Západočeská univerzita v Plzni

Fakulta právnická

Diplomová práce

Ochrana osobních údajů a obecné nařízení o ochraně osobních údajů

Tereza Tolarová

Plzeň 2018

Západočeská univerzita v Plzni

Fakulta právnická

Katedra ústavního a evropského práva

Studijní program Právo a právní věda

Studijní obor Právo

Diplomová práce

Ochrana osobních údajů a obecné nařízení o ochraně osobních údajů

Tereza Tolarová

Vedoucí práce:

JUDr. Tomáš Pezl

Katedra ústavního a evropského práva

Fakulta právnická Západočeské univerzity v Plzni

Plzeň 2018

Prohlašuji, že jsem práci zpracovala samostatně a použila jen uvedených pramenů a literatury.

Plzeň, březen 2018 ……

Ráda bych poděkovala JUDr. Tomášovi Pezlovi za odborné vedení práce, cenné rady a připomínky a také Mgr. Ing. Jaroslavovi Zahradníčkovi za jeho podporu při psaní této práce a především jeho rady a připomínky ohledně praktických zkušeností z oboru.

Zkratky

ESLP	Evropský soud pro lidská práva
EU	Evropská unie
GDPR	General Data Protection Regulation
Listina	Listina základních práv a svobod
Nařízení	Obecné nařízení Evropského parlamentu a Rady Evropské unie 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)
NSS	Nejvyšší správní soud
ObčZ	Zákon č. 89/2012 Sb. občanský zákoník
OECD	Organizace pro hospodářskou spolupráci a rozvoj
Pověřenec	Pověřenec pro ochranu osobních údajů
SEU	Smlouva o Evropské Unii
SFEU	Smlouva o fungování Evropské unie
Směrnice	Směrnice Evropského parlamentu a Rady Evropské unie 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů
Úmluva	Evropská úmluva o ochraně lidských práv a základních svobod
Úmluva 108	Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních údajů
Úřad	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud
WP29	Pracovní skupina pro ochranu údajů zřízená podle článku 29
ZOOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 183/2017 Sb.

Obsah

Úvod

Často se říká, že kdo má informace, má moc. Mít o někom určité informace, nám dává moc nad dotyčným a možnost ovládat ho. Především osobní údaje mají zvláštní význam. Technologický rozvoj a globalizace umožnily významný nárůst hodnoty osobních údajů. Osobní údaje jsou nyní cennou komoditou, která je vyhledávanou a žádoucí jak ze strany soukromých společností, tak orgánů veřejné moci. Osobní údaje tvoří ekonomickou hodnotu pro digitální trh. Zvláštní význam má v současné době profilování[1] a analýza velkých objemů dat (big data)[2], která hrají klíčovou roli v růstu digitální ekonomiky. Technologický rozvoj umožnil osobní údaje jednodušeji vytvářet, shromažďovat, šířit a ukládat. To s sebou přináší také nové výzvy pro ochranu osobních údajů. Fyzické osoby by měli mít možnost své osobní údaje chránit a mít pod kontrolou.

Na základě prohlubující evropské hospodářské, politické a sociální integrace došlo k hojnému nárůstu přeshraničních toků osobních údajů. Výměna osobních údajů se v rámci celé Evropské unie (dále jen „EU“) zvýšila. Rozdíly v úrovni ochrany práv na ochranu osobních údajů v souvislosti se zpracováním osobních údajů v členských státech mohou vytvářet překážky v rámci volného pohybu osobních údajů na území EU. V EU tak bylo třeba zajistit jednotné uplatňování pravidel ochrany fyzických osob.

Právě s tímto cílem, sjednotit úroveň ochrany osobních údajů fyzických osob, bylo v rámci EU přijato obecné nařízení Evropského parlamentu a Rady Evropské unie 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

[1] Profilováním je jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu (čl. 4 bod 4 Nařízení).

[2] Pojem big data souvisí s vývojem internetu a obrovským nárůstem generovaných dat, přičemž se nejedná pouze o informace osobní povahy, neboli osobní údaje, ale o data obecně, které jsou často úplně nestrukturovaná a nepřehledná, mluvíme tak o pojmu mnohem širším než osobní údaje. V tomto obrovském množství dat je však obsažena řada cenných informací, které můžou pro podnikatele představovat nové obchodní příležitosti nebo můžou sloužit např. k predikci některých společenských jevů či k statistickým účelům. Více viz RADIČOVÁ, Z., BURIAN, D. Profilování ve světle nového obecného nařízení o ochraně osobních údajů (GDPR). *epravo.cz* [online] 2.2.2017 [cit. 16. 3. 2018]. Dostupné z: https://www.epravo.cz/top/clanky/profilovani-ve-svetle-noveho-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-104926.html

(obecné nařízení o ochraně osobních údajů), (nebo také tzv. GDPR z anglického názvu General Data Protection Regulation, dále jen „Nařízení“), které vstoupí v účinnost dne 25. května 2018. V souvislosti s tímto Nařízením se zvedla vlna obav a nevole. Nařízení se často označuje za největší revoluci v oblasti ochrany osobních údajů. Je tomu tak ovšem doopravdy?

Cílem této práce je posoudit a porovnat se stávající úpravou, co nového Nařízení přináší. Jaké zavádí nové instituty, povinnosti a sankce za nedodržování těchto povinností v porovnání se současnou úpravou.[3] Otázkou, na kterou se práce snaží najít odpověď je, zda lze opravdu hovořit v souvislosti s Nařízením o revoluci v oblasti ochrany osobních údajů?

Za účelem naplnění cíle práce používá zejména metodu komparace a analýzy a dělí se na čtyři kapitoly. První kapitola pojednává o právu na soukromí a ochraně osobních údajů. Historickému vývoji konceptu soukromí je věnována pozornost jen krátce, jelikož historický úvod není pro práci stěžejní. Cílem této části je především rozlišit od sebe pojem práva na soukromí a ochranu osobních údajů. Kapitola se pak nadále věnuje popisu právní úpravy ochrany soukromí a osobních údajů na mezinárodní, evropské a národní úrovni. Druhá kapitola se věnuje základní pojmům a definicím dle Nařízení a jejich komparaci se stávající úpravou. Autorka se v této kapitole nevěnuje beze zbytku všem pojmům, ale pouze těm, které považuje za nejdůležitější, a to je osobní údaj, zpracování, správce, zpracovatel a příjemce a souhlas se zpracováním osobních údajů. Kapitola má poukázat na případné odlišnosti v definicích Nařízení v porovnání se stávající úpravou. Třetí kapitola se zaměřuje na klíčová ustanovení a instituty Nařízení. Kapitola se věnuje závaznosti a působnosti Nařízení. Dále zásadám Nařízení, právním důvodům zpracování osobních údajů, právům subjektu údajů. A novým institutům podle Nařízení, jako je pověřenec pro ochranu osobních údajů, posouzení vlivu na ochranu osobních údajů, ohlašovací a oznamovací povinnosti či záznamům o činnostech. V rámci této kapitoly dochází ke komparaci se stávající úpravou a zhodnocení nových institutů. Čtvrtá kapitola se věnuje krátce obrazu Nařízení v české společnosti a především sankcím, které jsou s nedodržováním Nařízení spojeny.

[3] Jedná se především o zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 183/2017 Sb. a směrnici Evropského parlamentu a Rady Evropské unie 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů.

Téma bylo zvoleno z důvodu jeho aktuálnosti. Co se literatury týče, práce vychází především ze stanovisek, pokynů a vodítek WP29, což je pracovní skupina pro ochranu údajů zřízená podle článku 29 Směrnice Evropského parlamentu a Rady Evropské unie 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů (dále jen „Směrnice“). Tato skupina vydává a veřejně diskutuje materiály, které mají co nejpodrobněji vysvětlit různé oblasti Nařízení, či v minulosti Směrnice. I když výkladová stanoviska WP29 nejsou právně závazná, mají podstatný význam, jelikož se jedná o právní názor kontrolního orgánu. Práce dále čerpá z velké části přímo z Nařízení a ze zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů a také z komentářů k těmto právním předpisům. I když v současnosti vychází mnoho článků na téma ochrany osobních údajů, autorka se raději přiklání k výše zmíněným zdrojům, jelikož se domnívá, že jsou pro práci relevantnější. A též z toho důvodu, že i tyto odborné články vychází z velké části právě z těchto stanovisek WP29. Ačkoliv je v osnově uveden odborný článek od Jacoba M. Victora, The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy, v práci nakonec jako zdroj použit nebyl vzhledem ke staršímu datu jeho vzniku a jinému zaměření článku.

1. Právo na soukromí a ochrana osobních údajů

1.1. Pojem soukromí

Pojem soukromí není v českém právu přímo definován a neexistuje žádná zákonná či všeobecně přijímaná teoretická definice tohoto výrazu. Pojetí soukromí je proměnlivé v čase i prostředí. Různé kultury mají různé představy o významu soukromí a o tom, co má být soukromím chráněno.

Koncept soukromí je nejčastěji spojován s anglo-americkou kulturou a ve své původní podobě vycházelo právo na soukromí z práva „right to be alone", tedy „právo být nechán o samotě" (proti státu). Poprvé bylo právo na soukromí v tomto pojetí zmíněno v 80. letech 19. století autorem Thomasem Cooley.[4] Koncept soukromí byl pak o pár let později komplexněji formulován v článku „The Right of Privacy" z roku 1890, jehož autory byl Samuel D. Warren a Louis D. Brandeis. Podle nich se nejednalo o nový koncept, ale o právo již existující, které vzniklo přirozeným vývojem zásady ochrany osoby v common law. Ochranu jedince před fyzickou újmou rozšířili i na lidskou povahu, pocity a intelekt. Dle autorů je rozšíření ochrany soukromí pouze dalším přirozeným krokem ve vývoji práva.[5] Postupem času se tento teoretický koncept práva na soukromí začal rozšiřovat do právních řádů států Evropy i celého světa.

Pojmem soukromí a právem na ochranu osobního soukromí se zabýval Ústavní soud ve svém nálezu sp. zn. II. ÚS 517/99, ve kterém rozlišuje pozitivní složku, tj. „právo fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným" a negativní složku práva na soukromí, tj. bránit se (vzepřít) „proti neoprávněným zásahům do této sféry ze strany jiných osob s rovným právním postavením".[6] Ve svém dalším nálezu Ústavní soud konstatuje, že „vedle tradičního vymezení soukromí v jeho prostorové dimenzi (ochrana obydlí v širším slova smyslu) a v souvislosti s autonomní existencí a veřejnou mocí nerušenou tvorbou sociálních vztahů (v manželství, v rodině, ve

[4] GLENN, R. *The Right to Privacy: rights and liberties under the law*. Santa Barbara: ABC-CLIO, 2003, s. 4.
[5] GLANCY, D. The Intention of the Right to Privacy, Arizona Law Review [online]. 1979, 21(1), s. 2 [cit. 12.3.2018]. Dostupné z: http://law.scu.edu/wp-content/uploads/Privacy.pdf
[6] Nález Ústavního soudu České republiky sp. zn. II. ÚS 517/99 ze dne 1. března 2000.

společnosti), právo na respekt k soukromému životu zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém.“[7]

Soukromí lze dále popsat jako „osobní, intimní sféru člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského tvora. Pojem soukromí obsahuje rovněž hmotný i myšlenkový prostor jednotlivce, součástí soukromého života je i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi“.[8]

Lze tedy shrnout, že právo na soukromí garantuje také právo jednotlivce rozhodovat dle svého uvážení o tom, zda, v jakém rozsahu, za jakých okolností a jakým způsobem mají být informace a údaje z jeho osobního soukromí zpřístupněny jiným subjektům. Koncept soukromí se překrývá s konceptem ochrany osobních údajů, nicméně tyto dva koncepty spolu nesplývají. Pojem soukromí je ochraně osobních údajů pojmem nadřazeným. Mimo to je soukromí uznáváno jako univerzální lidské právo, přičemž ochrana osobních údajů ne, alespoň prozatím.

1.2. Právní úprava ochrany soukromí a osobních údajů na mezinárodní, evropské a národní úrovni

Do druhé světové války bylo právo na soukromí chápáno úžeji, než je tomu dnes. Až zásahy do lidského soukromí uskutečňované totalitními režimy vedly k rozvoji pojetí práva na ochranu soukromí. Již v roce 1948 bylo právo na ochranu soukromí zahrnuto do Všeobecné deklarace lidských práv (čl. 12). V roce 1950 se k podpisům otevřela Evropská úmluva o ochraně lidských práv a základních svobod (dále jen „Úmluva“), která obsahuje právo na respektování soukromého a rodinného života (čl. 8). Právo na soukromý život bylo znovu deklarováno v čl. 17 Mezinárodního paktu o občanských a politických právech, který byl otevřen k podpisům v roce 1966.

Speciální právní předpisy upravující ochranu soukromí a osobních údajů se začínají přijímat s rozvojem nových technologií na začátku 70. let 20. století. S novými technologiemi vzrůstalo nebezpečí zásahů do lidského soukromí a úměrně tomu vzrůstala též obava z narušení soukromí. Vznikla tak potřeba toto prostředí regulovat. Prvním takovým pokusem byla nezávazná směrnice OECD

[7] Nález Ústavního soudu České republiky sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.
[8] Stanovisko Úřadu pro ochranu osobních údajů č. 6/2009, Ochrana soukromí při zpracování osobních údajů [online] Dostupné z: https://www.uoou.cz/files/stanovisko_2009_6.pdf

z roku 1980, ta měla sloužit především jako návod pro vytvoření legislativy na ochranu osobních údajů pro ty země, které ještě takovou právní úpravu neměly.[9]

Na mezinárodní úrovni je v tomto ohledu nejvýznamnější Úmluva, jež se stala jedním ze základních pilířů ochrany soukromí v Evropě a dodnes formuje to, jak právo na soukromí chápeme. Na princip ochrany soukromí obsažený v čl. 8 Úmluvy navazuje další Úmluva Rady Evropy, a to Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních údajů (dále jen „Úmluva 108"). Ovšem je nutné si uvědomit, že v jaké době Úmluva vznikala, tedy v době, kdy neexistovaly chytré mobilní telefony, internet, ani žádné jiné dnes běžně dostupné technologie. Úmluva 108 byla otevřena k podpisům v roce 1981 a pro státy, které jí ratifikovaly, je závazná. Česká republika Úmluvu 108 podepsala 8. září 2000.[10] Účelem Úmluvy 108 je zaručit každé fyzické osobě úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují.[11] K Úmluvě 108 byl přijat dále Dodatkový protokol, který pro Českou republiku nabyl účinnosti dne 1. července 2004. Mimo to Rada Evropy vydává řadu doporučení zaměřených na ochranu dat ve zvláště citlivých nebo problémových oblastech, jako jsou např. přímý marketing, nové informační technologie, finance, veřejná správa, statistika, policejní činnost, personalistika, sociální zabezpečení, zdravotnictví a genetika.[12]

Právní úprava ochrany osobních údajů v EU je obsažena již v primárním právu EU, a to v čl. 16 Smlouvy o fungování EU (dále jen „SFEU"), který garantuje právo na ochranu osobních údajů každému, kterého se týkají (čl. 16 odst. 1 SFEU). V druhém odstavci čl. 16 SFEU přiznává Evropskému parlamentu a Radě pravomoc přijímat řádným legislativním postupem pravidla o ochraně fyzických osob při zpracovávání osobních údajů.[13] Ochrana soukromí a výslovně ochrana osobních údajů je dále zakotvena v čl. 7 a čl. 8 Listiny základních práv

---

[9] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 57.

[10] Úřad pro ochranu osobních údajů. Rada Evropy [online] [cit. 12. 2. 2018]. Dostupné z: https://www.uoou.cz/rada-evropy/ds-1797/archiv=0&p1=1659

[11] Čl. 1 Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. ledna 1981, vyhlášená pod č. 115/2001 Sb. m. s.

[12] Úřad pro ochranu osobních údajů. Rada Evropy jako jeden z hlavních garantů evropské ochrany osobních údajů [online] [cit. 12. 2. 2018]. Dostupné z: https://www.uoou.cz/rada-evropy/ds-1797/archiv=0&p1=3938

[13] Čl. 16 Smlouvy o fungování Evropské unie.

Evropské unie. Článek 8 stanoví opět právo na ochranu osobních údajů každému, kterého se týkají. Navíc je doplněno, že „tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu“.[14] Dohled nad dodržováním těchto pravidel pak vykonává nezávislý orgán.

Nejvýznamnější pramenem právní úpravy EU v oblasti osobních údajů byla až donedávna Směrnice. Cílem této Směrnice bylo zajistit fungování jednotného trhu a účinnou ochranu základních práv a svobod fyzických osob. Ačkoliv cíle a zásady Směrnice platí i nadále, vzhledem k technickému pokroku a rozdílům v provádění a uplatňování Směrnice bylo nutné zvýšit a sjednotit úroveň ochrany práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů a zajistit jednotné uplatňování pravidel ochrany osobních údajů. To se stalo hlavními důvody pro přijetí Nařízení. Směrnice zůstává v účinnosti do té doby (24. května 2018), než vstoupí v účinnost[15] Nařízení (25. května 2018).

Aby bylo umožněno zajištění jednotné úrovně ochrany fyzických osob v celé EU a zamezilo se rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu, byla pro úpravu ochrany osobních údajů zvolena forma nařízení. Nařízení je na rozdíl od Směrnice přímo použitelné v členských státech EU, a to bez toho aniž by státy přijaly národní implementaci. Kdežto Směrnice členským státům pouze přikazovala dosáhnout cíle libovolnými prostředky.

V České republice je právo na soukromí a respekt k soukromému životu zakotveno v Listině základních práv a svobod (dále jen „Listina“). Ochrana soukromé sféry jednotlivce není obsažena pouze v jednom článku, jak je tomu například v Úmluvě (čl. 8), ale je rozložena do několika článků (čl. 7 odst. 1, čl. 10, 12 a 13 Listiny). Soukromí je chráněno také prostřednictví dalších předpisů, např. občanský zákoník v rámci institutu ochrany osobnosti, trestní zákoník, zákoník práce, zákon o elektronických komunikacích, zákon o některých službách informační společnosti, zákon o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon).

[14] Článek 8 Listiny základních práv Evropské unie.
[15] O účinnosti Nařízení se hovoří v kontextu českého práva. V rámci práva evropského se používá spíše pojem použitelnost Nařízení.

Obecným právním předpisem ochrany osobních údajů je zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „ZOOÚ“). Tímto zákonem byla implementována do českého právního řádu již zmiňovaná Směrnice. Základem ZOOÚ je vymezení práv fyzických osob, jejichž osobní údaje jsou zpracovávány, a povinností osob, které se na zpracovávání osobních údajů podílejí. Důraz je kladen také na předávání osobních údajů do jiných států.[16]

ZOOÚ měl být v souvislosti s účinností Nařízení zrušen a od 25. května 2018 mělo být použitelné pouze Nařízení. Nařízení je nutné přizpůsobit český právní řád. V souvislosti s Nařízením měl tak být přijat adaptační zákon, a to do 25. května 2018. Tento zákon by měl dotvářet některé dílčí aspekty rámce ochrany osobních údajů na zákonné úrovni, ale bude již jen doplňkovým zákonem k Nařízení.[17] Návrh adaptačního zákona, tedy zákona o zpracování osobních údajů, má zajistit soulad s Nařízením a zčásti by měl také implementovat směrnici Evropského parlamentu a Rady Evropské unie 2016/680 ze dne 27. dubna 2016 o ochraně osobních údajů 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. Návrh zákona byl již 18. srpna 2017 zveřejněn Ministerstvem vnitra. V době vzniku této práce ještě adaptační zákon přijat nebyl. Předpokládalo se, že by měl zákon nabýt účinnosti shodně s Nařízením, a to dne 25. května 2018.[18] Podle názoru autorky však přijetí tohoto zákona do konce května roku 2018 je velmi nepravděpodobné, vzhledem k tomu, že návrh zákona byl teprve schválen vládou 21. března 2018. I když možnost, že zákon bude přijat včas, stále existuje, pokud poslanecká sněmovna tento zákon schválí v prvním čtení.

