicky například zasláním požadavku skrze datovou schránku nebo s ověřeným podpisem. Závěrem této podkapitoly lze zmínit, že jedině řádným užíváním a nejlépe kombinací některých z výše zmíněných způsobů může docházet k efektivní ochraně osobních údajů. Přitom žádný z výše uvedených způsobů není povinně užívaným nástrojem zabezpečení. Je na každém ze správců či zpracovatelů, aby zvolil vhodný prostředek zabezpečení s přihlédnutím ke všem okolnostem a specifikům jeho zpracování.

6.2.2 Oznámení porušení zabezpečení osobních údajů

Se zabezpečením osobních údajů velmi úzce souvisí i povinnost správce oznamovat dozorovému úřadu porušení zabezpečení osobních údajů. Obecné nařízení reaguje na nedostatečnou úroveň zabezpečení, která byla často velmi neuspokojivá a správci neměli povinnost incidenty porušení zabezpečení hlásit orgánům veřejné moci či přímo subjektům údajů. Přestože se tato povinnost jeví jako zcela nová, není tomu tak zcela. Některé skupiny správců, měly i před účinností Obecného nařízení povinnost hlásit rizikové události.[107] S účinností Obecného nařízení byla tato povinnost rozšířena na všechny správce.

Stěžejním principem této oznamovací povinnosti správce je v prvé řadě detekovat porušení zabezpečení. Pokud v této souvislosti hovoříme o zaznamenání porušení zabezpečení, vyvstává nutnost tento bezpečnostní incident posoudit a zjistit, zda daná situace vůbec představuje porušení zabezpečení. Pokud vzniklá událost vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů, lze ji hodnotit jako bezpečnostní incident.

[106] METELKA, Jan. Ochrana osobních údajů skrze tokenizaci. *E-pravo.cz* [online]. 2016 [cit. 2018-11-02]. Dostupné z: https://www.epravo.cz/top/clanky/ochrana-osobnich-udaju-skrze-tokenizaci-104196.html

[107] Jednalo se zejména o správce a provozovatele systémů kritické informační infrastruktury podle § 8 zák. č. 181/2014 Sb., zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) nebo informační povinnost podnikatele zajišťujícího veřejnou informační síť dle § 98 odst. 4 zák. č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

V případě kladného vyhodnocení takové záležitosti přichází na řadu další posouzení, a to, zda by důsledkem zjištěného bezpečnostního incidentu mohlo být riziko pro práva a svobody fyzických osob. Tuto hrozbu lze charakterizovat jako závažný nežádoucí účinek na subjekt údajů, který může vyústit v újmu nebo majetkovou škodu. Sem lze zařadit ztrátu kontroly nad vlastními osobními údaji, omezení práv, diskriminaci, krádež identity či podvod, finanční ztrátu, neoprávněné zrušení pseudonymizace, narušení dobré pověsti, ztrátu důvěrnosti osobních údajů chráněných služebním tajemstvím. Dále sem řadíme jiné významné znevýhodnění jednotlivců z hospodářského hlediska nebo společenské znevýhodnění subjektu údajů.[108]

Zajištění účinného systému detekce hrozby se úzce prolíná s principem odpovědnosti správce a je tedy na něm, aby zajistil taková technická a organizační opatření, která jsou schopná incident zaznamenat, popř. takovou hrozbu přímo odvrátit. Klíčový prvek pak představuje schopnost tomuto porušení zabezpečení předcházet, a pokud k němu dojde, reagovat včas.

Okamžik vědomosti správce o porušení zabezpečení představuje důležitý časový mezník, ke kterému Obecné nařízení váže vznik povinnosti správce hlásit incident dozorovému úřadu, popřípadě i přímo subjektu údajů, jehož osobních údajů se hrozba týká. Je tedy bez rozdílu, zda se o tomto porušení například dozví nejprve řadový zaměstnanec správce, typicky z oblasti IT, či přímo vedoucí pracovník. Přestože správce nese celkovou zodpovědnost za ochranu osobních údajů subjektů údajů, zpracovatel hraje důležitou roli při oznámení bezpečnostního incidentu, který vznikl v souvislosti s okruhem osobních údajů, které má na starosti. Zpracovatel nemá povinnost porušení zabezpečení hlásit přímo dozorovému úřadu, ale musí učinit oznámení vůči správci, který pak provede další potřebné kroky. Jako vhodné se jeví tuto situaci přesně upravit ve zpracovatelské smlouvě nad rámec znění Obecného nařízení, zejména s určením časového úseku pro oznámení zpracovatele správci a také stanovení výslovné povinnosti zpracovatele být správci v případě bezpečnostního incidentu nápomocen. V této situaci se tak potvrzuje, jak důležité je proškolení zaměstnanců správce či zpracovatele, aby byli schopni daný incident správně vyhodnotit a reagovat na něj.

[108] *Article 29 Data Protection Working Party: Opinion 03/2017 on Guidelines on Personal data breach notification under Regulation 2016/679*[online].3.10.2017, (17/EN; WP250) [cit. 2018-06-17]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=47741, s.7

V případě, že tedy dojde k bezpečnostnímu incidentu, musí správce učinit oznámení bez zbytečného odkladu, pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. S oznámením by správce neměl meškat ani v případě, kdy v dané lhůtě není schopen přesně detekovat rozsah porušení zabezpečení, nebude moci posoudit pravděpodobné důsledky incidentu, či nemůže ohlášení provést se všemi jeho náležitostmi. Zejména pak v případech, kde by došlo k rozsáhlému porušení zabezpečení, bude pravděpodobně nutné, aby správce provedl interní vyšetřování incidentu, a doplňující údaje sdělí dozorovému úřadu hned, jakmile to bude možné. Obsahové náležitosti hlášení porušení zabezpečení zahrnují zejména popis okolností vzniku a průběhu bezpečnostního incidentu, pokud je to možné uvedení kategorií a přibližného počtu dotčených subjektů údajů a jejich přibližný počet. Dále by mělo hlášení obsahovat kontaktní údaje na pověřence, byl-li zvolen, či na jinou kompetentní osobu, která bude tento incident dále řešit. Další částí hlášení je popis pravděpodobných důsledků porušení zabezpečení a popis opatření, která již správce přijal nebo navrhl ke zmírnění porušení zabezpečení. Zejména poslední kategorie bude mít významný vliv na posouzení dozorovým orgánem, zda správce nejen předem minimalizoval riziko vzniku škodlivé události přijetím technických a organizačních opatření, ale také do jaké míry tato opatření napomohla k nápravě bezpečností situace.[109]

Po ohlášení porušení zabezpečení by měl dozorový úřad zaujmout k této situaci své stanovisko a předat správci další pokyny, jak danou situaci dále řešit. Za předpokladu, že by po provedení posouzení dospěl správce k závěru, že porušení zabezpečení bude mít za následek vysoké riziko pro práva a svobody subjektů údajů, musí dotčeným subjektům toto porušení oznámit. Přitom by měl dbát na to, aby sdělení obsahovalo náležitosti stejné jako hlášení dozorovému úřadu a zároveň bylo učiněno srozumitelnou a jednoznačnou formou. Může také dojít k situaci, kdy správce vyhodnotí situaci jako méně rizikovou a ohlásí ji tedy pouze dozorovému úřadu. Dozorový úřad provede šetření daného bezpečnostního incidentu a může vyvodit, že správce situaci nesprávně posoudil a je v daném případě potřeba provést oznámení o porušení zabezpečení vůči subjektu údajů. Výjimka z povinnosti oznamovat porušení zabezpečení se uplatní tehdy, když správce už v minulosti zavedl vhodná technická a organizační opatření, která zabránila, aby daná situace představovala vysoké riziko pro subjekty údajů.

[109] BUCHNER, Benedikt a Jürgen KÜHLING. *DS-GVO Datenschutz-Grundverordnung: Kommentar*. C. H. Beck, 2017. ISBN 978-3-406-70212-9, s. 615-617

Typickým příkladem je provedení šifrování souborů, které obsahují osobní údaje, které jsou chráněny např. i v případě ztráty či krádeže platformy, na které se nacházejí. Dále správce nemusí porušení zabezpečení sdělovat subjektu údajů, když dodatečně přijme taková dodatečná opatření, která rizika zmírní či by pro něj oznámení porušení zabezpečení subjektu údajů představovalo nepřiměřené úsilí, například proto, že kontaktní údaje subjektu údajů nejsou správci známy.
Stejně jako v předchozím případě může dozorový úřad výslovně ad hoc určit, že v dané situaci správce subjektu údajů porušení zabezpečení nemusí oznamovat.
O veškerých bezpečnostních incidentech by si měl správce vést evidenci, tedy i o těch, které nehlásil dotčenému subjektu nebo dozorovému úřadu a měl by být schopen ji při kontrole Úřadu předložit.

6.3 Posouzení vlivu na ochranu osobních údajů

Přístup založený na riziku tedy do jisté míry nutí správce přemýšlet dopředu a nejen předvídat možné komplikace, ale především udělat všechno pro to, aby taková rizika dopředu minimalizoval. Správce proto musí s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření, je-li pravděpodobné, že zvolený druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Správce je v takovém případě povinen zajistit úroveň zabezpečení odpovídající danému riziku. Riziko zcela pochopitelně nejvíce hrozí zejména u zpracování údajů na elektronické platformě, neboť s digitalizací těchto údajů hrozí rizika jejich ztráty nebo zneužití. Protože se v současné době jedná o převažující způsob zpracování, lze tedy vyvozovat, že velká část správců se bude potýkat s vyšší mírou rizika zpracování.

Pravděpodobnost vzniku rizika je pak klíčová při aplikaci zcela nové povinnosti správce, a to nutnosti posouzení vlivu na ochranu osobních údajů. Ne ve všech zemích evropského prostoru se jedná o novou povinnost správců. Například dosavadní britská či francouzská legislativa přikazovala správcům toto posouzení zpracovat ještě před účinností Obecného nařízení.[110] Obecné nařízení

[110] Soubor těchto operací je v dané legislativě znám pod zkratkou zkratkou PIA – Privacy Impact Assessment. PIA totiž zahrnuje soubor operací majících vliv na soukromí jednotlivce. V současnosti se v souvislosti s posouzením vlivu na ochranu osobních údajů častěji setkáváme se zkratkou DPIA – Data Privacy Impact Assessment, která se vyvinula z PIA a představuje

zakotvuje povinnost posouzení provést před zahájením zpracování, a to pro každou operaci zpracování. S ohledem na nákladnost provedení tohoto posouzení však Obecné nařízení umožňuje, aby pro soubor stejných nebo podobných operací správce vypracoval pouze jedno posouzení.

Ne všechny zamýšlené operace zpracování podléhají povinnosti správce provést posouzení zpracování. Před započetím zpracování musí správce provést prvotní analýzu stavu, a to s ohledem na případné další povinnosti, které mohou z tohoto hodnocení vyplynout. Výše zmíněné zpracování osobních údajů skrze elektronickou platformu není jediným rizikovým typem zpracování. Za rizikové je považováno také využívání nových technologií, neboť nelze v danou chvíli dostatečně obsáhnout všechny možnosti prolomení zabezpečení. Do rizikových činností lze zařadit i systematické a rozsáhlé vyhodnocování osobních aspektů týkající se fyzických osob, které je založeno na automatizovaném zpracování. Zároveň takové zpracování vyvolává právní účinky ve vztahu k subjektu údajů, které na ně mohou mít závažný dopad, a to zejména z toho důvodu, že dochází k rozhodování o subjektu údajů čistě technologickými prostředky bez lidského zásahu. Společně s tímto typem zpracování může být použito i tzv. profilování, které spočívá v použití osobních údajů subjektu a k jejich dalšímu hodnocení některých osobních aspektů a jejich rozboru nebo jejich dalšímu odhadu.[111]

Uvedený typ zpracování velmi často využívají zejména banky při prvotním posouzení zájemců o poskytnutí úvěru, které je prováděno zcela automatizovaně ze zadaných osobních údajů subjektů údajů včetně údajů o výši měsíční mzdy nebo platu či jiných aspektech sledujících bonitu subjektu údajů. Správce musí dále analyzovat, zda ve velkém rozsahu nezpracovává zvláštní kategorii osobních údajů nebo údaje týkající se rozsudků v trestních věcech a trestných činů, neboť toto zpracování bez dalšího podléhá povinnosti posouzení vlivu na zpracování osobních údajů. Posouzení vlivu se nevyhne ani ten správce, který rozsáhle monitoruje veřejně přístupné prostory.

Samostatnou skupinou rizikového zpracování představuje soubor operací, které za rizikové, a tedy podléhající posouzení vlivu, označil sám dozorový úřad. Úřad pro ochranu osobních údajů se obává vytvoření taxativního výčtu operací,

---

pouze jakousi její podmnožinu a je dílčím nástrojem ochrany soukromí jednotlivce se zaměřením na ochranu osobních údajů. Pro účely této práce je tak podstatný pojem DPIA.

[111] *Article 29 Data Protection Working Party:* Guidelines on Automated individual decision-making and Profiling for purposes of Regulation 2016/679 [online].3.10.2017, (17/EN; WP251) [cit. 2018-09-17]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=47742, s.6-8

neboť ten by pro účely zabezpečení nebyl konzistentní, zejména s ohledem na rychlý vývoj technologií a možnost některých správců povinnost posouzení vlivu obcházet. Proto se Úřad rozhodl jít cestou určení rizikovosti zpracování osobních údajů, kdy považuje za vhodné jednotlivé zpracování popsat podle parametrů a hodnot, jichž zpracování dosahuje a také určit míru rizika zpracování, zejména s ohledem na vysoké riziko. Metodika[112] stanovuje základní hodnotící kritéria pro určení rizikovosti daného zpracování, nikoli konkrétní operace. Hodnotícími kritérii jsou například užití profilování ze strany správce, kombinovaní osobních údajů z různých datových sad, zpracování osobních údajů zvláště zranitelných osob, inovativní užití či aplikace technologických a organizačních řešení či předávání osobních údajů mimo evropský prostor. V případě, že zamýšlená operace či soubor operací správce zahrnuje dvě a více z těchto kritérií, je správce povinen provést posouzení vlivu na ochranu osobních údajů.[113]

Metodika je pro správce důležitá i z jiného důvodu, neboť Úřad se v ní vyjádřil v rámci hodnotícího kritéria rozsahu zpracování. Za velký rozsah zpracování považuje zpracování osobních údajů více než 10.001 subjektů, za malý rozsah naopak zpracování údajů méně než 5000 subjektů údajů. Úřad rovněž charakterizoval několik souborů operací, které jsou z posuzování vlivu na ochranu osobních údajů výslovně vyloučeny, například vedení kartotéky pacientů obvodního lékaře do 5000 pacientů či advokát s méně než 5000 klienty, za předpokladu splnění dalších povinností, např. že zároveň nedochází k předání těchto údajů do třetích zemí apod.[114] Jedním z případů, kdy se tato výjimka nepoužije, představuje situace, kdy advokát zpracovává velké množství údajů v trestních věcech.

Úřad zveřejnil návrh seznamu operací zpracování osobních údajů[115], která nepodléhají posouzení vlivu na ochranu osobních údajů, přičemž připomíná, že tento seznam ještě může doznat změn. Řadí sem například zpracování osobou

---

[112] Metodika Úřadu pro ochranu osobních údajů: *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)*; online]. [cit. 2018-05-07]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003

[113] Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to reset in a high risk" for the purposes of Regulation 2016/ 679 [online]. 4.4.2017, (17/EN; WP 248) [cit. 2018-05-05]. Dostupné z: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[114] Metodika Úřadu pro ochranu osobních údajů: K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA); online]. [cit. 2018-05-07]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003

[115] Návrh seznamu operací zpracování osobních údajů, která nepodléhají posouzení vliv na ochranu osobních údajů. In: *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-09-21]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30738

k poskytování zdravotních služeb, která není v zaměstnaneckém poměru, zpracování zajišťovaná advokáty a notáři, fyzickými osobami poskytujícími sociální služby nebo při snímání veřejné komunikace kamerou umístěnou na vozidle. Výslovně také zmiňuje obchodní činnosti včetně věrnostních programů nebo pořádání soutěží. Podpůrně lze také využít kritéria nastíněná Pracovní skupinou WP29.[116] Není-li si správce jist, doporučuje autorka vnést dotaz směřovaný Úřadu, zda daná činnost spadá pod povinnost posouzení vlivu na ochranu osobních údajů. Při pochybnostech je vždy vhodnější posouzení vlivu provést.

6.3.1 Předchozí konzultace s dozorovým úřadem

V určitých situacích může dojít k tomu, že správce či zpracovatel po provedeném posouzení vlivu na ochranu osobních údajů zjistí, že zamýšlený okruh zpracování osobních údajů bude pravděpodobně představovat vysoké riziko pro subjekty údajů a v takovém případě vzniká správci povinnost konzultovat tuto skutečnost s dozorovým úřadem. Podle původního návrhu Obecného nařízení byla předpokládána povinnost nezahájit zpracování do doby, než správci dozorový úřad udělí k tomuto zpracování souhlas. Podle současného pojetí není rizikové zpracování podmíněno předchozím povolením dozorového úřadu. Na vyřízení dotazu má dozorový úřad osm týdnů, přičemž tato lhůta může být prodloužena o dalších šest týdnů. Konzultaci iniciuje správce jen tehdy, když sám shledá, že neexistují vhodné záruky, kterými by šlo takové zpracování zmírnit. Je tedy otázkou, jak se vyvine rozhodovací praxe Úřadu a zda v těchto případech nebude stanovován zákaz takového zpracování. Výjimku budou představovat například zpracování za účelem provedení medicínského výzkumu ve veřejném zájmu. Tato nová povinnost správce tak může být účinným nástrojem předcházení chybám ve správě a zpracování osobních údajů.[117]

6.4 Povinnost jmenovat pověřence

Často se lze nejen v laických zdrojích setkat s názorem, že povinnost jmenovat pověřence je jednou ze zcela nových povinností správce, které přineslo

[116] Annex 2 – Criteria for acceptable DPIA, Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to reset in a high risk“ for the purposes of Regulation 2016/ 679 [online]. 4.4.2017, (17/EN; WP 248) [cit. 2018-05-05]. Dostupné z: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[117] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 324

Obecné nařízení. Tento pohled však nelze považovat za zcela správný. Již Směrnice upravovala institut pověřence, avšak bylo ponecháno v dispozici členských států, zda ve svých vnitrostátních předpisech určily správcům povinnost takovou osobu jmenovat. Před účinností Obecného nařízení bychom pověřence pro ochranu osobních údajů mohli nalézt například v podobných modifikacích ve vnitrostátní legislativě Německa, Francie, Polska či Maďarska. Rovněž na Slovensku národní legislativa umožňovala správcům jmenovat pověřence ještě před účinností Obecného nařízení, přičemž využití této osoby přinášelo správci některé výhody.[118] V českém právním prostředí nejenže zákon o ochraně osobních údajů institut pověřence neupravoval, ale i český překlad Směrnice se zmiňuje o „osobě pověřené ochranou údajů“, nikoli výslovně o pověřenci, což také zřejmě hovoří o nepřílišném povědomí o tomto institutu.

Pověřenec pro ochranu osobních údajů je nezávislou osobou, dohlížející na soulad zpracování osobních údajů s Nařízením v instituci správce či zpracovatele, a je mu nadále nápomocen radami ohledně ochrany osobních údajů. Zároveň představuje pověřenec kontaktní místo nejen pro dozorový úřad, ale především pro samotné subjekty údajů. Jmenování pověřence ale správce nezbavuje odpovědnosti za samotné zpracování, a tato povinnost není přenesena na pověřence.

V této kapitole se hovoří o povinnosti jmenovat pověřence, která se vztahuje jak na správce, tak i na zpracovatele. Jsou-li proto v této kapitole zmiňovány skutečnosti týkající se povinnosti jmenovat pověřence pro správce, platí toto v obecné rovině rovněž pro zpracovatele. Na tomto místě je však vhodné vyložit právní vztah správce a zpracovatele s přihlédnutím k této povinnosti. V případě, že je pověřence povinen jmenovat správce, nemusí to nutně indikovat povinnost jmenovat pověřence také zpracovateli a naopak. Každý by měl na základě analýzy svého úseku zpracování osobních údajů vyvodit závěr, zda podléhá povinnosti jmenovat pověřence či nikoli. Avšak v případě, že se tato

[118] § 23 a násl. zák. č. 122/2013 Sb., o ochrane osobných údajov a o zmene a doplneni niektorých zákonov, který správcům umožňoval jmenovat tzv. zodpovědnou osobu, přičemž jmenování této osoby bylo dáno jako možnost nikoli povinnost správce. V případě, že se správce rozhodl jmenovat zodpovědnou osobu, nemusel vůči Úřadu pro ochranu osobních údajů splnit informační povinnost, týkající se jím využívaných informačních systémů, zpracovávajících osobní údaje zcela nebo částečně automatizovanými prostředky správce (§ 34 zákona)

povinnost bude vztahovat na správce i zpracovatele, jeví se jako vhodné, aby spolu v této záležitosti spolupracovali.[119]

V době blížícího se nabytí účinnosti Obecného nařízení bylo možné často v médiích slýchat, že správci budou muset jmenovat pověřence pro ochranu osobních údajů, což vyvolávalo obavy, a s tím spojené otázky veřejnosti, zda tedy každý správce bude muset pověřence jmenovat. Povinnost jmenovat pověřence se však vztahuje pouze na omezený okruh správců, kterými jsou ti, kteří naplní alespoň jednu z podmínek, uvedenou v Obecném nařízení. Obecně lze říci, že povinnost jmenovat pověřence vyvstává pro správce, jejichž zpracování osobních údajů vykazuje větší rizikovost zpracování. Tato povinnost se výslovně vztahuje na všechny orgány veřejné moci či veřejné subjekty. Předpokládá se, že vymezení těchto pojmů bude ponecháno v dispozici národních právních řádů, neboť právní vymezení orgánu veřejné moci se může v jednotlivých členských státech různit.[120] V českém právním prostředí orgán veřejné moci vystupuje jako autoritativní právnická osoba orgán veřejné moci, přičemž *„pod tento pojem můžeme subsumovat jak pojem státní orgán (státní úřad), tak subjekt nestátní tj. veřejnoprávní korporaci vykonávající prostřednictvím svých orgánů v přenesené působnosti státní správu a vlastní samosprávnou kompetenci nebo soukromou fyzickou anebo právnickou osobu pověřenou výkonem státní správy (tedy orgán veřejné správy).."* [121] Výjimku tvoří zpracování osobních údajů soudy, které jednají v rámci vlastní pravomoci. Nebude se tedy jednat o činnosti související se zpracováním pro své potřeby, typicky například pro personální agendu.

