UNIVERZITA KARLOVA

Právnická fakulta

Martin Švec

Vybrané otázky aktuální právní úpravy osobních údajů v Evropské unii

Diplomová práce

Vedoucí diplomové práce: JUDr. Magdaléna Svobodová, Ph.D.

Katedra evropského práva

Datum vypracování práce (uzavření rukopisu): 23.8. 2018

Prohlášení:

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

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 136 688 znaků včetně mezer.

V Kralupech nad Vltavou dne 23.8. 2018

_____

Martin Švec

Poděkování:

Děkuji JUDr. Magdaléně Svobodové, Ph.D. za vedení mé práce se vstřícným přístupem a za její cenné připomínky a rady jak před zahájením psaní práce, tak v jejím průběhu. Dále děkuji své rodině za veškerou možnou podporu během celého mého studia.

Obsah

Seznam použitých zkratek:

EU	Evropská unie
OSN	Organizace spojených národů
SFEU	Smlouva o fungování Evropské unie
OECD	Organisation for Economic Co-operation and Development
GDPR	General Data Protection Regulation
WP29	Working Party 29
DPIA	Data protection impact assessment
BDSG	Bundesdatenschutzgesetz
RFID	Radio frequency identification
ICO	Information Commissioner's Office
CNIL	Commission nationale de l'informatique et des libertés

Úvod

Ochrana osobních údajů se stala mezi odbornou i laickou veřejností velmi diskutovanou oblastí práva, a to z důvodu obecného nařízení o ochraně osobních údajů známou pod zkratkou GDPR. Tato čtyři písmenka nahání každému správci osobních údajů hrůzu. Správci v nich často nevidí nic jiného než další administrativní zátěž a výmysl Bruselu, které jim zvýší náklady a zaberou spoustu času. Na základě těchto reakcí by se člověk mohl domnívat, že před účinností GDPR žádná úprava ochrany osobních údajů neexistovala a že se GDPR objevilo z ničeho nic.

Cílem této práce je přiblížit vývoj ochrany osobních údajů v Evropské unii a porovnat úpravu GDPR s původní unijní úpravou, ale i s úpravami vybraných členských států. Ochrana osobních údajů v Evropě má kořeny už v 17. a 18. století a její vývoj jako samostatné právní oblasti lze pozorovat již od minulého století. Členské státy Evropské unie byly povinny transponovat do svých národních úprav směrnici 95/46/ES regulující komplexně ochranu osobních údajů, a to nejpozději do roku 1998. Ochrana osobních údajů měla tedy před příchodem GDPR svoji komplexní unijní úpravu již celých 20 let. GDPR je bezesporu přelomovou regulací už jen z toho pohledu, že harmonizuje nejednotné národní úpravy a garantuje tak subjektům údajů stejnou ochranu napříč členskými státy Evropské unie. Otázkou však je, jak moc je GDPR revoluční pro samotnou oblast ochrany osobních údajů. Cílem této práce tedy zhodnotit, jestli je GDPR přelomovou úpravou ochrany osobních údajů, i co se týče samotného znění nařízení.

Ačkoliv lze směrnici 95/46/ES a GDPR srovnávat v mnoha různých ohledech, není v rámci rozsahu diplomové práce možné srovnávat úplně vše, a tak jsem si vybral dle svého názoru ty nejdůležitější změny obsažené v GDPR a srovnal jsem je s původní úpravou obsaženou ve směrnici. Srovnání s úpravou českého zákona ochrany osobních údajů nebylo cílem této diplomové práce, ale pro zajímavost občas uvádím srovnání i s tímto naším českým zákonem.

V práci je zároveň věnována pozornost dvěma novým institutům unijního práva, a to institutu pověřence pro ochranu osobních údajů a posouzení vlivu na ochranu osobních údajů. Na základě komparace s německou federativní úpravou bych chtěl u institutu pověřence

zhodnotit jeho novost a celkové pojetí. U posouzení vlivu na ochranu osobních údajů bych chtěl objasnit a přiblížit celkový proces přijetí.