2. Předmět ochrany osobních údajů

Předmět Nařízení je stanoven v čl. 1 Nařízení. Předmětem jsou pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů a

[16] KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012, s. 3.
[17] Úřad pro ochranu osobních údajů. Základní příručka [online] [cit. 12. 2. 2018] Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744&archiv=1
[18] WEINHOLD LEGAL. Návrh zákona o zpracování osobních údajů. Legal Update 10/2017 [online] [cit. 8. 3. 2018] Dostupné z: www.beck-online.cz

pravidla týkající se volného pohybu osobních údajů. Nařízení chrání především právo na ochranu osobních údajů fyzických osob, přičemž je klíčové definovat pojmy s tím související, jako je osobní údaj, zpracování osobních údajů apod. Definice nejdůležitějších pojmů je obsažena v čl. 4 Nařízení. Kapitola se nevěnuje všem definicím dle tohoto článku, ale pouze těm, kterým autorka přiznává největší význam, jako je osobní údaj, zpracování, správce, zpracovatel, příjemce a souhlas se zpracováním osobních údajů. Kapitola se zaměří na definování klíčových pojmů dle Nařízení a jejich komparaci se stávající úpravou, případně se Směrnicí, tak kde je to příhodné. Na základě komparace dojde k vyhodnocení, zda klíčové pojmy byly oproti stávající úpravě pozměněny.

2.1. Osobní údaj

Pojem osobní údaj je stěžejní, jelikož se Nařízení vztahuje pouze na zpracování těch informací, které lze označit za osobní údaje.[19] Osobním údajem je podle Nařízení jakákoliv „informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“.[20]

Stejně tak jako ve Směrnici i v Nařízení zůstává definice osobního údaje široká, a to z toho důvodu, aby zahrnula veškeré informace, které mohou souviset s jednotlivcem. Nařízení definici navíc ještě rozšiřuje oproti Směrnici o další dva identifikátory člověka, a to o lokační údaje, síťový identifikátor a mezi prvky lidské identity přidává i prvek genetický.

Lokačním údajem je informace týkající se místa pobytu nebo pohybu dané osoby, typicky GPS. Dalším novým pojmem je síťový identifikátor. Fyzickým osobám mohou být přiřazeny síťové identifikátory využívající například cookies[21] či adresy internetového protokolu a v kombinaci s jedinečnými identifikátory a

[19] Ovšem EU se věnuje i volnému pohybu neosobních údajů v rámci EU. Více viz https://ec.europa.eu/info/law/better-regulation/initiative/111901/attachment/090166e5b5aad380

[20] Čl. 4 odst. 1 Nařízení.

[21] Cookies jsou krátké textové soubory, které server umisťuje do uživatelova počítače při načtení webové stránky. Technicky jde o sérii kódů, podle kterých prohlížeč shromažďuje a následně odesílá informace o našem chování zpět na příslušný server. Cookies obsahují informaci o tom, jak dlouho je má prohlížeč uchovávat (od jednorázových až po několikaleté).

dalšími informacemi jsou vytvářeny stopy, které mohou být použity k profilování fyzických osob a k jejich identifikaci.[22] Nařízení dále přidává i genetickou identitu člověka, jelikož z genetického genomu lze získat informace, na jejichž základě může být osoba jednoznačně identifikována. Genetické údaje jsou definovány jako osobní údaje týkající se zděděných nebo získaných genetických znaků určité fyzické osoby, které poskytují jedinečné informace o její fyziologii nebo zdraví.[23]

Nicméně lze konstatovat, že pojem osobní údaj nebyl oproti Směrnici výrazněji pozměněn. Již před účinností Nařízení judikatura Soudního dvora Evropské unie (dále jen „SDEU“) reagovala na vývoj moderních komunikačních technologií ve smyslu toho, co lze zahrnout pod pojem osobní údaj. Rozhodnutí SDEU ve věci C-582/14 Patrick Breyer proti Spolkové republice Německo již pouze potvrdilo dlouhodobé nahlížení na problematiku dynamických IP adres, které lze také považovat za osobní údaj.[24]

Pokud porovnáváme definici osobního údaje dle Nařízení a definici dle ZOOÚ, dochází též k rozšíření definice o výše zmíněné prvky, tedy lokační údaje, síťový identifikátor a genetický prvek. Zbylá část definice je významově totožná, odlišuje se jen volbou slov, například společenská a sociální identita, jakákoliv informace a veškeré informace, určený a určitelný proti identifikovaný a identifikovatelný subjekt údajů. Dle názoru autorky se jedná o synonyma a lze tedy konstatovat, že definice podle ZOOÚ, až na již výše zmíněné rozšíření, nebyla podstatně pozměněna.

I nadále tedy platí, že každý osobní údaj musí splňovat následující čtyři hlavní složky, které jsou obsaženy v definici uvedené v Nařízení. Tyto složky jsou spolu úzce provázány. Jedná se o „veškeré informace“, „o“ (vztah mezi informacemi a osobou), „identifikovaná nebo identifikovatelná“, „fyzická osoba“.

Veškerou informací se rozumí jakákoliv informace. Takovou informací je informace objektivní i subjektivní, tedy názor či hodnocení. Mezi subjektivní informace se řadí i velký podíl osobních údajů zpracovávaných v bankovnictví, pojišťovnictví nebo v souvislosti se zaměstnáním. Informace může být osobním údajem dokonce i bez ohledu na to, zda je pravdivá. Nesprávné a nepravdivé informace má subjekt údajů možnost napadnout pomocí vhodných prostředků pro

[22] Bod 30 odůvodnění Nařízení.
[23] Bod 34 odůvodnění Nařízení a čl. 4 odst. 13 Nařízení.
[24] Rozsudek Soudního dvora EU ve věci C-582/14, Patrick Breyer proti Spolkové republice Německo, ze dne 19. října 2016, Dostupné z: http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=CS

zajištění nápravy.[25] Rozhodující je, zda má údaj vztah ke konkrétní identifikované nebo identifikovatelné osobě, nikoli obsah údaje, jeho povaha či formát.

Ačkoliv se pojem osobní údaj vztahuje na údaje poskytující libovolný typ informací, je nutné se zamyslet nad důležitostí vypovídající hodnoty dané informace. Otázkou je, zda se bude jednat o osobní údaj i pokud takovýto údaj nemá žádnou vypovídající hodnotu, a to jak z pohledu subjektu údajů, tak z pohledu správce či zpracovatele. Například pokud správce přidělí v rámci svého systému subjektu údajů nějaké identifikační číslo. To splňuje kritéria definice osobního údaje. O jeho vypovídající hodnotě lze ovšem polemizovat. V souvislosti s právem subjektu údajů na přístup k osobním údajům má subjekt údajů právo získat od správce osobní údaje, které se ho týkají a jsou správcem zpracovávány.[26] Je tedy důvodné, aby subjekt údajů v rámci tohoto práva získával kopii zpracovávaných osobních údajů včetně těch, které pro něj nemají žádný význam či smysl? S ohledem na to, že právo na ochranu osobních údajů není právem absolutním,[27] se autorka přiklání spíše k názoru, že pro posouzení toho, zda je nějaký údaj údajem osobním, by informace měla mít i nějakou vypovídající hodnotu.

Vztah mezi informacemi a osobou tvoří druhou složku definice. Obecně lze konstatovat, že informace se týká jednotlivce, pokud je právě o tomto jednotlivci. To, kdy se informace týká osoby, bylo řešeno již v rámci Pracovní skupiny pro ochranu dat, která uvedla v Pracovním dokumentu o otázkách ochrany údajů, které souvisejí s technologií RFID[28], že „[ú]daje se týkají osoby, jestliže odkazují na totožnost, vlastnosti nebo chování osoby nebo jestliže jsou tyto informace použity k určení nebo ovlivnění způsobu, jak se s uvedenou osobou zachází nebo jak se hodnotí“.[29] Jedná se tak např. o identifikační údaje, údaje o zdravotním stavu a za osobní údaj je také nutné považovat informaci, která je shromažďována za účelem, který má dopad do práv dané osoby, tedy

[25] Stanovisko WP29 č. 4/2007 ze dne 20. 6. 2007 k pojmu osobní údaj, WP136 [online]. Dostupné z: https://www.uoou.cz/files/wp29-stanovisko_4-2007.pdf
[26] Článek 15 Nařízení.
[27] Bod 4 odůvodnění Nařízení.
[28] Moderní technologie identifikace objektů pomocí radiofrekvenčních vln.
[29] Dokument WP 105, ze dne 19. ledna 2005, Pracovní dokument o otázkách ochrany osobních údajů, které souvisejí s technologií RFID. 10107/05/CS Dostupné z: http://docplayer.cz/amp/3319012-Pracovni-dokument-o-otazkach-ochrany-udaju-ktere-souviseji-s-technologii-rfid.html

informaci, která je využita např. k jeho popisu, hodnocení nebo ke zpracování nabídky smlouvy.[30]

Aby se jednalo o osobní údaj, musí se informace týkat identifikované nebo identifikovatelné fyzické osoby, což je třetí složka definice. Za identifikovanou osobu se považuje osoba, která je odlišena od jiných osob. Identifikovatelnou je osoba, kterou je možné identifikovat, i když zatím identifikována nebyla. Tato druhá alternativa, tedy možnost osobu identifikovat, představuje prahovou podmínku určující, zda je informace z hlediska definice osobním údajem. Někdy je zjednodušeně a chybně vykládáno, že osobními údaji jsou identifikační údaje, na jejichž základě můžeme danou osobu odlišit od ostatních osob. Osobními údaji jsou však všechny skutečnosti a informace, které lze přiřadit ke konkrétnímu člověku.[31] Identifikace se provádí na základě identifikátorů, které jsou zmíněné v definici v čl. 4 Nařízení. Identifikace fyzické osoby může být přímá (jméno) nebo nepřímá (podle telefonního čísla, registračního čísla automobilu, čísla sociálního pojištění, čísla občanského průkazu a pasu nebo výběr vyčleněním, kdy prostřednictvím kombinace kritérií jako je věk, povolání, bydliště, je umožněno rozeznat osobu zúžením skupiny, do které náleží). Z uvedeného vyplývá, že zda jsou určité identifikátory dostačující, záleží na konkrétní situaci.

Čtvrtou složkou definice je fyzická osoba. Nařízení se vztahuje pouze na fyzické osoby. Osobními údaji jsou jen údaje týkající se identifikovaných nebo identifikovatelných žijících jednotlivců. Nařízení se nevztahuje na osobní údaje zesnulých osob.[32] Dále se Nařízení nevtahuje na zpracování osobních údajů právnických osob, a především podniků vytvořených jako právnické osoby. Rovněž do Nařízení nespadá ochrana dobrého jména právnické osoby.[33] To, zda jsou pod ochranu Nařízení zahrnuty i nenarozené děti záleží na postoji vnitrostátního právního systému k ochraně nenarozených dětí. V případě právní úpravy České republiky platí, že nenarozené dítě je subjektem údajů za podmínky, že se skutečně narodí.[34]

---

[30] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 78.
[31] KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012, s. 52.
[32] Bod 27 odůvodnění Nařízení.
[33] Bod 14 odůvodnění Nařízení.
[34] § 25 zákona č. 89/2012, občanský zákoník.

Zásady ochrany osobních údajů se nevztahují na anonymní údaje, které jsou opakem osobních údajů. Odůvodnění Nařízení uvádí, že v případě anonymních údajů se jedná o takové informace, které se netýkají identifikované či identifikovatelné fyzické osoby.[35] Dle stanoviska WP29 k pojmu osobní údaj lze anonymní údaj definovat jako „jakékoli informace týkající se fyzické osoby, z nichž tato osoba nemůže být identifikována ani správcem ani jakoukoli jinou osobou s přihlédnutím ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci daného jednotlivce“.[36] Anonymními údaji jsou také údaje anonymizované. Takové údaje dříve odkazovaly na identifikovatelnou osobu, ale po určité úpravě, anonymizaci, již identifikaci nelze provést. Anonymizace osobních údajů musí být provedena tak, aby žádný subjekt, který by měl k údajům legální přístup, nemohl tyto údaje žádným rozumně očekávatelným způsobem spojit s konkrétními osobami. Konkrétněji se technikám anonymizace věnuje stanovisko WP29 k anonymizaci.[37]

Od anonymizace je třeba odlišit pseudonymizaci. Nařízení pod tímto pojmem rozumí zpracování osobních údajů tak, že údaje není možné přiřadit k jejich subjektům bez použití dodatečných informací. Zpravidla jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření.[38] Pseudonymizace proto pouze napomáhá v zabezpečování údajů.

V rámci osobních údajů lze rozlišit i zvláštní kategorie osobních údajů[39] neboli dle české terminologie „citlivé údaje“.[40] I když Nařízení nezná pojem citlivý údaj, v českém prostředí se jedná o ustálený pojem, který bude dále v práci používán. Citlivé údaje jsou podle Nařízení takové údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a dále se jedná o genetické údaje, biometrické údaje, pokud jsou zpracovány za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby (§ 4 ZOOÚ). Nařízení, Směrnice a ZOOÚ citlivým

[35] Bod 26 odůvodnění Nařízení.
[36] Stanovisko WP29 č. 4/2007 ze dne 20. 6. 2007 k pojmu osobní údaj, WP136 [online]. Dostupné z: https://www.uoou.cz/files/wp29-stanovisko_4-2007.pdf
[37] Stanovisko WP 29 č. 5/2014 ze dne 10. 4. 2014 k technikám anonymizace, WP 216 [online]. Dostupné z: http://www.pdpjournals.com/docs/88197.pdf
[38] Článek 4 odst. 5 Nařízení.
[39] Článek 9 odst. 1 Nařízení.
[40] § 4 písm. b) ZOOÚ.

údajům přiznává zvláštní režim ochrany. Je jim poskytnuta zvýšená ochrana při jejich zpracování. Důvodem pro zvýšenou ochranu je charakter citlivých údajů. Zpracování citlivých údajů může již z jejich samotné povahy ohrozit základní právo subjektů údajů na soukromí. Takové údaje mohou subjekt údajů samy o sobě poškodit ve společnosti, zaměstnání, ve škole a mohou zapříčinit jeho diskriminaci. Je proto kladen důraz na jejich zvýšené zabezpečení.[41]

2.2. Zpracování osobních údajů

Dalším klíčovým pojmem je zpracování osobních údajů. Pokud porovnáme definici zpracování podle Nařízení se stávající právní úpravou, lze konstatovat, že na první pohled se definice změnila. Tyto změny však podle autorky nejsou podstatné, jelikož se jedná opět jen o volbu slov, která jsou prakticky synonymní. Jako příklad lze uvést ukládání na nosiče informací a zaznamenání, uspořádání a třídění, likvidace a výmaz či zničení.

Autorka se na základě toho domnívá, že oproti stávající právní úpravě Nařízení v praxi pro chápání toho, co je zpracování, nic nezměnilo. Zpracováváním je nadále jakákoliv operace či soustava operací, které správce provádí s osobními údaji za určitým účelem či cílem, a to bez ohledu na způsob a prostředky zpracování. Operací s osobními údaji je cokoliv, při čem správce s osobními údaji pracuje, nakládá a ovlivňuje je. Může se jednat o 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.[42] Za zpracování se také považuje například pouhé uvedení osobních údajů na internetové stránce, viz rozsudek Lindqvist.[43] Důležitá je také skutečnost, že z hlediska definice zpracování není rozhodné, jestli se jedná o jedinou operaci s osobními údaji či je třeba, aby správce provedl více operací s osobními údaji. Dále není rozhodné ani to, zda správce nebo zpracovatel osobní údaje zpracovává manuálně, elektronicky či kombinací obojího způsobu nebo využitím softwarového nástroje či řešení.

---

[41] Úřad pro ochranu osobních údajů. Zvláštní kategorie osobních údajů (citlivé údaje) [online] Poslední změna 5. 3. 2018 [cit. 12. 2. 2018] Dostupné z: https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaj-citlive-udaje/d-27274

[42] Článek 4 odst. 2 Nařízení.

[43] Rozsudek Soudního dvora Evropské unie ve věci C-101/01, Bodil Lindqvis, ze dne 6. listopadu 2003, bod 25.

Podmínkou, aby bylo možné úkony s osobními údaji považovat za zpracování, je systematičnost těchto operací. Prvek systematičnosti se přitom v Nařízení v definici zpracování nevyskytuje. Systematičnost je nutné vztáhnout k čl. 2 odst. 1 Nařízení, který stanoví, že „[t]oto 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“. V případě zcela nebo částečně automatizovaného zpracování osobních údajů je prvek systematičnosti již automaticky obsažen a není ho třeba dále posuzovat. Význam prvku systematičnosti je tedy třeba nutné posuzovat pouze u neautomatizovaného (manuálního) zpracovávání. Za systematické zpracovávání lze považovat takové zpracování osobních údajů, kdy jsou osobní údaje obsaženy v evidenci či rejstříku nebo do ní mají být zařazeny. Je zde prvek opakovanosti a jednotícího účelu. Nařízení se tedy vztahuje pouze na takové manuální zpracovávání osobních údajů, které jsou systematicky uspořádány podle určených hledisek.[44] Naopak záznamy, soubory záznamů ani jejich titulní strany, které nejsou uspořádány podle určitých kritérií, by do oblasti působnosti Nařízení spadat neměly.[45]

Prvek systematičnosti se objevuje v definici zpracování, na rozdíl od Nařízení, v ZOOÚ, který definuje zpracování osobních údajů jako jakoukoliv operaci nebo soustavu operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky.[46] Jedná se o specifikum českého zákona. Úřad pro ochranu osobních údajů (dále jen „Úřad“) dokonce zastává názor, že pojem „systematický“ je v definici zpracování v podstatě nadbytečný a jeho význam je okrajový.[47]

2.3. Správce, zpracovatel a příjemce

Správce je vedle subjektu údajů hlavní postavou celé právní oblasti ochrany osobních údajů. V podstatě ve všech případech je to správce, kdo rozhoduje o zpracovávání osobních údajů, za jakým účelem, jakých osob a jakými

[44] Více viz NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 65-66 nebo KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012, s. 69.
[45] Bod 15 odůvodnění Nařízení.
[46] Článek 4 písm. e) ZOOÚ.
[47] Stanovisko Úřadu č. 4/2013, K pojetí zpracování osobních údajů. [online] Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22256

prostředky. Správce provádí zpracování osobních údajů a odpovídá za něj vůči subjektu údajů, tak vůči státu, který nastavil veřejnoprávní úpravu povinností při zpracování osobních údajů.[48]

Správcem podle Nařízení je „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů“.[49] Tato definice je až na pár drobných změn totožná s definicí správce podle Směrnice. Do ZOOÚ byla definice správce přejata ze Směrnice, ač ne doslovně. Rozdílem mezi ZOOÚ a Nařízením je to, že definice správce v ZOOÚ obsahuje navíc definiční kritérium, že správce je každý subjekt, který „provádí zpracování a odpovídá za něj“[50]. Autorka se ovšem domnívá, že tento rozdíl není podstatný vzhledem k tomu, že v článku 5 Nařízení je odpovědnost správce za zpracování osobních údajů stanovena.

Veřejnoprávní odpovědnost správce lze také dovodit z každé normy Nařízení, kde je správci uložena určitá povinnost a nesplnění této povinnosti je sankcionováno. Soukromoprávní odpovědnost správce, tedy právo dotčené osoby na účinnou soudní ochranu vůči správci nebo zpracovateli je upravena v čl. 79 Nařízení. V ZOOÚ je odpovědnost správce za zpracování osobních údajů též vyplývá z dalších ustanovení zákona (například § 44 ZOOÚ), případně dalších předpisů. Uvádění odpovědnosti mezi definiční znaky správce je tak spíše nadbytečné. Vypuštění dalšího definičního znaku, že správce zpracování provádí, nepředstavuje žádnou velkou změnu a je spíš prospěšné. Formulace v ZOOÚ, že správce provádí zpracování je totiž nepřesná. Správce může zpracováním pověřit další subjekt, který pro něj bude údaje zpracovávat, tzv. zpracovatele. Zpracovatel může pro správce vykonávat například shromažďování údajů, utřídění, uchovávání, archivování, likvidování atd. I v takovém případě, kdy zpracování správce neprovádí, přesto správcem zůstává, jelikož určil účel zpracování a jeho prostředky.[51] Právě to, kdo určuje účel zpracování údajů, potažmo pak prostředky jejich zpracování, je rozlišovacím znakem obou pojmů, tj. správce a zpracovatel. K výše uvedenému se vyjadřoval i Nejvyšší správní soud (dále jen „NSS“) ve svém rozhodnutí sp. zn. 9 As 34/2008 k pojmům správce a zpracovatel osobních

[48] KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012, s. 78.
[49] Článek 4 bod 7 Nařízení.
[50] § 4 písm. j) ZOOÚ.
[51] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 89.