Podle návrhu adaptačního zákona budou mít povinnost jmenovat pověřence kromě orgánů veřejné moci také orgány, zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu. [122] Zákon tak reaguje na zvýšenou potřebu ochrany subjektu údajů v situacích, kdy tento nemá možnost ovlivnit, zda, a jakým způsobem budou jeho osobní údaje zpracovány, ale vzhledem k procesní úpravě je zpracování osobních údajů subjektu údajů nevyhnutelné. Typicky se bude jednat o plnění zákonem stanovených úkolů ve veřejném zájmu exekutorskými úřady či notářem. Povinnost jmenovat pověřence podle tohoto

[119] *Article 29 Data Protection Working Party: Guidelines on Data Protection Officers (´DPO´s)* [online].13.12.2016, (16/EN; WP 243) [cit. 2018-06-27]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=43823, s.9-10

[120] Tamtéž, s. 6

[121] SLÁDEČEK, Vladimír. *Obecné správní právo*. 3., aktualiz. a upr. vyd. Praha: Wolters Kluwer Česká republika, 2013. ISBN 978-80-7478-002-8, s. 28

[122] § 14 vládního návrhu zákona o zpracování osobních údajů, sněmovní tisk č. 138 cit. dne 27.6.2018

ustanovení se vztahuje také na Nejvyšší kontrolní úřad, Českou národní banku, veřejného ochránce práv či jiné instituce, které plní veřejnoprávní funkce státu a jsou svou povahou nejblíže orgánům veřejné moci, aniž by v dané situaci nutně musely autoritativně rozhodovat o právech a povinnostech subjektů údajů. Naopak tato povinnost nedopadá například na příspěvkové organizace, za předpokladu, že zároveň nesplňují další podmínky pro jmenování pověřence.[123]

Další případ nutného jmenování pověřence představuje situace, kdy správcova hlavní činností spočívá v operacích, které vyžadují rozsáhlé a systematické monitorování subjektů údajů. V daném případě je pak na posouzení správce, zda jde o klíčovou operaci směřující k dosažení cíle správce. Pověřence tak musí jmenovat například nemocnice, neboť ta nemůže poskytovat zdravotní služby bez zpracování zdravotní dokumentace pacientů. Výklad rozsáhlosti zpracování ve vztahu k poskytování zdravotních služeb pacientům se kloní k tomu, že zpracování údajů o pacientech jednotlivým lékařem už za rozsáhlé považovat nelze. Pověřence tak nemusí jmenovat například jednotlivě působící lékaři – specialisté, a to za předpokladu, že nenaplňují jiné podmínky pro povinnost jmenovat pověřence.[124]

Povinnost jmenovat pověřence se vztahuje i na ty správce, kteří rozsáhle a systematicky sledují subjekty údajů, a to bez ohledu na formu takového monitorování. Ať už jde o sledování chování subjektů údajů prostřednictvím online procesů či přímo fyzicky skrze kamerové či jiné monitorovací systémy. Činnost by přitom měla být soustavná, pravidelně se opakující a také systematická, tedy uskutečňující se jako součást plánu nakládaní s daty, která obsahují osobní údaje subjektů údajů. Pracovní skupina WP29 zároveň upozornila, že ve věcech zpracování kategorií osobních údajů, týkajících se rozsudků v trestních věcech a trestných činů je právě spojka „a“ zvolena nepříliš šťastně, neboť tato dvě kritéria nemusí být splněna současně. Postačuje tedy, aby správce zpracovával buď kategorii osobních údajů, týkajících se rozsudků v trestních věcech, nebo údaje týkající trestných činů subjektů údajů. V takovém případě je povinen rovněž jmenovat pověřence.[125]

---

[123] Důvodová zpráva k § 14 vládního návrhu zákona o zpracování osobních údajů cit. dne 27.6.2018, s. 67

[124] *Article 29 Data Protection Working Party: Guidelines on Data Protection Officers (´DPO´s)* [online].13.12.2016, (16/EN; WP 243) [cit. 2018-06-27]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=43823, s. 6-7

[125] Tamtéž, s. 9

Jak již bylo v této kapitole zmíněno, pověřenec zaujímá v rámci společnosti specifické postavení. Jeho role je zejména poradní, s přihlédnutím ke všem specifikům a konkrétním zájmům správce. Nejde však o pouhého rádce, správce by měl mít při výkonu své funkce přístup ke všem důležitým záležitostem. Zejména by se měl účastnit schůzí vedení společnosti, aby byl seznámen s dalším zamýšleným vývojem, který by mohl mít dopad na ochranu osobních údajů. Správce by měl rovněž zajistit přítomnost pověřence všude, kde dochází k rozhodováním, která mají vliv na ochranu osobních údajů. S tím souvisí i okruh úkolů, ukládající pověřenci Obecným nařízením, který by bylo možné rozdělit na dvě části. První část úkolů plní pověřenec uvnitř společnosti. Jedná se zejména o poskytování poradenství a informací správci o jeho povinnostech v oblasti zpracování osobních údajů a následné monitorování souladu s Obecným nařízením a národní legislativou ochrany osobních údajů. Správce si například může vyžádat jeho stanovisko v případě posuzování vlivu na ochranu osobních údajů nebo s ním konzultovat případy porušení zabezpečení. Pověřenec analyzuje procesy zpracování uvnitř organizace a ověřuje jejich soulad. Pověřenec také může provádět školení zaměstnanců správce v oblasti ochrany osobních údajů.

Druhý okruh úkolů pověřence zahrnuje jeho působení navenek organizaci správce. Pověřenec je kontaktní osobou jak pro subjekty údajů, tak pro dozorový úřad. Subjekty údajů mají právo se na pověřence obracet ve všech záležitostech souvisejících se zpracováním jejích osobních údajů a výkonem jejich práva. Jedná se zejména o poskytnutí informací o tom, jaké údaje a jakým způsobem o nich správce zpracovává, k pověřenci rovněž mohou směřovat námitky. Pověřenec je zároveň kontaktní osobou pro dozorový úřad ve všech záležitostech, týkajících se zpracování, včetně případného vedení konzultací.

Obecné nařízení dává správcům možnost, aby jmenovali společného pověřence pro několik provozoven.[126] Vždy však platí, že tento pověřenec musí být bez problémů dostupný z každého pracoviště správce a zároveň sloužit jako kontaktní místo pro subjekty údajů a dozorový úřad. Společný pověřenec tedy najde uplatnění spíše u lokálních skupin provozoven správce.

Pověřenec by měl mít k dispozici veškeré zdroje, které mu budou sloužit k naplňování jeho činnosti. Jedná se zejména o dostatek časového prostoru pro výkon jednotlivých úkolů pověřence, pokud je u správce zaměstnán, ale

[126] V českém překladu Obecného nařízení je ne příliš výstižně uveden podnik, přiléhavější charakteristiku však s ohledem na právní vymezení představuje pojem provozovna.

s ohledem na velikost společnosti také dostatečné personální zabezpečení agendy ochrany osobních údajů. V rámci funkce pověřence by měla být smluvně zajištěna povinnost mlčenlivosti o všech skutečnostech, o kterých se dozvěděl v souvislosti s jím prováděnou činností, a to i po skončení spolupráce popř. pracovního poměru ke správci. V neposlední řadě musí pověřenec splňovat dostatečné profesní kvality a úroveň odbornosti, která musí odpovídat citlivosti zpracovávaných údajů a také rozsahu zpracování. Obecné nařízení neudává povinnou úroveň vzdělání či jiné požadavky, neboť tyto mohou být s ohledem na zpracování v každé jednotlivé organizaci různé. Pověřenec by měl mít povědomí nejen z prostředí práva, ale ideálně také z IT a správce by mu měl umožnit, aby se dále vzdělával. V současné době je na trhu nabízena celá řada certifikací pro pověřence, které jsou často prezentovány tak, že bez jejich absolvování není možné funkci pověřence vůbec vykonávat. Obecné nařízení, přitom nestanovuje žádnou povinnou certifikaci a je tedy na správci, aby při výběru pověřence zhodnotil jeho profesní kvality, zkušenosti či jeho znalost a orientaci v právní úpravě, přičemž certifikace není nutná.[127]

Velké společnosti často mají celá organizovaná oddělení, zabývající se zpracováním osobních údajů a pověřencem je zvolen některý ze zaměstnanců. V daném případě se může takové řešení jevit jako vhodné, neboť provádí komplexní zpracování osobních údajů pro správce, má znalosti o procesech uvnitř společnosti. Zároveň je potřeba zajistit, aby u pověřence nedocházelo ke střetu zájmů, tedy nemůže například současně zastávat v dané společnosti pozici zaměstnance, jehož pracovní náplní je určování účelů a prostředků zpracování, jedná se zejména o pozice ve vyšším managementu. Samotné znění Obecného nařízení tyto situace předpokládá, když říká, že pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce, tedy nemůže se jednat o jednu a tutéž osobu. Ke střetu zájmů může dojít i v případě, kdy by měl pověřenec zastupovat správce v soudním či obdobném řízení v případech týkajících se ochrany osobních údajů.[128]

[127] Pověřenec pro ochranu osobních údajů. In: *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 2018-07-01]. Dostupné z: https://www.uoou.cz/poverenec-pro-nbsp-ochranu-osobnich-udaju/d-27307/p1=3938

[128] NEŠPŮREK, Robert, Jaroslav ŠUCHMAN a Ján JAROŠ. GDPR: nastane s nástupem nové regulace nedostatek pověřenců?. *E-pravo* [online]. 2018, 9.4.2018, (04) [cit. 2018-07-01]. Dostupné z: https://www.epravo.cz/top/clanky/gdpr-nastane-s-nastupem-nove-regulace-nedostatek-poverencu-107264.html

Z pohledu správce jako zaměstnavatele však může být problematická jeho limitace v případě sankcí za neplnění pracovních povinností, náhradě škody či v krajním případě ukončení pracovního poměru pověřence. Pověřenec v tomto požívá zvláštní ochrany, neboť nemůže být sankcionován za způsob výkonu funkce, například při vydávání jednotlivých stanovisek. Sankce v obecné rovině pracovněprávního vztahu se zaměstnavatelem však nejsou vyloučeny. Je tedy na zvážení zaměstnavatele, zda využije služeb externího pověřence, kterým může být například specializovaná společnost nebo advokát, přičemž se zaměstnavatel vyvaruje řešení situací, vyplývajících z pracovněprávního poměru. Další výhodu externího pověřence představuje zejména pro malé a střední podniky lepší finanční dostupnost na zajištění procesů, souvisejících se zpracováním osobních údajů a činností pověřence, které by pro ně v rámci společnosti bylo příliš nákladné. Rovněž tak lze předejít střetu zájmů. Nevýhodou pověřence – externisty je často nemožnost obsáhnout veškeré procesy probíhající v rámci zpracování uvnitř společnosti.

6.5 Povinnosti při předávání osobních údajů do zahraničí

V současné době dochází ke zvyšování digitalizace globální ekonomiky, která se však neobejde bez transferů osobních údajů do třetích zemí. Bez nich by totiž některé služby nemohly vůbec fungovat nebo by byl jejich provoz velmi finančně náročný. S předáním osobních údajů do třetích zemí se však zvyšuje riziko porušení jejich ochrany, a to zejména s ohledem na právní nejistotu, zda budou v dané třetí zemi či mezinárodní organizaci zajištěny stejné či obdobné standardy ochrany, jako je tomu v evropském prostoru. Tato kapitola shrnuje právní nástroje a prostředky, kterými lze přenášet osobní údaje tak, aby nebyla narušena integrita jejich ochrany.

Předáním osobních údajů do zahraničí se rozumí jakékoliv sdělení, zpřístupnění nebo jiné poskytnutí osobních údajů správci nebo zpracovateli ve třetí zemi mimo evropský prostor. O předání osobních údajů přitom nelze hovořit tehdy, jestliže jsou osobní údaje zveřejněny na internetové stránce, kterou je možné si prohlížet odkudkoli na světě, tedy i ze třetích zemí.[129]

[129] Rozsudek Soudního dvora EU ze dne 6. listopadu 2003, Bodil Lindqvist, věc C-101-01

6.5.1 Předání založené na rozhodnutí o odpovídající ochraně

Jak již bylo v této práci řečeno, ke zpracování osobních údajů potřebuje správce právní titul, na základě kterého bude osobní údaje zpracovávat. V případě, že správce předává osobní údaje do třetích zemí či mezinárodním organizacím mimo evropský prostor, vyžaduje se nad to právní důvod tohoto předání. Tyto právní důvody lze rozdělit do tří skupin. Prvním z nich je rozhodnutí Evropské komise o tom, že daná třetí země či mezinárodní organizace stojící mimo evropský prostor poskytuje dostatečnou úroveň ochrany osobních údajů, a to jednak v národní legislativě, tak i v rámci mezinárodních smluv, ke kterým daná země přistoupila a na základě nich se zavázala k ochraně osobních údajů. Obecné nařízení dále specifikuje vymezení teritoriální – tedy může se jednat o třetí zemi nebo jen o určité území. Dále vymezuje rozhodnutí na věcněprávním základě, kdy říká, že se může jednat i o jedno či více konkrétních odvětví či mezinárodní organizaci. Je-li uděleno takové rozhodnutí, osobní údaje jsou předávány stejně, jako by daná třetí země či mezinárodní organizace byla součástí evropského prostoru.[130]

Jak judikoval i Soudní dvůr Evropské unie, s ohledem na různost právních úprav ve třetích zemích zní požadavek na rovnocennou ochranu osobních údajů, jako je tomu v zemích evropského prostoru, neboť dosažení zcela identických právních východisek by nebylo možné zajistit, jak judikoval Soudní dvůr EU v případu *Schrems proti Data Protection Commissioner*[131] Uvedený rozsudek je však zajímavý i z jiného důvodu. Mezi třetí země, kam jsou nejčastěji předávány osobní údaje subjektů údajů z evropského prostoru, bezpochyby patří Spojené státy americké. Již za účinnosti Směrnice byly vzájemné vztahy předávání osobních údajů upraveny rozhodnutím Evropské komise[132], do kterého byly vtěleny zásady tzv. programu Safe Harbor. Tyto zásady spočívaly zejména dodržování speciálních pravidel nad rámec obecné legislativy Spojených států na ochranu osobních údajů, která byla sama o sobě shledána jako nedostatečná.

[130] Adequacy decisions. In: *European Commission* [online]. [cit. 2018-10-02]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en. K těmto státům patří Andorra, Argentina, Kanada, Faerské ostrovy, Guernsey, Izrael, ostrov Man, Jersey, Nový Zéland, Švýcarsko, Uruguay a Spojené státy americké – viz dále v práci rozebraná specifika předávání do USA.

[131] Rozsudek Soudního dvora EU ze dne 6. října 2015, Maximillian Schrems proti Data Protection Commissioner, věc C-362/14

[132] Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států

Cílem tohoto programu bylo zajistit vyšší míru ochrany osobních údajů, pocházejících z evropského prostoru a umožnit volný přenos těchto údajů do USA. Americké společnosti, které k tomuto programu dobrovolně přistoupily, pak byly shledány jako spolehlivými „vývozci“ osobních údajů se zaručením srovnatelné ochrany jako v evropském prostoru.

K tématu bezpečnosti předávaných osobních údajů do Spojených států se již v minulosti vyjadřovala Evropská komise[133] i Evropský parlament[134]. Také český Úřad pro ochranu osobních údajů upozornil, že samotné přistoupení k programu Safe Harbor nezaručuje dostatečnou ochranu předávaných osobních údajů a doporučil současné užití jiných právních titulů pro předávání. K tomuto dospěl zejména v souvislosti s odhalením programů Spojených států, v rámci kterých docházelo k předávání údajů občanů Evropské unie prostřednictvím některých internetových společností americkým veřejným orgánům, což mělo negativní dopad na důvěru ve způsob zpracování ochrany osobních údajů v USA.[135] Na základě výše zmíněného rozsudku Schrems proti Data Protection Commissione[136] však současně došlo ke zrušení rozhodnutí Evropské komise a tedy i ke zrušení programu Safe Harbor. Vzápětí poté tedy došlo k právnímu vakuu v oblasti tohoto právního titulu předávání se Spojenými státy a americké společnosti musely využít jiných právních titulů předávání. Tento stav byl po

[133] Sdělení Komise Evropskému parlamentu a Radě ze dne 27. listopadu 2013 „Obnovení důvěry v toky údajů mezi EU a USA“

[134] Usnesení Evropského parlamentu ze dne 21. února 2014 o programu agentury NSA pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů EU a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí, 2013/2188(INI)

[135] Neplatnost rozhodnutí Komise o tzv. Safe Harbor - doporučení Úřadu. In: *Úřad pro ochranu osobních údajů* [online]. 22.10.2015 [cit. 2018-07-08]. Dostupné z: https://www.uoou.cz/neplatnost-rozhodnuti-komise-o-tzv-safe-harbor-doporuceni-uradu/d-17119/p1=1099

[136] Rakouský občan Maximillian Schrems podal proti společnosti Facebook několik stížností u irského úřadu pro ochranu osobních údajů, neboť v Irsku si společnost Facebook zvolila své evropské sídlo. Reagoval tak zejména na únik informací v souvislosti s kauzou Edwarda Snowdena, kde Národní bezpečností agentura Spojených států získala přístup k serverům některých amerických poskytovatelů internetových služeb včetně Facebooku a tímto agentura získala přístup k osobním údajům subjektů údajů z Evropské unie. Pan Schrems s odvoláním na tuto kauzu napadl postup předávání osobních údajů. Irský úřad pro ochranu osobních údajů stížnost zamítl. V rámci soudního přezkumu irský Vrchní soud požádal SDEU o vyřešení předběžné otázky, zda je irský úřad pro ochranu osobních údajů při posuzování stížnosti, podle které ve Spojených státech údajně není zajištěna adekvátní ochrana pro subjekty údajů, absolutně vázán rozhodnutím Komise o programu Safe Harbor či může provést vlastní šetření. Generální advokát evropského soudu Yves Bot v září 2015 zveřejnil své stanovisko, podle něhož existence programu Safe Harbor nemůže vyloučit ani omezit pravomoc národních dozorových úřadů dohlížet na dodržování právních předpisů na ochranu osobních údajů. S odkazem na kauzu úniku osobních údajů prohlásil, že je dokonce možné tento program považovat za zcela neplatný, neboť občané EU nemají v USA možnost se proti tomuto masovému a neadresnému sledování bránit. SDEU se s tímto názorem ztotožnil a rozhodnutí Komise včetně programu Safe Harbor zrušil.

několika měsících jednání odstraněn až přijetím nového programu EU-US Privacy Shied.[137] Tento program je založen na systému certifikace, kterým se jednotlivé přistoupivší společnosti a organizace zavazují k dodržování souboru zásad ochrany soukromí a dále zásad vydaných Ministerstvem obchodu USA. Úroveň systému ochrany subjektů údajů byla zvýšena, neboť ty mají možnost podávat stížnosti vůči společnostem v roli správců, domáhat se řešení u domovského dozorového úřadu nebo podat stížnost u Federální obchodní komise USA. V případě, že stížnost nebude z pohledu subjektu údajů uspokojivě vyřešena, má dále možnost iniciovat závazné rozhodčí řízení před zvláštní rozhodčí komisí.[138] Dne 12. ledna 2017 k tomuto standardu ochrany osobních údajů přistoupilo také Švýcarsko za účelem chránit osobní údaje svých občanů při transferu dat do Spojených států.[139]

Právní důvod předávání na základě rozhodnutí Komise však není časově neomezený. Komise rozhoduje na základě prováděcího aktu, který stanovuje mechanismus pro pravidelný přezkum, prováděný nejméně každé čtyři roky. Významnou činností Komise představuje následné sledování vývoje u dotčených zemí či skupin, který by mohl mít vliv na fungování udělených rozhodnutí. V případě, kdy zjistí, že standardy ochrany osobních údajů nejsou dodržovány, rozhodne bez zpětné působnosti o zrušení, změně nebo pozastavení působnosti uděleného rozhodnutí. Komise má v rukou rovněž nástroj v podobě okamžitě použitelného právního aktu pro situace, kdy se jedná o naléhavé případy závažného porušení ochrany osobních údajů, například při soustavném porušování lidských práv či válečném konfliktu.

Za předpokladu, že jsou Komisí zjištěna pochybení, konzultuje daný stav s příslušnou třetí zemí či mezinárodní organizací s cílem odstranění nedostatků tak, aby mohlo pokračovat předávání na podkladě rozhodnutí. Ve vztahu k výše zmíněnému programu Privacy Shied začíná být znovu aktuální otázka, zda je ochrana osobních údajů, pocházejících z evropského prostoru, předávaných do Spojených států, dostačující, a to ani ne dva roky po jeho zavedení. V době

[137] Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle Směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí

[138] EU-U.S. Privacy Shied Framework - Key New Requirements for Participating Companies. In: *Privacy Shied Framework* [online]. 2018 [cit. 2018-07-08]. Dostupné z: https://www.privacyshield.gov/Key-New-Requirements

[139] Swiss-US Privacy Shied: better protection for data transferred to the USA. In: *The Federal Council* [online]. 11.1.2017 [cit. 2018-07-08]. Dostupné z: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-65210.html

tvorby této práce bylo vydáno Usnesení Evropského parlamentu[140], které zpochybňuje adekvátnost ochrany osobních údajů v rámci programu Privacy Shied, uplatňovaného ve Spojených státech, a to zejména s ohledem na postupné proměny přístupu Spojených států k imigrační politice.[141] Zvýšená kontrola v této oblasti však negativně dopadá i na ochranu osobních údajů, neboť není vyloučeno opakování situace, kdy orgány veřejné moci Spojených států dostaly přístup k osobním údajům občanů Evropské unie, či došlo k vynětí těchto osob z působnosti amerického zákona o ochraně soukromí.[142] K dalšímu skandálu došlo na jaře roku 2018, kdy společnost Cambridge Analytica, zabývající se politickým poradenstvím při volební kampani Donalda Trumpa, získala osobní data několika desítek milionů uživatelů Facebooku, z toho také několika milionů údajů pocházejících z evropského prostoru. Tyto údaje měla následně využít v rámci volebních kampaní.[143]

Eurokomisařka pro spravedlnost Věra Jourová vyjádřila znepokojení nad touto situací a projednala se Spojenými státy možnosti nápravy, a to do doby příštího výročního přezkumu. Z výsledků jednání vyplynulo, že řešení by mohlo přinést jmenování stálého ombudsmana, který by se měl zabývat stížnostmi občanů Evropské unie proti zpracování jejich osobních údajů ve Spojených státech, dále efektivnější a průběžné monitorování ze strany Komise a úpravu národní legislativy. Ze strany Spojených států se však toto jednání nevyvinulo v konstruktivní řešení problému a ochrana osobních údajů, pocházejících z evropského prostoru, zůstala na neakceptovatelné úrovni. S ohledem na tato znepokojení Evropský parlament ve svém usnesení stanovil Spojeným státům lhůtu k odstranění nedostatků do 1. září 2018 a v případě, že náprava nebude zjednána, vyzval Komisi, aby program Privacy Shied pozastavila. Právě s odkazem na již zmiňovaný rozsudek Maximillian Schrems proti Data Protection Commissione zdůrazňuje, že ochrana osobních údajů ve třetích zemích musí být

[140] European Parliament resolution on the adequacy of the protection by the EU-US Privacy Shied 2018/2645(RSP)

[141] *Executive Order: enhancing Public safety in the Interior of the United States* [online]. In: . 25.1.2017 [cit. 2018-07-08]. Dostupné z: https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/

[142] Trump order strips privacy rightsfrom non - U.S. citizens, could nix EU-US data flows. *TechCrunch* [online]. 26.1.2017 [cit. 2018-07-08]. Dostupné z: https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/

[143] Facebook data scandal also affect 2.7M EU citizens. In: *Techcrunch* [online]. 6.4.2018 [cit. 2018-07-10]. Dostupné z: https://techcrunch.com/2018/04/06/facebook-data-scandal-eu-citizens/

rovnocenná jako ve státech evropského prostoru. Není-li tedy v rámci národní legislativy Spojených států zajištěna možnost domáhat se obrany proti zpracování stejně jako toto právo přísluší americkým občanům, nelze o rovnocenných podmínkách hovořit. Usnesení má zásadní dopad, neboť právního titulu k přenosu osobních údajů využívá většina velkých společností, jako jsou například Google, Amazon, Microsoft či Twitter. V současné době je v tomto programu registrováno kolem čtyř tisíc společností a řešení otázky transatlantických dat proto představuje jeden ze základních kamenů fungování obchodních vztahů mezi Spojenými státy a Evropskou unií.[144]

Ve dnech 18. a 19. října 2018 proběhlo druhé výroční hodnocení rámce Privacy-Shield mezi Evropskou unií a USA, za účasti komisařky Věry Jourové a ministra obchodu Spojených států Wilbura Rosse. Dva dny podrobné diskuze se zabývaly všemi aspekty fungování tohoto programu. Od posledního výročního přezkumu byli jmenováni tři noví členové nezávislého výboru pro dohled nad soukromím a občanskými svobodami. Ve Spojených státech by rovněž měl vzniknout úřad ombudsmana pro tyto záležitosti. Výsledkem jednání bylo ponechání Privacy-Shield v účinnosti za současného stanovení další úzké spolupráce mezi EU a USA za účelem zajištění všech rámcových funkcí k řádnému fungování programu.[145]

Z právního hlediska zajímavá situace také nastane v případě odchodu Spojeného království z Evropské unie, neboť ta se tak stane „třetí zemí“, což znamená, že pokud nebude existovat zvláštní dohoda, úroveň ochrany osobních údajů Spojeného království by Evropská komise musela prohlásit za odpovídající, aby volný pohyb osobních údajů ze zemí evropského prostoru do Spojeného království pokračoval. Autorka práce má však za to, že tato situace nebude v praxi činit větší potíže, neboť ve Spojeném království je stejně jako v ostatních zemích evropského prostoru Obecné nařízení v současné chvíli aplikováno a má již vytvořen adaptační zákon. Dá se tedy říci, že pokud bude Spojené království pokračovat v současném nastavení ochrany osobních údajů, půjde spíše o formální záležitost.