1. Historický vývoj ochrany osobních údajů v Evropě

Úpravě ochrany osobních údajů předcházel vývoj a uznání práva na soukromí. Vytvoření konceptu práva na soukromí je přičítáno americkým právníkům Samuelu D. Warrenovi a L. Brandeisovi, kteří v roce 1890 publikovali esej s názvem "The Right to Privacy". V této eseji autoři mimo jiné formulovali pojetí soukromí jako práva člověka mít kontrolu nad zveřejňováním vlastních myšlenek, osobních informací a fotek. Přes originalitu této koncepce je však nutné zmínit, že obsah příspěvku vychází zejména z rozhodnutí evropských soudů týkajících se ochrany osobní cti a dobré pověsti.[1] Zajímavostí je, že tato esej vznikla jako reakce na narušování soukromí tiskem pomocí fotografií, které se na konci 19. století začínaly běžně používat. Obecně by se dalo říci, že úprava ochrany soukromí a později ochrany osobních údajů vždy reagovala na nějaký technologický pokrok.

První právní úprava ochrany osobních údajů pochází ze švédského zákona o svobodném přístupu k informacím z roku 1776. Tento zákon reguloval zpracovávání osobních údajů ve veřejných záznamech a stanovil princip, že nelze zpracovávat osobní údaje nad rámec oprávněných zájmů. Dalšími zákony pak byly francouzský zákon zakazující publikování údajů o soukromí z roku 1858 a norské zákony, které zase zakazovaly publikování údajů vztahující se k osobním nebo domácím záležitostem (1889). Výše uvedené zákony předcházely tedy vzniku koncepce práva na soukromí, avšak byly v Evropě pouze ojedinělé. Skutečný rozvoj úpravy ochrany osobních údajů přichází do Evropy postupně právě až s uznáním práva na soukromí[2].

Ochrana osobních údajů se stala velmi aktuální po druhé světové válce. Mezinárodní společenství si uvědomilo, že je nutné učinit kroky k tomu, aby se zabránilo opakování zvěrstev fašistického režimu. V roce 1948 tak byla Valným shromážděním OSN přijata Všeobecná deklarace lidských práv[3]. Tato Deklarace reagovala i na nedostatečnou ochranu soukromí, která usnadnila realizaci holocaustu. Perzekuce nacistickým režimem byla totiž usnadněna evidencí obyvatel, ve které byly mimo jiné například údaje o náboženském vyznání.

[1] NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). Str. 6. ISBN 978-80-7478-665-5.
[2] GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 5. ISBN 3319050222.
[3] dále také i jako „Deklarace“.

1.1. Úprava práva na soukromí v rámci OSN a Rady Evropy

Všeobecná deklarace lidských práv stanovila ve svém článku 12, že nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. I když je Všeobecná deklarace lidských práv nezávazný dokument, který ani neobsahuje definici vysvětlující samotný pojem soukromí, je článek 12 považován za základ dalšího rozvoje ochrany soukromí a později i ochrany osobních údajů.

V roce 1950 na deklaraci OSN navázala Rada Evropy schválením Úmluvy o ochraně lidských práv a základních svobod[4]. Úmluva zvolila ve svém článku 8 trochu odlišnou formulaci: "Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence". I když Úmluva z Všeobecné deklarace lidských práv vycházela, vypustila zmínku o útoku na čest a pověst. Tato slova byla pravděpodobně vypuštěna kvůli své neurčitosti.[5] Další odlišnost ve formulaci je viditelná v anglickém jazyce. Zatímco Deklarace v angličtině používá slovo „privacy", Úmluva zvolila použití slov „respect for private life". Stejně tak jako deklarace neobsahuje definici slova „privacy", ani Úmluva neobsahuje definici pojmu „respect for private life". Tento pojem byl interpretován až judikaturou Evropského soudu pro lidská práva, která se vyjádřila pro jeho extensivní výklad[6].

Dalším důležitým mezinárodním právním dokumentem, který zahrnul právo na soukromí mezi významná lidská práva, je Mezinárodní pakt o občanských a politických právech, který byl přijat na zasedání OSN v roce 1966. Tato mezinárodní smlouva navázala na Deklaraci a převzala ve svém článku 17[7] téměř doslova článek 12 Deklarace. Definice soukromí ale i v tomto dokumentu opět chyběla.