údajů. V rozhodnutí určoval, zda je správcem osobních údajů pojišťovna či pojišťovací zprostředkovatel.[52] NSS se v rozhodnutí přiklání k tomu, že hlavním a rozhodným rozlišovacím znakem obou pojmů správce a zpracovatel je především účel zpracování těchto údajů, potažmo pak prostředky jejich zpracování.[53]

Pod pojmem určení účelu je nutné rozumět cíl dané činnosti, kterého má být dosaženo zpracováním daných osobních údajů a tedy smysl a důvod zpracování jako takového. Smyslem zpracování může být například nabízení služeb fyzickým osobám, jejich marketingové oslovování, ochrana práv, ochrana majetku prostřednictvím kamerového sledování, provozování webové stránky, která shromažďuje a dále využívá osobní údaje návštěvníků, atd.[54]

Pokud jde o určení prostředků, jedná se o nástroje (technické otázky) a zvolené postupy (organizační otázky) pro konkrétní zpracování. Prostředky neodkazují pouze na technické způsoby zpracování osobních údajů, ale také na to, jak se bude zpracování provádět, tedy např. jaké údaje mají být zpracovávány, kdo má přístup k těmto údajům, kdy budou údaje likvidovány. Prostředky určuje správce, ale mohou být určeny i zpracovatelem údajů. V této souvislosti platí, že zatímco určení účelu zpracování vede v každém případě k označení subjektu za správce, určení prostředků tento následek zpravidla nevyvolává.[55]

Zpracovatelem je podle Nařízení „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce“.[56] Oproti ZOOÚ, které definuje zpracovatele jako „každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona“ se určení zpracovatele mění jen částečně. Nicméně o změnu s praktickými dopady se opět nejedná. ZOOÚ výčet subjektů, který může být v postavení zpracovatele obsažený ve Směrnici a který je totožný s Nařízením zjednodušil na „každý subjekt“. Ovšem Směrnice a nyní Nařízení volí velmi široké vymezení subjektů, které mohou být zpracovatelem, že mezi „každým“ a tímto výčtem může být v podstatě rovnítko.

Nařízení dále neobsahuje rozlišení dvou variant určení zpracovatele, a to buď na základě zákonného zmocnění, nebo na základě pověření správce. Ani

---

[52] MORÁVEK, J. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům.* Praha: Wolters Kluwer, a.s., 2015, s. 142.
[53] Rozhodnutí NSS ve věci sp. zn. 9 As 34/2008 ze dne 12. února 2009.
[54] KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012, s. 78.
[55] Stanovisko WP 29 č. 1/2010 ze dne 16. února 2010 k pojmům „správce“ a „zpracovatel“.
[56] Článek 4 bod 8 Nařízení.

v tomto případě se ale nejedná o významnou změnu, jelikož v obou uvedených případech zpracování, ať už na základě zákona nebo pověření, vykonává zpracování údajů pro správce zpracovatel. Autorka se tak domnívá, že z tohoto důvodu je definice dle Nařízení zdařilejší. Nicméně lze konstatovat, že i přesto se pojetí zpracovatele z hlediska Nařízení oproti stávající úpravě prakticky nemění.

Definice příjemce podle Nařízení obsahuje pozitivní vymezení: příjemcem je „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli“. A také negativní vymezení, kdy za příjemce se nepovažují „orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu“.[57] ZOOÚ definuje příjemce jako „každý subjekt, kterému jsou osobní údaje zpřístupněny“ a naopak „za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g)[58].“

Příjemcem nadále zůstává subjekt odlišný od správce, kterému mohou být osobní údaje v rámci zpracování dále předány či zpřístupněny. Status příjemce zakládá pouhé obdržení údajů. Důvodem pro institut příjemce, je zejména ochrana subjektu údajů, který by měl mít přehled a kontrolu nad tím, kdo zpracovává jeho osobní údaje a kdo k nim má přístup.[59] I když jsou definice v tomto případě odlišně formulovány, v podstatě se na skutečnosti, kdo je označován za příjemce, s Nařízením nic nemění.

2.4. Souhlas subjektu údajů

Souhlas subjektu údajů se zpracováním osobních údajů je jedním z právních titulů pro zpracování osobních údajů. Nařízení definuje souhlas subjektu údajů jako „jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, který subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“.[60] Zde lze oproti stávající úpravě, která definuje souhlas jako „svobodný a vědomý projev vůle subjektu údajů, jehož

[57] Článek 4 odst. 9 Nařízení.
[58] Například při výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci v případech zajištění veřejného pořádku a vnitřní bezpečnosti, předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů, v případě významného hospodářského či finančního zájmu ČR nebo EU.
[59] KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012, s. 93.
[60] Článek 4 odst. 11 Nařízení.

obsahem je svolení subjektu údajů se zpracováním osobních údajů“,[61] vidět změnu. Dosud musí souhlas subjektu údajů splňovat požadavky ZOOÚ a občanského zákoníku (dále jen „ObčZ“) a být tedy svobodný, vážný, určitý a srozumitelný (požadavky ObčZ) a současně vědomý (požadavek ZOOÚ).[62] To, že souhlas musí být informovaný sice v ZOOÚ není součástí definice souhlasu, nicméně tato povinnost je stanoven a v § 5 odst. 4 ZOOÚ. V tomto ohledu jsou požadavky na souhlas téměř totožné. Co Nařízení ale vnáší do definice souhlasu subjektu údajů se zpracováním osobních údajů nového, je požadavek, aby byl souhlas učiněn prohlášením či zjevným potvrzením.

Nově bude zapotřebí, aby se jednalo o aktivní udělení souhlasu. Nelze již považovat za souhlas například nečinnost subjektu. Za souhlas již nemůže být podle Nařízení považováno ani předvyplněné zaškrtávací pole, které subjekt údajů aktivně nevymaže. Souhlas nelze ani dovozovat z pouhého užívání webových stránek bez aktivního vyjádření souhlasu se zpracováváním osobních údajů prostřednictví identifikátorů cookies. Souhlasu se zpracováním osobních údajů se blíže věnuje kapitola týkající se právních důvodů zpracování osobních údajů dle Nařízení (kap. 3.3).

Na závěr lze tedy shrnout, že co se týče vymezení nejdůležitějších pojmů, Nařízení, nezavádí žádné přelomové změny. Většina pojmů zůstala prakticky nedotčena. Jediné co se s Nařízením v případě vymezení pojmů výrazněji mění, je souhlas se zpracováním osobních údajů.

3. Obecné nařízení o ochraně osobních údajů

Nařízení představuje revizi právního rámce a ochrany osobních dat. Prostředky využívané ke zpracování i zpracování samotné je daleko komplexnější, než před několika desítkami let, a proto i rizikovější pro práva a svobody fyzických osob. Zavedení nových institutů, povinností a úprava klíčových ustanovení má vést k přizpůsobení právního rámce ochrany osobních údajů dnešní době. Tato kapitola se zaměřuje právě na tyto klíčová ustanovení a instituty Nařízení a jejich komparaci se stávající úpravou.

[61] § 4 písm. n) ZOOÚ.
[62] Stanovisko Úřadu pro ochranu osobních údajů č. 2/2008, aktualizované v červenci 2014 [online] Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22284

3.1. Závaznost a působnost Nařízení

Jedním z důvodů proč Evropský parlament inicioval vznik evropské právní úpravy týkající se ochrany dat v polovině 70. let, byl nárůst zpracovávání údajů uvnitř EU. Po čtyřiceti letech technologického vývoje bylo nutné, aby tyto změny přinášející nové výzvy v oblasti ochrany dat byly reflektovány, proto v roce 2012 přišla Evropská komise s návrhem nového nařízení pro ochranu osobních údajů.[63]

Aby bylo docíleno toho, že úroveň ochrany práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů bude rovnocenná ve všech členských státech, bylo přijato Nařízení. Před přijetím Nařízení byla úprava ochrany osobních údajů harmonizována Směrnicí. Ta byla ovšem v členských státech různě prováděna a uplatňována. Nedalo se tak zabránit rozdílům a roztříštěnosti právní úpravy napříč členskými státy. Nařízení si právě klade za cíl tuto roztříštěnost odstranit a zajistit soudržné a jednotné uplatňování pravidel ochrany osobních údajů. Z těchto důvodů zvolil evropský zákonodárce akt ve formě nařízení podle čl. 288 SFEU. Nařízení je totiž přímo použitelné v každém členském státě EU, aniž by státy musely přijímat národní implementaci. Platné a účinné nařízení je závazné pro všechny členské státy EU. Z nařízení vyplývají práva a povinnosti nejen pro členské státy EU, ale také pro jednotlivce.

Forma nařízení obecně nedovoluje členským státům, aby si regulovanou oblast upravovaly národními právními předpisy. V některých případech jsou ale úpravy možné, či dokonce nezbytné. Nařízení o ochraně osobních údajů umožňuje v několika případech, aby se členský stát od úpravy Nařízení odchýlil. Členské státy mají možnost přijmout vnitrostátní předpisy, které budou dále konkretizovat uplatňování pravidel Nařízení, pokud jde o zpracování osobních údajů z důvodu splnění právní povinnosti, provádění určitého úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.[64]

V souvislosti s účinností Nařízení tak bude nutné přizpůsobit český právní řad. Očekává se přijetí adaptačního zákona, jak již bylo zmíněno v kapitole o právní úpravě ochrany osobních údajů. V době vyváření této práce ještě nebyl příslušný zákon přijat, nicméně již existuje návrh zákona o zpracování osobních

[63] LYNSKEY, O. *The Foundations of EU Data Protection Law.* Oxford: Oxford University Press, 2015, s. 4.
[64] Bod 10 odůvodnění Nařízení.

údajů. Tento zákon by měl dotvářet některé dílčí aspekty rámce ochrany osobních údajů na zákonné úrovni, ale bude již jen doplňkovým zákonem k Nařízení.[65]

Již podle existujícího návrhu zákona o zpracování osobních údajů je patrné, že v některých schválených případech se Česká republika hodlá od Nařízení odchýlit. Návrh zákona byl teprve projednán ve vládě a v některých ohledech aktualizován ke dni 21. března 2018. Neproběhlo ještě ani první čtení v poslanecké sněmovně. Z těchto důvodů se autorka nebude věnovat hlubší komparaci návrhu zákona s Nařízením. Autorka uvede pouze pro názornost jeden případ.

Členské státy mají možnost upravit si odlišně od Nařízení věkovou hranici dítěte pro souhlas se zpracováním osobních údajů v souvislosti s nabídkami služeb informační společnosti. Nařízení stanoví, že zpracování osobních údajů dítěte je v tomto případě zákonné, je-li dítě ve věku nejméně 16 let, ale členské státy mohou tuto hranici stanovit odlišně, nejméně však 13 let (čl. 8 odst. 1 Nařízení). V původním návrhu českého adaptačního zákona před jednáním vlády konané 21. března 2018 byla věková hranice dítěte pro souhlas se zpracováním stanovena právě na 13 let. Na tomto jednání byla věková hranice zvýšena na 15 let.[66]

Co se týče působnosti, Nařízení v čl. 2 vymezuje věcnou působnost Nařízení a v čl. 3 místní působnost Nařízení. Věcnou působností je myšlen okruh případů, na které se Nařízení vztahuje. Dle čl. 2 odst. 1 se Nařízení vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. ZOOÚ se vztahuje na osobní údaje, které zpracovávají statní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby a také na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky. ZOOÚ se nevtahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány. Na základě srovnání ZOOÚ a Nařízení lze tedy konstatovat, ač je v ZOOÚ působnost slovně vyjádřena trochu odlišně, Nařízení svou působnost oproti ZOOÚ nijak nerozšiřuje.

---

[65] Úřad pro ochranu osobních údajů. Základní příručka [online] [cit. 12. 2. 2018] Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744&archiv=1

[66] V praxi to znamená, že děti do 15 let by měly potřebovat souhlas rodičů například v případě, že by si chtěly založit účet na sociálních sítích.

V odst. 2 jsou stanoveny výjimky, na které se Nařízení nevztahuje. Mezi tyto výjimky patří zpracování osobních údajů prováděné při výkonu činností, které nespadají do oblasti působnosti práva Unie, např. zpracování osobních údajů v souvislosti se zajišťováním národní bezpečnosti členských států. Dále se Nařízení nevtahuje na zpracování osobních údajů členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 SEU, např. zpracovávání osobních údajů orgány Eurojust a Europol.[67] Nařízení dále nedopadá na fyzické osoby, které provádí zpracování v průběhu výlučně v rámci osobních či domácích činností, které postrádá jakoukoliv souvislost s profesní či obchodní činností, přičemž na tyto případy se nevztahuje ani ZOOÚ. Příkladem může být vedení adresářů nebo využívání sociálních sítí a internetu v souvislosti s těmito činnostmi.[68] Poslední zmíněnou výjimkou je zpracování příslušnými orgány za účelem prevence, vyšetřování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Zpracování těchto osobních údajů je upraveno zvláštním právním aktem EU, totiž směrnicí Evropského parlamentu a Rady (EU) 2016/680.[69] Zpracování osobních údajů orgány, institucemi a jinými subjekty EU je též upraveno samostatně, a to nařízením Evropského parlamentu a Rady (ES) č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.[70]

Co se týče místní působnosti, vztahuje se Nařízení na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v EU bez ohledu na to, zda zpracování probíhá v EU či mimo ní (čl. 3 odst. 1 Nařízení). Dále se Nařízení vztahuje i na ty situace, kdy se správce a zpracovatel nachází mimo území EU, ale zpracovávají osobní údaje subjektu údajů, které se nacházejí v EU (čl. 3 odst. 2 Nařízení). Extrateritoriální působnost Nařízení je dána v případech, pokud správce usazený mimo EU zpracovává údaje související s nabídkou zboží nebo služeb subjektům údajů v EU (čl. 3 odst. 2 písm. a) Nařízení) nebo zpracování souvisí s monitorováním chování subjektu údajů, ke kterému dochází v rámci EU (čl. 3 odst. 2 písm. b) Nařízení). Nařízení dále

[67] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 66.
[68] Bod 18 odůvodnění Nařízení.
[69] Bod 19 odůvodnění Nařízení.
[70] Článek 2 odst. 3 Nařízení.

dopadá také na zpracování osobních údajů správcem, který není usazen v EU, ale na místě, kde se uplatňuje právo členského státu na základě mezinárodního práva veřejného. Nařízení je v tomto ohledu průlomové, jelikož se netýká pouze entit v rámci EU, ale kohokoliv, kdo zpracovává osobní údaje občanů EU. Zde již o změně oproti ZOOÚ hovořit lze. ZOOÚ se vtahuje i na správce, který je usazen mimo území EU, ale který provádí zpracování na území v ČR a takový správce je v tomto případě povinen zmocnit zpracovatele na území ČR prostřednictvím smlouvy o zpracování osobních údajů (§ 3 odst. 5 a § 6 ZOOÚ). Nařízení však rozšiřuje svou působnost i na správce nebo zpracovatele, kteří zpracovávají osobní údaje mimo EU a zpracování souvisí již s výše zmíněnými případy. Oproti ZOOÚ tak dochází k rozšíření místní působnosti Nařízení, které má tak na rozdíl od ZOOÚ silnější extrateritoriální působnost.

3.2. Zásady Nařízení

Zásady zpracování osobních údajů jsou obsaženy v čl. 5 odst. 1 Nařízení. Tyto zásady jsou klíčové, jelikož se jimi řídí celý zbytek Nařízení a všechna ustanovení musí být vykládána v souladu s těmito zásadami. Základní zásady určují, jak může správce zpracovávat osobní údaje, ale jsou de facto zároveň pro správce povinností. Povinnost dodržovat tyto zásady pro správce je stanovena v čl. 5 odst. 2 Nařízení. Správce musí být zároveň schopen dodržování těchto zásad doložit. ZOOÚ sice výslovně neobsahuje ustanovení s výčtem zásad, nicméně stejné principy jsou v § 5 ZOOÚ, který obsahuje hlavní povinnosti správce v souvislosti se zpracováním osobních údajů.

Nařízení je postaveno na těchto zásadách: (1) zákonnost, korektnost, transparentnost, (2) účelové omezení, (3) minimalizace údajů, (4) přesnost, (5) omezení uložení, (6) integrita a důvěrnost a (7) zásada odpovědnosti.[71]

Zásada zákonnosti, korektnosti a transparentnosti stanoví, že správce musí zpracovávat osobní údaje na základě alespoň jednoho právního důvodu (může probíhat i na základě více právních důvodů) a vůči subjektu údajů transparentně.[72] Aby tedy zpracování bylo zákonné, osobní údaje musí být zpracovávány na základě souhlasu subjektu údajů nebo s ohledem na nějaký jiný legitimní základ

[71] Viz článek 5 Nařízení.
[72] Úřad pro ochranu osobních údajů. Zásady a právní důvody zpracování [online] Poslední změna 5. 3. 2018 [cit. 13. 3. 2018]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271

stanovený právními předpisy.[73] Zásada zákonnosti dále stanoví, že zpracování nesmí být v rozporu s Nařízením či v rozporu s právním řádem obecně. Nesmí být protiprávní. Zásada zákonnosti sice není v ZOOÚ výslovně uvedena, nicméně povinnosti správce zpracovávat osobní údaje na základě alespoň jednoho z právních titulů je stanovena v § 5 odst. 2 ZOOÚ.

Zásada transparentnosti vyžaduje, aby informace o zpracovávání osobních údajů byly snadno přístupné a srozumitelné. Tato zásada je důležitá s ohledem na povinnost správce informovat subjekt údajů o zpracování údajů, o totožnosti správce, účelech zpracování a o dalších záležitostech ve vztahu k dotčeným fyzickým osobám.[74]

Zásada účelového omezení stanoví, že osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely.[75] Prvním hlavní krokem pro správce je určit účel zpracování osobních údajů, tedy proč vlastně osobní údaje zpracovává. Tato zásada má dvě složky. Za prvé, správce má povinnost shromažďovat osobní údaje jen za určitým, výslovně vyjádřeným a legitimním účelem, a za druhé, jakmile jsou osobní údaje shromažďovány, musí být tyto údaje zpracovávány pouze za tímto účelem a v souladu s tímto účelem.[76] Této zásadě odpovídá povinnost správce shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu a zpracovávat je pouze v souladu s tímto účelem, viz § 5 odst. 1 písm. d) a písm. e) ZOOÚ.

Zásada minimalizace údajů stanoví, že je možné zpracovávat jen ty osobní údaje, které jsou přiměřené a relevantní a omezené na nezbytný rozsah vzhledem k účelu zpracování. Dle zásady přesnosti musí být osobní údaje přesné a v případě potřeby aktualizované. Této zásadě odpovídá povinnost správce vyplývající z § 5 odst. 1 písm. c) ZOOÚ, že správce je povinen „zpracovávat pouze přesné osobní údaje“.

Za nepřesné údaje se považují například údaje s gramatickými či výpočetními chybami nebo také formálně správné údaje, které však nevypovídají

---

[73] Bod 40 odůvodnění Nařízení.
[74] Bod 39 odůvodnění Nařízení.
[75] Článek 5 odst. 1 písm. b) Nařízení.
[76] WP29, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013. WP 203, s. 4. Dostupné z: http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

o pravdivém stavu v souvislosti s nějakou osobou. Pokud správce či zpracovatel zjistí, že jsou osobní údaje nepřesné, má povinnost je opravit nebo vymazat.[77]

Zásada omezení uložení znamená, že osobní údaje ve formě umožňující identifikaci mají být uloženy jen po dobu nezbytně nutnou pro účely, pro které jsou zpracovávány. V Nařízení je uvedena výjimka z tohoto pravidla pro ty osobní údaje, které jsou zpracovávány výhradně pro účely archivace ve veřejném zájmu, dále pro účel vědeckého a historického výzkumu nebo pro statistické účely.[78] Téměř totožnou povinnost a výjimku z této povinnosti stanoví i ZOOÚ v § 5 odst. 1 písm. e).