---

[144] LOMAS, Natasha. *EU parliament calls for Privacy Shield to be pulled until US complies*[online]. In: . 5.7.2018 [cit. 2018-07-10]. Dostupné z: https://techcrunch.com/2018/07/05/eu-parliament-calls-for-privacy-shield-to-be-pulled-until-us-complies/?guccounter=1

[145] Joint Press Statement from Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross on the Second Annual EU-U.S. Privacy Shield Review. In: *U.S. Department of Commerce*[online]. [cit. 2018-10-21]. Dostupné z: https://www.commerce.gov/news/press-releases/2018/10/joint-press-statement-commissioner-vera-jourova-and-secretary-commerce

6.5.2 Předání založené na vhodných zárukách

Právní titul podložený rozhodnutím Komise se pro správce a zpracovatele nejeví jako příliš ideální s ohledem na to, že rozhodnutí je vydáváno na omezenou dobu a pozastavení jeho účinnosti či dokonce zrušení není vyloučeno. V takovém případě je správce či zpracovatel nucen hledat jiné cesty, kterými by daně předání právně podložil, přičemž jednu z cest představuje přijetí vhodných záruk se současným zajištěním vymahatelné ochrany práv subjektů údajů v dané zemi či v rámci mezinárodní organizace. Tyto dvě podmínky musí být splněny současně.

Vhodné záruky můžeme rozdělit do dvou skupin. První skupinu představují takové vhodné záruky, na základě kterých může správce či zpracovatel předávat osobní údaje do třetích zemí či mezinárodním organizacím bez dalšího a nemusí získávat povolení od dozorového úřadu. Do této skupiny patří právně závazný a vymahatelný nástroj mezi orgány veřejné moci nebo veřejnými subjekty. Typickým příkladem jsou záznamy jmenné evidence cestujících tzv. PNR[146], jako záznamy poskytnuté cestujícími a shromážděné leteckými dopravci za účelem umožnění rezervace a provedení procesu odbavení. Předání těchto údajů mezi zeměmi evropského prostoru představuje efektivní nástroj předcházení terorismu a jiných forem závažné trestné činnosti. Některé třetí země poté projevily zájem o předávání těchto údajů i do jejich dispozice za účelem ochrany před terorismem, a proto byly ze strany Evropské unie uzavřeny bilaterální dohody o tomto předávání se Spojenými státy, Kanadou a Austrálií.[147] Mezi další bilaterální dohody patří dohoda mezi Evropskou unií a Spojenými státy o zpracování a předávání údajů o finančních transakcích za účelem sledování financování terorismu.[148]

V celé řadě případů dochází ke zpracování osobních údajů v rámci skupin podniků, které sídlí v různých státech, velmi často také mimo evropský prostor. Argumentace, že v rámci těchto podnikových uskupení dochází k transferu osobních údajů pouze interně, neobstojí. Stále se jedná o přesun údajů do

[146] Do práva EU transponována jako Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti

[147] Passanger Name Record (PNR). In: *European Commission: Migration and home affairs*[online]. 2018 [cit. 2018-07-11]. Dostupné z: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en

[148] Agreemnet between the European Union and The United States of America on the processing and transfer of Financial Messaging Data from the European Union on the United States for the purposes of the Terrorist Finance Tracking Program (TFTP)

dispozice třetích států. V těchto případech se jeví jako vhodné využít závazných podnikových pravidel. Skupina či uskupení podniků vypracuje návrh závazných podnikových pravidel, která jsou následně schválena místně příslušným dozorovým úřadem podle sídla hlavní pobočky skupiny podniků. Dozorový úřad posuzuje zejména právní závaznost všemi dotčenými členy dané skupiny, kategorie předávaných osobních údajů, zajištění vymahatelnosti práv subjektů údajů, způsob poskytnutí informací subjektům údajů, postup při vyřizování stížností či mechanismus spolupráce s dozorovým úřadem. K těmto pravidlům se vyjadřuje také Evropský sbor pro ochranu osobních údajů, a to za účelem dodržení principu jednotnosti uplatňování Obecného nařízení ve všech členských státech. Jsou-li závazná podniková pravidla schválena, může v rámci skupiny podniků docházet k volnému transferu osobních údajů bez ohledu na to, zda se některá dceřinná společnost nachází mimo evropský prostor. Závazná podniková pravidla však platí pouze v rámci dané skupiny či uskupení podniků a nelze je použít vně tohoto okruhu oprávněných subjektů. Doposud se jedná o nepříliš využívaný instrument, avšak lze očekávat, že bude postupně více využíván právě s ohledem na praktičnost jeho použití.[149]

Dalším nástrojem pro vytvoření vhodných záruk ochrany osobních údajů jsou standardní smluvní doložky. Jedná se o vytvoření vzorového textu smlouvy, kterou správce nebo zpracovatel z evropského prostoru uzavře se správcem či zpracovatelem v třetí zemi, kde hodlá zpracovávat osobní údaje. Smluvní doložky mohou také obsahovat ujednání, přiznávající subjektům údajů rozšířené možnosti uplatnění jejich práv, například vůči vývozcům či dílčímu zpracovateli. Obecné nařízení nevylučuje, aby ustanovení o smluvní doložce bylo včleněno přímo do textu smlouvy či bylo součástí obchodních podmínek. Evropská komise ještě v režimu Směrnice stanovila úpravu vzájemných práv a povinností v podobě tří standardních smluvních doložek. Dvě mezi dvěma správci a jednu mezi správcem a zpracovatelem. Pro každou takovou stranu je však zapotřebí mít uzavřenou jednotlivou smluvní doložku, včetně každého účelu zpracování osobních údajů.[150]

[149] Komise vede seznam schválených závazných podnikových pravidel, přičemž ke dni 24.5.2018 bylo zaevidováno kolem 150 schválených závazných podnikových pravidel viz List of companies for which the EU BCR cooperation procedure is closed. In: *European Commission* [online]. 24.5.2018 [cit. 2018-07-11]. Dostupné z: ec.europa.eu/newsroom/article29/document.cfm?doc_id=50116

[150] Standardní smluvní doložky. In: *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 2018-07-11]. Dostupné z: https://www.uoou.cz/standardni-smluvni-dolozky/ds-5074/p1=5074

V době zpracování této práce se k Evropskému soudnímu dvora dostala k projednání předběžná otázka, jejímž obsahem bylo mj. i posouzení stávajících smluvních doložek ve vztahu k zajištění adekvátní ochrany osobních údajů, přenášených z evropského prostoru na základě standardních smluvních doložek. V tzv. případu *Schrems II* stěžovatel Maximilian Schrems opět podal stížnost na irský dozorový úřad pro ochranu osobních údajů proti přenosu osobních údajů společností Facebook do Spojených států na základě standardních smluvních doložek.[151] Současná stížnost se velmi podobá jeho požadavku z roku 2015, který byl již v této kapitole zmiňován a vedl ke zrušení programu Safe Harbor. Pan Schrems tvrdí, že standardní smluvní doložky nepředstavují přiměřenou úroveň ochrany jeho osobních údajů.[152] K datu uzavření této práce nebyl výsledek řešení této předběžné otázky znám, avšak s ohledem na výše zmíněný postoj Evropské komise k otázce Privacy Shield, lze očekávat zajímavý výsledek sporu i s ohledem na to, že Obecné nařízení od doby žádosti o vyřešení předběžné otázky mezitím vešlo v účinnost. Současně užívané standardní smluvní doložky tak zůstávají nadále v účinnosti. Vhodné záruky poskytují rovněž schválené kodexy chování či schválený mechanismus pro vydání osvědčení, kterým je věnována kapitola 6.1.2 této práce.

Druhou skupinou vhodných záruk představují ty, ke kterým je potřeba předchozího povolení dozorového úřadu. Sem můžeme zařadit trojstranné smluvní doložky uzavřené s jiným správcem, zpracovatelem nebo příjemcem, který se nachází ve třetí zemi nebo je součástí mezinárodní organizace. Dalo by se tedy říci, že proti standardním smluvním doložkám se tyto „nestandardní“ odlišují právě v nutnosti souhlasu dozorového úřadu, kterému předchází posouzení, zda smluvní doložka poskytuje subjektům údajů dostatečnou ochranu a vymahatelnost jejich práv.

Dále Obecné nařízení definuje postup určený pro orgány veřejné moci a veřejné subjekty v případě, že nemají ujednán právně závazný a vymahatelný nástroj v této práci zmiňovaný například v souvislosti s PNR. V takovém případě

[151] Irish High Court Refers Chrems 2.0 to the ECJ. In: HEMMINGS, Justin. *Alston & Bird* [online]. 13.4.2018 [cit. 2018-07-11]. Dostupné z: https://www.alstonprivacy.com/irish-high-court-refers-schrems-2-0-to-the-ecj/

[152] Looming Ruling on EU Data Transfer Rules Carries Potentially Serious Implications. In: *JDSUPRA* [online]. 17.10.2017 [cit. 2018-07-11]. Dostupné z: https://www.jdsupra.com/legalnews/looming-ruling-on-eu-data-transfer-58017/

může veřejný orgán nebo veřejná instituce uskutečnit transfer osobních údajů do zahraničí skrze ustanovení vložené do správních ujednání mezi těmito orgány.[153] Jak při schvalování „nestandardních" smluvních doložek, tak při užití ustanovení vložených do správních ujednání, musí dozorový úřad postupovat na základě principu jednotnosti, který byl již v této kapitole zmiňován. Z tohoto důvodu je nutné, aby dozorový úřad schválený materiál postoupil Sboru, který vydá stanovisko k posouzení dodržení principu jednotnosti.

6.6 Další okolnosti předávání osobních údajů

Na každodenní bázi probíhají mezi státy evropského prostoru a třetími zeměmi předání osobních údajů, která nejsou založena na žádném z výše zmíněných právních titulů. Typicky sem můžeme zařadit transfery údajů, vyžadované z titulu rozhodnutí soudů či správních orgánů, nacházejících se mimo evropský prostor. Obecné nařízení k tomuto výslovně uvádí, že v takovém případě může správce či zpracovatel uvedené osobní údaje předat, pouze v případě, že existuje mezi státem evropského prostoru a třetí zemí mezinárodní úmluva, která v daném případě představuje právní titul předání. Do takové situace se dostala například společnost Microsoft[154], neboť soud Spojených států vydal soudní příkaz, ve kterém nařizoval společnosti Microsoft, aby předala americké vládě veškerou emailovou komunikaci uloženou na serverech v Irsku. Odvolací soud však následně příkaz zrušil s odůvodněním, že dotčenému předpisu nelze přikládat extrateritoriální aplikaci.[155]

Za předpokladu, že pro předání osobních údajů neexistuje právní titul na základě rozhodnutí Evropské komise o odpovídající úrovni ochrany či některá z vhodných záruk, stanovuje Obecné nařízení nadto několik výjimek, na základě kterých může i přesto k transferu do třetích zemí dojít. Do této skupiny řadíme výslovný souhlas subjektu údajů, kterým projevuje své srozumění s tím, že jeho údaje budou přeneseny do třetí země i přesto, že ochrana jeho údajů nemusí být ve třetí zemi dostatečným způsobem zajištěna. Obdobně tomu je také v případě, vyžaduje-li se transfer osobních údajů k uzavření či k dalšímu plnění smlouvy. Další výjimky představuje důležitý veřejný zájem, určení, výkon či obhajoba

[153] BUCHNER, Benedikt a Jürgen KÜHLING. *DS-GVO Datenschutz-Grundverordnung: Kommentar*. C. H. Beck, 2017. ISBN 978-3-406-70212-9, s. 815-816

[154] United States Court of Appeals for the second circuit: Microsoft Corporation v. United States of America, Doc. No. 14-2985, decided: July 14, 2016

[155] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 395

právních nároků za subjektem údajů, nebo pokud se subjekt údajů dostane do takové situace, kdy důležitý zájem na jeho straně, typicky zdravotní stav, převyšuje zájmy ochrany jeho osobních údajů. V takovém případě dojde k předání jeho osobních údajů do třetí země. Do kategorie výjimek se z logiky věci řadí i osobní údaje pocházející z veřejně dostupných rejstříků, vytvořených na základě vnitrostátní úpravy dané země evropského prostoru. Do účinnosti Obecného nařízení byly na základě Směrnice transponovány do zákona o ochraně osobních údajů obdobné výjimky, avšak k jejich aplikaci byl vyžadován rovněž souhlas dozorového úřadu.[156] Nad zmíněné výjimky definuje Obecné nařízení jakousi „výjimku z výjimek“, která se na základě Směrnice neaplikovala. Pod tyto zcela výjimečné případy lze zařadit jednorázový transfer, který se vztahuje pouze k omezenému počtu subjektů údajů, jeho předmětem nejsou celé kategorie osobních údajů a tento převod osobních údajů lze s ohledem na zájmy správce považovat za nezbytný. Užití tohoto právního titulu nezbavuje správce náležité informační povinnosti vůči subjektu údajů. Správce by měl užití tohoto zcela výjimečného právního titulu dobře zvážit, neboť v případě, že jej nebude schopen před dozorovým úřadem náležitě obhájit a zároveň nebude existovat jiný právní titul pro takové předání, vystavuje se sankci ze strany dozorového úřadu.[157]

Obecné nařízení výslovně podporuje rozvoj mezinárodní spolupráce mezi evropským prostorem a třetími zeměmi, zejména s ohledem na vytváření mezinárodních smluv a dohod, které samy o sobě zaštiťují přenos osobních údajů bez nutnosti využití výjimek.

[156] § 27 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

[157] BUCHNER, Benedikt a Jürgen KÜHLING. *DS-GVO Datenschutz-Grundverordnung: Kommentar*. C. H. Beck, 2017. ISBN 978-3-406-70212-9, s. 820-821

7. Dozorový úřad

7.1 Obecné aspekty postavení dozorového úřadu

Zřízení nezávislých orgánů dozoru v členských státech představuje zásadní prvek ochrany osob v souvislosti se zpracováním osobních údajů. Každý členský stát stanoví, že jeden nebo více nezávislých orgánů veřejné moci je pověřen monitorováním uplatňování Obecného nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním osobních údajů a usnadnit volný pohyb těchto osobních údajů uvnitř Unie. Dozorovým orgánem v České republice je Úřad pro ochranu osobních údajů (*dále jen „Úřad*"), který je i na základě připravovaného zákona o zpracování osobních údajů ústředním správním úřadem pro oblast ochrany osobních údajů. Tento zákon bude upravovat také aspekty týkající se Úřadu pro ochranu osobních údajů, zejména jeho opětovné zákonné ustanovení a organizaci.[158] V této práci je užíván pojem dozorový úřad, kterým je myšlena dozorující instituce v širším slova smyslu v kterémkoli členském státě a Úřad, kterým je výhradně český Úřad pro ochranu osobních údajů.

Obecné nařízení výslovně zmiňuje také možnost, že dozorových úřadů může být v rámci jednoho členského státu ustanoveno i více. V takovém případě musí členský stát určit dozorový úřad, který bude tyto úřady zastupovat ve sboru, přičemž se při naplňování role soustavy dozorových úřadů uplatní princip jednotnosti. Typickým příkladem, kde se uplatňuje mnohost na straně dozorujících úřadů je Spolková republika Německo. Na spolkové úrovni vystupuje jako orgán dohledu komisař pro ochranu údajů a svobodu informací a zároveň je dohled vykonáván úřady na úrovni jednotlivých spolkových států.[159] Nutnost zastupování jednotlivých spolkových států v Evropském sboru pro ochranu osobních údajů, je pak navenek řešena právě skrze spolkového komisaře.[160]

Do výkonu působnosti dozorového úřadu se promítá zcela stěžejní princip nezávislosti. Ten se uplatňuje nejen v rámci činnosti Úřadu jako takového,

[158] Role ÚOOÚ. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-09-19]. Dostupné z: https://www.uoou.cz/role-uoou/ds-4726/archiv=0&p1=3938

[159] § 40 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und –Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 (německý prováděcí zákon)

[160] SYDOW, Gernot. *Europäische Datenschutzgrundverordnung: Handkommentar*. 2. Auflage. Nomos Verlagsgesellschaft, 2018. ISBN 978-3-8487-4892-1, s. 1070, 1074

zejména tím, že každý členský stát je povinen zajistit dozorovému úřadu potřebné lidské, technické a finanční zdroje, infrastrukturu a prostory tak, aby mohl účinně vykonávat své pravomoci. Princip nezávislosti se vztahuje také na plnění úkolů každého jednotlivého člena dozorového úřadu, který musí být nezávislý na vnějším vlivu, přímém či nepřímém a od nikoho nesmí vyžadovat ani přijímat pokyny. Rozhodovací pravomoc by měla oproštěna od jakýchkoli vnějších vlivů na osobu vykonávající dozor.[161] Při výkonu svých úkolů musí orgány dozoru jednat objektivně a nestranně.[162]

Podmínky výkonu funkce jednotlivých členů dozorového úřadu určuje Obecné nařízení pouze obecně, kdy hovoří o způsobu jmenování, kvalifikaci, zkušenostech a skončení funkčního období. Prováděcí zákon stanovuje podrobnější pravidla pro vstup do funkce předsedy Úřadu, například potřebný věk, bezúhonnost a svéprávnost a konkretizuje potřebné vzdělání. Upravuje také neslučitelnost funkcí s funkcí předsedy Úřadu. Za členy dozorového úřadu podle čl. 53 Obecného nařízení se považují pouze předseda a dva místopředsedové Úřadu.[163] Obecné nařízení výslovně ukládá státům, aby tyto podrobnosti upravily prováděcím předpisem, včetně samotné skutečnosti zřízení dozorového úřadu. Jak již bylo v této práci několikrát zmiňováno, Česká republika dosud nemá v účinnosti tento prováděcí zákon, což může v aplikační praxi působit problémy.

Každý dozorový úřad je na území svého členského státu příslušný k plnění úkolů a výkonu pravomocí, které mu byly svěřeny v souladu s tímto Nařízením. Z působnosti Obecného nařízení je pak zcela vyňata možnost dozorovat operace zpracování, které provádějí soudy jednající v rámci svých soudních pravomocí. Sem lze zahrnout také operace zpracování, kdy soudy zpracovávají osobní údaje za účelem provedení dokazování. Případné použití práva námitek ze strany subjektů údajů by mohlo mít závažné důsledky do oblasti nezávislosti soudů. Jak již bylo zmiňováno v této práci v rámci podkapitoly věnované pověřenci pro ochranu osobních údajů, činnosti dozorového úřadu vůči soustavě soudů nejsou omezeny vůči zpracování osobních údajů, které soudy provádí v rámci běžné agendy, jako například soukromí správci.

[161] SYDOW, Gernot. *Europäische Datenschutzgrundverordnung: Handkommentar*. 2. Auflage. Nomos Verlagsgesellschaft, 2018. ISBN 978-3-8487-4892-1, s. 1295-1296

[162] Více k tomuto např. Rozsudek Soudního dvora EU ze dne 9. března 2010, Evropská komise proti Spolkové republice Německo, věc C-518/07

[163] § 50-51 vládního návrhu prováděcího zákona, Sněmovní tisk č. 138

7.2 Pravomoci a úkoly dozorového úřadu

Jak už název vypovídá základním posláním dozorového úřadu je dozorová činnost. V souladu s čl. 51 odst. 1 Obecného nařízení ve spojení s § 2 a 3 zákona o ochraně osobních údajů je pro oblast ochrany osobních údajů v rozsahu stanoveném Obecným nařízením a zvláštními předpisy Úřad pro ochranu osobních údajů. Správní dozor je činnost, při které dozorující orgán sleduje chování nepodřízených subjektů a porovnává je s žádoucím stavem. V návaznosti na zjištěný nesoulad potom využívá nápravné nebo sankční prostředky. Správní dozor se tedy skládá ze dvou fází. První fáze kontroly, spočívající ve zjišťování a hodnocení a dále fáze aplikace nápravných nebo sankčních prostředků, která nastává jako fakultativní fáze a je vázána na výsledek zjištění a hodnocení.[164]

Výčet úkolů dozorového úřadu uvádí čl. 57 Obecného nařízení, které lze rozdělit do několika základních okruhů, a to uplatňování Obecného nařízení v praxi, vzdělávání, mezinárodní spolupráci, již zmiňovaný výkon dozoru a další činnosti. Pro aplikační praxi jednu z nejdůležitějších činností Úřadu představuje právě sledování dopadů Obecného nařízení. Za tímto účelem je sice možné využít obecných výkladových stanovisek skupiny WP29, avšak ta mají obecný charakter, aby mohla být využitelná ve všech členských státech. Úřad vydává vlastní doplňující stanoviska zejména k otázkám české aplikační praxe se zohledněním veškerých aspektů domácí legislativy. Pozitivně autorka práce hodnotí dosavadní publikační činnost Úřadu určenou běžným občanům i společnostem ohledně otázek, týkajících se aplikace Obecného nařízení v různých životních situacích a oborech činnosti, a to zejména formou často kladených otázek.[165] Lze tedy předpokládat, že Úřad tak bude postupovat i po účinnosti českého prováděcího zákona, což by bylo jedině pozitivní, neboť by správci a zpracovatelé rychleji tuto úpravu zapracovali do činností zpracování.

Obecné nařízení rovněž akcentuje vzdělávací a poradenskou činnost dozorových úřadů, přičemž autorka této práce má za to, že provádění tohoto úkolu ze strany Úřadu v jistých otázkách poněkud zaostává. Ačkoli je výše zmíněná publikační činnost a vydávání podpůrných materiálů ze strany Úřadu poměrně široké, logicky není možné obsáhnout veškeré aspekty aplikace Obecného nařízení. Úřad by však měl být schopen na požádání poskytnout subjektům údajů

[164] Dozorová činnost. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-09-24]. Dostupné z: https://www.uoou.cz/dozorova-cinnost/ds-1277/p1=1277

[165] např. Často kladené otázky podle oblastí; *Úřad pro ochranu osobních údajů* https://www.uoou.cz/casto-kladene-otazky-podle-oblasti/ds-2619/p1=2619

informace ohledně výkonu práv a podporovat povědomí správců a zpracovatelů o jejich povinnostech dle Obecného nařízení. Tento úkol však naplňuje pouze zčásti, neboť jak vyplývá z vyjádření Úřadu, odpovědi na jednotlivé otázky bude vyřizovat pouze ve vymezeném rozsahu – nejvíce při uplatnění práv subjektů údajů a otázky pověřenců. [166] V případě jiného okruhu otázek, typicky například ze strany správců Úřad odkazuje na již vydané podpůrné materiály. Ačkoli si je autorka práce vědoma omezených personálních kapacit Úřadu, není možné, aby se Úřad distancoval od zodpovídání jednotlivých dotazů, nespadajících do příslušných kategorií a zákonně vymezeným konzultacím před zahájením zpracování podle čl. 36, a aby následně Úřad ukládal nápravná a sankční opatření za nedodržení Obecného nařízení. Rovněž pořádání edukativních akcí ze strany Úřadu je z velké části směřováno zejména na pověřence a běžní správci jsou nuceni využít vzdělávací akce soukromých společností, jejichž kvalita mnohdy neodpovídá ceně za tato školení. Na druhé straně je nutno říci, že Úřad v roce 2018 zorganizoval vzdělávací akce pro podnikatelské subjekty v několika krajských městech, ale kapacita těchto školení nebyla ze strany správců zcela vyčerpána. V rámci jednotlivých oborů činnosti lze doporučit správcům využít možnosti informovat se také u příslušných ministerstev, profesních komor a neziskových organizací, které často vydávají vlastní podpůrné materiály, například Ministerstvo školství[167], Česká advokátní komora[168] apod.