Definice práva na soukromí, respektive práva na ochranu soukromí, má podle odborné literatury několik základních rovin. A to rovinu informační, která ochraňuje údaje o jednotlivci, jeho korespondenci apod. zejména před neoprávněným zveřejněním. Dále pak rovinu

[4] dále také i jako „Úmluva".
[5] GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 38. ISBN 3319050222 citováno z RUÍZ MIGUEL, Carlos. 1992. La configuración constitucional del derecho a la intimidad. Madrid: Universidad Complutense de Madrid, Str. 99.
[6] GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 95. ISBN 3319050222.
[7] Mezinárodní pakt o občanských a politických právech, čl. 17 odst. 1: Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence ani útokům na svou čest a pověst.

fyzickou, která ochraňuje tělesnou integritu jednotlivce, rozhodovací, která poskytuje jednotlivci možnost svobodné volby, a případně vlastnickou, zdůrazňující oprávněné majetkové zájmy.[8] Samotná ochrana osobních údajů se pak postupem času začala vymezovat z roviny informační.[9]

1.2. Úprava ochrany osobních údajů na mezinárodní úrovni

Mezinárodní organizací, která značným způsobem ovlivnila vývoj ochrany osobních údajů na konci 20. století, byla Organizace pro hospodářskou spolupráci a rozvoj[10]. OECD se, stejně jako mnohé státy v Evropě, začala věnovat problematice ochrany údajů především ve spojitosti s jejich automatizovaným zpracováním, které se s rozvojem technologií začalo objevovat v 70. letech. Hlavním cílem OECD je rozvoj mezinárodního obchodu. A tak úsilím organizace bylo především zamezení vzniku překážek pro volný pohyb informací, které z důvodu rozdílných národních úprav vznikaly. OECD proto v roce 1978 založila expertní skupinu, která dostala za úkol vytvořit pravidla pro ochranu soukromí a přeshraniční toky osobních údajů[11]. Pravidla OECD se vztahují na všechny druhy zpracování osobních údajů, při kterých hrozí nebezpečí pro práva a svobody fyzických osob. Vztahují se tedy jak na automatizované, tak na manuální zpracování a to jak ve veřejném, tak soukromém sektoru[12]. Ačkoliv jsou Pravidla nezávazným dokumentem, systematická úprava ochrany osobních údajů posloužila jako referenční rámec pro budoucí národní zákony i mezinárodní smlouvy.

Prvním mezinárodně právně závazným dokumentem zabývajícím se ochranou osobních údajů byla Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních údajů, která byla přijata Radou Evropy v roce 1981[13]. Úmluvě 108 předcházely dvě rezoluce na ochranu osobních údajů přijaté v rámci Rady Evropy Výborem ministrů v letech 1973 a 1974. Cílem těchto rezolucí bylo zjistit, zda Úmluva z roku 1950 poskytuje dostatečnou

[8] NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). Str. 16. ISBN 978-80-7478-665-5 citováno z ALLEN, A. L. Genetic Privacy: Emerging Concepts and Values. In ROTHSTEIN, M. A. (ed.) Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era. New Haven, CT: Yale University Press, 1997, Str. 31–59.
[9] NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). Str. 8. ISBN 978-80-7478-665-5.
[10] Anglicky Organisation for Economic Co-operation and Development, dále také jako „OECD".
[11] Anglicky Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, dále také i jako „pravidla OECD".
[12] Čl. 2 pravidel OECD.
[13] dále také i jako „Úmluva 108".

ochranu práva na soukromí v návaznosti na rozvoj technologií. Závěrem těchto rezolucí bylo, že ochrana dostatečná není. I když rezoluce obsahovaly vodítka a doporučované principy, jednalo se pouze o nezávazné dokumenty.