Zásada integrity a důvěrnosti klade požadavky na zpracování osobních údajů takovým způsobem, který zajistí náležité zabezpečení osobních údajů. Správce má povinnost zajistit osobní údaje před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, a to pomocí vhodných technických nebo organizačních opatření.[79]

Všechny zmíněné zásady byly Nařízením mírně upraveny a zpřesněny oproti ZOOÚ. Nicméně největší změna významná pro správce a zpracovatele je obsažena v zásadě odpovědnosti, kdy správce musí také nově soulad s výše uvedenými zásadami nejen dodržet, ale také být schopen doložit. K doložení souladu mohou sloužit např. kodexy, které mají sloužit jako vodítko správné praxe při zpracování osobních údajů, dále osvědčení či certifikace, které mají sloužit k prokázání souladu zpracování s Nařízením, případně záznamy o činnostech zpracování, které obsahují informace o prováděném zpracování. Záznamy o činnostech zpracování ulehčí orientaci v činnostech zpracovávání osobních údajů, která správce či zpracovatel provádí.[80]

Lze shrnout, že základní zásady a principy ochrany osobních údajů zůstávají oproti stávající právní úpravě de facto neměnné. Tyto zásady však byly podrobněji rozpracovány a zpřesněny. Nařízení v tomto ohledu přináší i určité nové povinnosti. Jedná se především o povinnost správce doložit soulad zpracování osobních údajů v rámci zásady odpovědnosti správce. Nově tedy musí

---

[77] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 112.
[78] Článek 5 odst. 1 písm. e) Nařízení.
[79] Článek 5 odst. 1 písm. f) Nařízení.
[80] Úřad pro ochranu osobních údajů. Základní příručka. [online] [cit. 13. 3. 2018]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744&archiv=1

správce vést záznamy o činnostech zpracování osobních údajů, za něž odpovídá (čl. 30 Nařízení). Více viz samostatná kapitola (3.8. Záznamy o činnostech).

3.3. Právní důvody zpracování osobních údajů dle Nařízení

Aby bylo zpracování osobních údajů ze strany správce legální, je nutné, aby správce disponoval řádným právním titulem ke zpracování osobních údajů. To je jedním z hlavních projevů zásady zákonnosti. Právní titul je podmínkou pro zpracování osobních údajů, jinak je zpracování nelegální. Osobní údaje mohou být správcem zpracovávány pro různé účely a je nutné, aby správce měl právní titul pro každý účel zpracování osobních údajů. Tyto osobní údaje musí být zlikvidovány tehdy, když správce ztratí poslední právní důvod ke zpracování oněch osobních údajů.[81] Mezi právní důvody zpracování osobních údajů patří tyto:

- souhlas se zpracováním osobních údajů pro jeden či více konkrétních účelů;
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu;
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva svobody subjektu údajů vyžadující ochranu osobních údajů.[82]

V Nařízení je definovaných šest právních titulů pro zpracování osobních údajů. V ZOOÚ jich lze identifikovat osm. Pro přehlednost a další srovnání je přiložena tabulka.

---

[81] Úřad pro ochranu osobních údajů. Zásady a právní důvody zpracování. [online] Poslední změna 5. 3. 2018 [cit. 13. 3. 2018]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271

[82] Článek 6 odst. 1 Nařízení.

	Nařízení	**ZOOÚ**
1.	**souhlas se zpracováním osobních údajů** pro jeden či více konkrétních účelů Čl. 6 odst. 1 písm. a)	správce může zpracovávat osobní údaje pouze se **souhlasem subjektu** údajů § 5 odst. 2
2.	zpracování je nezbytné pro **splnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu Čl. 6 odst. 1 písm. b)	zpracování je nezbytné pro **plnění smlouvy** § 5 odst. 2 písm. b)
3.	zpracování je nezbytné pro **splnění právní povinnosti**, která se na správce vztahuje Čl. 6 odst. 1 písm. c)	zpracování je nezbytné pro **dodržení právní povinnosti** správce § 5 odst. 2 písm. a)
4.	zpracování je nezbytné **pro ochranu životně důležitých zájmů** subjektu údajů nebo jiné fyzické osoby Čl. 6 odst. 1 písm. d)	zpracování je nezbytně třeba **k ochraně životně důležitých zájmů** subjektu údajů, v tomto případě je třeba bez zbytečného odkladu získat jeho souhlas § 5 odst. 2 písm. c)
5.	zpracování je nezbytné pro **splnění úkolu prováděného ve veřejném zájmu** nebo **při výkonu veřejné moci**, kterým je pověřen správce Čl. 6 odst. 1 písm. e)	X
6.	zpracování je nezbytné pro účely **oprávněných zájmů** příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva svobody subjektu údajů vyžadující ochranu osobních údajů Čl. 6 odst. 1 písm. f)	zpracování je nezbytné **pro ochranu práv a právem chráněných zájmů** správce, příjemce, nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života § 5 odst. 2 písm. e)
7.	X	jedná-li se oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem § 5 odst. 2 písm. d)
8.	X	pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení § 5 odst. 2 písm. f)
9.	X	jedná-li se o zpracování výlučně pro účely archivnictví § 5 odst. 2 písm. g)

Tituly, které zůstávají ve více či méně změněné podobě, jsou čtyři, jedná se o souhlas se zpracováním osobních údajů, zpracování nezbytné pro splnění smlouvy, zpracování nezbytné pro splnění právní povinnosti a zpracování nezbytné pro účely oprávněných zájmů. V Nařízení pak chybí právní titul zpracování oprávněně zveřejněných osobních údajů, právní titul poskytování osobních údajů o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy a právní titul zpracování pro účely archivnictví.[83] Pro tyto zpracování bude nutné najít jiný právní titul. Pravděpodobně se bude jednat o oprávněný zájem. Co je naopak v Nařízení novým titulem ve srovnání se ZOOÚ je právní titul zpracování nezbytného pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci. Tento právní titul by měl být přínosem zejména pro orgány veřejné moci.

Tento, dle Nařízení, nový titul slouží pro zpracování osobních údajů orgány veřejné moci nebo subjekty soukromého práva pověřené výkonem určitého úkolu veřejné moci. Na rozdíl od právního titulu plnění právní povinnosti však není potřeba, aby správce zpracováním plnil konkrétní právní povinnost.[84] Rozdíl mezi těmito právními tituly je ve formulaci ustanovení zvláštního předpisu, které dává zmocnění ke zpracování osobních údajů. V případě titulu plnění právní povinnosti nemá správce na výběr, zda tak učiní či ne. Naopak u právního titulu zpracování při plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci si může správce v rámci svého uvážení zvolit, jakým způsobem úkol ve veřejném zájmu splní. Pokud při plnění tohoto úkolu bude zpracovávat osobní údaje, může tak činit na základě právě tohoto titulu.[85]

U právních titulů zpracování, které byly zachovány, proběhly u některých určité změny. Co se týče zpracování nezbytného pro ochranu životně důležitých zájmů,[86] je Nařízení ve srovnání se ZOOÚ mírnější. Nařízení nestanovuje podmínku, že správce musí v tomto případě od subjektu bez zbytečného odkladu

[83] Zde je nutno dodat, že další zpracování pro účely archivace ve veřejném zájmu je dle Nařízení považováno za slučitelné zákonné operace zpracování (bod 50 odůvodnění Nařízení).
[84] Právní povinnost musí vyplývat ze zákona, ale upřesněna může být i v podzákonném předpisu. Musí se jednat o povinnost vyplývající z práva členského státu nebo EU.
[85] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 130.
[86] Typicky se bude jednat například zpracování osobních údajů účastníků nehody. Dále o zpracování nezbytné pro humanitární účely, včetně monitorování epidemií a jejich šíření nebo v naléhavých humanitárních situacích, zejména v případech přírodních a člověkem způsobených katastrof.

získat souhlas a bez souhlasu zpracování ukončit a údaje zlikvidovat. Nicméně dle zásady účelového omezení a omezení uložení po vymizení daného účelu již stejně správce takto získané osobní údaje nesmí nadále zpracovávat a uchovávat.

Právní titul zpracování nezbytný k plnění smlouvy podle ZOOÚ v situaci, ve které dochází ke sjednávání nové smlouvy, k plnění smlouvy již uzavřené nebo ke změně uzavřené smlouvy včetně jejího zániku nedoznal v porovnání s Nařízením větších změn. Nadále je zpracování zákonné, pokud je nezbytné v souvislosti s plněním smlouvy nebo úmyslem smlouvu uzavřít. Lze polemizovat, zda nahrazení slova „plnění" za „splnění" něco prakticky změní. Autorka se domnívá, že nikoli.

U dalšího právního titulu, oprávněného zájmu, také došlo k určitým změnám. ZOOÚ za oprávněný zájem považuje pouze zpracování nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce, nebo jiné dotčené osoby. Zpracování však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. Dle ZOOÚ musí být splněny tedy tyto dvě podmínky: za prvé, zpracování je nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce či jiné dotčené osoby, a za druhé, zpracování nesmí zasahovat nepřiměřeně do soukromí subjektů. Nezbytnost zpracování znamená, že ochrany práv nelze dosáhnout jiným způsobem. Posouzení nezbytnosti je prováděno na základě objektivních skutečností. Nestačí pouhý pocit správce, že je dané zpracování z jeho hlediska nezbytné. Zda lze osobní údaje na základě tohoto titulu zpracovávat bez souhlasu subjektu údajů, závisí na posouzení váhy chráněného práva na straně správce a míry zásahu do soukromí subjektu údajů. Zpracování pro ochranu práv a právem chráněných zájmů znamená, že zájem musí být uznaný právním řádem. Například se jedná o právo na majetek a s ním související právo na ochranu vlastnictví, případně právo na život. Ani v tomto případě se tedy nejedná o subjektivní názor správce.[87] Nově v Nařízení bude již subjektivně stanovený oprávněný zájem správce možný, podle komentáře k Nařízení.[88]

[87] KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012, s. 146.
[88] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 132.

Z toho lze nabít dojmu, že získání tohoto právního titulu by mělo být dle Nařízení snazší než je tomu doposud. To se však autorka nedomnívá. Teoreticky by se o změnu jednat mohlo, prakticky se však spíše nic nezmění.

Pro to, aby správce mohl zpracovávat osobní údaje na základě tohoto titulu, musí provést komplexní posouzení toho, zda je zájem oprávněný a jestli je zpracování opravdu nezbytné. Na závěr musí provést balanční test, tedy komplexní posouzení toho, zda nad oprávněným zájmem nepřevažují zájmy nebo základní práva a svobody subjektu údajů.[89]

Vodítko, jak správně provést balanční test v sedmi krocích, lze najít ve stanovisku WP29. V prvním kroku správce musí určit, na základě jakého právního titulu má dojít ke zpracovávání osobních údajů. Pokud je zřejmé, že nejvhodnější právní titul je oprávněný zájem, lze postoupit k dalšímu kroku. V druhém kroku správce posoudí, zda je zájem legitimní či nelegitimní. Aby byl zájem posouzen jako legitimní, musí splňovat tyto podmínky: být zákonný, tedy v souladu s právem EU a národním právem, dále musí být zájem srozumitelně vyjádřen a musí být dostatečně konkrétní, aby mohl být proveden balanční test. Zájem také nesmí být spekulativní, ale musí vyjadřovat reálný a současný zájem. Ve třetím kroku je třeba rozhodnout, zda je zpracování nezbytné k dosažení sledovaného zájmu. Zde je třeba posoudit, zda neexistují méně invasivní prostředky k dosažení identifikované zájmu. Čtvrtý krok spočívá v posouzení, zda zájmy správce na zpracování údajů nejsou převáženy základními právy či zájmy subjektu údajů. Je třeba také posoudit povahu zájmů správce, zda se jedná o základní práva, jiný typ zájmu či veřejný zájem a vzít v potaz povahu údajů, jestli se jedná např. o citlivé údaje. Posoudit status subjektu údajů (nezletilý, zaměstnanec, atd.) a správce (např. zda se jedná o obchodní společnost s dominantním postavením na trhu). Zhodnotit možné dopady a důsledky pro subjekt údajů a porovnat s očekávanými benefity plynoucími ze zpracování údajů správcem. V tomto kroku je nutné vzít v úvahu mnoho faktorů a právě tento krok je balančním testem v pravém slova smyslu. Za páté, k vyrovnání zájmů správce a subjektu údajů může správce přijmout dodatečné záruky pro ochranu práva svobod subjektu údajů. To lze provést na základě různých technických či organizačních prostředků, dále např. minimalizace dat, anonymizace dat, pseudonymizace, deklarace neomezené

[89] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC adpoted on 9 April 2014, WP 2177. Dostupné z: http://www.dataprotection.ro/servlet/ViewDocument?id=1086

možnosti opt-outu či umožnění portability. V šestém kroku správce sepíšu analýzu těchto pěti kroků, kde je obsaženo ospravedlnění pro zpracování údajů. Tato analýza má být provedena sepsána před samotným zpracováváním. Správce by měl také informovat subjekty údajů o důvodech svědčících v jeho prospěch pro zpracování údajů. Tuto analýzu si ponechává správce k dispozici pro příslušný dozorový úřad. V sedmém kroku se řeší případ, pokud jedinou možnou zárukou je právo opt-outu a subjekt údajů má námitku proti zpracování, měl by být zajištěn vhodný a uživatelsky přátelský mechanismus k přehodnocení rovnováhy zájmů v případě jedince a zpracování jeho údajů ukončit, pokud se ukáže, že jeho zájmy převládají.[90]

Pokud srovnáme systematiku Nařízení a ZOOÚ, je jasně patrné, že v Nařízení jsou právní tituly rovnocenné, kdežto v ZOOÚ v § 5 odst. 2 dominuje jeden právní titul, a to je souhlas subjektu údajů. Ostatní důvody jsou zde pro případ, že správce daný souhlas nezíská. Na základě toho lze konstatovat, že ZOOÚ přiznává tomuto právnímu titulu větší váhu než Nařízení. Nařízení staví souhlas subjektu údajů na stejnou úroveň jako ostatní důvody pro zpracování osobních údajů.

Naopak se situace spíše obrací, jelikož podmínky užívání právního titulu souhlasu se zpracování osobních údajů se zpřísňují. Správce by měl tak raději uvažovat, zda nemůže použít jiný právní titul, než je souhlas. Až tehdy, pokud zpracování na základě jiného titulu není možné realizovat, by měl správce získávat souhlas subjektu údajů.[91]

Souhlas se zpracováním osobních údajů podle Nařízení zaznamenal podstatné změny. Mění se již samostatná definice souhlasu. Zatímco podle ZOOÚ je souhlas subjektu údajů „svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“ (§ 4 písm. n) ZOOÚ), dle Nařízení přibývají další požadavky na souhlas. Souhlas musí být též svobodný, ale navíc se musí ještě jednat o konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování osobních údajů (čl. 4 bod 11 Nařízení).

---

[90] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC adopted on 9 April 2014, WP 2177, s. 55-56. Dostupné z: http://www.dataprotection.ro/servlet/ViewDocument?id=1086

[91] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 124.

Změna v definici znamená, že nyní souhlas dle Nařízení vyžaduje, aby byl souhlas udělen prohlášením či zjevným potvrzením, tedy jedná se o aktivní udělení souhlasu. Souhlas musí být jednoznačný. Jednoznačné potvrzení souhlasu může mít podobu písemného prohlášení, které může být učiněno i elektronicky, nebo ústního prohlášení.[92] Není možné již za souhlas považovat neaktivitu subjektu, př. nevymazání předvyplněného zaškrtávacího pole, které subjekt aktivně nevymaže. Změna proběhne také v případě získávání a zpracování identifikátoru cookies, pokud dochází jejich prostřednictvím ke zpracování osobních údajů, již nelze za souhlas se zpracováním osobních údajů považovat pouhé užívání webové stránky.[93]

I když se může na první pohled zdát, že požadavek, aby byl souhlas se zpracováním osobních údajů svobodný, se nemění, není tomu tak. Nařízení klade mnohem větší důraz na svobodu udělení souhlasu. Subjekty mají mít opravdový výběr a kontrolu nad udělováním souhlasu. Například je-li souhlas součástí smluvních podmínek v pasáži, kterou nelze změnit, má se za to, že souhlas udělen svobodně nebyl. Souhlas též není považován za svobodný, pokud nemá subjekt údajů možnost odmítnout či odvolat souhlas, aniž by mu tím vznikla újma.[94] Pokud by bylo plnění smlouvy podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné, nejedná se o svobodný souhlas (čl. 7 odst. 4 Nařízení). Nařízení se tímto snaží omezit obvyklou praxi tzv. „take it or leave it“, která spočívající v podmiňování uzavření smlouvy se subjektem údajů poskytnutím jeho souhlasu se zpracováním údajů, které pro plnění takové smlouvy není nezbytné.[95]

Souhlas musí být dále konkrétní, což znamená, že souhlas subjektu údajů musí být udělen pro konkrétní účel (jeden či více) a subjekt má ohledně každého z nich na výběr. Požadavek konkrétnosti má zajistit větší míru kontroly ze strany subjektu údajů a transparentnosti. [96] V tomto případě se hovoří o tzv. granularitě získávání souhlasu nebo vrstevnatosti souhlasu. Je to tedy takový mechanismus získávání souhlasu, kdy souhlas se zpracováním musí být štěpen ve vztahu ke

---

[92] Bod 32 odůvodnění Nařízení.
[93] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 93.
[94] Vodítka WP 29 k souhlasu podle Nařízení 2016/679 ze dne 28. listopadu 2017. WP259. s. 6.
[95] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 152.
[96] Vodítka WP 29 k souhlasu podle Nařízení 2016/679 ze dne 28. listopadu 2017. WP259. s. 13.

každé operaci zpracování pro více než jeden účel.[97] Reálně by to vypadalo tak, že pokud probíhá více jednotlivých operací zpracování osobních údajů, subjekt údajů by měl mít možnost výběru, s jakými operacemi bude souhlasit. Například se bude jednat o možnost zaškrtávat různá políčka. Subjekt údajů by neměl být již nucen souhlasit se všemi účely zpracování najednou. Pokud není možné vyjádřit samostatný souhlas s jednotlivými operacemi zpracování osobních údajů, i když je to v daném případě vhodné, lze předpokládat, že souhlas není svobodný.[98] Autorka se domnívá, že v praxi to může vést k tomu, že správce se bude snažit minimalizovat jednotlivé operace zpracování osobních údajů, aby se omezil počet nutných políček k zaškrtávání. Z pohledu autorky je totiž pro subjekt údajů přijatelnější dát souhlas s jednou operací zpracování osobních údajů, než pokud má subjekt udělit takovýchto souhlasů více.

Nařízení dále klade větší důraz na to, aby byl souhlas také informovaný. Subjektům mají být poskytnuty informace ještě před udělením jejich souhlasu, aby mohly provést informované rozhodnutí, chápaly, k čemu dávají souhlas a mohly využít práva na odvolání souhlasu. Pokud by správce srozumitelnou informaci neposkytl, souhlas by mohl být neplatným základem pro zpracování. Aby se jednalo o informovaný souhlas, správce by měl subjektu údajů poskytnout informace jako je totožnost správce, účel každé z operací zpracování, pro které je žádáno o souhlas, jaké údaje budou shromažďovány a používány, existence práva souhlas odvolat, informace o použití dat k rozhodnutím čistě na bázi automatizovaného zpracování a pokud se souhlas týká předávání, správce by měl informovat také o možných rizikách přenosu dat do třetích zemí při absenci rozhodnutí o odpovídající úrovni ochrany dat a náležitých zabezpečovacích opatření (čl. 49 odst. 1 písm. a) Nařízení).[99] Tyto informace mohou být předloženy písemně či ústně. Nařízení nenařizuje, jakou formou mají být informace poskytnuty. Správce by však měl při vyžadování souhlasu užívat jasný a jednoduchý jazyk.[100]

Co se týče souhlasů, které byly získány před účinností Nařízení, ty mohou být využívány správci i nadále, pokud je způsob udělení daného souhlasu

---

[97] HORKÁ, N. Souhlas se zpracováním osobních údajů ve světle nové legislativy. In: *epravo.cz* [online] 9. 2. 2018 [cit. 12. 3. 2018]. Dostupné z: https://www.epravo.cz/top/clanky/souhlas-se-zpracovanim-osobnich-udaju-ve-svetle-nove-legislativy-106991.html

[98] Bod 43 odůvodnění Nařízení.