Plnění úkolů Úřadu je bezplatné, výslovně se o tomto Obecné nařízení vyslovuje ve vztahu k zodpovídání dotazů ze strany pověřenců a výkonu práv subjektů údajů vůči Úřadu. Podle názoru autorky však poněkud nelogicky vymezuje Obecné nařízení tyto skupiny adresátů, byť výkon povinností správců vůči Úřadu – typicky například předchozí konzultační povinnost, by měla být rovněž bezplatná. Obdobně jako při výkonu práv subjektů údajů vůči správci může Úřad některé úkony zpoplatnit, a to v případě nedůvodných či nepřiměřených požadavků.

Jedním z důležitých úkolů Úřadu je také usnadňovat subjektům údajů podávání stížností. Za tímto účelem Úřad vytvořil kontaktní formulář, při jehož

[166] Informace ke konzultačním službám. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-09-23]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30721

[167] Metodická pomůcka k aplikaci GDPR ve školství. *Ministerstvo školství, mládeže a tělovýchovy ČR* [online]. 2017 [cit. 2018-09-23]. Dostupné z: http://www.msmt.cz/dokumenty-3/metodicka-pomucka-k-aplikaci-obecneho-narizeni-o-ochrane

[168] GDPR pro advokáty. *Česká advokátní komora* [online]. 2018 [cit. 2018-09-23]. Dostupné z: https://www.cak.cz/scripts/detail.php?id=18817

vyplňování je subjekt údajů krok za krokem veden tak, aby Úřad zjistil všechny potřebné informace nutné pro zvolení účinného a cíleného postupu vůči správci či zpracovateli. Subjekt údajů by měl podrobně identifikovat správce či zpracovatele, poskytnout Úřadu informace, jakým způsobem a formou uplatnil svá práva napřed přímo u správce či zpracovatele a popřípadě jak byl tento podnět ze strany správce řešen, kdy závěrem následuje prostor pro podrobný popis skutečností, ve kterých subjekt údajů spatřuje pochybení na straně správce při zpracování osobních údajů.[169] Formulář je snadno dohledatelný na webových stránkách Úřadu a má přehledný charakter, a proto dle názoru autorky usnadňuje podání takové stížnosti. S účinností Obecného nařízení přibyly dozorovým úřadům některé nové úkoly, jako zavedení mechanismů pro vydávání osvědčení se současným předáním informací o akreditačním subjektu Evropskému sboru pro ochranu osobních údajů nebo činnosti související s nutností provedení posouzení vlivu na ochranu osobních údajů.

Co se týká pravomocí dozorového úřadu, jejich rozsah se příliš neliší od dosavadního stavu, Obecné nařízení upravuje kompetence k některým novým institutům. Vždy je však nutné mít na paměti, že výkon pravomocí dozorového úřadu může probíhat pouze v souladu s vnitrostátní procesní úpravou. Recitál Obecného nařízení ukládá některé základní zásady výkonu těchto pravomocí. Ty by měly být vykonávány nestranně, spravedlivě a v přiměřených lhůtách.[170]

Pravomoci dozorového úřadu lze rozdělit do tří okruhů, a to na pravomoci vyšetřovací, nápravné, povolovací a poradní. Vyšetřovací pravomoci zahrnují soubor nástrojů, kterými může dozorový úřad efektivně prošetřit souladnost zpracování u správce, tedy například žádat předložení potřebných materiálů či vstupovat do všech prostor, kde správce či zpracovatel působí. V případě, že je zjištěno pochybění na straně správce či zpracovatele, přichází v úvahu široká paleta nápravných a sankčních pravomocí dozorového úřadu. Nápravné pravomoci dozorového úřadu se uplatní ve druhé fázi úkolů za předpokladu, že byl zjištěn skutkový stav, který byl dále vyhodnocen jako neuspokojivý. Od mírnějších forem zjednání nápravy v podobě napomenutí či upozornění až v možnost udělit správní pokutu. Poslední okruh pravomocí dozorového úřadu spočívá v plnění jeho poradní a povolovací funkce. Dalo by se říci, že se jedná o

[169] Příloha č. 2 Formulář pro podávání stížností
[170] Bod 129 Recitálu k Obecnému nařízení

úkoly vedlejší. Sem patří například vydávání stanovisek, akreditace subjektů pro vydávání osvědčení nebo přijímání standardních doložek o ochraně údajů.[171]

Nejčastějším důvodem zahájení kontrolního šetření ze strany Úřadu je stížnost ze strany subjektu údajů. Úřad takový podnět vyhodnotí, a je-li shledán důvodným a závažným, zahájí kontrolní řízení. Nejčastěji Úřad řeší užití kamerových systémů s ohledem na ochranu osobních údajů, telemarketing, nevyřešení dotazu subjektu údajů ze strany správce a na přelomu účinnosti Obecného nařízení také agresivní získávání souhlasů ze strany správců. V první fázi nejčastěji osloví správce nebo zpracovatele informačním dopisem, který měl ve vztahu k danému subjektu údajů pochybit při zpracování jeho osobních údajů, a snaží se s ním vyjasnit situaci. Obecně Úřad vykonává kontroly v rámci kontrolního plánu, který je zaměřen na určitě kategorie správců a z nich jsou pak vytipovány jednotlivé kontrolované subjekty – například nemocnice, správci poskytující věrnostní programy pro zákazníky apod. Posledním důvodem zahájení kontroly ze strany Úřadu představuje skupina nových zpracování, zejména s ohledem na nové technologie, např. fitness hodinky, vyhodnocující citlivé údaje uživatelů se současným propojením s mobilní aplikací. Kontrolní činnost Úřadu se přitom řídí kontrolním řádem[172] a jejím účelem je zjistit faktický stav s přihlédnutím k právům a povinnostem kontrolovaného, přičemž Úřad již mnohokrát připomínal, že provedení kontroly automaticky neznamená uložení sankce. Kontrolní řízení přitom může probíhat také korespondenčně, například si Úřad vyžádá veškeré písemnosti k uplatnění práva subjektu údajů a není tedy nutné místní šetření v sídle či pobočce správce.[173]

7.3 Mezinárodní spolupráce a princip jednotnosti výkonu úkolů

Jak již bylo zmíněno v úvodu této kapitoly, při výkonu činností dozorových úřadů se uplatňuje stěžejní princip jednotnosti, a to nejen v rámci jednoho členského státu v případě existence soustavy dozorových úřadů, ale zejména a v praxi častěji na úrovni ústředních dozorových úřadů jednotlivých členských států. Důvodem změn právní úpravy ochrany osobních údajů bylo mimo jiné zajistit jednotnost aplikace předpisů práva ochrany osobních údajů. Za

[171] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 426-430

[172] Zákon č. 255/2012 Sb., o kontrole (kontrolní řád)

[173] ŽŮREK, Jiří. *Seminář Ochrana osobních údajů ve firmách v době účinnosti GDPR- Úřad pro ochranu osobních údajů v době účinnosti GDPR* uskutečněný dne 17.10.2018 v Ústí nad Labem, pořádající Ministerstvo průmyslu a obchodu a Technologické centrum AV ČR

tímto účelem vyzdvihuje Obecné nařízení princip jednotnosti jako nástroj koherentní aplikace ve všech členských státech. Velká část dozorových úřadů byla ustanovena na základě transpozice směrnice 95/46/ES, a tedy i rozsah jejich pravomocí v rámci spolupráce s dalšími dozorovými úřady byl stanoven různě. Uplatňováním principu jednotnosti se zvýší efektivita horizontální administrativní spolupráce mezi členskými státy, což lze hodnotit jedině pozitivně.[174]

Mechanismy spolupráce mezi dozorovými úřady probíhají na tzv. principu One-Stop-Shop. Ten se uplatňuje zejména tam, kde správci provádějí přeshraniční zpracování osobních údajů. Správci působící ve více členských státech a provádějících toto přeshraniční zpracování museli podle dosavadní právní úpravy plnit povinnosti vůči všem dozorovým úřadům. Princip One-Stop-Shop přináší zjednodušení, neboť se z této skupiny dotčených dozorových úřadů vyčlení místně příslušný úřad podle hlavní provozovny správce, který bude vedoucím dozorovým úřadem, a u tohoto úřadu bude správce plnit své povinnosti. Obecné nařízení specifikuje spolupráci mezi vedoucím dozorovým úřadem a na něj jsou napojeny ostatní dozorové úřady, které vystupují jako úřady dotčené, nebo také dožádané. Vedoucí dozorový úřad může požádat dotčené dozorové úřady o vzájemnou pomoc nebo ve spolupráci s nimi provádět společné postupy. Dotčené dozorové úřady pak mohou sdělovat vedoucímu dozorovému úřadu svá stanoviska a proti jeho rozhodnutí mají právo vznést námitky. Finální rozhodnutí vedoucího dozorového úřadu se oznamuje správci či zpracovateli k přijetí opatření k zajištění souladu zpracování s tímto rozhodnutím.[175]

7.3.1 Vzájemná pomoc a společné postupy

Za účelem soudržného provádění a uplatňování Obecného nařízení musí být ze strany dozorových úřadů členských států zavedeny mechanismy vzájemné pomoci, které budou zahrnovat zejména vyřizování žádostí o informace a opatření v oblasti dozoru, například žádosti o předchozí povolení a konzultace, inspekce a šetření. Každý dozorový úřad musí být vybaven takovými technickými a personálními prostředky, aby byl schopen zajistit účinnou a včasnou pomoc dožadujícímu úřadu jiného členského státu. Dozorové úřady si poskytují

[174] SYDOW, Gernot. *Europäische Datenschutzgrundverordnung: Handkommentar*. 2. Auflage. Nomos Verlagsgesellschaft, 2018. ISBN 978-3-8487-4892-1, s. 1207

[175] BUCHNER, Benedikt a Jürgen KÜHLING. *DS-GVO Datenschutz-Grundverordnung: Kommentar*. C. H. Beck, 2017. ISBN 978-3-406-70212-9, s. 895-896

informace ve standardizovaném elektronickém formátu a poskytnutí takové pomoci musí být až na výjimky provedeno bezplatně. Vzájemná pomoc zahrnuje kromě poskytnutí informací také povinnost provést úkon pro daný dožadující úřad.

Dozorové úřady dále mohou provádět společné postupy, šetření a společně vést donucovací prostředky, do nichž jsou zapojeni pracovníci dozorových úřadů jiných členských států. Společné postupy se uplatní zejména tam, kde správce či zpracovatel provozuje svoji činnost na území více členských států a jeho aktivity se dotýkají většího množství subjektů údajů. S tím souvisí i možnost vyslat pracovníky jednoho dozorového úřadu k jinému. Pro správce a zpracovatele má mezinárodní spolupráce dozorových úřadů dopady zejména tím, že mnohdy mohou spadat pod pravomoc cizozemského dozorového úřadu.

7.4 Evropský sbor pro ochranu osobních údajů

Evropský sbor pro ochranu osobních údajů (dále jen *„Sbor“*) je nezávislý evropský subjekt, který přispívá k jednotnému uplatňování pravidel ochrany údajů v celém evropském prostoru a prosazuje spolupráci mezi úřady pro ochranu osobních údajů v evropském prostoru. Do účinnosti Obecného nařízení vykonávala tuto působnost skupina WP29, zřízené podle čl. 29 Směrnice, která však byla zejména poradním orgánem. Ke zpracování této práce bylo použito množství pokynů a výkladových stanovisek, které tato skupina vydala. Na její místo po účinnosti Obecného nařízení nastoupil právě Sbor, který rovněž pokračuje v poradní činnosti, a to zejména poskytování poradenství Komisi ohledně záležitostí, týkajících se ochrany osobních údajů, vydávání obecných stanovisek. Dosavadní stanoviska, vydaná skupinou WP29, Sbor přijal.[176] V době tvorby této práce se již objevily některé nové výkladové pokyny, vydané přímo Sborem, a to ohledně vydávání osvědčení podle článků 42 a 43 Obecného nařízení a výjimek pro specifické situace podle článku 49 Obecného nařízení.[177]

Cílem Sboru je zajišťovat jednotné uplatňování Obecného nařízení v evropském prostoru. Jeho postavení je nezávislé, což znamená, že není vázán

[176] Endorsement of GDPR WP29 guidelines by the EDPB. *The European Data Protection Board* [online]. 2018 [cit. 2018-10-07]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

[177] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679. In: *European Data Protection Board* [online]. 2018 [cit. 2018-10-03]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

pokyny žádné jiné instituce Evropské unie. Vztah ke Komisi je vymezen jednak jejím právem účastnit se zasedání Sboru skrze svého zástupce, avšak bez hlasovacího práva, ale také možnosti požádat Sbor o konzultaci nebo vydání výkladového stanoviska. Obecné nařízení mu přiznává vlastní právní subjektivitu, což má důsledky zejména v rozšíření jeho pravomocí. Kromě poradní funkce je to výkon pravomocí nad osobami a dozorovými úřady. Jedná se například o provádění akreditace subjektů, vydávání osvědčení a její pravidelný přezkum, monitoring a zajištění řádného uplatňování Obecného nařízení nebo prošetřování uplatňování Obecného nařízení. Sbor je složen ze zástupců jednotlivých členských států, přičemž tímto zástupcem je vedoucí příslušného dozorového úřadu nebo jeho zástupce. Sbor si pak z řad svých členů volí předsedu a dva místopředsedy.[178]

[178] About EDPB. In: *European Data Protection Board* [online]. [cit. 2018-10-07]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb_cs

8. Možnosti právní ochrany, sankce a odpovědnost

Následující kapitola si klade za cíl postihnout možnosti právní ochrany v případech, kdy dochází k nesprávnému zpracování osobních údajů nebo postupu dozorového orgánu. „Poškozenému“ je dána celá řada prostředků, jakým způsobem se může bránit. Jedním z hlavních důvodů, proč je Obecné nařízení tolik diskutovaným tématem současné doby, je možnost uložení sankcí za jeho neplnění, zejména správních pokut, jejichž maximální výše byla Obecným nařízením výrazně zvýšena. Zejména ze strany médií se vyskytla snaha šokovat a vyděsit veřejnost, z čehož vzešla celá řada mýtů, týkající se výkladu Obecného nařízení. Cílem této kapitoly bude obsáhnout různé druhy sankcí s důrazem na to, že uložení správní pokuty je pouze jednou z možností, která je ukládána za nejzávažnější porušení.

8.1 Právo podat stížnost u dozorového úřadu

Možnost podat stížnost proti zpracování u dozorového úřadu již byla v této kapitole zmiňována, zejména v souvislosti s tím, že dozorový úřad má povinnost ulehčovat podávání takových stížností. Právo podat stížnost se uplatňuje v okamžiku, kdy se subjekt údajů domnívá, že v průběhu zpracování jeho osobních údajů došlo ze strany správce či zpracovatele k porušení ustanovení Obecného nařízení, například že správce nemá ke zpracování právní titul, tedy zpracovává jeho osobní údaje neoprávněně či nereaguje na uplatnění práv subjektu údajů.

Obecné nařízení výslovně zakotvuje možnost volby subjektu údajů, jaký zvolí místně příslušný dozorový úřad, a to buď v místě svého obvyklého bydliště, místě výkonu zaměstnání nebo místě, kde došlo k namítanému porušení zásad zpracování. Výrazně se tím posilují práva subjektu údajů na možnost volby uplatnění práva. Z pohledu dozorového úřadu může docházet ke komplikacím, zejména v případě přeshraničního zpracování.

Obecné nařízení také dává subjektu údajů výslovně možnost nechat se při podání stížnosti zastoupit neziskovým subjektem. Tímto krokem se Obecné nařízení snaží přispět k posílení práv subjektů údajů, které často nemusí mít dostatek znalostí a zkušeností, aby mohly využít některé z možností právní ochrany. Tuto možnost připouštěla také Směrnice, zákon o ochraně osobních údajů však toto zastoupení neupravoval. Tento neziskový subjekt musí být

založen podle práva členského státu a jeho hlavní činnost nesmí být komerční. V této souvislosti rozlišujeme zastoupení subjektu údajů s pověřením neziskového subjektu. Stanoví-li tak právní řád členského státu, je možné uplatnit v případě, že bude poškozených subjektů více, hromadnou žalobu. Návrh zákona o zpracování osobních údajů však s tímto institutem nepočítá. Druhý typ představuje zastoupení subjektu bez pověření subjektu údajů, což v praxi znamená, že by neziskový subjekt mohl podat stížnost u dozorového úřadu, bez přičinění subjektu údajů. V tomto případě je opět dáno k úvaze členským státům, zda v prováděcích předpisech tento institut zakotví. Ani s tímto český prováděcí předpis nepočítá.[179] Dle názoru autorky však zavedení možnosti využít pomoci neziskových subjektů v této oblasti v mnohých případech povede ke zneužívání práva ze strany subjektů údajů, neboť se již na evropské úrovni objevily případy takových neziskových subjektů, které sice budou subjekt údajů bezplatně zastupovat v rámci daného řízení, ale v případě vymožení plnění zejména z titulu náhrady nemajetkové újmy by na tomto měly zájem participovat, a to ačkoli se jedná o neziskové subjekty. Autorka této práce má za to, že by pozice neziskových subjektů měla zůstat v roli informační a poradenské, bez možnosti zastupování, kdy jen praxe ukáže, zda se tyto obavy naplní či nikoli.

8.2 Právo na soudní ochranu

Právo na soudní ochranu se dělí do dvou větví, v prvé řadě na soudní ochranu proti nečinnosti dozorového úřadu a ve druhé na soudní ochranu proti porušení práv subjektu údajů ze strany správce či zpracovatele. Jak bude dále popsáno v této práci, příslušných soudů může být i několik, a to napříč soudy jednotlivých členských států. Autorka proto upozorňuje, že se proto může stát, že řízení bude zahájeno ohledně stejného předmětu řízení, pokud jde o zpracování prováděné týmž správcem či zpracovatelem, u více soudů zároveň. Soudy by tedy takovou skutečnost měly zkoumat od počátku. Poněkud nekonzistentně s obecnými právními zásadami udává Obecné nařízení soudu, který zjistí, že o řízení se stejným předmětem a účastníky je již řízení zahájeno u jiného soudu členského státu, který ho zahájil jako první, může soud „druhý či další v pořadí“ své řízení přerušit. Obecné nařízení také zmiňuje slovo „může“ nikoli musí a ponechává tuto volbu na uvážení soudu. Podle obecné překážky litispendence,

[179] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 472-473

jako typického institutu procesního práva, které vychází ze zásady ne bis in idem, by však měl soud takové řízení zastavit, a to právě s ohledem na nepřekonatelnou překážku řízení v podobě věci zahájené. Obdobně by měl soud postupovat i v případě rei iudicata. Nejedná se však o chybu českého překladu, výraz přerušení se objevuje i v jeho originálním znění. Pouhé přerušení řízení tento problém z logiky věci neřeší a mohlo by tak docházet v soudní praxi k zásadním vadám řízení, kdy by bylo např. právo vzešlé ze stejného řízení se stejnými účastníky přiznáno dvěma soudy zároveň nebo by se dokonce rozhodnutí jednotlivých soudů lišila.

8.2.1 Právo na soudní ochranu proti dozorovému úřadu

U prvně zmiňovaného případu může být v pozice žalobce aktivně legitimován jak subjekt údajů, tak správce či zpracovatel. Tato situace se bude lišit podle toho, o jaký výkon pravomocí ze strany dozorového úřadu půjde. Je-li napadáno závazné rozhodnutí dozorového úřadu, je aktivně legitimován ten, kdo tvrdí, že se ho takové rozhodnutí dotýká, což bude nejčastěji správce nebo zpracovatel. Ačkoli Obecné nařízení zakotvuje tento typ soudní ochrany výslovně, stejně tak jako tomu bylo doposud, se podpůrně užije nejprve postup v rámci správního řízení a dále správního soudnictví. Protože je ochrana osobních údajů natolik specifickou oblastí práva a v České republice existuje pouze jednostupňová soustava správních orgánů, kterou představuje Úřad pro ochranu osobních údajů, je nejprve nutné podat proti rozhodnutí Úřadu rozklad. Při podání rozkladu se zřizuje rozkladová komise, která se bude tímto podáním zabývat. O rozkladu pak rozhoduje vedoucí Úřadu.[180] Po vyčerpání tohoto opravného prostředku v rámci správního řízení přichází na řadu ochrana v rámci správního soudnictví.

Obecné nařízení výslovně zmiňuje také soudní ochranu určenou proti nečinnosti dozorového úřadu v případě podání stížnosti ze strany subjektu údajů. Nečinnost představuje jednak to, že se dozorový úřad stížností vůbec nezabývá, neinformuje subjekt údajů do 3 měsíců o pokroku v započatém řešení podané stížnosti nebo nepodá informaci o meritorním rozhodnutí ve věci. Dále by měl dozorový úřad výslovně poučit subjekt údajů o faktické možnosti tohoto soudního přezkumu. V českém právním řádu je pak dále specifikováno, aby před podáním

[180] § 152 zákona č. 500/2004 Sb., správní řád

žaloby na ochranu proti nečinnosti žalobce vyčerpal všech procesních nástrojů ochrany.[181]

Oba výše zmíněné druhy ochrany se uplatní u místně příslušného soudu členského státu, kde je dozorový úřad zřízen, což je v případě České republiky v řízeních proti Úřadu pro ochranu osobních údajů Městský soud v Praze, coby prvoinstanční soud. Bylo-li v dané věci vydáno stanovisko Sboru nebo rozhodnutí dozorového úřadu, přikládají se tyto dokumenty k žalobnímu návrhu. Závěrem této podkapitoly je třeba zmínit, že podáním žaloby proti dozorovému úřadu nejsou vyloučeny prostředky jiné soudní či mimosoudní ochrany, zejména v oblasti náhrady škody či jiné újmy.[182]

8.2.2 Právo na soudní ochranu proti správci či zpracovateli

Subjektu údajů je přiznáno právo na soudní ochranu v případě, že byla porušena jeho práva zaručená Obecným narušením ze strany správce či zpracovatele. Toto právo se navzájem nevylučuje s jinou dostupnou správní či mimosoudní ochranou, včetně možnosti podat stížnost u dozorového úřadu. Žalobní důvod přitom Obecné nařízení definuje jako situaci, kdy subjekt údajů pociťuje zpracování osobních údajů ze strany správce či zpracovatel jako porušení práv, které Obecné nařízení zaručuje. Pro úplnost lze dodat, že jako stížnostní důvod podle čl. 77 Obecného nařízení je definováno „porušení Nařízení." Fakticky se však stížnostní důvody stírají s těmi žalobními. Například typicky v případě, že správce opírá zpracování o svůj oprávněný zájem, přitom subjekt údajů má za to, že tato podmínka není naplněna a současně správce nedisponuje jiným právním titulem zpracování.

Řízení proti správci či zpracovateli bude zahájeno podáním žalobního návrhu u soudu členského státu, v němž má daný správce nebo zpracovatel provozovnu. Žalobu je možné také podat i u soudu členského státu, kde má subjekt údajů obvyklé bydliště. Tato možnost se vylučuje v případě, kdy je správcem či zpracovatelem, coby žalovaným orgán veřejné moci některého členského státu, který jedná v rámci výkonu veřejné moci. Ani v tomto případě není vyloučeno, aby se subjekt údajů nechal zastoupit neziskovou organizací.