Úmluva 108 je aplikovatelná na veškeré zpracování údajů prováděné jak soukromým, tak veřejným sektorem, takže se vztahuje i na justiční a donucovací orgány. Chrání jednotlivce před zneužíváním, které může doprovázet shromažďování a zpracování osobních údajů, a zároveň usiluje o regulaci předávání údajů do zahraničí.[14] Jak napovídá úplný název, Úmluva 108 upravuje především automatizované zpracování[15] s možností rozšířit ochranu na manuální zpracování ve vnitrostátním právu. Vzhledem k tomu, že je Úmluva 108 prvním závazným dokumentem, je nutné zmínit i důležitost zakotvených zásad, které myšlenkově navazují na princip ochrany soukromí. Mezi tyto zásady patří především zásada legitimity, účelnosti, přiměřenosti, přesnosti, omezení uložení a zásada bezpečnosti.[16] Vzhledem k ratifikaci Úmluvy 108 všemi členskými státy Evropského společenství se její zásady staly východiskem pro pozdější evropské předpisy a i pro národní úpravu členských států. I když byla Úmluva 108 přijata Radou Evropy, není její přijetí limitované pouze na její členské státy[17].

V roce 2001 byl k Úmluvě 108 přijat dodatkový protokol, který upravil předávání osobních údajů do zemí, které nejsou stranami Úmluvy 108 („třetích zemí"). Předávání osobních údajů do třetích zemí je v rámci dodatkového protokolu možné pouze za předpokladu, že třetí země poskytne dostatečnou úroveň ochrany osobních údajů.

1.3. Národní úpravy ochrany osobních údajů v Evropě ve 20. století

Prvním státem, který ve 20. století přijal zákonnou úpravu ochrany osobních údajů, bylo Německo, a to konkrétně federální stát Hesse, který v roce 1970 přijal zákon s názvem Datenschutz[18]. Tento zákon reagoval na technologický pokrok spojený především s rozvojem počítačů a v návaznosti na něj reguloval automatické zpracovávání osobních údajů

[14] Agentura Evropské unie pro základní práva, Příručka evropského práva v oblasti ochrany údajů, Úřad pro publikace Evropské unie 2014, Str. 16. ISBN 978-92-871-9933-1.
[15] Automatickým zpracováním jsou podle čl. 2 Úmluvy 108 zpracování, které jsou uskutečňovány zcela nebo zčásti pomocí automatizovaných postupů. Těmito postupy jsou: ukládání na nosiče dat, provádění logických a aritmetických operací s těmito daty, jejich změna, výmaz vyhledávání nebo rozšiřování.
[16] Čl. 5 a čl. 7 Úmluvy 108.
[17] Nečlenské země, které ratifikovaly Úmluvu 108: Uruguay, Mauritius, Senegal, Tunisko.
[18] V českém překladu jako „ochrana údajů".

ve veřejných záznamech. Datenschutz je z hlediska historického vývoje ochrany osobních údajů důležitý také zavedením prvních práv subjektu údajů, jako je například právo na opravu. Navíc byla také zavedena institucionální kontrola nad dodržováním tohoto zákona, a to ve formě Datenschutzbeauftragter.[19]

Dalším průkopníkem ochrany osobních údajů bylo Švédsko, které v roce 1973 přijalo zákon s názvem Datalag[20]. Datalag byl cílen na ochranu osobních údajů v databankách, a to jak ve veřejných, tak i v soukromých. Švédský zákon na rozdíl od německého zákona přímo spojoval ochranu osobních údajů se základními právy. [21]

Po Německu a Švédsku následovaly další státy, které přijaly národní úpravy ochrany osobních údajů. Za zmínku stojí určitě Francie nebo další Skandinávské státy, jako je Dánsko a Norsko. Tyto národní úpravy pak zapříčinily postupné uznávání problémů spojených s automatickým zpracováváním a postupně vedly až k národním úpravám na ústavní úrovni[22].

Na konci 20. století byl vývoj ochrany osobních údajů spojen především s angažovaností mezinárodních organizací a se snahou o úpravu pomocí mezinárodních smluv a jiných instrumentů.