[99] Vodítka WP 29 k souhlasu podle Nařízení 2016/679 ze dne 28. listopadu 2017. WP259, s. 12.

[100] Vodítka WP 29 k souhlasu podle Nařízení 2016/679 ze dne 28. listopadu 2017. WP259. s. 13.

v souladu s podmínkami Nařízení.[101] Pokud ovšem tyto souhlasy nebyly získány v souladu s Nařízením, nelze na ně již spoléhat a nebudou již nadále představovat platný právní titul pro zpracování osobních údajů. Vzhledem k výše uvedenému, ke zpřísnění podmínek získání souhlasu, se autorka domnívá, že souhlasů, které byly uděleny na základě Směrnice a které umožní pokračovat ve zpracování i po dni použitelnosti Nařízení, je minimum. Správci tedy budou muset ve většině případů získávat souhlasy po účinnosti Nařízení znovu, a to v souladu s novými podmínkami, které stanoví Nařízení.

Co se týče odvolání souhlasu se zpracováním osobních údajů, v současné právní úpravě (ZOOÚ, Směrnice) výslovně možnost odvolat souhlas stanovena není. Ovšem tato možnost se dovozovala z čl. 6 odst. 3 a čl. 9 odst. 1,2 směrnice o soukromí a elektronických komunikacích, jejíž ustanovení o možnosti kdykoliv odvolat souhlas se zpracováním provozních či lokalizačních údajů uživatelem hovoří.[102] Odvolání souhlasu možné podle ZOOÚ je, nicméně tomu tak není vždy a za všech okolností. Explicitně tato možnost ani v ZOOÚ nikde stanovena není.[103] Podle Nařízení má být odvolání souhlasu mnohem snazší. V Nařízení je právo subjektu údajů na možnost odvolat kdykoliv svůj souhlas výslovně uvedeno v článku 7 odst. 3 Nařízení. Odvolání souhlasu by mělo být dokonce tak snadné jako jej poskytnout. Vzhledem k tomu, že subjekt údajů může svůj souhlas kdykoliv odvolat, mění se pozice tohoto právního titulu. Souhlas již pravděpodobně do budoucnosti nebude preferovaným právním titulem pro zpracování, jako tomu bylo doposud.

3.4. Práva subjektu údajů

Nařízení, ale i ZOOÚ přiznávají subjektům údajů práva, jejichž účelem je vztah mezi správcem a subjektem údajů vyrovnat. Nařízení však oproti ZOOÚ posiluje systém práv subjektu údajů. Nařízení nejen aktualizuje stávající práva subjektu údajů, ale také přináší některá nová práva, jako je např. právo na

[101] Bod 171 odůvodnění Nařízení.
[102] Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích).
[103] NONNEMANN, F. Odvolání souhlasu se zpracováním osobních údajů. *Právní rozhledy* [online], 23. prosince 2011, roč. 19, 24/2011, s. 877. [cit. 12. 3. 2018]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=8769

přenositelnost (tzv. portabilitu, čl. 20 Nařízení).[104] Mezi další práva pak patří právo subjektu údajů na přístup k osobním údajům (čl. 15 Nařízení) a jejich opravu (čl. 16 Nařízení), právo na výmaz údajů (tzv. právo být zapomenut, čl. 17 Nařízení), právo na omezení zpracování (čl. 18 Nařízení), možnost podání námitky vůči zpracování (čl. 21 Nařízení).

3.4.1. Právo subjektu údajů na přístup k osobním údajům

Právo subjektu údajů na přístup k osobním údajům není nic nového. Již podle ZOOÚ má subjekt údajů toto právo (§ 12 ZOOÚ) a může po správci požadovat konkrétní informace o zpracování jeho osobních údajů. Správce subjektu údajů na základě žádosti podává informace o účelu zpracování osobních údajů, o osobních údajích, dále o povaze automatizovaného zpracování a o příjemci/příjemcích. Nařízení ve srovnání se ZOOÚ dále rozšiřuje právo na přístup k osobním údajům o povinnost správce poskytnout na žádost informace týkající se plánované doby, po kterou budou osobní údaje uloženy či veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů. Nově je správce povinen spolu s těmito výše zmíněnými informacemi subjektu údajů také sdělit jeho práva vztahující se ke zpracování osobních údajů, a to konkrétně právo požadovat od správce opravu nebo výmaz osobních údajů a právo podat stížnost u dozorového úřadu.

Podle ZOOÚ za poskytnutí informací může správce požadovat přeměřenou úhradu. Ta by neměla převyšovat náklady nezbytné na poskytnutí informace (§ 12 odst. 3 ZOOÚ). Podle Nařízení již poskytnutí kopie zpracovávaných osobních údajů bude bezúplatné (čl. 15 odst. 3 Nařízení). Nutno podotknout, že bezúplatná je pouze první kopie, za další kopie na žádost subjektu údajů již správce přiměřený poplatek účtovat může. Poplatek by měl být stanoven na základě administrativních nákladů. Zda toto opatření bude mít v praxi opravdu za následek prudký nárůst žádostí o přístup k osobním údajům, si autorka netroufá odhadovat. Pravděpodobně se dá ale počítat v porovnání se současností s nárůstem využívání tohoto institutu.

Pokud by docházelo ke zneužívání tohoto práva ze strany subjektu údajů, například prostřednictvím opakovaných žádostí uplatňovaných krátce po sobě, má správce možnost žádostem nevyhovět. Správce musí být ovšem tuto skutečnost

[104] Úřad pro ochranu osobních údajů. Práva subjektu údajů [online] Poslední změna 5. 3. 2018 [cit. 13. 3. 2018]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

schopen prokázat. Pro začátek se doporučuje místo odmítnutí vyřízení opakované žádosti radši přistupovat k zavedení administrativního poplatku za další kopie. Alespoň do té doby, než se vyjasní, jaké situace budou dozorujícím úřadem a soudy považovány za legitimní.[105]

Zde je také na místě zamyslet se, po jaké době má subjekt právo znovu požadovat bezplatnou kopii. V Nařízení není stanovena doba, po jaké by subjekt údajů mohl bezplatně své právo na přístup k osobním údajům znovu využít. Podle názoru autorky však nelze dovozovat, že by snad subjekt údajů měl právo u konkrétního správce na bezplatnou kopii obsahující informace o zpracování jeho osobních údajů pouze jedinkrát. Autorka se domnívá, že takováto doba by mohla být stanovena na jeden kalendářní rok. Oporu pro toto tvrzení nachází v samotném ZOOÚ před novelizací zákonem č. 439/2004 Sb. Před touto novelizací bylo v ZOOÚ stanoveno, že „správce je povinen jednou za kalendářní rok bezplatně, jinak kdykoli za přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace, subjektu údajů na základě písemné žádosti poskytnout informace o osobních údajích o něm zpracovávaných“.[106]

Vzhledem k tomu, že má správce povinnost usnadňovat výkon tohoto práva, na žádost subjektu údajů má reagovat bez zbytečného odkladu, a to nejpozději do jednoho měsíce. V případě velkého počtu žádostí o přístup k osobním údajům, či s ohledem na jejich složitost se tato lhůta dá prodloužit až o další dva měsíce (čl. 12 odst. 3 Nařízení).

To, zda je společnost v souladu s Nařízením bude možné pozorovat právě na uplatňování tohoto institutu. Společnost by měla mít přehled, o tom jaké osobní údaje zpracovává, a kde se nacházejí. Jinak by v případě nárůstu žádostí o přístup k osobním údajům mohlo dojít k ochromení organizace a nedodržování lhůt.[107]

3.4.2. Právo na opravu

Na základě zásady přesnosti má správce povinnost přijmout veškerá rozumná opatření, aby zpracovával přesné a aktuální údaje (čl. 5 odst. 1 písm. d) Nařízení). V souladu s touto zásadou má subjekt údajů právo na to, aby správce

[105] ŠKORNIČKOVÁ, E. Zvládli jste přípravu na GDPR? Prověří to právo na přístup k osobním údajům. e*pravo.cz magazine*, 4/2017, s. 34.
[106] Zákon č. 101/2000 Sb. o ochraně osobních údajů ve znění zákona č. 517/2002 Sb.
[107] ŠKORNIČKOVÁ, E. Zvládli jste přípravu na GDPR? Prověří to právo na přístup k osobním údajům. e*pravo.cz magazine*, 4/2017, s. 34.

opravil nepřesné osobní údaje, a to bez zbytečného odkladu. Subjekt údajů má dále právo na doplnění neúplných osobních údajů (čl. 16 Nařízení).

Vzhledem k výše uvedenému má správce povinnost na základě žádosti ověřit, zda jsou osobní údaje přesné. Než přesnost údajů ověří, je zpracování těchto osobních údajů omezeno dle čl. 18 Nařízení. Poté, co správce údaje ověří, informuje subjekt údajů, že omezení bude zrušeno a může pokračovat ve zpracování osobních údajů. Co se týče doplnění osobních údajů, tohoto práva může subjekt údajů využít tehdy, když chce správci z vlastní iniciativy poskytnout dodatečné osobní údaje. V takovém případě se přihlíží k účelům zpracování tak, aby správce nezpracovával osobní údaje, které nejsou pro účely zpracování potřebné.[108]

Toto právo je uvedeno rovněž v ZOOÚ § 12 odst. 1 písm. b), dle názoru autorky tak Nařízení v tomto ohledu neznamená pro správce významnou změnu. Právo na opravu neznamená, že by správce musel sám aktivně nepřesné údaje vyhledávat. Je pouze jeho povinností zabývat se žádostí subjektu údajů, který požaduje opravu svých osobních údajů.

3.4.3. Právo být zapomenut

Právo, které nově Nařízení subjektům údajů přiznává, je právo výmaz neboli právo být zapomenut. Z pohledu autorky je toto právo obzvláště významné v dnešní technologické době. V samotném odůvodnění Nařízení je toto právo spojováno především s internetovým prostředím.[109] Zahrnutí tohoto práva do Nařízení reflektuje technologický vývoj a judikaturu SDEU.

Přelomovým byl v tomto ohledu rozsudek SDEU ve věci C 131/12 *Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ve kterém soud konstatoval, že subjekt údajů má právo na to, aby informace týkající se jeho osoby již nebyla nadále spojena s jeho jménem prostřednictvím zobrazeného seznamu výsledků vyhledávání provedeného na základě jeho jména.[110] V tomto případu šlo především o to, zda může subjekt údajů podat námitku proti indexování svých osobních údajů

[108] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 206-207.
[109] Bod 66 odůvodnění Nařízení.
[110] Rozsudek SDEU ve věci C 131/12, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ze dne 13. května 2014.

vyhledávačem, jestliže ho šíření uvedených údajů prostřednictvím vyhledávače poškozuje a současně převažují zájmy subjektu údajů nad legitimními zájmy provozovatele uvedeného vyhledávače a obecným zájmem na svobodě informací. Otázkou také bylo, zda základní právo na ochranu údajů a základní právo na soukromí zahrnují i právo být zapomenut.[111]

Zde je důležité zmínit, že právo být zapomenut se ve Směrnici nenachází. Podle Směrnice má subjekt údajů podle čl. 12 právo na výmaz, pokud zpracování osobních údajů není v souladu se Směrnicí, zejména z důvodů nepřesnosti nebo neúplnosti údajů. O to se však v tomto případu nejednalo. Pan González se domáhal výmazu informace o nuceném prodeji jeho nemovitosti z důvodu nesplaceného dluhu na sociálním pojištění, který byl ale později splacen. Po šestnácti letech nelze takovou informaci vnímat jako nezbytnou.[112] SDEU tak konstatoval, že „uvedený subjekt může s ohledem na svá základní práva podle článku 7 a 8 Listiny požadovat, aby dotčená informace již nebyla nadále poskytována široké veřejnosti na základě jejího zahrnutí do takového seznamu výsledků, převládají uvedená práva v zásadě nejen nad hospodářským zájmem provozovatele vyhledávače, ale rovněž nad zájmem veřejnosti nalézt uvedenou informaci při vyhledávání prováděném na základě jména subjektu údajů.“[113]

I když tedy Směrnice výslovně spojovala výmaz osobních údajů s nepřesnými a neúplnými informacemi a nesouladem se Směrnicí, SDEU výklad nesouladu se Směrnicí rozšířil a judikoval, že „může plynout nejen ze skutečnosti, že uvedené údaje jsou nepřesné, ale konkrétně také ze skutečnosti, že jsou nepřiměřené, nepodstatné a přesahují míru s ohledem na účely, pro které jsou zpracovávány, že nejsou aktualizovány nebo že jsou uchovávány po dobu delší, než je nezbytně nutné, pokud nejsou uchovávány pro historické, statistické nebo vědecké účely.“[114]

Téma práva být zapomenut bylo na základě tohoto rozsudku více rozpracováno Isabelle Falque-Pierrotin, prezidentkou CNIL, francouzského

---

[111] Rozsudek SDEU ve věci C 131/12, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ze dne 13. května 2014, bod 91.
[112] SLANINA, J., Právo být zapomenut a další dopady rozsudku SDEU C-131/12 Google Spain, *epravo.cz*, [online] 9.6.2014 [cit. 13. 3. 2018] Dostupné z: https://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-sdeu-c-13112-google-spain-94498.html
[113] Rozsudek SDEU ve věci C 131/12, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ze dne 13. května 2014, bod 97.
[114] Rozsudek SDEU ve věci C 131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ze dne 13. května 2014, bod 92.

dozorového úřadu a současně předsedkyní WP29 a zahrnuto do návrhu Nařízení a následně v této podobě schváleno.[115] Nařízení tak obsahuje toto právo v čl. 17 Nařízení, podle kterého má správce povinnost bez zbytečného odkladu z určitých důvodů osobní údaje týkající se subjektu údajů vymazat. Mezi tyto důvody patří: odvolání souhlasu, na jehož základě byly údaje zpracovány a neexistuje žádný další právní důvod pro zpracování nebo subjekt údajů vnesl námitku proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování, osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány, osobní údaje musí být vymazány ke splnění právní povinnosti plynoucí z práva EU nebo členského státu, osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti na základě souhlasu dítěte mladšího dle věkové hranice stanovené členským státem, a neposledním důvodem v řadě je protiprávnost zpracování osobních údajů.[116]

Právo být zapomenut a povinnost osobní údaje vymazat neplatí bezvýhradně. Z tohoto práva existují výjimky, které jsou stanoveny v čl. 17 odst. 3 Nařízení. Právo na výmaz se neuplatní, pokud jde o právo na svobodu projevu a informace, plnění právní povinnosti, veřejný zájem, veřejné zdraví, právní nároky a dále pokud jde o archivní, vědecké nebo statistické účely.[117]

Právo být zapomenut, tak jak je nyní definováno, je nové jak ve srovnání se Směrnicí, tak se ZOOÚ. Podle ZOOÚ má správce, potažmo zpracovatel, povinnost provést likvidaci osobních údajů pouze v případě, že pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti subjektu (§ 20 ZOOÚ). Subjekt může žádat o likvidaci osobních údajů týkající se jeho osoby, pokud zjistí nebo se domnívá, že správce/zpracovatel zpracovává osobní údaje v rozporu s ochranou soukromého a osobního života nebo v rozporu se zákonem, zejména pokud jsou údaje nepřesné s ohledem na účel zpracování (§ 21 ZOOÚ).

Je tedy patrné, že důvody pro výmaz osobních údajů byly Nařízením rozšířeny. Autorka se domnívá, že nejvýznamnější změnou je především povinnost správce vymazat osobní údaje na základě odvolání souhlasu subjektu údajů se zpracováním a též na základě vznesení námitky proti zpracování dle čl.

---

[115] KOLAH, A., FOSS, B., Unlocking the power of data under the new EU General Data Protection Regulation, *Journal of Direct, Data and Digital Marketing Practice*, 2015, 16(4), s. 272.
[116] Článek 17 odst. 1 Nařízení.
[117] WYBITUL, T., *EU-Datenschutz-Grundverordnung im Unternehmen*, Frankfurt: Deutscher Fachverlag, 2016, s 61.

21 Nařízení. Souhlas subjektu údajů prošel mnoha změnami, jak bylo již na několika místech v této práci zmíněno. Tím, že subjekt údajů může souhlas se zpracováním osobních údajů kdykoliv odvolat, činí souhlas jako právní titul značně nestabilní. Na základě toho se autorka domnívá, že správci se budou inklinovat k tomu zpracovávat údaje na základě jiných právních titulů, pokud to bude možné.

Subjekty údajů budou nově moci zamezit zpracovávání osobních údajů i z jiných právních titulů, než je souhlas, a to právní titul zpracování nezbytného pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci a dále zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany. Po vznesení námitky proti zpracování osobních údajů ze strany subjektu údajů, nesmí správce nadále osobní údaje zpracovávat, dokud neprokáže závažné oprávněné důvody pro zpracování převažující nad zájmy nebo právy a svobodami subjektu údajů. Z výše uvedeného je patrné, že Nařízení značně zvýšilo kontrolu, kterou má subjekt údajů nad osobními údaji, jež se ho týkají.

3.4.4. Právo na omezení zpracování

Právo na omezení zpracování má subjekt údajů podle Nařízení ve čtyřech případech. Za prvé, pokud je subjektem údajů popírána přesnost osobních údajů, musí správce omezit zpracování údajů, dokud neověří přesnost těchto osobních údajů. Za druhé, správce omezí zpracování, pokud je zpracování protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití. Za třetí, správce omezí zpracování osobních údajů v případě, že osobní údaje již nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků. A posledním případem je, že subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1 Nařízení a dokud nebude ověřeno, zda převažují oprávněné důvody správce nad oprávněnými důvody subjektu údajů, má správce též povinnost zpracování osobních údajů omezit.[118]

Omezení zpracování může být správcem provedeno různými způsoby. Může se jednat například o přesunutí vybraných údajů do jiného systému zpracování, znepřístupnění vybraných osobních údajů uživatelům nebo dočasné odstranění zveřejněných údajů z internetových stránek. V případě

[118] Článek 18 odst. 1 Nařízení.

automatizovaného zpracování by systém měl obsahovat technické prostředky, které zajistí omezení zpracování, tak aby se na tyto osobní údaje již žádné další operace zpracování nevztahovaly. V systému by mělo být také jasně vyznačeno, že zpracování osobních údajů je omezeno.[119]

V ZOOÚ existuje právo na blokaci osobních údajů, které je právu na omezení zpracování podobné avšak omezené pouze na případ, kdy subjekt údajů „zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování".[120] Je tedy patrné, že právo na blokaci podle současné právní úpravy má oproti právu na omezení zpracování menší uplatnění.[121]

3.4.5. Právo na přenositelnost údajů

Mezi práva, která značně rozšiřují práva subjektů údajů, je právo být zapomenut a dále právo na přenositelnost, tzv. právo na portabilitu. I toto právo je zcela nové[122] a bylo vytvořeno v rámci EU k podpoře konkurence na digitálním trhu a usnadnění přesouvání, kopírování a předávání osobních údajů z jednoho IT prostředí do jiného.[123] Subjekt údajů má tak nově právo získat automatizovaně zpracovávané osobní údaje, které se ho týkají, jež poskytl správci na základě souhlasu nebo na základě smlouvy ve strukturovaném, běžně používaném a strojově čitelném formátu.[124] Právo na portabilitu se nevztahuje na údaje, které jsou zpracovávané na základě jiného právního titulu, než je souhlas nebo smlouva. Z tohoto důvodu není možné toto právo uplatňovat vůči správcům, kteří zpracovávají osobní údaje v rámci výkonu veřejné moci nebo kdy je zpracování osobních údajů nezbytné pro splnění právní povinnosti.[125]

V praxi by právo na přenositelnost mělo být využito především různými aplikacemi, jakou jsou např. sportovní či běžecké aplikace, hudební platformy,

---

[119] Bod 67 odůvodnění Nařízení.
[120] § 21 odst. 1 ZOOÚ.
[121] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 216.
[122] Právo na přenositelnost údajů je nové právo, nicméně jiné druhy přenositelnosti již existují nebo jsou projednávány v dalších oblastech práva, např. v kontextu ukončení smlouvy, roamingu v oblasti komunikačních služeb a přeshraničního přístupu k službám.
[123] POMAIZLOVÁ, K., FÜRSTOVÁ, M. Právo na přenositelnost dat, *Právní rádce,* 6/2017, s. 31.
[124] Článek 20 Nařízení.
[125] Bod 67 odůvodnění Nařízení.

sdílené kalendáře, elektronická pošta, vyhledávače zaměstnání, aplikace shromažďující informace o zdravotním stavu, platformy umožňující seznámení, uložiště fotografií a mělo by se dotýkat zejména poskytovatelů internetových služeb a e-commerce.[126] Je tedy patrné, že toto právo reaguje na technologický vývoj v současné době. Právo na přenositelnost by mělo zajistit subjektům údajů volněji disponovat se svými osobními údaji.