[181] § 79 a násl. zákona č. 150/2002 Sb., soudního řádu správního

[182] Tuto problematiku upravuje zákon č. 82/1998 sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád)

8.3 Právo na náhradu újmy a odpovědnost

Obecné nařízení výslovně přiznává každému, kdo v důsledku tohoto nařízení utrpěl hmotnou či nehmotnou újmu, aby uplatňoval náhradu této újmy na správci či zpracovateli. Ze strany správce či zpracovatele se jedná o objektivní odpovědnost, bez ohledu na zavinění, což znamená, že ke vzniku újmy mohlo dojít byť i jen nedbalostním jednáním správce či zpracovatele. Jak již bylo v této práci zmíněno v kapitole věnující se povinnostem správce, odpovědnost zpracovatele je omezenější než odpovědnost správce. Zpracovatel ručí za způsobenou újmu pouze tehdy, jestliže porušil některou svou povinnost stanovenou Obecným nařízením, překročil pokyny udělené správcem nebo jednal zcela v rozporu s nimi. V případě, že je do téhož zpracování zapojeno více správců či zpracovatelů odpovědných z téhož zpracování, jsou za náhradu újmy odpovědni společně a nerozdílně, tj. uplatní se solidární odpovědnost. Soud příslušný k projednání náhrady újmy se určuje stejně, jako tomu bylo při uplatnění soudní ochrany v případě porušení práv subjektu údajů, tedy primárně u soudu členského státu, kde se nachází provozovna správce či zpracovatele. Odpovědnosti se správce či zpracovatel zprostí, prokáže-li, že nenese žádným způsobem odpovědnost za událost, která ke vzniku vedla. Sem mohou spadat některé mimořádné události jako např. živelná událost, při které došlo k úniku osobních dat nebo vloupání do prostor správce, a to i přesto, že byly tyto prostory řádně zabezpečeny. Odpovědnost za nehmotnou újmu či škodu se neuplatní pouze za porušení zpracování nejen podle Nařízení, ale také při porušení jiných pravidel práva Unie nebo členského státu. [183] Typicky půjde například o prováděcí zákon.

8.4 Správní pokuty

Jedním z důvodů proč je v současné době Obecné nařízení tak diskutovaným tématem je bezpochyby výše pokut, hrozících za jeho nedodržení, které mohou dosáhnout drakonických částek. Aby však mohla být ochrana osobních údajů naplňována efektivně, musí existovat účinná sankce za nedodržení Obecného nařízení. V rámci transpozice Směrnice jednotlivými členskými státy do jejich právních řádů došlo více než kde jinde k tomu, že se systém a výše správních sankcí ukládaných za porušení povinností značně lišila. Například právní systémy Dánska a Estonska neumožňují uložení pokut v podobě stanovené

[183] Bod 146 Recitálu Obecného nařízení

Obecným nařízením. Na to však Obecné nařízení pamatuje a nastiňuje řešení v případě, kdy není v kompetencích dozorového úřadu, aby pokutu uložil. V případě Dánska pokutu může uložit vnitrostátní soud jako trestní sankci a v Estonsku pokutu uloží dozorový úřad v přestupkovém řízení. Uplatnění takových pravidel má v uvedených členských státech účinek, který je rovnocenný správním pokutám uloženým dozorovými úřady. Příslušné vnitrostátní soudy by tedy měly zohlednit doporučení dozorového úřadu, který dal podnět k uložení pokuty.[184]

Uložení správní pokuty by mělo být účinné, přiměřené a odrazující. Jak už bylo v této práci zmíněno, orgánem, do jehož pravomoci spadá ukládání správních pokut, je dozorový úřad. Správní pokuta je přitom vedle nápravných opatření nejpřísnější sankcí, jakou může dozorový úřad uložit. Při ukládání správních pokut dává Obecné nařízení dozorovému úřadu soubor kritérií, které by měl v rámci své diskreční pravomoci v této oblasti zvážit. Patří sem například povaha, rozsah a závažnost porušení nebo skutečnosti na straně správce – zda se jednalo o úmysl či nedbalost, zda již podnikl kroky k nápravě nebo zda se jedná o recidivu při porušení povinností.[185] Podrobné pokyny k uplatňování a stanovování správních pokut zpracovala skupina WP29[186] Tato kritéria se přitom nijak neliší od těch stávajících.

Zákon o ochraně osobních údajů definuje skutkové podstaty přestupků, kterých se může správce či zpracovatel dopustit. Přestupky přitom rozděluje na ty, které může spáchat fyzická osoba, pak je stanovena maximální výše pokuty na 5.000.000,-Kč a v případě, že je naplněna skutková podstata přestupku u právnické či fyzické podnikající osoby, pak maximální výše pokuty činí 10.000.000,-Kč. Obecné nařízení nedělí kategorie správních pokut podle toho, komu jsou ukládány, ale podle závažnosti porušení. V případě méně závažných pochybení správce či zpracovatele, kam můžeme zařadit například neumožnění výkonu práv subjektu údajů, při porušení povinností ve vztahu k zabezpečení osobních údajů nebo nesplnění úkolů pověřence. Za tato porušení Obecného nařízení může dozorový úřad udělit správní pokutu až do výše 10.000.000 EUR,

[184] Bod 151 Odůvodnění Obecného nařízení

[185] Kompletní výčet kritérií při rozhodování dozorového úřadu při ukládání správních pokut je uveden v čl. 83 odst. 2 Obecného nařízení

[186] *Article 29 Data Protection Working Party: Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* [online]. 3.10.2017, (17/EN/WP253) [cit. 2018-10-20]. Dostupné z: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

nebo jedná-li se podnik, až ve výši 2% celkového ročního celosvětového obratu za předchozí finanční rok podle toho, která hodnota je vyšší. Stejná výše pokuty hrozí také akreditovanému subjektu, monitorujícího podle čl. 41 odst. 4 Obecného nařízení dodržování kodexu chování. K připomenutí se jedná například o laxní přístup akreditovaného subjektu v případě nevyřízení stížnosti na porušování kodexů chování.

Závažným porušením rozumí Obecné nařízení například neumožnění výkonu práv subjektu údajů, porušení zásad při předání osobních údajů do třetích zemí nebo porušení při zpracování zvláštní kategorie osobních údajů. Za výslovnou zmínku stojí také porušení Obecného nařízení v souvislosti se získáváním a správou souhlasu, tedy že správce musí mít k využití tohoto právního titulu náležitý souhlas subjektu údajů, tento musí být schopen prokázat. Do tohoto porušení také spadá nadužívání souhlasu tam, kde to ze strany správce či zpracovatele vůbec není potřeba. Za tato závažná porušení hrozí správní pokuta v dvojnásobné výši, a to až 20.000.000 EUR nebo, jedná-li se o podnik, pokuta ve výši až 4% celkového ročního celosvětového obratu za předchozí finanční rok v závislosti na tom, která hodnota je vyšší. Stejná výše pokuty hrozí i v případě nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2, tedy například aby správce uvedl operace zpracování do souladu s Obecným nařízením nebo aby subjektu údajů oznámil porušení zabezpečení jeho osobních údajů. Při ukládání správních pokut se přitom uplatní absorpční zásada, spočívající v tom, že pokud správce či zpracovatel u stejných nebo souvisejících operací zpracování poruší více ustanovení Obecného nařízení, nesmí celková výše správní pokuty předkročit výši stanovenou pro nejzávažnější porušení.

K tomuto velmi diskutovanému tématu se již Úřad vyjádřil tak, že nemá v úmyslu se odchylovat od dosavadní praxe při ukládání správních pokut, a že v rozsahu správních sankcí v České republice nemá v úmyslu těchto drakonických sankcí využívat, a to s ohledem na to, že tyto výše jsou předpokládány při závažných porušeních u velkých nadnárodních podniků. Cílem Úřadu není správce a zpracovatele likvidovat, ale odrazovat.[187] V současné době lze vycházet pouze z rozhodovací praxe Úřadu před účinností Obecného nařízení, neboť řízení o přestupku od zjištění porušení přes stádium šetření a kontroly až po pravomocné

[187] Šéfka Úřadu pro ochranu osobních údajů: Vysokými pokutami chceme firmy odrazovat, ne likvidovat. *E15* [online]. 2018 [cit. 2018-10-24]. Dostupné z: https://www.e15.cz/rozhovory/sefka-uradu-pro-ochranu-osobnich-udaju-vysokymi-pokutami-chceme-firmy-odrazovat-ne-likvidovat-1334926

rozhodnutí o dané správní pokutě je dlouhodobý proces. Z tohoto důvodu tedy zatím nebyla ze strany Úřadu uložena správní pokuta za porušení vzniklé po dobu účinnosti Obecného nařízení, tedy po 25. květnu 2018, neboť v současné chvíli Úřad stále řeší dříve zjištěná pochybení správců a zpracovatelů.

Nejvyšší pokuta doposud uložená Úřadem však přitom nedosáhla ani poloviny maximální výše pokuty stanovené zákonem o ochraně osobních údajů. Tu Úřad udělil společnosti EURYDIKAPOL, s.r.o. ve výši 4.250.000,- Kč v roce 2017 za šířená nevyžádaných obchodních sdělení, a to zejména s ohledem na intenzitu zasílání a množství dotčených subjektů. Společnost neprokázala, že by disponovala souhlasy subjektů, kterým tato sdělení zasílala.[188]

Možná více veřejně známou kauzou, bylo uložení pokuty společnosti T-Mobile Czech Republic a.s. ve výši 3,6 mil. Kč za nepřijetí dostatečných opatření k zabezpečení osobních údajů obsažených v elektronické databázi, obsahující osobní údaje zhruba 1,2 milionu zákazníků, kdy v důsledku nepřijetí dostatečných opatření došlo k odcizení osobních dat zaměstnancem této společnosti.[189] Ve srovnání se sousedním Německem však tyto pokuty skutečně nedosahují až tak extrémních výší. Nevyšší pokuta byla v Německu udělena v roce 2010 řetězci supermarketů Lidl ve výši 1,5 milionu eur za neoprávněné sledování zaměstnanců skrze videokamery.[190]

Zároveň má autorka této práce za to, že u přestupků proti zpracování, spáchaných v přechodném období po účinnosti Obecného nařízení, ale před účinností adaptačního zákona, bude moci Úřad vycházet pouze z katalogu přestupků a na něj navazujících sankcí podle zákona o ochraně osobních údajů, neboť až adaptačním zákonem je Úřad výslovně zmocněn k ukládání správních pokut v takové výši, v jaké je zmiňuje Obecné nařízení.[191]

---

[188] Tisková zpráva: ÚOOÚ udělil rekordní pokutu za spam. In: *Úřad pro ochranu osobních údajů* [online]. 2017 [cit. 2018-10-24]. Dostupné z: https://www.uoou.cz/tiskova-zprava-uoou-udelil-rekordni-pokutu-za-nbsp-spam/d-23838

[189] Tisková zpráva: Správní řízení se společností T-Mobile Czech Republic a.s. In: *Úřad pro ochranu osobních údajů* [online]. 2017 [cit. 2018-10-24]. Dostupné z: https://www.uoou.cz/tiskova-zprava-uoou-udelil-rekordni-pokutu-za-nbsp-spam/d-23838

[190] BOMMEL, Robert. Bußgelder bei Datenschutzverstößen. In: *Brandi Rechtsanwälte* [online]. [cit. 2018-10-24]. Dostupné z: https://www.brandi.net/fileadmin/user_upload/Bussgelder_bei_Datenschutzverstoessen_1_2017.pdf

[191] § 62 vládního návrhu prováděcího zákona, Sněmovní tisk č. 138

8.4.1 Ukládání správních pokut orgánům veřejné moci

Při pohledu na praktické dopady Obecného nařízení nelze vynechat otázku trestání orgánů veřejné moci. I tyto orgány coby správci či zpracovatelé se mohou dopustit porušení Obecného nařízení. Členským státům je dána výslovná možnost stanovit, zda vůbec a popřípadě v jaké výše budou trestat orgány veřejné moci správními pokutami. V České republice přitom není nijak neobvyklé, že se správní sankce ukládají rovněž veřejnoprávním subjektům. Uložení pokuty za takové porušení se však jeví jako ne zcela efektivní, neboť orgány veřejné moci často operují s veřejnými prostředky a uložením finanční sankce by mohlo v krajním případě dojít k dočasnému omezení jejich činnosti. To samozřejmě není pro fungování veřejné moci efektivní. V těchto případech by nemělo smysl stanovit horní hranici shodně s nejvyšší možnou sankcí pro podnikatelské subjekty, neboť zejména v případě institucí s menším rozpočtem by se jednalo fakticky o přesuny finančních prostředků v rámci státního rozpočtu, neboť takové instituce by musely o finanční prostředky na úhradu pokuty dodatečně požádat. Takový trest pak postrádá svůj smysl, neboť by se fakticky jednalo pouze o administrativní transfery mezi veřejnými rozpočty. Při nahlédnutí do schvalovaného adaptačního zákona je patrné, že umožnění ukládání správních pokut orgánům veřejné moci zůstává zachováno shodně s dosavadní úpravou se stanovením maximální výše správní pokuty 10.000.000,- Kč.[192] Závěrem je třeba připomenout, že možnost ukládání správních pokut orgánům veřejné moci nemá vliv na výkon dalších pravomocí dozorového úřadu vůči těmto orgánům nebo na povinnost k náhradě škody či jiné újmy za porušení zpracování.

8.5 Sankce v rovině trestního práva

V neposlední řadě je třeba připomenout, že Obecné nařízení, stejně jako tomu bylo dosud, nevylučuje ani vznik trestní odpovědnosti za porušení ochrany osobních údajů. Sem budou spadat nejzávažnější porušení nakládání s osobními údaji, Trestní zákoník definuje skutkovou podstatu trestného činu neoprávněného nakládání s osobními údaji[193], jehož chráněným zájmem je právo na ochranu před neoprávněným zveřejňováním osobních údajů a jejich zneužitím, jakož i ochrana dalších práv a oprávněných zájmů, které zveřejněním osobních údajů mohou být

[192] Důvodová zpráva k § 60 vládního návrhu zákona o zpracování osobních údajů cit. dne 26.10.2018, s. 92-93

[193] § 180 zákona č. 40/2009 Sb., trestního zákoníku

poškozeny. Zmíněné ustanovení trestního zákoníku obsahuje dvě samostatné základní skutkové podstaty. První skutková podstata, vymezená v odstavci 1, chrání každého před neoprávněným zveřejněním, sdělením, zpřístupněním, jiným zpracováním nebo přisvojením si osobních údajů shromážděných o jiném v souvislosti s výkonem veřejné moci.

Druhá skutková podstata, kterou definuje odstavec 2, sankcionuje neoprávněné zveřejnění, sdělení nebo zpřístupnění osobních údajů třetí osobě, získaných v souvislosti s výkonem povolání, zaměstnání nebo v souvislosti s porušením státem uložené nebo uznané povinnosti. Jsou-li naplněny znaky skutkové podstaty trestného činu podle odstavce 1 či 2, musí daným skutkem současně dojít ke způsobení vážné újmy na právech či oprávněných zájmech osoby, již se osobní údaje týkají. Oběma skutkovými podstatami je přitom postihováno jak úmyslné, tak i nedbalostní jednání. Přitěžujícími okolnostmi jsou spáchání takového činu v rámci organizované skupiny, spáchání činu skrze média nebo počítačovou síť, vyšší rozsah způsobené škody nebo spáchání v úmyslu získat prospěch. [194]

V této souvislosti je třeba zmínit, že nesprávné nakládání s osobními údaji může založit vznik trestní odpovědnosti nejen u fyzických, ale také u právnických osob. Je tomu tak proto, že trestný čin neoprávněného nakládání s osobními údaji se nenachází v negativním výčtu trestných činů, které není možné udělit právnickým osobám. [195] Tuto odpovědnost obvykle založí protiprávní jednání typicky zaměstnanců dané společnosti, kteří přicházejí do styku s osobními údaji.[196]

[194] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 1790-1792

[195] § 7 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim

[196] PAVLÍČEK, Libor. GDPR a TOPO a jejich význam pro obchodní společnosti. *E-pravo.cz* [online]. [cit. 2018-12-02]. Dostupné z: https://www.epravo.cz/top/clanky/gdpr-a-topo-a-jejich-vyznam-pro-obchodni-spolecnosti-106475.html

9. Některé zvláštní situace zpracování osobních údajů

Jak již bylo zmíněno v úvodu této práce, právo na ochranu osobních údajů patří mezi základní lidská práva a svobody, nelze ho však považovat za právo absolutní. Za současné aplikace zásady proporcionality může dojít k omezení tohoto práva ve prospěch jiného, převažujícího zájmu. V této kapitole by autorka práce ráda přiblížila některé speciální situace zpracování, kdy může docházet k tomu, že právo na ochranu osobních údajů ustoupí o krok vzad a do popření se dostává jiný, zejména veřejný zájem. K tomuto posouzení slouží test proporcionality, který říká, že základní právo či svobodu lze omezit pouze v zájmu jiného základního práva či svobody. Poměřování ve vzájemné kolizi stojících základních práv a svobod spočívá v kritériu vhodnosti, dále kritériu potřebnosti a v poslední fázi porovnáním závažnosti obou v opozici stojících základních práv.[197]

9.1 Střet svobody projevu a ochrany osobních údajů

Zveřejňování osobních údajů v periodickém tisku, ale i v jiných médiích, je nepochybně jednou z problematických oblastí, kde se střetávají dva zcela odlišné zájmy a očekávání – na straně jedné oprávněný požadavek dotčených osob na ochranu soukromí a na straně druhé neméně důležitá svoboda šíření informací. Tyto střety se však postupem času stávají častějšími, neboť narůstá objem informací šířených nejen klasickými periodiky, ale typicky skrze internet. Tyto informace jsou pak viditelnější a dotýkají se i jiných osob, než osob mediálně známých nebo politiků.[198] Svoboda projevu a právo na informace jsou ústavně zaručenými právy.[199] Jak potvrdil i Ústavní soud, základní právo na svobodný projev je třeba považovat za konstitutivní znak demokratické pluralitní společnosti, v níž je každému dovoleno vyjadřovat se k věcem veřejným a vynášet o nich hodnotící soudy.[200] Čl. 85 Obecného nařízení cílí na ochranu svobody projevu a informací, a to zejména co se týká zpracování pro novinářské účely a

[197] Nález Ústavního soudu ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94. In: MORÁVEK, Jakub. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Praha: Wolters Kluwer, 2015. Judikatura (Wolters Kluwer ČR). ISBN 978-80-7552-018-0, s. 20-21

[198] Stanovisko č. 5/2009: ve znění aktualizace z února 2014. In: *Úřad pro ochranu osobních údajů*[online]. [cit. 2018-10-30], s. 1

[199] Čl. 17 Listiny základních práv a svobod

[200] Nález Ústavního soudu ze dne 17. července 2007, sp. zn. IV. ÚS 23/05

pro účely akademického, uměleckého a literárního projevu. Zpracování údajů za těmito účely je pak vzhledem k právu na svobodu projevu a obecně k úloze médií v demokratické společnosti výkonem oprávněného zájmu.[201]

Obecné nařízení výslovně zakotvuje členským státům, aby prostřednictvím právních předpisů uvedly právo na ochranu osobních údajů do souladu s právem na svobodu projevu a informací, včetně zpracování pro novinářské účely a pro účely akademického, uměleckého či literárního projevu. Navazuje také na judikaturní závěry Evropského soudu, které říkají, že orgány a soudy členských států musí vykládat své vnitrostátní právo (tehdy) v souladu se Směrnicí a rovněž dbát na to, aby se neopíraly o takový její výklad, jaký by byl v rozporu se základními právy chráněnými právním řádem Společenství nebo jinými obecnými zásadami práva Společenství, typicky se zásadou proporcionality.[202] Směrnice byla v této problematice poměrně obecná, nicméně vyznačovala se určitou pružností ve vztahu k vnitrostátním právním řádům členských států. Zmiňovaný test proporcionality by pak měl být proveden v každém jednotlivém případě, tedy jiná bude situace v případě, kdy se jedná o veřejně známou osobnost, jiná u „běžných" osob.

V této souvislosti stojí za zmínku zajímavý případ Von Hannover proti Německu[203], ve kterém se řešilo zveřejnění fotografií monacké princezny Caroline Von Hannover při různých událostech, například při společenské akci, pobytu na horách, jízdě na koni nebo fotografiím ze zahradní restaurace, které byly otištěny v německých novinách a časopisech. Princezna Von Hannover se domáhala stažení těchto fotografií, neboť se domnívala, že tím došlo k porušení jejího práva na soukromí, kdy se zveřejněním těchto fotografií nesouhlasila. Spolkový soudní dvůr společně s německým ústavním soudem stály před nelehkou otázkou. Provedení testu proporcionality v tomto případě zahrnovalo posouzení spočívající ve společenském postavení princezny, místem pořízení záběrů a v neposlední řadě zájmem veřejnosti na informování o životě dcery monackého knížete. Evropský soud pro lidská práva následně uzavřel, že test proporcionality na úrovni německých soudů byl proveden v souladu s judikaturou ESLP, kdy osoby veřejně známé nemohou požadovat ochranu ve stejném rozsahu jako osoby veřejnosti

[201] Ve smyslu čl. 6 odst. 1 písm. f) Obecného nařízení
[202] Rozsudek Soudního dvora EU ze dne 6. listopadu 2003, Bodil Lindqvist, věc C-101-01
[203] Rozsudek Evropského soudu pro lidská práva ze dne 24. června 2004 Von Hannover proti Německu ze dne 24. června 2004, stížnost č. 59320/00 a na něj navazující rozsudky Von Hannover proti Německu II. a III.

neznámé a musí do jisté míry takový zásah strpět. Současně je dán i zájem na informování veřejnosti o životě knížete a jeho rodiny za předpokladu, že účelem není sdělení fantaskních informací z jejich života nebo informací a fotografií jinak nevhodných. Test proporcionality v tomto případě obsáhl i posouzení místa pořízení fotografie, kdy se uplatní tzv. prostorová izolace. Pořizování snímků z hlediska místa tak není absolutní, pokud se jedná o snímky princezny, pořízené v soukromí, například ve zmiňované zahradní restauraci, došlo již k překročení přípustné míry zásahu do práva na ochranu soukromí a osobních údajů.[204] Autorka práce si dovolila zmínit toto zajímavé rozhodnutí zejména proto, že je možné na konkrétním případě demonstrovat obsah testu proporcionality ve střetu svobody projevu a práva na ochranu osobních údajů. Zároveň je na tento judikát hojně odkazováno i v závěrech judikatury pocházející z českého právního prostředí.[205]

Test proporcionality by měl dále zahrnovat posouzení charakteru publikovaných informací, tedy zda se například nejedná o zvláštní kategorii osobních údajů. V neposlední řadě přichází v úvahu také smysl a účel zveřejnění, typicky při plnění odstrašující role trestu v trestním řízení, kdy informování veřejnosti o potrestání má za cíl odradit případné další pachatele.