1.4. Vývoj ochrany osobních údajů v rámci Evropského hospodářského společenství a Evropské unie

Ochranou osobních údajů se začalo Evropské hospodářské společenství zabývat už v 70. letech 20. století, a to opět především z důvodu technologického pokroku a možnosti automatického zpracování. Komise Evropského hospodářského společenství vyjádřila v roce 1973 důležitost ochrany osobních údajů v zásadách společenství o zpracování údajů[23] a zájem co nejdříve stanovit jednotný postoj k ochraně osobních údajů. Snažila se tak předejít možnému konfliktu

[19] GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 57. ISBN 3319050222. Datenschutzbeauftragter v českém překladu jako „komisař pro ochranu údajů".
[20] V anglickém překladu jako „Data Act".
[21] GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 70. ISBN 3319050222.
[22] Portugalsko bylo prvním státem, které ústavně zakotvilo právo na ochranu údajů z GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 66, ISBN 3319050222.
[23] V anglickém překladu jako Community policy on data processing.

národních úprav a zvýšené náročnosti harmonizace v budoucnu[24]. V návaznosti na to byly v letech 1975 a 1976 přijaty dvě rezoluce Evropského parlamentu[25]. V nich členové Parlamentu vyjádřili obavu z konfliktních národních úprav a vyzvali Komisi, aby začala pracovat na právní úpravě v rámci Evropského hospodářského společenství. Komise na tyto rezoluce zareagovala zahájením neformálního dialogu se členskými státy o možné harmonizaci a zároveň dala podmět k vypracování studií týkajících se možností zabezpečení ochrany osobních údajů. V roce 1979 následovala další rezoluce Evropského parlamentu, která rozšířila rozsah předmětu ochrany i na zpracování, která nejsou automatizovaná a v rámci doporučení se pokusila zformulovat i konkrétní principy. Komise však ani po této rezoluci nezačala pracovat na žádném návrhu odvolávajícím se na přijetí Úmluvy 108 Radou Evropy. Po přijetí Úmluvy 108 v roce 1981 vyjádřila Komise k této Úmluvě pozitivní postoj a konstatovala její vhodnost jako výchozího právního dokumentu pro budoucí harmonizační úpravu v rámci Evropského společenství. Komise přijala již v roce 1981 doporučení k Úmluvě 108[26], ve kterém vyzvala všechny členské státy k ratifikaci Úmluvy do konce roku 1982.

1.4.1. Schengenský informační systém

V roce 1985 uzavřely Francie, Belgie, Německo, Nizozemsko a Lucembursko Schengenskou smlouvu, jejímž cílem bylo umožnit zavedení společného hraničního režimu. Schengenská smlouva předpokládala přijetí prováděcí úmluvy, ve které měly být specifikovány konkrétní podmínky pro otevření hranic mezi smluvními státy. Schengenská prováděcí úmluva[27] byla přijata v roce 1990 a zřídila tzv. Schengenský informační systém. Schengenský informační systém spočívá v bezpečnostní databázi, ve které jsou shromažďovány informace o osobách i věcech překračujících hranice Schengenského prostoru a obsahuje tedy velké množství osobních údajů. Schengenská prováděcí úmluva však na ochranu osobních údajů pamatovala a ochranu osobních údajů upravuje[28]. Nařizuje smluvním stranám přijmout náležitá opatření,

[24] GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 119. ISBN 3319050222.
[25] OJ C60/48, Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing and OJ C100/27, Resolution of the European Parliament of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing.
[26] 81/679/EEC: Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data.
[27] Úmluva k provedení Schengenské dohody ze dne 14. června 1985, uveřejněna v Úředním věstníku EU L 239, 22/09/2000 S. 0019 – 0062.
[28] Tamtéž, kapitola 3 - ochrana osobních údajů a zabezpečení údajů v schengenském informačním systému

která se úrovní ochrany rovnají požadavkům plynoucím z Úmluvy 108. Ve svém článku 114 například ustanovuje povinnost smluvním stranám určit kontrolní orgán. Ten má za povinnost kontrolovat soubor údajů vnitrostátní součásti Schengenského informačního systému a ověřovat to, zda zpracování a využívání údajů uložených v Schengenském informačním systému neporušuje práva dotyčné osoby.

Pro přesnost je nutné dodat, že Schengenský informační systém se na začátku vyvíjel mimo Evropské společenství v rámci mezivládní spolupráce. Součástí prvního pilíře se Schengenský informační systém stal v roce 1999, kdy vstoupila v platnost Amsterdamská smlouva.