Právo na přenositelnost má dva aspekty, jednak právo subjektu získat osobní údaje, a dále pak právo přenést tyto osobní údaje k jinému správci. V prvním případě jde vlastně o rozšíření práva na přístup. V druhém případě jde o právo subjektu údajů, aby jeho osobní údaje byly předány jedním správcem druhému správci, čímž má dojít k usnadnění přesouvání osobních údajů bez překážek z jednoho systému do druhého.[127] I když právo na přenositelnost úzce souvisí s právem na přístup k údajům, v mnoha ohledech se od něj liší. Podle ZOOÚ a práva na přístup k údajům byl subjekt údajů omezen formátem zvoleným správcem údajů při poskytování požadovaných informací. V rámci tohoto práva musí správce nově poskytnout subjektu údajů osobní údaje ve formátu, který podporuje opakované použití. Formát by měl být zvolen tak, aby byl interoperabilní, zjednodušeně řečeno v takovém formátu, které je v daném odvětví běžně používaný, a který umožní subjektu údajů vysoký stupeň přenositelnosti. Vhodným tedy jistě nebude takový formát, který například podléhá nákladným omezením v oblasti udělování licencí.[128] Naopak co do rozsahu osobních údajů, je právo na přenositelnost užší než právo na přístup k údajům. Správce poskytuje totiž pouze osobní údaje, které se subjektu údajů týkají a které subjekt údajů správci poskytl.

Co se může v praxi jevit jako problematické, je výklad termínu „osobní údaje poskytnuté správci“, a to na jaká data se bude právo na přenositelnost vztahovat. Při poskytování osobních údajů nemusí jít jen o informace poskytnuté a zadané vědomě a aktivně subjektem údajů, ale může se jednat také o údaje získané prostřednictvím využívání služby či zařízení (např. lokalizační údaje, počet přehrání určité skladby, data přihlášení do aplikace). Nejedná se však o data odvozená nebo dovozená z údajů poskytnutých jejich subjektem na základě

[126] POMAIZLOVÁ, K., FÜRSTOVÁ, M. Právo na přenositelnost dat, *Právní rádce,* 6/2017, s. 31.
[127] KALÍŠEK, J., VĚŽNÍKOVÁ, P. Právo na přenositelnost údajů („data portability“) dle nařízení GDPR, *epravo.cz magazine,* 4/2017, s. 31.
[128] Pokyny WP29 týkající se práva na přenositelnost údajů přijaté dne 13. prosince 2016 a naposledy revidované a přijaté dne 5. dubna 2017. WP 242 rev.01.

analýz, profilování, hodnocení či jiných podobných procesů (např. uživatelský profil vytvořený analýzou základních dat z chytrého měření, vyhodnocení kredibility na základě osobních údajů získaných od subjektu údajů o jeho zaměstnání, věku či provedených transakcí).[129]

3.4.6. Právo vznést námitku

Právo vznést námitku bylo již částečně rozebráno u práva být zapomenut. Co je ale z pohledu autorky další významnou změnou v rámci práva vznést námitku, je, že Nařízení přiznává subjektu údajů právo vznést námitku proti zpracovávání osobních údajů za účelem přímého marketingu. Na základě této námitky již pak správce nesmí osobní údaje nadále zpracovávat (čl. 21 odst. 2,3 Nařízení). Subjekt může námitku proti zpracování pro účely přímého marketingu vznést kdykoliv a bezplatně. Navíc na toto právo musí být správcem výslovně upozorněn. Upozornění musí být pro subjekt údajů zřetelné, a proto musí být navíc odděleno od všech ostatních informací.[130] Proto, aby subjekt mohl vznést námitku proti zpracování osobních údajů pro účely přímého marketingu, nemusí mít žádné důvody, jako v případě práva na vznesení námitky podle odst. 1 čl. 21 Nařízení. Správce neporovnává zájmy, práva a svobody subjektu se svými. Se zpracováním musí okamžitě přestat, jakmile obdrží námitku.

V případě, že správce provádí zpracovatelské činnosti za účelem přímého marketingu online, pak musí subjektům údajů umožnit realizovat svá práva také online a automatizovaně.[131] Což je dle názoru autorky plně v souladu s myšlenkou Nařízení, že souhlas se zpracováním by mělo být pro subjekt údajů stejně jednoduché dát, jako odvolat.

I když autorka přikládá větší význam právu vznést námitku proti zpracování pro účely přímého marketingu, je na místě ještě zmínit právo vznést námitku proti zpracování pro účely vědeckého nebo historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 Nařízení, a to z důvodů týkajících se jeho konkrétní situace (čl. 21 odst. 6 Nařízení). Zde záleží na posouzení správce, zda vyhodnotí, že zpracování osobních údajů subjektu údajů je nezbytné pro splnění

[129] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 223.
[130] Bod 70 odůvodnění Nařízení.
[131] NEZMAR, L. *GDPR. Praktický průvodce implementací*. Praha: GRADA Publishing, 2017, s. 92.

úkolu prováděného z důvodu veřejného zájmu. Pokud zpracování nezbytné pro takový úkol je, probíhá zpracování osobních údajů i nadále. Nejedná se tedy o právo absolutní, na rozdíl od práva vznést námitku proti zpracování pro účely přímého marketingu. Ovšem správce musí také zhodnotit, zda nelze daný úkol splnit i způsobem takovým, při kterém zpracovávání osobních údajů daného subjektu údajů nutné není.

3.5. Pověřenec pro ochranu osobních údajů

Zcela novým institutem v českém prostředí dosud neznámým, které Nařízení zavádí, je pověřenec pro ochranu osobních údajů, tzv. DPO (Data Protection Officer, dále jen „Pověřenec"). Pro ČR je sice tento pojem nový, ale podobný institut zvaný „Bundesbeauftragten für den Datenschutz und die Informationsfreiheit"[132] existuje v Německu na spolkové úrovni již od roku 1978.[133] Na úrovni jednotlivých spolkových zemí, konkrétně v Hesensku, byl dokonce ustanoven první zmocněnec pro ochranu osobních údajů („Datenschutzbeauftragter") ještě dříve.[134] Institut Pověřence je zakotven v čl. 37 až 39 Nařízení. Úprava v této části stanoví podrobnosti o jmenování Pověřence, postavení Pověřence a jeho úkoly.

Není povinností každého správce a zpracovatel jmenovat Pověřence. Tuto povinnost mají pouze orgány veřejné moci či veřejné subjekty, s výjimkou soudů jednajících v rámci svých soudních pravomocí,[135] dále správci a zpracovatelé, jejichž hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektu údajů nebo jejichž hlavní činnosti spočívají v rozsáhlém zpracování tzv. citlivých údajů[136] a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.[137] Z výše uvedeného vyplývá, že navzdory všeobecně rozšířenému mínění o povinnosti jmenování Pověřence, pravděpodobně většina společností tuto povinností mít v ČR nebude. Důležité je

[132] Volně přeloženo jako Spolkový pověřenec pro ochranu dat a informační svobodu.
[133] Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Stellenausschreibung. [online] [cit. 18. 3. 2018]. Dostupné z: https://www.bfdi.bund.de/DE/BfDI/Dienststelle/Stellenausschreibungen/Stellenausschreibungen_node.html
[134] Viz MIELKE, S., REUTTER, W., *Länderparlamentarismus in Deutschland. Geschichte – Struktur – Funkcionen.* Wiesbaden: VS Verlag für Sozialwissenschaften, 2006, s. 239.
[135] Jedná se například o obce a školy.
[136] Dle pojmosloví současné úpravy.
[137] Dle čl. 10 Nařízení.

ovšem zdůraznit slovo pravděpodobně, jelikož čl. 37 odst. 4 umožňuje členským státům přijmout doplňkovou právní úpravu týkající se Pověřenců. Členské státy si tak mohou definovat více organizací, které budou mít povinnost Pověřence jmenovat. A jak bylo zmíněno již dříve v této práci, český adaptační zákon k Nařízení se prozatím nachází jen ve formě návrhu a není ani jisté, že bude do doby účinnosti Nařízení schválen.

Pokud by se jevilo jako sporné, zda má organizace Pověřence jmenovat či nikoli, pracovní skupina WP29 ve svých pokynech doporučuje, aby správci a zpracovatelé vypracovali interní analýzu, kde by byly řádně zohledněny relevantní faktory, zda by Pověřenec měl či neměl být jmenován. Organizace, které povinnost jmenovat Pověřence nemají a není to u nich ani sporné, mohou Pověřence jmenovat dobrovolně. V takovém případě se však na Pověřence budou vztahovat požadavky podle článku 37 až 39 Nařízení, jako kdyby bylo jmenování povinné. Tomuto se lze vyhnout tak, že organizace, která nemá povinnost ustanovit Pověřence, může najmout externího poradce či zaměstnat pracovníka, jež by řešil úkoly s ochranou osobních údajů souvisejících. Je pak ale nutné jasně uvést jak v rámci organizace, tak navenek, že se nejedná o funkci Pověřence,[138] na poradce či pracovníka se poté se články 97 až 39 nevztahují.

Co se týče náplně funkce Pověřence, tak jeho hlavní činností je hlavně poskytování poradenství správcům nebo zpracovatelům a zaměstnancům, kteří zpracování provádějí. Poradenství poskytuje na požádání, pokud se týká posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle čl. 35 Nařízení. Jeho úkolem je dále monitorování souladu (tzv. compliance) s Nařízením, ale také i dalšími předpisy EU a národními předpisy v oblasti ochrany osobních údajů. Pověřenec je dále povinen spolupracovat s dozorovým úřadem a je kontaktním místem pro styk dozorového úřadu se správcem nebo zpracovatelem.[139] Aby Pověřenec mohl plnit své úkoly, je mu správce a zpracovatel povinen zajistit součinnost při jejich plnění. Správce a zpracovatel například musí Pověřenci poskytnout zdroje nezbytné k plnění úkolů, přístup k osobním údajům a operacím zpracování a musí ho též zapojit do všech záležitostí souvisejících s ochranou osobních údajů, a to náležitě a včas.[140]

---

[138] Pokyny WP29 týkající se pověřenců pro ochranu osobních údajů přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017. WP 243 rev.01, 16/CS, s. 6-7.
[139] Dle čl. 39 Nařízení.
[140] Článek 38 Nařízení.

Pověřenec je jmenován na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39.[141] Tento popis je dosti široký a je nejasné, jaké konkrétní atributy by měl Pověřenec splňovat. V tomto případě je schopnost plnit stanovené úkoly neméně důležitá v porovnání se znalostí práva. Koneckonců právní radu lze získat i od právních poradců, takže klíčovým prvkem bude schopnost plnit úkoly, což vyžaduje významnou úroveň praktických zkušeností a zkušeností se zajištěním souladu s právním rámcem ochrany osobních údajů.[142] Atributy, které by měl Pověřenec splňovat podle WP29 jsou: odborné znalosti v oblasti vnitrostátní a evropské praxe a právních předpisů na ochranu osobních údajů, je zřejmě, že Pověřenec by měl také rozumět Nařízení. Dále byl mě Pověřenec rozumět prováděným operacím zpracování, informačním technologiím a zabezpečení osobních údajů, ideálně znát také podnikatelské odvětví a organizaci. Též by měl mít schopnost pěstovat v rámci organizace kulturu ochrany osobních údajů.[143]

Podle názoru autorky je zřízení funkce Pověřence pro organizaci přínosné, a to především v současné době, kdy organizace ještě povinnost Pověřence jmenovat nemá, protože Nařízení v době sepisování práce ještě není použitelné. Naopak dle názoru autorky, je jmenování Pověřence před použitelností Nařízení pro organizace mimořádně výhodné, jelikož Pověřenec organizaci pomůže zajistit soulad s Nařízením ještě před vstupem Nařízení v účinnost.

3.6. Posouzení vlivu na ochranu osobních údajů

Zcela nově zavádí Nařízení v čl. 35 Nařízení posouzení vlivu na ochranu osobních údajů. Institut posouzení vlivu je postup určený k zajištění a doložení, že správce provádí zpracování v souladu s Nařízením. Záměrem posouzení vlivu je popis zpracování údajů, posouzení jeho nezbytnosti a přiměřenosti a řízení rizik pro práva a svobody fyzických osob plynoucích ze zpracování osobních údajů. Posouzení vede ke stanovení opatření k jejich řešení. Na základě posouzení správce dokládá, že plní příslušné povinnosti Nařízení a že byla přijata příslušná

[141] Článek 37 odst. 5 Nařízení.
[142] IT GOVERNANCE PRIVACY TEAM. *EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide.* 2nd edition, Cambridgeshire: IT Governance Publishing, 2017, s. 71.
[143] Pokyny WP29 týkající se pověřenců pro ochranu osobních údajů (často kladené otázky), WP243 Příloha [online] 7. 3. 2018 [cit. 16. 3. 2018]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29165

opatření s cílem zajistit soulad s Nařízením. Je to důležitý nástroj zajištění odpovědnosti správce.[144]

O tom, zda se opravdu jedná o zcela novou povinnost, by se dalo polemizovat. Z evropského či globálního hlediska se o zcela novou povinnost nejedná.[145] Pro správce usazené v ČR by se o novou povinnost jednat mohlo. Ovšem ani to se někteří nedomnívají.[146] Již v rámci oznamovací povinnosti dle § 16 ZOOÚ má správce povinnost písemně oznamovat Úřadu, že hodlá zpracovávat osobní údaje. Oznámení mimo jiné obsahuje popis opatření k zajištění ochrany osobních údajů podle § 13 ZOOÚ. Součástí těchto opatření je také posouzení rizik. Posouzení rizik, dle odst. 3 § 13 ZOOÚ, bylo do zákona doplněno v souvislosti s přípravou ČR do schengenského prostoru novelou provedenou zákonem č. 170/2007 Sb. Tento odstavec stanoví povinnost pro správce a zpracovatele zvážit možná bezpečnostní rizika.[147] A proto se někteří domnívají, že posouzení vlivu na ochranu osobních údajů není zcela novým institutem. Ovšem autorka se přiklání spíše k názoru, že se o nový institut jedná, jelikož pokud bude mít správce povinnost provést posouzení vlivu, bude se jednat o písemnou a mnohem více formalizovanou analýzu než v případě posouzení rizik. Nařízení sice o písemné formě posouzení vlivu na ochranu osobních údajů nehovoří, nicméně ta vyplývá z čl. 35 odst. 7 Nařízení. V pokynech WP29[148] se také hovoří o povinnosti předkládat zprávu o posouzení vlivu na ochranu osobních údajů příslušnému dozorovému úřadu, pokud je mu tato povinnost uložena, což je v souladu s čl. 24 odst. 1 Nařízení, který stanoví odpovědnost správce a jeho

---

[144] Pokyny WP29 pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, přijaté dne 4. dubna 2017, přijaté dne 4. října v aktualizovaném znění. WP 248 rev.01, 17/CS. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29169

[145] Viz posuzovaní rizik „Privacy impact assessment“ dle legislativy (Data Protection Act) ve Spojeném království; Information Commissioner’s Office. Conducting privacy impact assessments. Code of practice. [online] 25. 2. 2014 [cit. 18. 3. 2018]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[146] NEŠPŮREK, R., ŠUCHMAN, J., JAROŠ, J. GDPR: Kdy a jak posuzovat vliv zpracování na ochranu osobních údajů a kdy konzultovat dozorový orgán? *Právní prostor,* [online] 9.11.2017 [cit. 18. 3. 2018]. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/gdpr-kdy-a-jak-posuzovat-vliv-zpracovani-na-ochranu-osobnich-udaju-a-kdy-konzultovat-dozorovy-organ

[147] KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012, s. 236.

[148] Viz pokyny WP29 pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, přijaté dne 4. dubna 2017, přijaté dne 4. října v aktualizovaném znění. WP 248 rev.01, 17/CS, s.23. Dostupné z:
https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29169

povinnost doložit, že zpracování je v souladu s Nařízením. Posouzení rizik se dle současné úpravy spíše neprovádí. Splnění oznamovací povinnosti ohledně popisu opatření k zajištění ochrany osobních údajů podle § 13 ZOOÚ, v jehož rámci se dělá posouzení rizik, totiž spočívá v zaškrtávání několika polí v elektronickém formuláři zveřejněném na webových stránkách Úřadu. O písemné a formalizované analýze tak nemůže být řeč, a z tohoto důvodu se autorka domnívá, že pro správce spíše bude jednat o nový institut.