Ve světle rozsudku ve věci *Bodil Lindqvist* určuje Obecné nařízení stejně jako Směrnice členským státům, aby pro tyto účely vymezily příslušné výjimky. Česká republika této možnosti využila a v návrhu adaptačního zákona počítá s uplatněním výjimek při zpracování osobních údajů pro zpravodajské, vědecké a literární účely. Upravuje také možnosti zpracování zvláštní kategorie osobních údajů pro tyto účely, kdy musí být proporcionálně posouzena nezbytnost k dosažení oprávněného cíle a převaha oprávněného zájmu na zpracování takových údajů nad oprávněnými zájmy subjektu údajů. Toto zpracování není podmíněno povolením či schválením Úřadu. Lze zmínit, že adaptační zákon rovněž počítá s omezením práva na námitky. Subjekt údajů, jehož osobní údaje jsou zpracovávány, sice může vznést námitku proti zpracování, avšak současně nese břemeno důkazní, kdy musí prokázat, při kterém konkrétním zpracování převažuje oprávněný zájem na ochraně jeho práv a svobod. V této souvislosti je také omezena informační a poučovací povinnost správce, zejména s ohledem na

[204] ONDŘEJOVÁ, Eva. Desetiletá cesta od Rozsudku Von Hannover 1 k Rozsudku Von Hannover 3. *Bulletin advokacie* [online]. 9.1.2015 [cit. 2018-11-17]. Dostupné z: http://www.bulletin-advokacie.cz/desetileta-cesta-od-rozsudku-von-hannover-1-k-rozsudku-von-hannover-3

[205] Např. Rozsudek Nejvyššího soudu ze dne 12. prosince 2012, sp. zn. 30 Cdo 3770/2011

to, že by bylo obtížně představitelné, aby správce před započetím každého zpracování podrobně informoval subjekt údajů např. před započetím rozhovoru, telefonátu, natáčení apod. Totéž platí například pro vědecký výzkum. V takových případech plně postačuje, pokud bude subjekt údajů znát identitu správce, další informace si následně může dohledat na internetových stránkách správce. Uplatní se také výjimka z práva na výmaz.[206] Zároveň se na toto zpracování vztahuje zásada ochrany zdroje, spočívající v tom, že opravňuje správce odložit nebo odepřít subjektu údajů sdělení zdroje, ze kterého osobní údaje pocházejí z důvodu potřeby ochrany tohoto zdroje.[207]

Lze shrnout, že úprava obsažená v připravovaném adaptačním zákoně se výrazně neliší od výjimek a zvláštností, zahrnutých v zákoně o ochraně osobních údajů. Nacházíme také možnou podobnost s občanským zákoníkem, který zmiňuje proporcionálnost zájmů na obou stranách.[208] Podle názoru autorky by tak v přechodném období po účinnosti Obecného nařízení, ale zároveň před účinnosti adaptačního zákona, nemělo docházet k větším potížím. Současně není dotčena aplikovatelnost zvláštních předpisů, typicky například tiskového zákona, zákona o neperiodických publikacích nebo zákona o svobodném přístupu k informacím, a to včetně výjimek a zvláštností z nich plynoucích. Adaptační zákon si tak klade za cíl zachovat standard svobody tisku za současného zachování standardu ochrany osobnostních práv.[209]

9.2 Užití kamerových systémů ve vztahu k osobním údajům

Pravděpodobně v současné době najdeme velmi malé množství veřejně přístupných míst, která by nebyla sledována kamerovými systémy. Ty se nyní užívají hojně k zabezpečení pořádku veřejných prostor, škol, nemocnic, veřejných institucí, bytových domů, ale i firemních či soukromých prostor. O kamerových systémech se dá bez dalšího tvrdit, že jsou dobrým sluhou, ale špatným pánem. Velmi dobře poslouží k zabezpečení a monitorování určitých prostor, ale v případě jejich nadužívání či úniku z nich získaných informací – záznamů, může dojít k závažné újmě. Provoz kamerových systémů je neoddělitelně spjat

[206] podle čl. 17 odst. 3 písm. a) Obecného nařízení
[207] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 496-498
[208] § 89 a 90 zákona č. 89/2012 Sb., občanského zákoníku
[209] Důvodová zpráva k § 16 vládního návrhu zákona o zpracování osobních údajů cit. dne 30.10.2018, s. 70-72

s ochranou soukromí v nejširším slova smyslu. Právo na soukromí zejména v opozici s právem na ochranu vlastnictví představují dvě ústavně zaručená práva, která se v tomto případě dostávají do konfliktu. Každý, kdo provozuje kamerové systémy, by si tak měl před zahájením tohoto provozu položit otázku, z jakého důvodu takové systémy instaluje, čí zájem tím chrání, zda nelze dosáhnout požadovaného cíle jinými způsoby a podobně. V této souvislosti by si měl každý provozovatel kamerových systémů uvědomit, že tímto provozem provádí zpracování osobních údajů.[210]

Provozování kamerového systému je považováno za zpracování osobních údajů podléhající povinnostem podle Obecného nařízení, pokud je automatizovaně prováděn záznam monitorovaného veřejného prostoru a zároveň je účelem pořizovaných informací a záznamů využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové jsou osobními údaji za předpokladu, že na základě těchto záznamů – informace z obrazových či zvukových nahrávek, lze přímo či nepřímo identifikovat konkrétní fyzickou osobu. Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky, zejména obličej, a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným jednáním.[211]

Z tohoto plyne, že provozování kamerových záznamů je bezpochyby zpracováním osobních údajů, z něhož vyplývá pro správce celá řada povinností a závazků. Nejzásadnější z nich představuje zajištění právního titulu k takovému zpracování, tedy jaké důvody ho vedly k instalaci kamerového zařízení. Při užívání kamerových systémů vyplývají dva právní tituly. Jako první přichází v úvahu plnění zákonných povinností správce či zpracovatele. V českém právním řádu bychom nalezli hned několik zákonných ustanovení, která ukládají správci či zpracovateli povinnost sledovat dané prostory skrze kamerový systém. Tímto je například zákon o hazardních hrách, ukládající správci povinnost monitorovat po celou provozní dobu prostory herny nebo kasina[212], dále povinnost vybavit

[210] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3, s. 206-207

[211] K provozování kamerových systémů. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-11-14]. Dostupné z: https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535/p1=0

[212] § 72 zákona č. 186/2016 Sb., o hazardních hrách

kamerovým systémem prostory, kde je stáčen a značen líh[213] nebo monitorování v souladu se zachováním kybernetické bezpečnosti.[214] V těchto případech jsou prostory monitorování definovány přímo zákonem.[215]

Nejčastějším důvodem užívání kamerových systémů však bude monitorování na základě oprávněného zájmu správce nebo zpracovatele. Zatímco v případě zákonem určených případů sledování se neuplatnil princip proporcionality a veřejný zájem převážil nad zájmy na ochranu soukromí bez dalšího, v případě oprávněného zájmu správce bude nutné převažující zájem prokázat. Z praktického hlediska by si měl správce či zpracovatel položit tuto otázku ještě před započetím monitorování a provést test proporcionality, spočívající v posouzení, zda zájem správce převažuje nad zájmem na ochranu soukromí monitorovaných osob. A to i z toho důvodu, že oprávněný zájem pravděpodobně bude jediným právním titulem takového zpracování a nebude-li dostatečně silný, nemůže správce kamerový systém použít. Za vhodné se také jeví posoudit nezbytnost takového zpracování ve vztahu k účelu zpracování a tuto skutečnost společně se záznamem o provedeném testu proporcionality zaznamenat do záznamů o činnostech zpracování. Podkladem pro oprávněný zájem správce bude typicky ochrana majetku, zajištění bezpečnosti prostor, přičemž daného účelu nelze dosáhnout jinými prostředky.[216]

Tím, že provozování kamerových systémů představuje zpracování osobních údajů, přirozeně i v tomto případě vyplývá správci celá řada povinností. Kromě již zmiňovaného jednoznačného vymezení účelu pořizování záznamů se jedná o praktický problém, a to vymezení doby pro uchování záznamů. Nahrávka by měla být uchovávána v rámci časové smyčky, přičemž záznam se v rozsahu přibližně několika dní přemaže novým záznamem. Velmi podstatné také bude umístění daného kamerového systému, které úzce souvisí s účelem, pro který je instalován.[217]

Velmi zajímavým je v této souvislosti případ pana Františka Ryneše, který se v pozici novináře stal společně se svou rodinou terčem neznámých útočníků,

[213] § 22 zákona č. 307/2013 Sb., o povinném značení lihu

[214] § 16 vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

[215] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3, s. 207-208

[216] Tamtéž, s. 207-208

[217] K provozování kamerových systémů. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-11-14]. Dostupné z: https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535/p1=0

kterým se mimo jiné několikrát podařilo rozbít okna jeho domu. Policie těmto útokům nedokázala zabránit a poradila poškozenému, aby na svůj dům instaloval bezpečnostní kamery. Ty skutečně později zachytily oba útočníky, které policie ztotožnila a zahájila proti nim trestní stíhání. Jeden z těchto útočníků dal podnět policii, aby prověřila provoz kamerového systému poškozeného a vyslovil podezření, že jeho provozem dochází k porušení zákona o ochraně osobních údajů. Policie následně tento případ postoupila k řešení Úřadu pro ochranu osobních údajů. Kamera na domě totiž zabírala kromě prostranství před domem ve vlastnictví poškozeného také část protější ulice, včetně vstupu do domu. Úřad uložil Františku Rynešovi pokutu za neoprávněné zpracování osobních údajů zaznamenaných osob, neboť ke zpracování docházelo bez jejich souhlasu, tedy neměl k tomuto zpracování právní titul, a dále vůči těmto osobám nesplnil informační povinnost. V té době také obdobné zpracování podléhalo předchozímu povolení Úřadu, které rovněž nesplnil.[218] Dotyčný napadl uvedené rozhodnutí žalobou u Městského soudu, kde argumentoval tím, že se jedná o zpracování pro osobní potřebu a uplatní se tak výjimka ze zákona o ochraně osobních údajů. Avšak Městský soud tuto žalobu zamítl jako nedůvodnou.[219] František Ryneš napadl rozsudek Městského soudu kasační stížností, kde namítal nezákonnost spočívající v nesprávném posouzení právní otázky soudem v předcházejícím řízení. Nejvyšší správní soud toto řízení přerušil a položil předběžnou otázku Soudnímu dvoru Evropské unie, zda lze provozováním kamerového systému umístěného na rodinném domě za účelem ochrany majetku, zdraví a života majitelů domu podřadit pod výjimku zpracování pro soukromé účely ve smyslu Směrnice. Soudní dvůr se s touto otázkou vypořádal tak, že dané provozování kamerového systémů pod tuto výjimku nespadá.[220] I přesto Nejvyšší správní soud rozhodl[221], že byl František Ryneš sankcionován protizákonně a protiústavně, neboť jednoznačnost aplikace a tudíž i užití nebylo dosud v rámci výkladu této otázky řešeno. V daném případě aplikoval princip proporcionality a rozhodnutí Úřadu o udělení pokuty zrušil. Dále uvedl, že pokuta, která byla v tomto případě uložena, naprosto nekoresponduje s okolnostmi případu a kamerový systém byl nastaven efektivně, když zabíral kromě bezprostředního okolí domu také část

[218] FOREJTOVÁ, M. The right to respect for private life and the right to personal data protection - is there any conflict?. *Państwo i Prawo*, 2017, roč. 72, č. 9, ISSN: 0031-0980, s. 115-116

[219] Rozsudek Městského soudu v Praze ze dne 25. dubna 2012´, č.j. 9 Ca 41/2009-60-70

[220] Rozsudek Soudního dvora ze dne 11. prosince 2014, Ryneš v Úřad pro ochranu osobních údajů, věc C-212/13

[221] Rozsudek Nejvyššího správního soudu ze dne 25. února 2015 č.j. 1 As 113/2012-133

veřejného prostranství, odkud útoky přicházely. Nejvyšší správní soud tak rozhodl do určité míry odlišně od toho, k jakým závěrům dospěl Soudní dvůr. Každý jednotlivý případ by tak měl projít testem proporcionality, aby byl posouzen vztah práva na ochranu majetku a obydlí s právem na ochranu soukromí a osobních údajů.[222]

Kromě výběru místa je rovněž důležité zajistit ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným přístupem, změnou, zničením nebo ztrátou. Interní postupy a pravidla pro provoz kamerového systému a nakládání se záznamy se jeví jako vhodné upravit v rámci vnitřní směrnice a provést školení pověřených zaměstnanců. Ani v případě užití kamerových záznamů se správce nevyhne informační povinnosti, kterou však jednoduše splní tím, že monitorovaný prostor označí informací o tom, že je monitorován, současně s uvedením jména provozovatele kamerového systému. Povinnost jmenovat pověřence pro tento účel zpracování se také pro valnou většinu správců neuplatní, a to za předpokladu, že jejich hlavní činností není právě takovýto druh zpracování. Pověřence tak musí mít například bezpečnostní agentury.

Ve všech případech bude nutné posoudit situaci podle již výše zmiňovaného testu proporcionality. Důsledky užívání kamerových systémů jsou u dotčených osob pociťovány různým způsobem, což dokládá i počet stížností předkládaných Úřadu. Obecně lze říci, že se jedná o jeden z nejfrekventovanějším okruhů, kterým se Úřad zabývá, a to zejména ve vztahu ke sledování veřejného prostranství nebo jejich užití v rámci pracoviště. Ačkoli Obecné nařízení výslovně nezmiňuje problematiku kamerových systémů a udává zásady zpracování obecně, výrazným způsobem ovlivňuje výkladovou praxi tím, že členským státům ukládá aplikovat tato pravidla jednotně. Zatímco doposud byl sjednotitelem nejednotného výkladu Směrnice Soudní dvůr, Obecné nařízení do jisté míry těmto nejasnostem předchází, když tyto povinnosti určuje přímo. Autorka práce tak má za to, že k větším výkladovým potížím ohledně kamerových systémů by docházet nemělo, neboť mnohým problémům předchází přímá použitelnost Obecného nařízení ve všech členských státech a zároveň je již dosavadní judikatura k tomuto tématu poměrně široká.

[222] FOREJTOVÁ, M. Analysis on preliminary ruling (Interpretation of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data). In Challenges of Today - Politics and Society. Gdańsk : Research Institute for European Policy in the cooperation of the Department of Political Science at University of Gdansk., 2015,ISBN: 978-83-944614-1-6, s. 177-195

10. Praktická část – dopady Obecného nařízení na činnost spolků a svazů spolků

Autorka práce se v rámci výkonu své advokátní praxe již několikrát setkala se zaváděním Obecného nařízení do praxe v rámci činnosti spolků. Kolem Obecného nařízení panuje celá řada mýtů. Tato skutečnost se u spolků a svazů spolků projevuje vůbec možná nejčastěji, neboť členové jejich statutárních orgánů se s celou řadou těchto dezinformací, putujících zejména po internetu, často nedokáží sami vypořádat a nemají dostatek relevantních informací, jak správně uvést nakládání s osobními údaji do souladu s Obecným nařízením. Další častý problém představuje laxnost spolků se touto oblastí zabývat s odkazem na to, že se jich tato problematika netýká. Snahou autorky práce bude některé skutečnosti uvést na pravou míru a na modelových případech nastínit, že se spolky nemusí Obecného nařízení obávat, a že proces compliance s novou právní úpravou nepředstavuje ve většině případů pro spolky složitou záležitost.

Cílem této kapitoly není podrobný popis všech povinností spolku coby správce či zpracovatele, které jsou obsaženy v předchozích kapitolách této práce, ale nalézt specifika uplatňování Obecného nařízení v této oblasti. Za předpokladu, že spolky věnovaly pozornost již dosavadní úpravě v podobě zákona o ochraně osobních údajů a tomuto přizpůsobily činnosti zpracování, bude pro ně transformace představovat pouze několik kosmetických změn. Vzhledem ke zkušenostem byly i dosavadní povinnosti spojené s osobními údaji často podceňovány a panovala bezradnost v tom, jak s Obecným nařízením vůbec naložit. Spolky ve většině případů nejsou zvyklé s ochranou osobních údajů zacházet, většina jich tuto problematiku doposud neřešila. V této kapitole proto budou zohledněny všechny body, kterým by měly spolky věnovat pozornost.

Na počátku se jeví za vhodné vypracovat stručný projekt implementace, který nemusí být nikterak složitý. V první fázi by měl spolek zmapovat všechny činnosti, při nichž dochází ke zpracování osobních údajů fyzických osob a vytvořit schéma zpracování. Zejména se jedná o postihnutí toho, jak se tato data shromažďují, kam se ukládají, kdo má k těmto osobním údajům přístup a kdo s nimi může nakládat. Tímto zároveň spolek naplňuje jednu z povinností správce – vytvořit záznamy o činnostech zpracování. Byť se tato povinnost nevztahuje na každého správce, lze ji doporučit provést každému jako prvotní analýzu zpracování, která poskytne kvalitní obraz o aktuální situaci a nezbytnosti provést

další úkony k uvedení do souladu. Sem je také vhodné zařadit důvody zpracování, tedy proč spolek takové osobní údaje potřebuje, včetně kategorií zpracovávaných osobních údajů, od jakých osob údaje shromažďuje a po jak dlouhou dobu. Pokud spolek osobní údaje zpřístupňuje také dalším příjemcům, pak i tyto charakterizovat s odůvodněním, proč jsou jim tato data předávána. S tím souvisí i pravdivý rozbor stávajícího zabezpečení údajů a zhodnocení technického a organizačního hlediska zpracování. K tomuto kompendiu informací je vhodné zároveň provést krátké zhodnocení rizikovosti daného zpracování ve vztahu k subjektům údajů a právní titul, od něhož se zpracování odvíjí. Zároveň musí být spolek schopen souladnost zpracování později prokázat, jeví se jako vhodné tuto analýzu písemně sepsat do záznamů o činnostech zpracování a popřípadě také přijmout podpůrné zásady v rámci zápisu z členské schůze spolku.

V souvislosti s prováděním prvotních analýz lze zmínit nejčastější „nešvar“ spolků, a to využívání souhlasů se zpracováním osobních údajů. Spolky v průběhu činnosti často získaly souhlasy se zpracováním osobních údajů svých členů nebo je po nich hojně vyžadovaly v době před nabytím účinnosti Obecného nařízení, a to zejména v souvislosti s vedením seznamu členů. Je však třeba zmínit, že spolky pro svoji činnosti ve většině případů institut souhlasu vůbec nepotřebují. V situaci vedení seznamu členů se uplatňují ustanovení občanského zákoníku[223], podle nichž je vedení evidence členské základny zákonným zpracováním a není tedy nutné tento souhlas vyžadovat. Jedinou výjimku představuje zveřejnění seznamu členů, k čemuž je souhlas vyžadován.[224] Benevolentnější situace nastává u zveřejňování jmenných údajů členů, typicky například hráčů sportovních klubů. V případě veřejně provozovaných aktivit, zejména sportu, jsou různě formy prezentace hráčů s uváděním jejich jmenných údajů nezbytné a přirozené. Zveřejnění takových údajů, například společně s fotografiemi nebo na výsledkových listinách se neděje na základě souhlasu hráčů, přičemž tento ani nemůže být vyžadován, ale je dovoleným zpracováním na základě oprávněného zájmu klubu.[225]

Naopak nadbytečným získáváním souhlasů se může spolek paradoxně dostat do rozporu s Obecným nařízením, kdy vyžaduje souhlasy tam, kde to není vůbec potřeba. Spolky také často nesmyslně neumožňovaly členství bez stvrzení

[223] § 236 zákona č. 89/2012 Sb., občanského zákoníku
[224] § 236 odst. 3 zákona č. 89/2012 Sb., občanského zákoníku
[225] K činnosti spolků. In: *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/k-cinnosti-spolku/ds-5084/p1=5084

tohoto souhlasu. Zároveň si je potřeba v obecné rovině uvědomit, že každý udělený souhlas má omezenou platnost a v této době může být odvolán. Souhlas spolek rovněž nepotřebuje při zasílání nekomerčních sdělení, pozvánek a zpravodajů na poštovní či emailové adresy členů spolku, neboť se jedná o zpracování za účelem plnění oprávněného zájmu. Pokud spolek poskytuje služby třetím osobám a zpracovává jejich osobní údaje, jedná se o právní titul zpracování na základě plnění smlouvy, byť ta nemusí mít vždy písemnou podobu, tedy opět souhlas by byl vyžadován nadbytečně. To však nevylučuje již v této práci zmiňovanou informační povinnost správce. V případě, že už spolek z nějakého důvodu souhlasy se zpracováním ke své činnosti potřebuje, vyvstává nutnost je revidovat a zjistit, zda splňují nároky kladené na udělení souhlasu i v současné době. V opačném případě musí zpracování podložit jiným právním titulem, vyžádat si souhlasy od subjektů údajů znovu v řádné podobě nebo v krajním případě takové osobní údaje nezpracovávat. Ve všech těchto případech by ale měla proběhnout revize okruhu získávaných údajů s důrazem na zásadu minimalizace, tedy zda spolek nezpracovává nadbytečné osobní údaje. Spolek by měl provést uvážení, které osobní údaje skutečně potřebuje, typicky například údaje o zaměstnání nebo osobním stavu.

Spolky jsou činné v mnoha různých oblastech, z nichž mnoho z nich samo pořádá různé sportovní či kulturní akce. Velmi často si pak spolky při této příležitosti kladou otázku, zda mohou zveřejňovat fotografie z těchto pořádaných akcí, představení a veřejných vystoupení, když na fotografiích jsou společně s pořadateli, vystupujícími, herci a dalšími účastníky zachyceni také návštěvníci akcí a širší veřejnost. Opět se jedná o podobnou situaci jako v případě vedení seznamu členů, neboť se opět užijí ustanovení občanského zákoníku.[226] Při pořizování a zveřejňování reportážních a propagačních fotografií se nejedná primárně o problematiku ochrany osobních údajů, ale o postup, kde je třeba se při jejich pořizování chovat korektně a dodržovat ustanovení občanského zákoníku, upravující pořizování podobizny.[227] Není tedy potřeba vyžadovat souhlas s pořizováním a zveřejněním takových fotografií. I v případě fotografií z veřejných akcí existují určité hranice. Zvláštní pozornost je nutné věnovat takovým akcím, kterých se účastní nezletilé osoby, typicky například u dětských

[226] § 84 zákona č. 89/2012 Sb., občanského zákoníku

[227] K činnosti spolků. In: *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/k-cinnosti-spolku/ds-5084/p1=5084

sportovních zápasů. U malých hráčů často budou existovat oprávněné zájmy, které vylučují zveřejnění fotografií. V dané situaci připadá v úvahu obstarat si souhlas zákonných zástupců. Stejné pravidlo se uplatní u skupinových fotografií pořízených během tréninků.[228]

Je tedy nezbytné, aby si spolky udělaly pořádek v procesech zpracování a přehodnotily svůj přístup k ochraně osobních údajů jako takové. Za vhodné se jeví přijmout tyto zásady o činnostech zpracování a zachytit je v písemné podobě. Ve druhé fázi podle analýzy získané v prvním kroku by mělo dojít k vyhodnocení stávajícího stavu. V této části připadá v úvahu věnovat pozornost náležitému zabezpečení osobních údajů a probrat tuto záležitost se správcem sítě, jsou-li osobní údaje spravovány i elektronicky. Velkým mýtem, který se rychle rozšířil napříč internetem, je také nutnost pořídit uzamykatelné skříně nebo schránky na data obsažená v listinné podobě. Obecné nařízení žádnou takovou povinnost výslovně nedefinuje. Stanovením principu založeném na riziku nese nebezpečí spojené se zabezpečením správce či zpracovatele a je jen na něm, jakým způsobem údaje zabezpečí. Pokud budou prostory, kde spolek uchovává data v listinné podobě, dobře zabezpečeny, rozhodně není nutné pořizovat nad rámec běžného zabezpečení uzamykatelné skříně nebo speciální schránky, jak se snaží někteří prodejci tohoto zboží předestírat.

Zároveň na tomto místě přichází v úvahu revize smluv se zpracovateli, tedy osobami, kterým spolek osobní údaje předává, typicky IT nebo účetní a daňové kanceláři. I tito zpracovatelé musí přijmout taková vhodná technická a organizační opatření, aby byli schopni zabezpečit svěřená data. Ve druhé fázi by dále mělo proběhnout proškolení členů spolku, kteří budou s osobními údaji pracovat. Základní okruh tohoto školení by měl spočívat alespoň v tom, jakým způsobem umožnit řádný výkon práv subjektů údajů. Nejčastěji půjde o to, jak a v jaké lhůtě vyřídit žádost subjektu údajů, jak vyhodnotit a řešit bezpečnostní incident a jak mít data dostatečně zabezpečená. Souladnost s Obecným nařízením však představuje kontinuální proces, a ačkoli velká část úkolů bude soustředěna na počátek implementace, neznamená to, že po dokončení těchto operací již nebude nutné se mu věnovat. Povinnosti správce tímto nekončí, a to zejména s ohledem na výkon práv subjektů údajů.