1.4.2. Ochrana osobních údajů v primárním právu Evropské unie

Ochrana osobních údajů byla v primárním právu pevně zakotvena až s přijetím Smlouvy o EU v roce 1992. Smlouva o EU ve svém článku 6 stanovuje, že Unie je založena na zásadách svobody, demokracie, dodržování lidských práv a základních svobod, právního státu a zásadách, které jsou společné členským státům. Dále článek uvádí, že Unie ctí základní práva zaručená Evropskou úmluvou o ochraně lidských práv a základních svobod, pod která spadá i právo na soukromí a z něho odvozené právo na ochranu osobních údajů. Právo na ochranu osobních údajů je pak dále zakotveno i v článku 16 Smlouvy o fungování Evropské unie[29] a v Listině základních práv Evropské unie.

Listina základních práv Evropské unie byla vyhlášena v roce 2000 na mezivládní konferenci v Nice ve formě deklarace a nebyla tedy právně závazná. Právně závaznou se stala až vstupem Lisabonské smlouvy v platnost v roce 2009. Lisabonská smlouva stanovila v pozměněném článku 6 Smlouvy o EU, že Listina základních práv EU má stejnou právní sílu jako Smlouva o EU a SFEU. Listina tedy není častí zakládajících smluv, ale z právního hlediska je na stejné úrovni. Pro ochranu osobních údajů je v Listině důležitý článek 7 a článek 8. Článek 7 říká, že každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace. Tento článek je téměř doslova přejatý z Úmluvy o ochraně lidských práv a základních svobod z roku 1950 s výjimkou toho, že se právo na respektování korespondence zaměnilo za právo na respektování komunikace z důvodu širší působnosti této formulace.

[29] Dále také jako „SFEU“.

Článek 8 explicitně upravuje, že každý má právo na ochranu osobních údajů, které se ho týkají. Osobní údaje mohou být podle článku 8 zpracovávány přesně a pouze pro výslovně stanovené účely a na základě souhlasu nebo zákonem oprávněného důvodu. Subjekt údajů musí mít vždy možnost přístupu ke svým osobním údajům a právo na jejich opravu. Je nutné dodat, že Listina upravuje právo na ochranu osobních údajů zvlášť a ne v rámci práva na soukromí. Úmluva 108 a i v té době již přijatá směrnice 95/46/ES odkazují na ochranu osobních údajů ve spojitosti s ochranou základních práv a svobod fyzických osob, a to konkrétně právě s právem na soukromí. Je možné, že byla při psaní Listiny brána v potaz skutečnost, že některé členské státy odkazují ve svých národních ústavních zákonech na ochranu soukromí a některé zmiňují konkrétně právo na ochranu osobních údajů[30]. Nicméně tato úprava vznesla otázku, v jakém vztahu tyto dva články jsou a jakým způsobem by se subjekt údajů měl svých práv dovolávat.

1.4.3 Směrnice 95/46/EC

V roce 1990 vydala Komise dvě důležitá sdělení ve spojitosti s ochranou osobních údajů. Prvním z těchto sdělení byl návrh směrnice rady týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů[31]. Druhé sdělení obsahovalo návrh na směrnici rady týkající se ochrany osobních údajů a soukromí ve veřejných telekomunikačních sítích[32]. Komise tímto upozorňovala na stále trvající problém odlišných národních úprav ochrany osobních údajů, stejně tak jako na potřebu konkretizovat a rozšířit zásady práva na soukromí uvedené v Úmluvě 108. Ve znění návrhu směrnice uvedla Komise jako hlavní důvod pro přijetí především nutnost zabezpečit základní práva a svobody fyzických osob, a to především právo na soukromí a s ním související právo na ochranu osobních údajů. Dalším důvodem pak byla potřeba zabezpečit volný pohyb osobních údajů v rámci plánovaného vnitřního trhu.[33] Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[34] byla přijata v roce 1995

[30] GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 199. ISBN 3319050222 citace z MARTÍNEZ MARTÍNEZ, RICARD, Una aproximación crítica a la autodeterminación informativa. Madrid: Thomson Civitas 2004, Str. 219.

[31] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (90/C 277/03).

[32] Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks (90/C 277/04).

[33] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (90/C 277/03), odůvodnění 1 a 2.