Povinnost provést posouzení vlivu je povinné, pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob. V takovém případě provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.[149] Nařízení uvádí tyto tři případy, ve kterých je posouzení vlivu nutné: 1) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad; 2) rozsáhlé zpracování citlivých údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestních činů; nebo 3) rozsáhlé systematické monitorování veřejně přístupných prostorů.[150] Konkrétnější vymezení činností zpracování, které vyžadují posouzení vlivu, v Nařízení není, proto Nařízení stanoví povinnost dozorovému úřadu sestavit seznam druhů operací zpracování, u kterých posouzení vlivu nutné je a u kterých není, a informovat o tomto seznamu Evropský sbor pro ochranu osobních údajů.[151]

Úřad místo taxativního výčtu zpracování, která podléhají posouzení vlivu na ochranu osobních údajů, který by byl v čase proměnlivý, zvolil cestu určování rizikovosti zpracování pomocí parametrů a hodnot,[152] na jejichž základě bude vyhodnoceno, zda je zpracování vysoce rizikové, rizikové nebo ostatní. Pro stanovení, zda je zpracování osobních údajů rizikové či vysoce rizikové, je dle Pokynů WP29 a návrhu Úřadu stanoveno 9 obecných kritérií. Obecně platí, že pokud zpracování splňuje dvě kritéria, vyžaduje posouzení vlivu na ochranu

[149] Přesné znění viz čl. 35 odst. 1 Nařízení.
[150] Článek 35 odst. 3 Nařízení.
[151] Článek 35 odst. 4 a 5 Nařízení.
[152] Tyto parametry a hodnoty byly vytvořeny na základě pokynů WP29 pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679.

osobních údajů. A čím více kritérií zpracování splňuje, tím větší pravděpodobnost, že je zpracování vysoce rizikové pro práva a svobody subjektu údajů, a bude proto vyžadovat posouzení vlivu na ochranu osobních údajů.[153] Kritéria jsou následující: provádí-li se 1) ohodnocení nebo hodnocení bonity fyzických osob, včetně profilování a předpovědi, 2) automatické rozhodování s právním nebo obdobným významným účinkem, 3) systematické monitorování, včetně monitorování veřejně přístupných prostor, 4) zpracování citlivých údajů, 5) zpracování velkého rozsahu, 6) kombinace nebo propojování dat různých zpracování, 7) zpracování údajů týkající se zranitelných subjektů údajů, 8) zpracování s obtížně uplatnitelnými právy subjektu údajů – pro procesy prováděné ve veřejné oblasti, jimž se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnou přístup subjektů údajů k službě nebo uzavření smlouva, 9) dochází-li k inovativnímu využití nebo aplikaci technologických nebo organizačních řešení.[154]

Pro zpracování osobních údajů, které nepodléhají posouzení vlivu na ochranu osobních údajů, připravil Úřad návrh seznamu.[155] Tento návrh vznikl na základě odůvodnění Nařízení bodu 91 a také pokynů WP29,[156] ve kterých jsou uvedeny příklady zpracování, u kterých není posouzení vlivu na ochranu osobních údajů nutné. Podle tohoto návrhu seznamu posouzení vlivu na ochranu osobních údajů nebude třeba provádět například při zpracování zajišťovanými jednotlivými lékaři nebo zdravotníky, při zpracování zajišťovanými právníky, zpracování týkající se obchodní činnosti, zpracování prováděná za účelem vedení účetnictví, zpracování při provozování kamerových systémů či fotopastí, pokud nedochází k nadměrnému monitorování veřejných prostranství nebo například při zpracování

[153] Pokyny WP29 pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, přijaté dne 4. dubna 2017, přijaté dne 4. října v aktualizovaném znění. WP 248 rev.01, 17/CS, s. 12 Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29169

[154] Úřad pro ochranu osobních údajů. K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA) [online] 7. 2. 2018 [cit. 18. 3. 2018]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003

[155] Úřad pro ochranu osobních údajů. K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA) [online] 7. 2. 2018 [cit. 18. 3. 2018]. Dostupné z: https://www.uoou.cz/k-nbsp-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385

[156] Pokyny WP29 pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, přijaté dne 4. dubna 2017, přijaté dne 4. října v aktualizovaném znění. WP 248 rev.01, 17/CS. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29169

při provozování kamery na jednotlivém vozidle monitorující nezbytný prostor před, případně za vozidlem.[157]

Za provedení posouzení vlivu na ochranu osobních údajů odpovídá správce údajů.[158] Pokud jmenoval Pověřence, vyžádá si jeho posudek (čl. 35 odst. 2 Nařízení), což ale neznamená, že provádění posouzení vlivu na ochranu osobních údajů je automaticky úkolem Pověřence. Správce i tak zůstává za posouzení vlivu odpovědným, a to i v případě, pokud vypracováním posouzení vlivu na ochranu osobních údajů pověří jinou externí či interní osobu. Nařízení hovoří, že ve vhodných případech si správce získá k zamýšlenému zpracování také stanovisko subjektů údajů nebo jejich zástupců (čl. 35 odst. 9 Nařízení). Není ovšem povinností se stanoviskem subjektu údajů, ani stanoviskem Pověřence řídit. Nicméně pokud se správce rozhodne stanoviskem Pověřenci či subjektu údajů neřídit, musí to náležitě odůvodnit v dokumentaci posouzení vlivu.[159]

3.7. Ohlašování a oznamování

Mezi další nové povinnosti, které Nařízení zavádí, je povinnost ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a oznamování případu porušení zabezpečení osobních údajů subjektu údajů. I když v rámci ZOOÚ existuje též oznamovací povinnost podle § 16 ZOOÚ, jedná se v tomto případě zcela o jinou oznamovací povinnost než dle Nařízení. Obsahem oznamovací povinnost dle § 16 ZOOÚ je totiž povinnost oznamovat Úřadu to, že správce hodlá zpracovávat osobní údaje nebo změnit registrované zpracování. Tato povinnost se netýká bezpečnosti osobních údajů jako v Nařízení a mimo jiné bude s účinností Nařízení povinnost oznamovat zamýšlené zpracování zrušena a s tím dojde i k uzavření veřejného registru oznámených a zaregistrovaných zpracování osobních údajů.[160]

---

[157] Více viz Materiál úřadu pro ochranu osobních údajů k povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA) [online] 7. 2. 2018 [cit. 18. 3. 2018] Dostupné na: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003

[158] Článek 24 odst. 1 Nařízení.

[159] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 322.

[160] Úřad pro ochranu osobních údajů. S účinností GDPR končí oznamovací povinnost správců [online] 1. 3. 2018 [cit. 18. 3. 2018]. Dostupné z: https://www.uoou.cz/s-nbsp-ucinnosti-gdpr-konci-oznamovaci-povinnost-spravcu/d-28855

Nicméně povinnost ohlašování a oznamování není pro ČR něčím zcela úplně neznámým. Již zákon o elektronických komunikacích[161] stanoví povinnost poskytovatelům služeb elektronických komunikací řešit případy porušení ochrany osobních údajů (tzv. data breaches) a porušení ochrany Úřadu oznámit. A pokud by takové porušení mohlo ovlivnit zvláštně závažným způsobem soukromí fyzické osoby má podnikatel povinnost oznámit takovou skutečnost také dotčené fyzické osobě.[162]

Jak je tedy patrné povinnost ohlašování a oznamování není tak zcela nová. Vznikla na základě vzrůstajících rizik spojených s masivními úniky dat, např. útoky hackerů nebo jiné případy úniku nebo zničení dat. Dle Nařízení, zjistí-li správce, že zabezpečení osobních údajů bylo jakkoliv porušeno, je jeho povinností toto porušení nahlásit dozorovému úřadu, a to do 72 hodin,[163] ve všech případech, ledaže je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody fyzických osob.[164] Pokud by takové porušení mohlo mít za následek riziko pro práva a svobody fyzických osob, musí toto porušení správce oznámit také bez odkladu subjektu údajů. Správce porušení subjektu údajů oznamovat nemusí tehdy, když zavedl taková technická opatření jako např. šifrování nebo pseudonymizace údajů, která zapříčiní nesrozumitelnost pro kohokoliv, kdo není oprávněn mít k osobním údajům přístup.[165] Opatření mohou být preventivní i následná. Zajistí-li správce, že rizika se pravděpodobně neprojeví, oznamovací povinnost nemá. Nemá ji ani v tom případě, že by oznámení vyžadovalo nepřiměřené úsilí.[166] V takovém případě správce může zvolit oznámení pomocí veřejných sdělovacích prostředků nebo oznámení na úvodní stránce po přihlášení do online služby.

Co se týče povinnosti ohlašování, Nařízení stanoví lhůtu pro ohlášení, co má být obsahem tohoto ohlášení, co do formy ohlášení však Nařízení mlčí. Lze ovšem s největší pravděpodobností předpokládat, že ohlášení se bude provádět formou formuláře dostupného na stránkách Úřadu. Stejně tak, jak je to nyní

---

[161] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) ve znění zákona č. 252/2017 Sb.
[162] § 88 odst. 4 a odst. 5 Zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) ve znění zákona č. 252/2017 Sb.
[163] Pokud ohlášení neprovede do 72 hodin, musí být současně s ohlášením uvedeny důvody zpoždění.
[164] Článek 33 odst. 1 Nařízení.
[165] Článek 34 odst. 2 Nařízení.
[166] Článek 34 odst. 2 písm. c) Nařízení.

možné v případě oznámení o narušení bezpečnosti osobních údajů podle zákona o elektronických komunikacích.

3.8. Záznamy o činnostech

Jak bylo zmíněno v předchozí podkapitole, povinnost oznamovat zamýšlené zpracování bude zrušena. Je to i z toho důvodu, že bude do jisté míry nahrazena jinými nástroji ochrany osobních údajů. Takovým nástrojem je i například povinnost správce vést záznamy o činnostech zpracování podle čl. 30 Nařízení. Záznamy o činnostech by měly obsahovat jméno a kontaktní údaje správce, účely zpracování, kategorie subjektů údajů a osobních údajů, kategorie příjemců, informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, a je-li to možné také plánované lhůty pro výmaz jednotlivých kategorií údajů a také obecný popis technických a organizačních bezpečnostních opatřeních (čl. 30 Nařízení). Pokud to porovnáme s obsahem informací v rámci oznamovací povinnosti dle § 16 ZOOÚ, je patrné, že až na zdroje osobních údajů, popis způsobu zpracování osobních údajů a místo nebo místa zpracování osobních údajů se obsah informací téměř nezměnil.

Na základě záznamů o činnostech správce nebo zpracovatel dokládá soulad zpracování s Nařízením. Na žádost dozorového úřadu musí správce nebo zpracovatel záznamy o činnostech předložit.[167] Povinnost vést záznamy o činnostech se však nevztahuje na všechny správce a zpracovatele, ale pouze na takové, kteří zaměstnávají 250 a více zaměstnanců. Toto se neuplatní v případě, kdy správce provádí zpracování rizikové pro práva a svobody subjektu údajů, zpracování citlivých údajů nebo zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů nebo také pokud zpracování není příležitostné.[168] Lze se tak domnívat, že povinnost vést záznamy bude platit pravděpodobně pro všechny zaměstnavatele, jelikož zaměstnavatelé osobní údaje zpracovávají z povahy věci standardně a opakovaně, nikoliv příležitostně.[169]

Pokud srovnáme se ZOOÚ, neplatí již krom výše uvedeného žádné výjimky z povinnosti vedení záznamů o činnostech. Kdežto v ZOOÚ se oznamovací povinnost nevztahovala na zpracování osobních údajů, které jsou

[167] Bod 82 odůvodnění Nařízení.
[168] Článek 30 odst. 5 Nařízení.
[169] MACKOVIČOVÁ, M., HÁJKOVÁ, M. Nařízení GDPR a zaměstnavatelé, *epravo.cz magazine*, 4/2017, 2017, s. 41.

součástí datových souborů veřejně přístupných, které správci ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona nebo jde-li o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti sdružení.[170]

Z uvedeného vyplývá, že Nařízení se v tomto ohledu dotkne nově zaměstnavatelů, jak již bylo výše naznačeno. Zaměstnavatelé oznamovací povinnost podle § 16 ZOOÚ nemají, pokud nezpracovávají osobní údaje i pro jiné účely, než jsou jim uloženy zvláštními zákony (např. zákoníkem práce). Po účinnosti Nařízení však většina zaměstnavatelů již povinnost vést záznamy o činnostech zpracování mít bude.

4. Vliv GDPR na ochranu osobních údajů

V souvislosti s Nařízením propukla v ČR téměř hysterie. Tato přehnaná reakce je ze strany Evropy nepochopitelná a neopodstatněná. Často se v souvislosti s Nařízením hovoří také o „největší revoluci v oblasti ochrany osobních údajů“. Je tomu tak skutečně? Sama předsedkyně Úřadu pro ochranu osobních údajů zmínila na konferenci o novém evropském nařízení o ochraně osobních údajů na konci listopadu roku 2017, že není třeba Nařízení démonizovat. Právo na ochranu osobních údajů v České republice existovalo již před Nařízením. V ústavním pořádku je zakotveno již od počátku samotné existence České republiky. Všechny zásady zpracování osobních údajů a většina základních zásad ochrany osobních údajů jsou obsaženy již v Úmluvě 108, ke které Česká republika přistoupila v roce 2000.[171]

Ano, jak je patrné z předchozích kapitol, Nařízení opravdu přináší nové povinnosti, jako je povinnost ohlašovat případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů, oznamovat případy porušení zabezpečení osobních údajů subjektu údajů, vést záznamy o činnostech zpracování, pro některé správce je povinnost provést posouzení vlivu na ochranu osobních údajů a ustanovit pověřence pro ochranu osobních údajů. Jednou z dalších změn dle Nařízení je posílení odpovědnosti správce osobních údajů. Správce je odpovědný za soulad zpracování osobních údajů s Nařízením a musí

[170] § 18 ZOOÚ.
[171] VEJVODOVÁ, A. GDPR očima expertů: Žádný strašák, ale příležitost, *Právní rádce*, 4/2017, str. 25.

jej být schopen kdykoliv doložit. Nicméně je však patrné, že základní principy, zásady a klíčové instrumenty zůstávají do velké míry nezměněné. Nařízení je pouze hlouběji rozpracovalo a konkretizovalo, což bylo s technologickým vývojem nezbytné, pokud má být udržena určitá úroveň ochrany osobních údajů v rámci EU.

Nařízení navazuje na cíle a zásady Směrnice a cíle a zásady ZOOÚ. Autorka se tak ztotožňuje s názory, že o revoluci v ochraně osobních dat se nejedná. Již ZOOÚ garantoval poměrně vysokou úroveň ochrany práv osobních údajů a zaváděl pro správce jisté povinnosti, které jestli byly ze strany správce dodržovány, tak se účinností Nařízení pro některé správce až tak mnoho nezmění. To však závisí na aspektech zpracování, které provádí. Avšak samotný Úřad tvrdí, že „[p]okud správce řádně plní povinnosti vyplývající ze současného zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, nemělo by Obecné nařízení pro něj představovat výrazný problém, se kterým by si neporadil.“[172] Autorka s tímto souhlasí a domnívá se, že problém budou mít v zásadě ty společnosti, které dosud ignorovaly platné národní předpisy o ochraně osobních údajů. Jedním z důvodů vzniklé hysterie kolem Nařízení může být i to, že Nařízení zavádí citelnější sankce za porušování tohoto Nařízení. Autorka se domnívá, že především strach z udělení těchto sankcí, zajistí dodržování souladu s Nařízením.

Sankce ve formě správních pokut jsou jednou z nejviditelnějších změn, které Nařízení zavádí. Správci podle Nařízení nesou větší odpovědnost za zajištění účinné ochrany osobních údajů a dozorové úřady disponují pravomocemi, aby se dodržování Nařízení zajistilo. Správní pokuty jsou klíčovou součástí donucovacích prostředků dozorových úřadů. Správní pokuty by měly být stejně jako ostatní nápravná opatření účinné, přiměřené a odrazující. Měly by být adekvátní reakcí na povahu, závažnost a důsledky porušení,[173] a to podle okolností každého jednotlivého případu. Zohledňují se okolnosti jako povaha, závažnost a délka trvání porušení, zda k porušení došlo úmyslně nebo z nedbalosti, veškerá relevantní předchozí porušení správcem či zpracovatelem,

[172] Úřad pro ochranu osobních údajů. Správce, zpracovatel [online] Poslední změna 5. 3. 2018 [cit. 20. 3. 2018]. Dostupné z: https://www.uoou.cz/7-spravce-zpracovatel/d-27278

[173] Pokyny WP29 k uplatňování a stanovování správních pokut pro účely nařízení 2016/679, přijaté dne 3. října 2017, WP253, 17/CS, s. 4, 6 Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29172

kategorie osobních údajů dotčené daným porušením atd.[174] Zároveň je důležité zmínit, že pokuta nemusí být uložena za každé porušení Nařízení. Dozorový úřad má i jiné nápravné pravomoci, kterých může využít. Správce tak může být například uděleno napomenutí či může být dozorovým úřadem upozorněn, že zamýšlené operace zpracování pravděpodobně porušují Nařízení. Úřad může také nařídit správci nebo zpracovateli, aby uvedl operace zpracování do souladu s Nařízením, uložit dočasné nebo trvalé omezení zpracování, nařídit opravu či výmaz osobních údajů, atd. Udělení správní pokuty podle čl. 83 Nařízení je tak jen jednou z možností, která může být udělena vedle nebo namísto opatření výše uvedených a dalších opatření.[175] Není tak pravdou, že každé porušení Nařízení bude představovat uložení správní pokuty.[176]

Co je ovšem pravdou je, že výše horní hranice správních pokut se s Nařízením oproti ZOOÚ výrazně zvýšila. ZOOÚ stanoví hranici nejvyšší možné pokuty do 10 000 000 Kč, kterou lze uložit za ohrožení většího počtu osob neoprávněným zasahování do soukromého a osobního života, nebo za porušení povinnosti pro zpracování citlivých údajů dle § 9 ZOOÚ.[177] Naproti tomu Nařízení stanoví za porušení některých ustanovení Nařízení možnost uložit správní pokutu až do výše 10 000 000 EUR, nebo v případě podniku až do výše 2% celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší. Za porušení základních zásad, včetně podmínek týkajících se souhlasu podle článků 5, 6, 7 a 9 Nařízení, práv subjektu údajů podle článků 12 až 22 Nařízení, předání osobních údajů příjemci ve třetí zemi nebo mezinárodní organizaci podle článku 44 až 49 či nesplnění příkazu dozorového úřadu lze udělit pokutu až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4% celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.[178]

Důležité je zmínit, že členské státy mají možnost svou národní úpravou vyjmout orgány veřejné moci. Zda a do jaké míry by se měly správní pokuty vztahovat na orgány veřejné moci, bude určeno v zákonu o zpracování osobních údajů. V odůvodnění se také doporučuje, aby dozorový úřad zohledňoval výše

[174] Článek 83 odst. 2 Nařízení.
[175] Článek 58 odst. 2 Nařízení
[176] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: GRADA Publishing, 2017, s. 43.
[177] § 45 odst. 2 ZOOÚ.
[178] Článek 83 Nařízení.

správních pokut ukládané osobám, které nejsou podnikem, a to s ohledem na obecnou úroveň příjmů v daném členském státě, jakož i ekonomickou situaci dané osoby.[179]

V současné době se ukazuje, jak důležitá je ochrana osobních dat, viz velmi aktuální kauza Facebook a Cambridge Analytica. Společnost Cambridge Analytica získala z Facebooku velké množství informací a údajně je zneužila ve volebních kampaních.[180] Facebook, Google a další jsou zdrojem obrovského objemu osobních údajů, které mohou být zneužitelné v případě jejich nedostatečné ochrany. Autorka se tak domnívá, že nastavení vysokých sankcí je důvodné, aby sankce byly vůbec citelné například i pro takové společnosti jako je Facebook či Google. Odrazující výše sankcí by snad také měla zajistit důslednější dodržování souladu zpracování osobních údajů s Nařízením.

[179] Bod 150 odůvodnění Nařízení.
[180] KLAPAL, O. Šéf Facebooku se omluvil a slíbil v kauze úniků dat spolupráci s americkým Kongresem, *irozhlas.cz,* [online] 22. 3. 2018 [cit. 22. 3. 2018]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/mark-zuckerberg-facebook-new-york-times-cambridge-analytica-data-zneuziti_1803220652_gol

Závěr

V České republice je právo na soukromí a s tím i právo na ochranu osobních údajů zakotveno již v ústavním pořádku. Od roku 2000 platí v ČR ZOOÚ, který vychází se Směrnice, a ten samý rok také ČR přistoupila k Úmluvě 108, která obsahuje všechny zásady zpracování osobních údajů a většinu základních zásad ochrany osobních údajů. Přijetí Nařízení je jen dalším vývojovým krokem v oblasti ochrany osobních údajů. Nařízení reaguje na rapidní technologický vývoj a globalizaci a jeho cílem je sjednotit úroveň ochrany osobních údajů fyzických osob v rámci celé EU.

Cílem této práce bylo posoudit a porovnat Nařízení se stávající úpravou, a co nového Nařízení přináší. Jaké zavádí nové instituty, povinnosti a sankce za nedodržování souladu s Nařízením. Otázku, kterou si autorka kladla, bylo, zda lze v souvislosti s Nařízením hovořit o revoluci v ochraně osobních údajů. Za účelem naplnění cíle práce používala zejména metodu komparace. První kapitola byla spíše teoretická a krátce se věnovala vývoji práva na soukromí. Následně se kapitola věnovala právní úpravě ochrany soukromí a osobních údajů na mezinárodní, evropské a národní úrovni. Druhá kapitola se věnovala klíčovým pojmům dle Nařízení a jejich komparaci se stávající úpravou. Za stěžejní pojmy autorka považuje tyto: osobní údaj, zpracování, správce, zpracovatel, příjemce a souhlas subjektu údajů. Definice osobního údaje se dle Nařízení oproti ZOOÚ rozšířila o další dva identifikátory člověka, lokační údaje a síťový identifikátor. Mezi prvky lidské identity pak přidala i prvek genetický. Rozšíření definice reaguje pouze na technologický vývoj. V ostatním ohledu se definice významně nezměnila. Definice zpracování zůstává, až na volbu slov, která jsou synonymní, stejná. Jedinou změnou v definici dle Nařízení oproti ZOOÚ je chybějící aspekt systematičnosti, jehož význam je v definici okrajový. Definice správce podle ZOOÚ obsahuje ve srovnání s Nařízením o jedno definiční kritérium navíc. Jedná se odpovědnost správce za zpracování. Toto definiční kritérium je dle názoru autorky nadbytečné, vzhledem k tomu, že odpovědnost správce za zpracování je stanovena v článku 5 Nařízení. Změna v tomto případě tak není významná a nemá na chápání toho, kdo je správce žádný vliv. Jak u definice správce, tak zpracovatele, je v definici změna ve výčtu toho, kdo může být správce či zpracovatel. ZOOÚ říká, že „každý subjekt“, v Nařízení je „každý subjekt“ nahrazen vyjmenováním těchto subjektů, takže správcem či zpracovatelem může

být „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt“. Výčet subjektů je však v tomto případě tak široký, že mezi tímto výčtem a slovem „každý“ může být prakticky rovnítko. Definice zpracovatele podle ZOOÚ navíc obsahuje rozlišení dvou variant určení zpracovatele, a to na základě zákonného zmocnění, nebo na základě pověření správce. O významnou změnu se nejedná, jelikož v obou případech vykonává zpracování údajů pro správce zpracovatel. Ani pojetí zpracovatele se tak s Nařízením nijak nemění. To samé lze říci i o definici příjemce. Ačkoliv jsou definice příjemce podle Nařízení a ZOOÚ formulovány odlišně, na skutečnosti, kdo je označován za příjemce se opět nic nemění. Větších změn tak doznala pouze definice souhlasu dle Nařízení. Nařízení nově požaduje, aby souhlas subjektu údajů byl učiněn prohlášením či zjevným potvrzením. Nově bude tedy zapotřebí, aby se jednalo o aktivní udělení souhlasu. Závěrem lze shrnout, že co se nejdůležitějších pojmů týče, Nařízení nezavádí žádné přelomové změny. Většina pojmů zůstala prakticky nedotčena. Jedinou důležitou změnou prošla definice souhlasu.