[228] *GDPR v kostce: praktický průvodce povinnostmi pro podniky a spolky*. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-704-0, s. 49-52

Na tomto místě se jeví jako vhodné vymezit vzájemné postavení spolku a svazu spolků při ochraně osobních údajů. Ve valné většině případů u spolků a svazů spolků odpadá nutnost jmenovat pověřence a provádět předběžné konzultace s dozorovým úřadem, zejména s ohledem na nízkou míru rizika zpracování. Ve vztahu mezi spolkem a svazem spolků vystupuje každý jako samostatný správce osobních údajů, které zpracovává. Svaz spolků a spolek nemohou být ve vztahu správce a zpracovatel, neboť každý určuje vlastní prostředky zpracování, zpracovává osobní údaje svých členů, popřípadě i dalších osob a nese tak plnou zodpovědnost za toto zpracování. Každý jednotlivý spolek je tak samostatným správcem. Svaz spolků jako hlavní spolek však může podpůrně vytvořit materiály usnadňující činnost správce pobočným spolkům, může jim být nápomocen radami. V případě potřeby si může více spolků jmenovat společného pověřence a podobně. Takový společný postup stanovila například Česká obec sokolská.[229]

Závěrem této kapitoly lze uzavřít, že spolky a svazy spolků jsou zvláštní formou právnických osob, a tudíž jim, jak bylo řečeno v kapitole věnované sankcím, hrozí v případě porušení Obecného nařízení nejvyšší možná správní pokuta ve výši 20.000.000 EUR. Jak bylo ale zároveň poznamenáno, maximální výše správních sankcí rozhodně nebude užito proti spolkům. Obecné nařízení cílí na velké, nadnárodní podniky, avšak právní úprava dopadá i na velmi malé správce či zpracovatele, ke kterým lze řadit právě spolky a jejich svazy. Jakkoli velký spolek či svaz spolků zcela pravděpodobně nebude středem zájmu kontrol ze strany Úřadu. Přesto autorka práce nespatřuje uvedení zpracování do souladu s Obecným nařízením za zbytečné, neboť se jedná o důležitý krok ke změně přístupu k osobním údajům, které spolky zpracovávají. Vždy je však třeba postupovat rozumně a nepodléhat zejména médii předestíraným mýtům v ochraně osobních údajů. Jedině tak lze v případě spolků splnit požadavky stanovené Obecným nařízením bez větší technické a finanční zátěže.

[229] Společný postup při ochraně osobních údajů - GDPR. In: *Česká obec sokolská* [online]. [cit. 2018-10-28]. Dostupné z: http://www.sokol.eu/obsah/19599/spolecny-postup-pri-ochrane-osobnich-udaju-gdpr

11. Závěr

Přestože většina správců a zpracovatelů pohlíží na ochranu osobních údajů jako na něco zcela zbytečného a obtěžujícího, jedná se o důležitou otázku, které je vhodné se věnovat nejen proto, aby se předešlo uložení správních sankcí ze strany dozorového úřadu. Jakkoli mohou vznikat polemiky o nutnosti vůbec zakotvit ochranu osobních údajů v právním předpisu či o vhodnosti daného řešení, vyvstává nutnost respektovat fakt, že tato právní úprava existuje, je zapotřebí se jí řídit a implementovat ji. Autorka si vzala za cíl v této práci postihnout dopady Obecného nařízení na činnost správců a zpracovatelů a demonstrovat některé aplikační problémy. Za tímto účelem se snažila tuto problematiku mimo jiné přiblížit i na vybraných zahraničních judikátech a využila také některé myšlenky zahraničních autorů.

V *první* a *druhé* kapitole této práce autorka předestírá ochranu osobních údajů jako jedno ze základních lidských práv. Zároveň ho zasazuje do kontextu evropského právního rámce a při té příležitosti monitoruje proces jeho přijetí, včetně připomínek, která měla Česká republika. Protože Obecné nařízení je normou evropského práva, sluší se na tomto místě připomenout jeho právní formu, princip přímého účinku a vztah k původní Směrnici. Součástí druhé kapitoly je také vymezení pojmu „evropský prostor“. V rámci těchto dvou kapitol přibližuje čtenáři zasazení této normy i do českého právního prostředí.

Nebylo možné opomenout ani pojem „osobní údaj“, coby základní stavební kámen celé této práce, kterému se věnuje *třetí* kapitola. S tím souvisí i vymezení pojmu identifikovaná či identifikovatelná osoba. V další podkapitole charakterizuje autorka důležitou skupinu tzv. zvláštní kategorie osobních údajů, dříve známých pod pojmem „citlivé údaje“. V poslední části této kapitoly zmiňuje speciální skupinu osobních údajů, které jsou obsaženy v rozsudcích v trestních věcech.

Čtvrtá kapitola podává charakteristiku pojmu zpracování osobních údajů, které je v této souvislosti neméně důležitým pojmem. Dále uvádí základní zásady zpracování, které již samy o sobě obsahují elementární povinnosti správců a zpracovatelů. Jednu ze základních podmínek zpracování osobních údajů představuje právní titul takového zpracování. Autorka práce věnuje pozornost zejména nejdiskutovanějšímu z nich – souhlasu se zpracováním osobních údajů s vymezením jeho základních náležitostí. V této souvislosti autorka upozorňuje na úskalí, které užití tohoto právního titulu přináší. V neposlední řadě přichází

v úvahu i zpracování zvláštní kategorie osobních údajů. Tuto část práce uzavírá zajímavá podkapitola, věnující se zpracování osobních údajů dítěte.

Neoddělitelnou součástí ochrany osobních údajů představuje uplatnění práv subjektů údajů, a to i z toho důvodu, že ve vztahu se správcem je subjekt údajů slabší stranou. Jedná se zejména o právo na informace, právo na přístup, opravu a doplnění, právo na výmaz a omezení zpracování, právo na přenositelnost, právo na námitku proti zpracování a v neposlední řadě i práva vyplývající v souvislosti s automatizovaným zpracováním. Tomuto tématu se věnuje *pátá* kapitola práce.

Šestá kapitola do jisté míry navazuje na čtvrtou kapitolu, kdy podrobně rozebírá povinnosti správců a zpracovatelů a je do jisté míry těžištěm této práce. Základními principy jsou princip odpovědnosti správce a princip založený na riziku, od kterých se jednotlivé povinnosti odvíjí. Nelze říci, že by některé povinnosti byly důležitější než jiné. Avšak z pohledu praxe se do jisté míry jedná o určitý právní alibismus, kdy je primárně vhodné se věnovat těm povinnostem, které se aplikují navenek a které bude chtít Úřad prezentovat v případě uskutečnění kontroly. Některé z povinností se plošně neaplikují na všechny správce – například povinnost provést DPIA, povinnost mít pověřence nebo vést předchozí konzultace s dozorovým úřadem. Zvláštní pozornost v této kapitole věnuje autorka práce povinnostem správce při předání osobních údajů do zahraničí.

Aby mohla být ochrana osobních údajů efektivní, musí existovat nezávislý orgán dohledu a kontroly, který zajistí dodržování právního rámce ochrany osobních údajů. Cílem *sedmé* kapitoly je vymezit působnost a pravomoci dozorových úřadů. Každý členský stát má k dispozici jeden nebo více dozorových úřadů, přičemž je kladen důraz na mezinárodní spolupráci a jednotnost uplatňování Obecného nařízení. Za tímto účelem vedoucí dozorových úřadů v jednotlivých členských státech vytváří Evropský sbor pro ochranu osobních údajů. Do doby účinnosti Obecného nařízení tuto působnost vykonávala skupina WP29.

Osmá kapitola seznamuje čtenáře s možnostmi právní ochrany – zejména o právu podat stížnost a právu na soudní ochranu. Soudní ochrana je zaručena jak vůči správci či zpracovateli, tak proti dozorovému úřadu, a to v případě ochrany proti jeho rozhodnutí nebo v případě nečinnosti. Dále tato kapitola popisuje uplatnění práva na náhradu újmy nebo majetkové škody v souvislosti s ochranou

osobních údajů. V rámci této kapitoly jsou také nastíněny okolnosti ukládání správních pokut, které jsou bezpochyby jedním z nejdiskutovanějších témat v souvislosti s Obecným nařízením. Kapitolu uzavírá možnost uložení sankcí v rovině trestního práva.

Právo na ochranu osobních údajů není právem absolutním, může docházet k situacím, kdy dojde ke střetu dvou ústavně zaručených lidských práv a v některých případech musí právo na ochranu osobních údajů ustoupit jiné hodnotě. Tohoto zajímavého jevu se dotýkají zejména zvláštní druhy zpracování. Autorka si v *deváté* kapitole práce vybrala dvě z nich, které podrobněji rozebrala a na praktických případech a vybrané zajímavé judikatuře se pokusila demonstrovat tento střet. Pro tyto účely zvolila střet svobody projevu a práva na ochranu osobních údajů a dále užití kamerových systémů. Obecně lze říci, že k posouzení lze užít test proporcionality, udávající základní premisu, která říká, že základní právo na svobodu lze omezit pouze v zájmu jiného práva nebo svobody.

V poslední, *desáté* kapitole práce se autorka pokusila předestřít praktickou aplikaci Obecného nařízení, pro něž si zvolila činnost spolků a jejich svazů. Pozornost zaměřuje zejména na některé problematické aspekty zpracování, týkající se například užití souhlasů se zpracováním nebo pořizováním fotografií. V rámci této kapitoly byl také vymezen vzájemný vztah spolku a svazu spolků z hlediska ochrany osobních údajů, zejména z titulu odpovědnosti za zpracování.

Autorka měla v rámci průběhu tvorby práce možnost stát se pozorovatelem procesu příprav na účinnost Obecného nařízení a rovněž i možnost sledovat období v rozsahu několika měsíců po jeho účinnosti. Jakkoli před jeho účinností panovala místy až hysterie, po 25. květnu 2018 jako by zájem o toto téma opadnul. Jak již bylo v této práci zmíněno, compliance s Obecným nařízením však představuje kontinuální proces, a to zejména s ohledem na výkon práv subjektů údajů vůči správci či zpracovateli. Obecné nařízení by se mělo stát v rozumném čase, zejména po přijetí adaptační normy, pravidelným compliance liniovým procesem a bude nadále docházet ke konsolidaci aplikační praxe. Tuto otázku nelze opomíjet, neboť zřejmě již v příštím roce nabude účinnosti nařízení E-privacy, které dokreslí některé otázky vyplývající z Obecného nařízení a konkretizuje procesy ochrany osobních údajů v elektronických komunikacích. Jakkoli Obecné nařízení neshledává u většiny správců a zpracovatelů pozitivní ohlasy, zejména u těch, kteří této oblasti věnovali minimální pozornost, jedná se o důležitý mezník v přístupu k ochraně osobních údajů v evropském i světovém

měřítku. K tomu, aby docházelo k efektivní ochraně osobních údajů, již původní Směrnice nemohla zejména v důsledku rozvoje technických prostředků obstát. Ačkoli autorka práce vítá zvýšení právního povědomí o ochraně osobních údajů v důsledku účinnosti Obecného nařízení, nelze přehlížet, že tato norma cílila zejména na velké správce a zpracovatele. V konečném důsledku ale dopadá na všechny správce, včetně těch nejmenších, u nichž může implementace Obecného nařízení způsobovat negativní dopady v podobě zvýšené finanční a administrativní zátěže. Zákonodárce však tuto skutečnost opominul a nestanovil pro tyto správce téměř žádné výjimky. Celou situaci navíc ztěžuje i dosavadní neexistence adaptační normy v podmínkách českého práva. S ohledem na to nelze jednoznačně vyslovit, zda Obecné nařízení zajišťuje v konečném důsledku efektivní ochranu osobních údajů. Tuto otázku zodpoví až další aplikační praxe, kterou bude autorka i nadále sledovat.

12. Résumé

Although most administrators regard personal data protection as completely unnecessary and intrusive, it is a pivotal issue which is worth paying attention to - not solely to evade administrative sanctions from the data protection supervisory. The thesis aims to cover the impacts of the Regulation on the activities of administrators and processors, and to demonstrate some of the implementation difficulties. To achieve this goal, chosen Czech and foreign judicial decisions were used to illustrate the issue, including views of foreign authors.

Chapters I and II feature personal data protection as one of the fundamental human rights. This right is contextualised within the European legislative framework and the acceptance process is monitored, including suggestions made by the Czech Republic. The two chapters also provide information on embedding the regulation in the Czech legislative environment.

Chapter III elaborates on the notion of personal data, which is the key aspect of the whole thesis. An important group of personal data, so called special category personal data, is characterized in a subchapter. The final part of Chapter III deals with another special category of personal data, i.e. personal data included in criminal law judgements.

Chapter IV characterizes personal data processing, which is another essential aspect. The chapter comprises the key principles of the processing, including elementary obligations of data administrators and processors. One of the fundamental conditions of personal data processing is the legal title to processing. The main focus has been placed on the most debated title, i.e. the consent to personal data processing and specification of its fundamental requirements. The chapter is concluded by an interesting subchapter addressing children's personal data processing.

The exercise of the data subjects' rights is an integral part of personal data protection, as the data subject constitutes the weaker party within the relationship with the administrator. These rights include especially the right to information, the right to access, the right to rectify and complete, the right to erasure and the right to restrict processing, the right to data portability, the right to object to the

processing and last but not least the rights arising in relation to automated processing. All these rights are dealt with in Chapter V.

Chapter VI elaborates on Chapter IV to some extent, as it features a detailed analysis of administrators' and processors' obligations and thus forms a core of the thesis. The fundamental principles are the principle of the administrator's responsibilities and the principle based on risk, from which the individual obligations are derived. Some of the obligations are not applied universally to all administrators – e.g. the obligation to carry out a DPIA, the obligation to appoint a data protection officer or to ensure prior consultation with the data protection supervisory. A major focus has been placed on the administrator's obligations when transferring personal data abroad.

To ensure efficient protection of personal data, there has to be an independent supervisory and monitoring body which ensures compliance with the legislative framework of personal data protection. Chapter VII aims to specify the competences and powers of supervisory authorities.

In Chapter VIII, legal protection options are addressed – especially the right to file a complaint with the data protection supervisory and the right to judicial protection. The chapter also features ways to enforce the entitlement to receive compensation for harm or material damage related to personal data protection. Chapter VIII also describes circumstances under which administrative fines are imposed, undoubtedly one of the most debated issues related to the Regulation. Finally, the chapter specifies ways of imposing sanctions in criminal law.

The right to personal data protection is not an absolute right, thus it may occur that two constitutionally guaranteed human rights conflict. In some cases, the right to personal data protection has to be withdrawn in favour of another value. This peculiar phenomenon relates particularly to special types of processing. Chapter IX includes a detailed analysis of two such cases, demonstrating the conflict on practical examples and relevant judicial decisions.

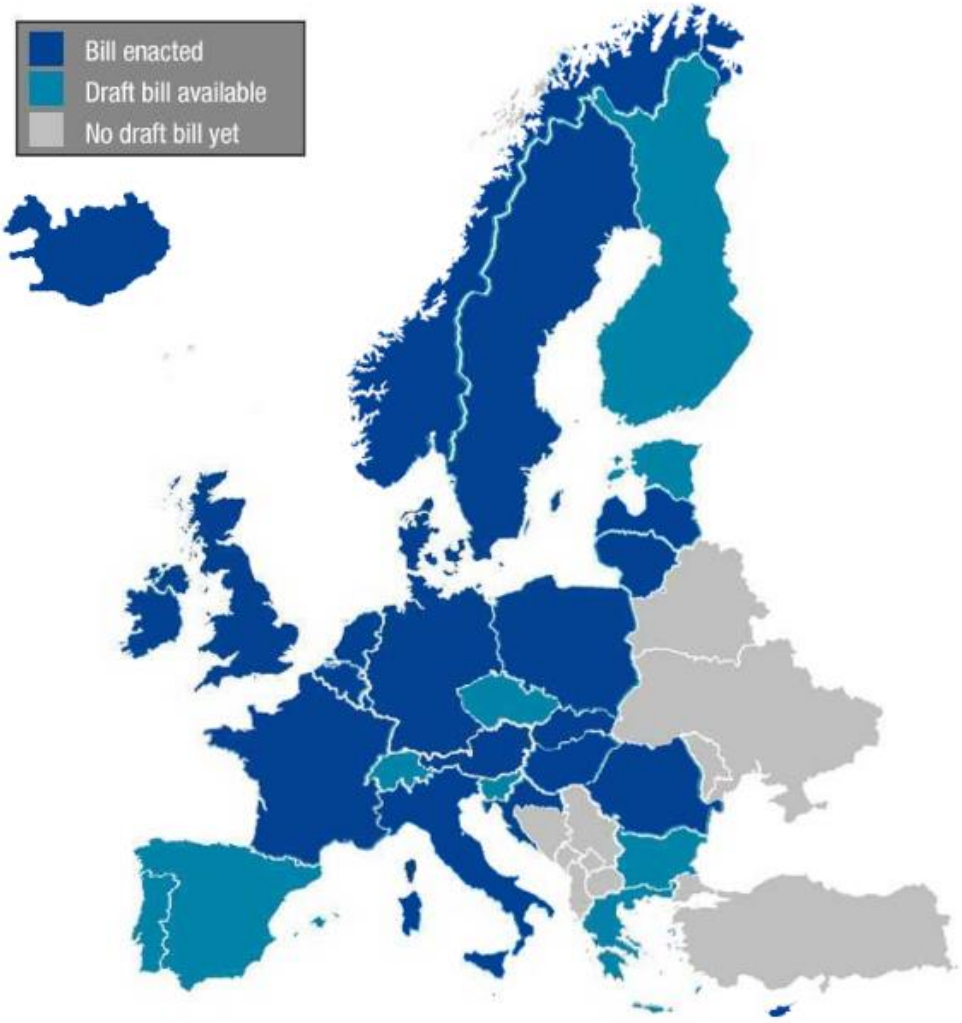
The concluding chapter (Chapter X) addresses practical application of the Regulation, specifically demonstrated on the activities of associations and their unions. Some problematic aspects of processing are illuminated, e.g. those associated with using consent to process and take photographs.

While working on the thesis, the author had the opportunity to observe the process of preparations for the Regulation coming into effect and likewise to

observe a period of several months after the Regulation came into effect. The issue of personal data protection cannot be ignored, as the E-privacy regulation is likely to come into effect as early as next year. The E-privacy regulation shall provide a further specification of some issues arising from the Regulation. It also aims to specify the processes of personal data protection in electronical communication. Although the Regulation has not been accepted positively by most administrators and processors (mainly by those who had not attended to the issue appropriately), it has marked an important milestone in approaching personal data protection both in Europe and worldwide.

The original Guidelines could no longer ensure efficient personal data protection, especially due to technical tools development. The author of the thesis welcomes the rise in legal awareness of personal data protection, since the Regulation came into effect. However, it is obvious that the norm was aimed especially at major administrators and processors. As a result, the Regulation impacts all administrators, including the minor ones. These minor administrators may suffer from negative impacts of increased financial and administrative burden. Nevertheless, the legislators have omitted this fact and almost no exemptions were provided. The situation as a whole is being aggravated by the non-existence of norm adaptation in the Czech legal conditions. Taking these facts into account, it cannot be unequivocally stated whether the Regulation, in the end, provides efficient personal data protection. This question shall be answered within further practical application which the author will continue to monitor.

Příloha č. 1 – Mapka rozlišující existenci prováděcích předpisů v jednotlivých státech evropského prostoru[230]



[230] GDPR Local Implementation. In: *Morrison & Foerster* [online]. [cit. 2018-11-15]. Dostupné z: https://www.mofo.com/special-content/gdpr-readiness-center/gdpr-local-implementation.html (Ve stavu poslední aktualizace k 15.11.2018). Tmavě modře jsou vyobrazeny státy, které již mají účinný prováděcí předpis, světle modře ty, kde proces přijímání stále probíhá.

Příloha č. 2 – Formulář pro podávání stížností [231]

Formulář pro podávání stížností

Oznámení konkrétního podezření na zpracování osobních údajů v rozporu s obecným nařízením o ochraně osobních údajů.

Prosím, věnujte pozornost vyplnění tohoto formuláře.
Podání, které upozorňuje na podezření z porušení obecného nařízení o ochraně osobních údajů, musí obsahovat takové konkrétní informace, aby mohl být bez prodlení zvolen účinný a cílený postup.

Stěžovatel/ka (subjekt údajů, tj. osoba dotčená zpracováním)

Jméno a příjmení

Bydliště

e-mail*

telefon*

* *Nepovinné údaje.*

Označení subjektu, proti kterému směřuje podnět/stížnost

Název subjektu (Jméno a příjmení)

Adresa sídla nebo místa podnikání

IČ (u právnické osoby a fyzické osoby podnikající)

Uplatnil/a jste vůči správci nebo zpracovateli některé z následujících práv na:

- vznesení námitky proti zpracování
- opravu
- výmaz
- omezení zpracování
- přístup k osobním údajům

Kdy a jakou formou jste uvedené právo uplatnil/a? Uveďte další relevantní informace.

Jakou odpověď a kdy jste obdržel/a?

[231] Formulář pro podávání stížností. In: *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-10-03]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31628

Podrobný popis stížnosti

Uveďte konkrétně, v čem spatřujete porušení povinností při zpracování Vašich osobních údajů.

– popis činnosti zahrnující zpracování osobních údajů, v jejímž průběhu mělo dojít k porušení obecného nařízení o ochraně osobních údajů,

– uvedení osobních údajů (nebo alespoň jejich kategorií) zpracovaných v rozporu s obecným nařízením o ochraně osobních údajů,

– listiny či jiné materiály (příp. jejich kopie), které dokládají vztah mezi oznamovatelm (stěžovatelem) a subjektem, který jeho osobní údaje měl chybně zpracovávat, nebo které se vztahují k vytýkanému zpracování. V některých případech je nutné uvést i Váš vztah ke správci (např. zaměstnanec, zákazník atd).

– případné uvedení odkazů na dostupné zdroje, které mohou svědčit o popisovaných skutečnostech.

Vyplněný formulář společně s dokumenty dokládajícími závadný stav a dalšími relevantními podklady zasílejte na **stiznosti@uoou.cz** nebo klikněte na tlačítko **Odeslat**.

Podatel je vždy Úřadem informován o posouzení a vyřízení jeho podání.