[34] Dále také i jako „směrnice 95/46/ES“.

v návaznosti na první výše uvedené sdělení Komise. Tato Směrnice se stala základním právním dokumentem sekundárního práva ochrany osobních údajů v Evropském společenství. Na rozdíl od Úmluvy 108, která upravovala pouze automatizované zpracování osobních údajů, se směrnice 95/46/ES vztahuje i na zpracování neautomatizované. V rámci Úmluvy 108 mohly smluvní strany pouze dobrovolně přijmout pomocí dodatkového protokolu, že se na ně bude vztahovat i zpracování neautomatizované. Některé smluvní strany včetně České republiky dodatkový protokol přijaly, ne však všechny.

Jak Úmluva 108, tak i směrnice 95/46/ES poskytuje ochranu pouze fyzickým osobám, a nikoliv osobám právnickým[35]. Věcná působnost směrnice 95/46/ES je omezena na činnosti vnitřního trhu a nespadá do ní zejména spolupráce policie, otázky bezpečnosti státu a záležitosti trestního soudnictví. Tyto oblasti mají vlastní právní úpravu ochrany osobních údajů. Mimo působnost jsou také vyloučena všechna zpracování, která jsou prováděna fyzickou osobou pro výkon výlučně osobních či domácích činností. Směrnice 95/46/ES měla rozšířit a konkretizovat zásady stanovené v Úmluvě 108, jak i deklarovala ve svém odůvodnění. V něm říká: "…Zásady ochrany lidských práv a svobod, zejména práva na soukromí, obsažené v této směrnici upřesňují a rozšiřují zásady obsažené v Úmluvě Rady Evropy ze dne 28. ledna 1981 o ochraně osob s ohledem na automatizované zpracování osobních údajů"[36]. Avšak o zásadách se směrnice 95/46/ES zmiňuje pouze ve svém článku 6 ve spojitosti s kvalitou údajů, který je svým obsahem téměř totožný s článkem 5 Úmluvy 108, jehož zásady měla směrnice upřesnit a rozšířit. Podle směrnice 95/46/ES se tedy stejně jako podle Úmluvy 108 musí osobní údaje zpracovávat korektně a zákonným způsobem. Musí být shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely. Zpracovávané osobní údaje musí být vždy přiměřené k účelu, přesné a aktualizované. Osobní údaje by dále neměly být zpracovány déle, než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány nebo dále zpracovávány[37]. Stejně jako Úmluva 108 i směrnice 95/46/ES vymezuje zvláštní kategorie osobních údajů. Zvláštní kategorie osobních údajů jsou citlivé osobní údaje, které podléhají z důvodu většího rizika případného zneužití větší ochraně. Jedná se zejména o údaje vztahující se k rasovému či etnickému

[35] Podle čl. 3 odst. 2 písm. b) Úmluvy 108 však může smluvní strana rozšířit působnost i na právnické osoby přijetím dodatkového protokolu.
[36] Odůvodnění 11 směrnice 95/46/ES.
[37] Čl. 6 směrnice 95/46/ES.

původu, politickým názorům, náboženskému nebo jinému přesvědčení, údaje týkající se zdraví nebo sexuálního života, ale i údaje ve spojitosti s odsouzením za protiprávní jednání. Směrnice 95/46/ES na rozdíl od Úmluvy 108 přidává mezi zvláštní kategorie i údaje o etnickém původu a informace o odborové příslušnosti. Pro pozdější referenci bych také rád zmínil, že směrnice 95/46/ES upravovala 6 právních titulů, na základě kterých je možné osobní údaje zpracovávat. Jedná se o souhlas, plnění smlouvy, jejíž smluvní stranou je nebo bude subjekt údajů, plnění právní povinnosti, která se na správce vztahuje, ochranu životně důležitých zájmů, vykonání úkolu ve veřejném zájmu nebo výkon veřejné moci a jako poslední tzv. oprávněný zájem[38]. Směrnice 95/46/ES upravuje i práva subjektů údajů ve vztahu ke zpracovávání jejich osobních údajů. Subjekt údajů by měl být vždy minimálně obeznámen s totožností správce, s účely zpracovávání a s existencí svých práv. Směrnice 95/46/ES umožňuje subjektu údajů uplatnit právo na přístup ke svým osobním údajům, právo vznést námitku k některým druhům zpracování a právo nebýt subjektem rozhodnutí, které je založené na automatizovaném zpracování osobních údajů. Subjekty údajů mají navíc nově právo obrátit se na nezávislý orgán dozoru, jehož založení je pro členské státy podle směrnice 95/46/ES povinnost. V době přijetí směrnice 95/46/ES měly sice mnohé státy už vlastní národní úpravu zohledňující ochranu osobních údajů, ale ne vždy už měly institucionální dozor, který by byl garantem dodržování povinností z těchto zákonů plynoucích. Příkladem může být například Česká a Slovenská federativní republika, která sice už v roce 1992 přijala zákon 256/1992 Sb. O ochraně osobních údajů v informačních systémech, nezávislý orgán dozoru však ale nezavedla. Tento zákon navíc nepředpokládal ani žádné sankce za nedodržování povinností, a tak nebyl v praxi dodržován a měl spíše deklaratorní povahu. Směrnice 95/46/ES zřizuje kromě povinných orgánů dozoru i tzv. pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů[39].