Třetí kapitola se zaměřila na klíčová ustanovení a instituty Nařízení a jejich komparaci se stávající úpravou. Co se závaznosti a působnosti týče, novinkou je určitě forma nařízení, díky této formě je Nařízení přímo použitelné v každém členském státě EU, aniž by státy musely přijímat národní implementaci. To plně koresponduje s cílem Nařízení sjednotit úroveň ochrany osobních údajů fyzických osob v rámci EU. Oproti ZOOÚ má Nařízení rozšířenou místní působnost. Nově se Nařízení vztahuje i na zpracování osobních údajů správcem či zpracovatelem bez ohledu na to, zda zpracování probíhá v EU či mimo ní, a to v případě, že zpracování souvisí s nabídkou zboží nebo služeb subjektům údajů v EU nebo zpracování souvisí s monitorováním chování subjektu údajů v EU, pokud k němu dochází v rámci EU. Nařízení má tak na rozdíl od ZOOÚ silnější extrateritoriální působnost. Dále se kapitola věnovala zásadám Nařízení. Zde lze shrnout, že všechny zásady byly Nařízením mírně upraveny a zpřesněny. Největší změnou však prošla zásada odpovědnosti, kdy správce musí soulad s Nařízením nejen dodržet, ale také být schopen doložit. Správci tak vzniká na základě Nařízení tato nová povinnost.

Právní důvody zpracování osobních údajů dle Nařízení byly již ve srovnání s ZOOÚ upraveny výrazněji. V Nařízení je definovaných šest právních titulů pro zpracování osobních údajů, kdežto v ZOOÚ jich je osm. V Nařízení je novým právním titulem zpracování nezbytné pro splnění úkolu prováděného ve

veřejném zájmu nebo při výkonu veřejné moci, který by měl být hlavně přínosem pro orgány veřejné moci. U právních titulů, které byly zachovány, proběhly u některých určité změny. Autorka však za jednu z nejvýznamnějších změn považuje to, že z pohledu Nařízení již žádný právní titul nedominuje. V ZOOÚ dominoval souhlas subjektu údajů. Ten je nyní postaven na roveň ostatním právním titulům. Naopak do budoucna by se právní titul souhlasu subjektu údajů mohl stát spíše poslední možnosti pro správce, pokud se nemůže zpracování provádět na základě jiného právního titulu. Nařízení totiž klade přísnější podmínky na užívání právního titulu souhlasu. Nově bude také podle Nařízení souhlas subjektu údajů mnohem jednodušší odvolat. Tedy odvolání souhlasu má být tak snadné, jako jej poskytnout. Z těchto důvodu je pravděpodobné, že souhlas již nebude do budoucnosti preferovaným právním titulem.

Třetí kapitola se dále věnovala právům subjektu údajů. Nařízení přiznává subjektům údajů oproti ZOOÚ některá nová práva, jako je právo na to být zapomenut nebo právo na přenositelnost. Nařízení také oproti ZOOÚ rozšiřuje právo na přístup k osobním údajům o povinnost správce poskytnout na žádost informace týkající se plánované doby, po kterou budou osobní údaje uloženy či veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů. Poskytnutí kopie s požadovanými informacemi musí také nově správce poskytnout bezúplatně. Tyto práva mají především zajistit větší kontrolu subjektu údajů nad svými osobními údaji, stejně tak jako právo vznést námitku. Dle Nařízení může subjekt údajů také nově vznést námitku proti zpracování osobních údajů za účelem přímého marketingu, přičemž správce nadále nesmí osobní údaje zpracovávat.

Hojně diskutovanou novinkou je nový institut Pověřence, kterého budou mít povinnost od 25. května 2018 jmenovat orgány veřejné moci či veřejné subjekty, nebo správci a zpracovatelé, jejichž hlavní činnost spočívá v rozsáhlém zpracování citlivých údajů nebo zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů. Lze předpokládat, že většina společností povinnost jmenovat Pověřence mít nebude. Z pohledu autorky je však tento institut velmi přínosný. Pověřenec na základě svých odborných schopností pomůže správci s dodržováním souladu zpracování osobních údajů s Nařízením.

Novou povinností podle Nařízení oproti ZOOÚ je také povinnost ohlašování případů porušení zabezpečení dozorovému úřadu a oznamování

případu porušení zabezpečení osobních údajů subjektu údajů. O zcela novou povinnost se však nejedná, jelikož tuto povinnost stanoví již zákon o elektronických komunikacích. Naopak povinnost vést záznamy o činnostech dosud nikde zakotvena nebyla a Nařízení ji tak zavádí jako další novinku. Tato povinnost se však nevztahuje na všechny správce a zpracovatele, ale pouze na takové, kteří zaměstnávají 250 a více zaměstnanců nebo na takové, kteří provádí zpracování rizikové pro práva a svobody subjektu údajů, zpracování citlivých údajů nebo zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů nebo pokud zpracování není příležitostné. Povinnost vést záznamy o činnostech se tak dotkne pravděpodobně všech zaměstnavatelů, jelikož nezpracovávají data pouze příležitostně, ale standardně a opakovaně.

Čtvrtá kapitola se pak věnovala sankcím a správním pokutám, jejichž horní hranice byla výrazně zvýšena, což vyvolalo v české společnosti značný rozruch. Nicméně autorka se domnívá, že výše správních pokut nemá sloužit k likvidování drobných živnostníků, ale spíš zajistit, aby sankce byly vůbec citelné například i pro takové společnosti jako je Facebook či Google, které zpracovávají obrovské objemy dat.

Závěrem lze říci, že ačkoliv Nařízení zavádí řadu změn a nových institutů, je patrné, že tyto změny jsou pouhou reakcí na technologický vývoj. Pro subjekt údajů znamená Nařízení mnohem větší kontrolu nad svými osobními údaji. Správcům a zpracovatelům přibydou na základě Nařízení oproti ZOOÚ nové povinnosti, což jak se autorka domnívá, nemusí být nutně špatně. Vyšší nároky při zpracování osobních údajů budou kladeny především na velké správce, již zpracovávají velké množství osobních údajů, které je zároveň ze své podstaty rizikové pro práva a svobody subjektu údajů. Pro menší správce, pokud dodržovali již zásady zpracování a povinnosti dle ZOOÚ, by Nařízení nemělo představovat žádný větší problém. Osobní data se stávají čím dál tím více ceněnou komoditou a zvýšení jejich ochrany se tak jeví jako vhodné opatření proti jejich zneužití. O revoluci se tak dle názoru autorky nejedná. Jde spíš o přirozený vývoj legislativy v oblasti ochrany osobních údajů.

Resumé

The submitted thesis deals with personal data protection and General Data Protection Regulation (GDPR). The GDPR will be applicable from 25 May 2018, thus the topic of personal data protection is very actual and discussed issue in current days. Rapid technological developments and globalization have brought new challenges for the protection of personal data. Those developments require a strong and more coherent data protection framework in the European Union. For this purpose, the GDPR was adopted. The aim of this graduation thesis is to compare the GDPR with the current legislation. The primary purpose of this thesis is to determine whether the GDPR really can be labelled as revolution for personal data protection.

The thesis itself is composed of four chapters. Chapter 1 is introductory and deals with the concept of privacy and the legislation of privacy and personal data protection on the international, European and national level. Chapter 2 focuses on the main definitions of the GDPR, as personal data, processing, controller, processor, recipient and consent. These definitions are compared with the current legislation. Chapter 3 concentrates on the key provisions and new institutes under the GDPR. This chapter describes material scope and territorial scope. After that, this chapter deals with the new institutes under the GDPR, namely data protection officer, data protection impact assessment, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, and records of processing activities. Chapter 4 concerns shortly with the image of GDPR among the Czech society. Then the fourth chapter focuses primarily on the penalties and the administrative fines, which are linked to non-compliance with the GDPR.

On the basis of the results of these comparisons, it can be concluded that the GDPR does not represent a revolution. Although, there are some changes which the GDPR is bringing, these changes are necessary and inevitable due to rapid technological developments and with that related new challenges for the protection of personal data.

Seznam použité literatury a pramenů

Monografie, publikace, sborníky

GLENN, R. *The Right to Privacy: rights and liberties under the law*. Santa Barbara: ABC-CLIO, 2003. ISBN 1-57607-717-9.

IT GOVERNANCE PRIVACY TEAM. *EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide.* 2nd edition, Cambridgeshire: IT Governance Publishing, 2017. ISBN 978-1-84928-946-7.

KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář*, 1. vydání. Praha: C. H. Beck, 2012. ISBN 978-80-7179-226-0.

LYNSKEY, O. *The Foundations of EU Data Protection Law.* Oxford: Oxford University Press, 2015. ISBN 978-0-19-871823-9.

MIELKE, S., REUTTER, W., *Länderparlamentarismus in Deutschland. Geschichte – Struktur – Funkcionen.* Wiesbaden: VS Verlag für Sozialwissenschaften, 2006. ISBN 978-3-8100-3893-7.

MORÁVEK, J. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Praha: Wolters Kluwer, a.s., 2015. ISBN 978-80-7552-018-0.

NEZMAR, L. GDPR: *Praktický průvodce implementací*. Praha: GRADA Publishing, 2017. ISBN 978-80-271-0920-3.

NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-763-3.

WYBITUL, T., *EU-Datenschutz-Grundverordnung im Unternehmen*, Frankfurt: Deutscher Fachverlag, 2016. ISBN 978-3-8005-1634-6.

Odborné články

HORKÁ, N. Souhlas se zpracováním osobních údajů ve světle nové legislativy. In: *epravo.cz* [online] 9. 2. 2018 [cit. 12. 3. 2018]. Dostupné z:

https://www.epravo.cz/top/clanky/souhlas-se-zpracovanim-osobnich-udaju-ve-svetle-nove-legislativy-106991.html

GLANCY, D. The Intention of the Right to Privacy, *Arizona Law Review* [online]. 1979, 21(1) [cit. 12.3.2018]. Dostupné z: http://law.scu.edu/wp-content/uploads/Privacy.pdf

KALÍŠEK, J., VĚŽNÍKOVÁ, P., Právo na přenositelnost údajů („data portability“) dle nařízení GDPR, *epravo.cz magazine*, 4/2017. ISSN 1802-1492.

KOLAH, A., FOSS, B. Unlocking the power of data under the new EU General Data Protection Regulation, *Journal of Direct, Data and Digital Marketing Practice*, 2015, 16(4). ISSN 1746-0174.

MACKOVIČOVÁ, M., HÁJKOVÁ, M. Nařízení GDPR a zaměstnavatelé, *epravo.cz magazine*, 4/2017, 2017. ISSN 1802-1492.

NEŠPŮREK, R., ŠUCHMAN, J., JAROŠ, J. GDPR: Kdy a jak posuzovat vliv zpracování na ochranu osobních údajů a kdy konzultovat dozorový orgán? *Pravní prostor*, [online] 9. 11. 2017 [cit. 18. 3. 2018]. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/gdpr-kdy-a-jak-posuzovat-vliv-zpracovani-na-ochranu-osobnich-udaju-a-kdy-konzultovat-dozorovy-organ

NONNEMANN, F. Odvolání souhlasu se zpracováním osobních údajů. *Právní rozhledy* [online], 23. prosince 2011, roč. 19, 24/2011 [cit. 12. 3. 2018]. Dostupné z:
https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=8769

POMAIZLOVÁ, K., FÜRSTOVÁ, M., Právo na přenositelnost dat, *Právní rádce,* 6/2017. ISSN 1210-4817.

RADIČOVÁ, Z., BURIAN, D. Profilování ve světle nového obecného nařízení o ochraně osobních údajů (GDPR). *epravo.cz* [online] 2. 2. 2017 [cit. 16. 3. 2018]. Dostupné z: https://www.epravo.cz/top/clanky/profilovani-ve-svetle-noveho-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-104926.html

SLANINA, J., Právo být zapomenut a další dopady rozsudku SDEU C-131/12 Google Spain, *epravo.cz*, [online] 9. 6. 2014 [cit. 13. 3. 2018] Dostupné z:

https://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-sdeu-c-13112-google-spain-94498.html

ŠKORNIČKOVÁ, E. Zvládli jste přípravu na GDPR? Prověří to právo na přístup k osobním údajům. *epravo.cz magazine,* 4/2017. ISSN 1802-1492.

VEJVODOVÁ A. GDPR očima expertů: Žádný strašák, ale příležitost, *Právní rádce,* 4/2017. ISSN 1210-4817.

VICTOR, J. M. The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy, *The Yale Law Journal*, 2013, Vol. 123, No. 2, s. 513. ISSN 0044-0094.

Odborná stanoviska

Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC adpoted on 9 April 2014, WP 2177 [online]. Dostupné z: http://www.dataprotection.ro/servlet/ViewDocument?id=1086

Stanovisko WP 29 č. 4/2007 ze dne 20. 6. 2007 k pojmu osobní údaj, WP136.

Stanovisko WP 29 č. 5/2014 ze dne 10. 4. 2014 k technikám anonymizace, WP 216.

Stanovisko Úřadu č. 4/2013, K pojetí zpracování osobních údajů [online]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22256

Stanovisko Úřadu č. 2/2008, aktualizované v červenci 2014 [online]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22284

Stanovisko Úřadu č. 6/2009, Ochrana soukromí při zpracování osobních údajů [online]. Dostupné z: https://www.uoou.cz/files/stanovisko_2009_6.pdf

Stanovisko WP 29 č. 1/2010 ze dne 16. února 2010 k pojmům „správce“ a „zpracovatel“.

Vodítka WP29 k souhlasu podle Nařízení 2016/679 ze dne 28. listopadu 2017. WP259.

Opinion of WP29 03/2013 on purpose limitation adopted on 2 April 2013. WP 203.

Pokyny WP29 týkající se práva na přenositelnost údajů přijaté dne 13. prosince 2016 a naposledy revidované a přijaté dne 5. dubna 2017. WP 242 rev.01.

Pokyny WP29 k uplatňování a stanovování správních pokut pro účely nařízení 2016/679, přijaté dne 3. října 2017, WP253, 17/CS.

Pokyny WP29 pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, přijaté dne 4. dubna 2017, přijaté dne 4. října v aktualizovaném znění. WP 248 rev.01, 17/CS.

Pokyny WP29 týkající se pověřenců pro ochranu osobních údajů přijaté dne 13. prosince 2016, naposledy revidované a přijaté dne 5. dubna 2017. WP 243 rev.01, 16/CS.

Elektronické zdroje

Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Stellenausschreibung. [online] [cit. 18. 3. 2018]. Dostupné z: https://www.bfdi.bund.de/DE/BfDI/Dienststelle/Stellenausschreibungen/Stellenausschreibungen_node.html

Dokument WP 105, ze dne 19. ledna 2005, Pracovní dokument o otázkách ochrany osobních údajů, které souvisejí s technologií RFID. 10107/05/CS Dostupné z: http://docplayer.cz/amp/3319012-Pracovni-dokument-o-otazkach-ochrany-udaju-ktere-souviseji-s-technologii-rfid.html

Information Commissioner’s Office. Conducting privacy impact assessments. Code of practice. [online] 25. 2. 2014 [cit. 18. 3. 2018]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

KLAPAL, O. Šéf Facebooku se omluvil a slíbil v kauze úniků dat spolupráci s americkým Kongresem, *irozhlas.cz,* [online] 22. 3. 2018 [cit. 22. 3. 2018]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/mark-zuckerberg-facebook-new-york-times-cambridge-analytica-data-zneuziti_1803220652_gol

Materiál úřadu pro ochranu osobních údajů k povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA) [online] 7. 2. 2018 [cit. 18. 3. 2018] Dostupné na: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003

Úřad pro ochranu osobních údajů. K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA) [online] 7. 2. 2018 [cit. 18. 3. 2018]. Dostupné z: https://www.uoou.cz/k-nbsp-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385

Úřad pro ochranu osobních údajů. Práva subjektu údajů [online] Poslední změna 5. 3. 2018 [cit. 13. 3. 2018]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

Úřad pro ochranu osobních údajů. Rada Evropy [online] [cit. 12. 2. 2018]. Dostupné z: https://www.uoou.cz/rada-evropy/ds-1797/archiv=0&p1=1659

Úřad pro ochranu osobních údajů. Rada Evropy jako jeden z hlavních garantů evropské ochrany osobních údajů [online] [cit. 12. 2. 2018]. Dostupné z: https://www.uoou.cz/rada-evropy/ds-1797/archiv=0&p1=3938

Úřad pro ochranu osobních údajů. S účinností GDPR končí oznamovací povinnost správců [online] 1. 3. 2018 [cit. 18. 3. 2018]. Dostupné z: https://www.uoou.cz/s-nbsp-ucinnosti-gdpr-konci-oznamovaci-povinnost-spravcu/d-28855

Úřad pro ochranu osobních údajů. Správce, zpracovatel [online] Poslední změna 5. 3. 2018 [cit. 20. 3. 2018]. Dostupné z: https://www.uoou.cz/7-spravce-zpracovatel/d-27278

Úřad pro ochranu osobních údajů. Základní příručka [online] [cit. 12. 2. 2018] Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744&archiv=1

Úřad pro ochranu osobních údajů. Zásady a právní důvody zpracování [online] Poslední změna 5. 3. 2018 [cit. 13. 3. 2018]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271

Úřad pro ochranu osobních údajů. Zvláštní kategorie osobních údajů (citlivé údaje) [online] Poslední změna 5. 3. 2018 [cit. 12. 2. 2018] Dostupné z: https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaj-citlive-udaje/d-27274

WEINHOLD LEGAL. Návrh zákona o zpracování osobních údajů. Legal Update 10/2017 [online] [cit. 8. 3. 2018] Dostupné z: www.beck-online.cz

Pokyny WP29 týkající se pověřenců pro ochranu osobních údajů (často kladené otázky), WP243 Příloha [online] 7. 3. 2018 [cit. 16. 3. 2018]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29165

Právní předpisy

Listina základních práv Evropské unie.

Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích).

Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích).

Smlouva o fungování Evropské unie.

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

Zákon č. 101/2000 Sb. o ochraně osobních údajů ve znění zákona č. 183/2017 Sb.

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) ve znění zákona č. 252/2017 Sb.

Soudní rozhodnutí

Nález Ústavního soudu České republiky sp. zn. II. ÚS 517/99 ze dne 1. března 2000.

Nález Ústavního soudu České republiky sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.

Rozhodnutí NSS ve věci sp. zn. 9 As 34/2008 ze dne 12. února 2009.

Rozsudek SDEU ve věci C 131/12, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ze dne 13. května 2014.

Rozsudek Soudního dvora EU ve věci C-582/14, Patrick Breyer proti Spolkové republice Německo, ze dne 19. října 2016.

Rozsudek Soudního dvora Evropské unie ve věci C-101/01, Bodil Lindqvis, ze dne 6. listopadu 2003.