Seznam použité literatury

1) Zahraniční

a) Monografie, publikace a statě ve sbornících

- BUCHNER, Benedikt a Jürgen KÜHLING. *DS-GVO Datenschutz-Grundverordnung: Kommentar*. C. H. Beck, 2017. ISBN 978-3-406-70212-9.
- De BÚRCA, G., CRAIG, P. EU Law: Text, Cases, and Materials. Oxford: Oxford University Press, 2011, ISBN: 978-0-19-927389-8.
- EßER, Martin, Philipp KRAMER a Kai VON LEWINSKI. *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze: Kommentar*. 5. Auflage. Carl Heymanns Verlag, 2017. ISBN 978-3-452-28841-7.
- FOREJTOVÁ, M. Analysis on preliminary ruling (Interpretation of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data). In Challenges of Today - Politics and Society. Gdańsk : Research Institute for European Policy in the cooperation of the Department of Political Science at University of Gdansk., 2015,ISBN: 978-83-944614-1-6.
- FOREJTOVÁ, M. The right to respect for private life and the right to personal data protection - is there any conflict?. *Państwo i Prawo*, 2017, roč. 72, č. 9, ISSN: 0031-0980.
- PAAL, Boris a Daniel PAULY. *Datenschutz-Grundverordnung: Beck´sche Kompakt-Kommentare*. C.H. Beck, 2017. ISBN 978-3-406-69570-4.
- SYDOW, Gernot. *Europäische Datenschutzgrundverordnung: Handkommentar*. 2. Auflage. Nomos Verlagsgesellschaft, 2018. ISBN 978-3-8487-4892-1.

b) Časopisecké a elektronické zdroje

- About EDPB. In: *European Data Protection Board* [online]. [cit. 2018-10-07]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb_cs
- BOMMEL, Robert. Bußgelder bei Datenschutzverstößen. In: *Brandi Rechtsanwälte* [online]. [cit. 2018-10-24]. Dostupné z:

https://www.brandi.net/fileadmin/user_upload/Bussgelder_bei_Datenschutzverstoessen_1_2017.pdf

- CNIL. Methodology for Privacy Risk Management: How to implement the Data Protection Act, s. 9-10 [online]. [cit. 2018-02-27]. Dostupné z: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf
- Consultation: Children and the GDPR guidance. *Infomration Commisssioner´s Office* [online]. 2017 [cit. 2018-02-23]. Dostupné z: https://ico.org.uk/about-the.../children-and-the-gdpr-guidance, s. 29
- CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law 2016* [online]. 2016, 3-4 [cit. 2018-02-27]. Dostupné z: http://data-reuse.eu/wp-content/uploads/2016/01/International-Data-Privacy-Law-2016-Custers.pdf
- EU-U.S. Privacy Shied Framework - Key New Requirements for Participating Companies. In: *Privacy Shied Framework* [online]. 2018 [cit. 2018-07-08]. Dostupné z: https://www.privacyshield.gov/Key-New-Requirements
- Facebook data scandal also affect 2.7M EU citizens. In: *Techcrunch* [online]. 6.4.2018 [cit. 2018-07-10]. Dostupné z: https://techcrunch.com/2018/04/06/facebook-data-scandal-eu-citizens/
- FÄRBER, Claus Dr. European General Data Protection Regulation to Apply from May 2018. *McDermott Will & Emery* [online]. 2016 [cit. 2018-02-16]. Dostupné z: https://www.mwe.com/en/thought-leadership/publications/2016/06/european-general-data-protection-regulation
- GDPR Local Implementation. In: *Morrison & Foerster* [online]. [cit. 2018-11-15]. Dostupné z: https://www.mofo.com/special-content/gdpr-readiness-center/gdpr-local-implementation.html
- CHORZEMPA, Martin, Paul TRIOLO a Samm SACKS. China´s Social Credit System: A Mark of Progress or a Threat to Privacy?. *Peterson institute for international economics* [online]. [cit. 2018-11-12]. Dostupné z: https://piie.com/system/files/documents/pb18-14.pdf

- Incorporation of the GDPR into the EEA Agreement [online]. In: . 13.4.2018 [cit. 2018-08-01]. Dostupné z: http://www.efta.int/EEA/news/Incorporation-GDPR-EEA-Agreement-508041
- Irish High Court Refers Chrems 2.0 to the ECJ. In: HEMMINGS, Justin. *Alston & Bird* [online]. 13.4.2018 [cit. 2018-07-11]. Dostupné z: https://www.alstonprivacy.com/irish-high-court-refers-schrems-2-0-to-the-ecj/
- Joint Press Statement from Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross on the Second Annual EU-U.S. Privacy Shield Review. In: *U.S. Department of Commerce*[online]. [cit. 2018-10-21]. Dostupné z: https://www.commerce.gov/news/press-releases/2018/10/joint-press-statement-commissioner-vera-jourova-and-secretary-commerce
- List of companies for which the EU BCR cooperation procedure is closed. In: *European Commission* [online]. 24.5.2018 [cit. 2018-07-11]. Dostupné z: ec.europa.eu/newsroom/article29/document.cfm?doc_id=50116
- LOMAS, Natasha. *EU parliament calls for Privacy Shield to be pulled until US complies*[online]. In: . 5.7.2018 [cit. 2018-07-10]. Dostupné z: https://techcrunch.com/2018/07/05/eu-parliament-calls-for-privacy-shield-to-be-pulled-until-us-complies/?guccounter=1
- Looming Ruling on EU Data Transfer Rules Carries Potentially Serious Implications. In: *JDSUPRA* [online]. 17.10.2017 [cit. 2018-07-11]. Dostupné z: https://www.jdsupra.com/legalnews/looming-ruling-on-eu-data-transfer-58017/
- MALDOFF, Gabriel. The Risk-Based Approach in the GDPR: Interpretation and Implications. *IAPP Westin Fellow* [online]. 2017 [cit. 2018-02-27]. Dostupné z: https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf
- Odůvodnění hlasování 7920/1/16 REV 1 (Interinsitutcionální spis: 2012/0011 (COD)). In: *Rada Evropské unie* [online]. 7.11.2016 [cit. 2018-08-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CONSIL:ST_7920_2016_REV_1&from=EN

- Ochrana údajů: Rada se dohodla na obecném přístupu. In: *Rada Evropské unie* [online]. 2015 [cit. 2018-08-05]. Dostupné z: http://www.consilium.europa.eu/cs/press/press-releases/2015/06/15/jha-data-protection/
- Passanger Name Record (PNR). In: *European Commission: Migration and home affairs*[online]. 2018 [cit. 2018-07-11]. Dostupné z: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en
- Swiss-US Privacy Shied: better protection for data transferred to the USA. In: *The Federal Council* [online]. 11.1.2017 [cit. 2018-07-08]. Dostupné z: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-65210.html
- Trump order strips privacy rightsfrom non - U.S. citizens, could nix EU-US data flows. *TechCrunch* [online]. 26.1.2017 [cit. 2018-07-08]. Dostupné z: https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/

c) Pokyny a výkladová stanoviska pracovní skupiny WP29 a Evropského sboru pro ochranu osobních údajů

- *Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data* [online]. 20.6.2007, (01248/07/EN) [cit. 2018-02-03]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
- Article 29 Data Protection Working Party: Opinion 15/2011 on the definition of consent [online]. 13.6.2011, (01197/11/EN) [cit. 2018-02-03]. Dostupné z: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1308,
- *Article 29 Data Protection Working Party: Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing*[online]. 22.9.2015, (2588/15/EN; WP232) [cit. 2018-05-05]. Dostupné z: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf
- *Article 29 Data Protection Working Party: Opinion 03/2017 on Guidelines on Personal data breach notification under Regulation*

2016/679[online].3.10.2017, (17/EN; WP250) [cit. 2018-06-17]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=47741

- Article 29 Data Protection Working Party: Guidelines on the implementatiion of the court of justice of the European union judgment on „Google Spain and inc v. Agencia Espanola de Protección de datos (AEPD(and Mario Costeja González“ [online].26.11.2014, (14/EN; **WP225**) [cit. 2018-09-5]. Dostupné z: http://www.dataprotection.ro/servlet/ViewDocument?id=1080
- *Article 29 Data Protection Working Party: Guidelines on the right to data portability*[online].13.12.2016, (16/EN; **WP 242** rev. 01) [cit. 2018-09-05]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099
- *Article 29 Data Protection Working Party: Guidelines on Data Protection Officers (´DPO´s)* [online].13.12.2016, (16/EN; **WP 243**) [cit. 2018-06-27]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=43823
- Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to reset in a high risk“ for the purposes of Regulation 2016/ 679 [online]. 4.4.2017, (17/EN; **WP 248**) [cit. 2018-05-05]. Dostupné z: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- Annex 2 – Criteria for acceptable DPIA, Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to reset in a high risk“ for the purposes of Regulation 2016/ 679 [online]. 4.4.2017, (17/EN; **WP 248**) [cit. 2018-05-05]. Dostupné z: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- *Article 29 Data Protection Working Party:* Guidelines on Automated individual decision-making and Profiling for purposes of Regulation 2016/679 [online].3.10.2017, (17/EN; **WP251**) [cit. 2018-09-17]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=47742
- *Article 29 Data Protection Working Party: Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* [online]. 3.10.2017, (17/EN/**WP253**) [cit. 2018-10-20].

Dostupné z: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

- *Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679*[online]. 28.11.2017, (17/EN/**WP259**) [cit. 2018-02-03]. Dostupné z: ec.europa.eu/newsroom/just/document.cfm?doc_id=48849
- *Article 29 Working Party: Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679* [online].6.2.2018, (18/EN) [cit. 2018-07-07]. Dostupné z: ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877, s. 9
- Endorsement of GDPR WP29 guidelines by the EDPB. *The European Data Protection Board* [online]. 2018 [cit. 2018-10-07]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf
- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679. In: *European Data Protection Board* [online]. 2018 [cit. 2018-10-03]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

2) Česká

a) Monografie, publikace a statě ve sbornících

- BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi (vybrané problémy)*. 4. Wolters Kluwer, 2016. ISBN 978-80-7552-141-5.
- FOREJTOVÁ, Monika a Michaela TRONEČKOVÁ. *Evropské právo v praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. Monografie (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-301-8.
- *GDPR v kostce: praktický průvodce povinnostmi pro podniky a spolky*. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-704-0.
- HAMUĽÁK, Ondrej. *Právo Evropské unie v judikatuře Ústavního soudu České republiky: Reflexe členství a otázek evropského práva v ústavní judikatuře*. Leges. 2010. ISBN 978-80-87212-43-1.

- MORÁVEK, Jakub. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Praha: Wolters Kluwer, 2015. Judikatura (Wolters Kluwer ČR). ISBN 978-80-7552-018-0.
- NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.
- NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.
- ONDŘEJKOVÁ, Jana. *Princip přednosti evropského práva v teorii a soudní praxi*. Leges, 2012.
- PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě. Komentář*. Leges, 2018. ISBN 978-80-7502-288-2.
- SLÁDEČEK, Vladimír. *Obecné správní právo*. 3., aktualiz. a upr. vyd. Praha: Wolters Kluwer Česká republika, 2013. ISBN 978-80-7478-002-8.
- STEHLÍK, Václav, Ondrej HAMUĽÁK a Michal PETR. *Právo Evropské unie: ústavní základy a vnitřní trh*. Praha: Leges, 2017. Student (Leges). ISBN 978-80-7502-277-6.
- ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5.
- TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. *Právo Evropské unie*. Praha: Leges, 2013. Student (Leges). ISBN 978-80-87576-53-3.
- *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0.
- ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3.

b) Časopisecké a elektronické zdroje

- Často kladené otázky podle oblastí; *Úřad pro ochranu osobních údajů* https://www.uoou.cz/casto-kladene-otazky-podle-oblasti/ds-2619/p1=2619
- Dozorová činnost. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-09-24]. Dostupné z: https://www.uoou.cz/dozorova-cinnost/ds-1277/p1=1277

- GDPR pro advokáty. *Česká advokátní komora* [online]. 2018 [cit. 2018-09-23]. Dostupné z: https://www.cak.cz/scripts/detail.php?id=18817
- HORKÁ, Nikola. Souhlas se zpracováním osobních údajů ve světle nové legislativy. *E-pravo.cz*[online]. 2018, , 1-3 [cit. 2018-02-19]. Dostupné z: https://www.epravo.cz/top/clanky/souhlas-se-zpracovanim-osobnich-udaju-ve-svetle-nove-legislativy-106991.html
- Informace ke konzultačním službám. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-09-23]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30721
- KOMÍNKOVÁ, Magda. Jak vznikalo Nařízení o ochraně osobních údajů (GDPR)?. *Euroskop.cz* [online]. 2018, 27.3.2018 [cit. 2018-08-05]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/
- KŘEPELKA, Filip. Nahrazování směrnic nařízeními (důvody, skutečnost, možnosti). In: *Právník*. 03/2017, s. 215, 222-223
- METELKA, Jan. Ochrana osobních údajů skrze tokenizaci. *E-pravo.cz* [online]. 2016 [cit. 2018-11-02]. Dostupné z: https://www.epravo.cz/top/clanky/ochrana-osobnich-udaju-skrze-tokenizaci-104196.html
- Metodická pomůcka k aplikaci GDPR ve školství. *Ministerstvo školství, mládeže a tělovýchovy ČR* [online]. 2017 [cit. 2018-09-23]. Dostupné z: http://www.msmt.cz/dokumenty-3/metodicka-pomucka-k-aplikaci-obecneho-narizeni-o-ochrane
- NEŠPŮREK, Robert, Jaroslav ŠUCHMAN a Ján JAROŠ. GDPR: nastane s nástupem nové regulace nedostatek pověřenců?. *E-pravo* [online]. 2018, 9.4.2018, (04) [cit. 2018-07-01]. Dostupné z: https://www.epravo.cz/top/clanky/gdpr-nastane-s-nastupem-nove-regulace-nedostatek-poverencu-107264.html
- NULÍČEK, Michal. Právo být zapomenut. *Bulletin advokacie*. 2017(06).
- ONDŘEJOVÁ, Eva. Desetiletá cesta od Rozsudku Von Hannover 1 k Rozsudku Von Hannover 3. *Bulletin advokacie* [online]. 9.1.2015 [cit. 2018-11-17]. Dostupné z: http://www.bulletin-advokacie.cz/desetileta-cesta-od-rozsudku-von-hannover-1-k-rozsudku-von-hannover-3

- PAVLÍČEK, Libor. GDPR a TOPO a jejich význam pro obchodní společnosti. *E-pravo.cz* [online]. [cit. 2018-12-02]. Dostupné z: https://www.epravo.cz/top/clanky/gdpr-a-topo-a-jejich-vyznam-pro-obchodni-spolecnosti-106475.html
- Předkládací zpráva návrhu zákona o zpracování osobních údajů a Vypořádání připomínek k návrhu zákona o zpracování osobních údajů. *Ministerstvo vnitra* [online]. 2017 [cit. 2018-02-22]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5
- Role ÚOOÚ. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-09-19]. Dostupné z: https://www.uoou.cz/role-uoou/ds-4726/archiv=0&p1=3938
- Rozhodnutí Úřadu pro ochranu osobních údajů č.j. 26/05/SŘ- OSČ, č.j. 50/05/SŘ-OSČ, č.j. 70/05/SŘ-OSČ. Úřad *pro ochranu osobních údajů* [online]. 2013 [cit. 2018-08-11]. Dostupné z: https://www.uoou.cz/k-plneni-informacni-povinnosti/d-1596
- Společný postup při ochraně osobních údajů - GDPR. In: *Česká obec sokolská* [online]. [cit. 2018-10-28]. Dostupné z: http://www.sokol.eu/obsah/19599/spolecny-postup-pri-ochrane-osobnich-udaju-gdpr
- Standardní smluvní doložky. In: *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 2018-07-11]. Dostupné z: https://www.uoou.cz/standardni-smluvni-dolozky/ds-5074/p1=5074
- Stanovisko Úřadu pro ochranu osobních údajů č. 2/2011, ve znění aktualizované verze z února 2014
- Šéfka Úřadu pro ochranu osobních údajů: Vysokými pokutami chceme firmy odrazovat, ne likvidovat. *E15* [online]. 2018 [cit. 2018-10-24]. Dostupné z: https://www.e15.cz/rozhovory/sefka-uradu-pro-ochranu-osobnich-udaju-vysokymi-pokutami-chceme-firmy-odrazovat-ne-likvidovat-1334926
- Tisková zpráva: Správní řízení se společností T-Mobile Czech Republic a.s. In: *Úřad pro ochranu osobních údajů* [online]. 2017 [cit. 2018-10-24]. Dostupné z: https://www.uoou.cz/tiskova-zprava-uoou-udelil-rekordni-pokutu-za-nbsp-spam/d-23838

- Tisková zpráva: ÚOOÚ udělil rekordní pokutu za spam. In: *Úřad pro ochranu osobních údajů* [online]. 2017 [cit. 2018-10-24]. Dostupné z: https://www.uoou.cz/tiskova-zprava-uoou-udelil-rekordni-pokutu-za-nbsp-spam/d-23838
- VARVAŘOVSKÝ, Petr a Libor ZBOŘIL. Trestněprávní směrnice jako doplnění obecného nařízení na ochranu osobních údajů. *E-pravo.cz* [online]. 9.8.2018 [cit. 2018-08-20]. Dostupné z: https://www.epravo.cz/top/clanky/trestnepravni-smernice-jako-doplneni-obecneho-narizeni-na-ochranu-osobnich-udaju-108013.html
- Základní příručka k GDPR. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-01-24]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=3938

3) Použitá judikatura

a) Zahraniční

- Rozsudek Evropského soudního dvora ze dne 5. února 1963 N.V. Algemene Transport- en Expeditie Onderneming van Gend & Loos proti Nederlandse administratie der belastingten, věc 26/62
- Rozsudek Soudního dvora ze dne 15. července 1964 Flaminio Costa proti E.N.E.L., věc 6/64
- Rozsudek Soudního dvora ze dne 17. prosince 1970, Internationale Handelsgesellschaft GmbH proti Einfuhr- und Vorratsstelle für Getreide und Futtermittle, věc 11/70
- Rozsudek Soudního dvora ze dne 9. března 1978 Amministrazione delle Finanze dello Stato proti Simmenthal SpA., věc 106/77
- Rozsudek Soudního dvora ze dne 20. května 2003 Österreichischer Rundfunk aj., spojené věci C-465/00, C-38/01 a C-139/01 (Urteil des Gerichtshofes vom 20. Mai 2003, Österreichischer Rundfunk und andere, Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01)
- Rozsudek Soudního dvora EU ze dne 6. listopadu 2003, Bodil Lindqvist, věc C-101-01
- Rozsudek Evropského soudu pro lidská práva ze dne 24. června 2004 Von Hannover proti Německu ze dne 24. června 2004, stížnost č. 59320/00 a na něj navazující rozsudky Von Hannover proti Německu II. a III.

- Rozsudek Soudního dvora ze dne 7. května 2009 College van burgmester en wethouders van Rotterdam v. M.E.E. Rijkeboer, věc C-553/07
- Rozsudek Soudního dvora EU ze dne 9. března 2010, Evropská komise proti Spolkové republice Německo, věc C-518/07
- Rozsudek Soudního dvora EU ze dne 13. května 2014 ve věci Google Spain SL, Google Inc. proti Agencia Española De Protección de Datos (AEPD), Mario Costeja González, věc C-131/12
- Rozsudek Soudního dvora ze dne 1. října 2015 Weltimmo, s.r.o., proti Nemzeti Adatbéfrlmi és Információszabadság Hatóság, věc C-230/14
- Rozsudek Soudního dvora EU ze dne 6. října 2015, Maximillian Schrems proti Data Protection Commissione, věc C-362/14
- Rozsudek Soudního dvora ze dne 19. října 2016 Patrick Breyer proti Spolkové republice Německo, věc C-213/15
- Rozsudek Soudního dvora ze dne 9. března 2017 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatore Mannimu, věc C-398/15
- United States Court of Appeals for the second circuit: Microsoft Corporation v. United States of America, Doc. No. 14-2985, decided: July 14, 2016

b) Česká

- Nález Ústavního soudu ze dne 9. března 2004, sp. zn. Pl. ÚS 38/02
- Nález Ústavního soudu ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94
- Nález Ústavního soudu ze dne 17. července 2007, sp. zn. IV. ÚS 23/05
- Rozsudek Nejvyššího správního soudu ze dne 25. února 2015 č.j. 1 As 113/2012-133
- Rozsudek Nejvyššího soudu ze dne 12. prosince 2012, sp. zn. 30 Cdo 3770/2011
- Rozsudek Městského soudu v Praze ze dne 25. dubna 2012, č.j. 9 Ca 41/2009-60-70

4) Právní předpisy

a) Unijní a jiné

- Smlouva o Evropské unii
- Smlouva o fungování Evropské unie
- European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025 (INI))
- Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und –Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 (německý prováděcí zákon)
- Listina základních práv Evropské unie 2012/C 326/02
- 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 (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti
- Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti
- Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech
- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 115/2001 Sb. m. s. ze dne 28. ledna 1981
- zákon č. 122/2013 Sb., o ochrane osobných údajov a o zmene a doplneni niektorých zákonov

b) České

- Listina základních práv a svobod
- Ústava České republiky
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
- Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
- Zákon č. 255/2012 Sb., o kontrole (kontrolní řád)
- Zákon č. 500/2004 Sb., správní řád
- Zákon č. 150/2002 Sb., soudní řád správní
- Zákon č. 82/1998 sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád)
- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 186/2016 Sb., o hazardních hrách
- Zákon č. 307/2013 Sb., o povinném značení lihu
- Důvodová zpráva k zákonu č. 101/2000 Sb., Sněmovní tisk 374/0
- Důvodová zpráva k vládnímu návrhu zákona o zpracování osobních údajů
- Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

4) Ostatní zdroje

a) Zahraniční

- Adequacy decisions. In: *European Commission* [online]. [cit. 2018-10-02]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Agreemnet between the European Union and The United States of America on the processing and transfer of Financial Messaging Data from

the European Union on the United States for the purposes of the Terrorist Finance Tracking Program (TFTP)

- Decision of the European Economic Area Joint Committee No. 154/2018 of 6 July 2018 amending Annex XI (Electronic communication audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement (2018/1022)
- European Parliament resolution on the adequacy of the protection by the EU-US Privacy Shied 2018/2645(RSP)
- Modelový příklad užití GAP analýzy v oblasti ochrany osobních údajů http://www.powysthb.wales.nhs.uk/sitesplus/documents/1145/IMT%26G_Item_3.6_GDPR_Appendix%202.pdf
- Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí
- Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států
- Sdělení Komise Evropskému parlamentu a Radě ze dne 27. listopadu 2013 „Obnovení důvěry v toky údajů mezi EU a USA“
- Usnesení Evropského parlamentu ze dne 21. února 2014 o programu agentury NSA pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů EU a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí, 2013/2188(INI)

b) České

- Důvodová zpráva k § 15 vládního návrhu zákona o zpracování osobních údajů cit. dne 7.7.2018.
- Formulář pro podávání stížností. In: *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-10-03]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31628

- Kodexy chování. In: *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 2018-07-07]. Dostupné z: https://www.uoou.cz/kodexy-chovani/d-29493/p1=3938
- K provozování kamerových systémů. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-11-14]. Dostupné z: https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535/p1=0
- K činnosti spolků. In: *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/k-cinnosti-spolku/ds-5084/p1=5084
- Metodika Úřadu pro ochranu osobních údajů: *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)*; online]. [cit. 2018-05-07]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003
- Návrh seznamu operací zpracování osobních údajů, která nepodléhají posouzení vliv na ochranu osobních údajů. In: *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-09-21]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30738
- Neplatnost rozhodnutí Komise o tzv. Safe Harbor - doporučení Úřadu. In: *Úřad pro ochranu osobních údajů* [online]. 22.10.2015 [cit. 2018-07-08]. Dostupné z: https://www.uoou.cz/neplatnost-rozhodnuti-komise-o-tzv-safe-harbor-doporuceni-uradu/d-17119/p1=1099
- Pověřenec pro ochranu osobních údajů. In: *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 2018-07-01]. Dostupné z: https://www.uoou.cz/poverenec-pro-nbsp-ochranu-osobnich-udaju/d-27307/p1=3938
- Sdělení ÚOOÚ k přístupu založenému na riziku. Úřad pro ochranu osobních údajů [online]. 2017 [cit. 2018-02-27]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=26872
- Stanovisko č. 5/2009: ve znění aktualizace z února 2014. *Úřad pro ochranu osobních údajů*

Informace získané z účasti autorky na odborných seminářích

- KALÍŠEK, Jindřich. *Seminář GDPR pro advokáty* uskutečněný dne 13.9.2018 v Praze, pořádající Česká advokátní komora.
- KŘENKOVÁ, Hana. *Praktický seminář GDPR*, uskutečněný dne 18.4.2018 v Praze, pořádající Mgr. Hana Křenková, advokátka.
- NAVRÁTIL, Jiří. *Seminář Ochrana osobních údajů*, uskutečněný dne 10.5.2018 v Brně, pořádající Česká advokátní komora.
- ŽŮREK, Jiří. *Seminář Ochrana osobních údajů ve firmách v době účinnosti GDPR- Úřad pro ochranu osobních údajů v době účinnosti GDPR* uskutečněný dne 17.10.2018 v Ústí nad Labem, pořádající Ministerstvo průmyslu a obchodu a Technologické centrum AV ČR