WP29 byla ustanovena článkem 29 směrnice 95/46/ES jako nezávislý poradní orgán, který se skládá z národních zástupců dozorových úřadů členských zemí. Většinou se jedná o hlavní představitele těchto úřadů. Cílem WP29 je především sjednotit aplikační praxi směrnice 95/46/ES národních dozorových úřadů a posuzovat veškeré otázky týkající se uplatňování vnitrostátních předpisů přijatých k provedení této směrnice s cílem přispívat k jejich

[38] Čl. 7 směrnice 95/46/ES.
[39] V anglickém překladu jako Working Party 29, dále jen „WP 29“.

jednotnému uplatňování[40]. WP29 není poradním orgánem pouze ve vztahu k uplatňování Směrnice 95/46/ES, ale její působnost se vztahuje k jakékoli otázce týkající se ochrany osob v souvislosti se zpracováním osobních údajů ve Společenství. Za zmínku stojí například vyjádření podpory WP29 v roce 1999 tomu, aby se právo na ochranu osobních údajů stalo součástí základních práv Evropské unie[41]. Ačkoliv Komise není WP29 vázána a její výstupy mají pouze doporučující charakter, Komise ve většině případů postoje WP29 respektuje a s jejich návrhy dále pracuje. Dalším úkolem WP29 je podávat Komisi, Evropskému parlamentu a Radě výroční zprávu o stavu ochrany fyzických osob v souvislosti se zpracováním osobních údajů ve Společenství a třetích zemích a zaujímat stanoviska o úrovni ochrany ve Společenství a ve třetích zemích.

1.4.4. Ochrana soukromí a ochrana osobních údajů v odvětví elektronických komunikací

Ochranou soukromí v elektronické komunikaci se Komise, jak již bylo zmíněno výše, zaobírala již v roce 1990, kdy vydala návrh směrnice rady týkající se ochrany osobních údajů a soukromí ve veřejných telekomunikačních sítích. V tomto návrhu směrnice Komise konstatovala potřebu ochrany soukromí i na úrovni elektronické komunikace, která byla na konci 20. století na vzestupu. V roce 1997 byla na základě návrhu Komise přijata směrnice 97/66/ES o zpracovávání osobních údajů a ochraně soukromí v odvětví telekomunikací[42]. Tato směrnice vychází z pojmosloví a zásad stanovených ve Směrnici 95/46/ES a pouze je poupravuje pro oblast elektronické komunikace. Za zmínku stojí, že vzhledem k oblasti úpravy se na rozdíl od směrnice 95/46/ES vztahuje jak na fyzické, tak i na právnické osoby. Z důvodu rychlého vývoje technologií v oblasti telekomunikací byla už v roce 2002 přijata nová směrnice 2002/58/ES[43], která směrnici 97/66/ES nahradila. Tato směrnice primárně upravuje zpracování dvou druhů údajů. A to údajů tzv. provozních, které směrnice definuje jako jakékoli údaje zpracovávané pro účely přenosu sdělení sítí elektronické komunikace nebo pro jeho účtování, a tzv. lokalizačních údajů, které zase definuje jako jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné

[40] Čl. 30 směrnice 95/46/ES.
[41] GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, v.16, Str. 193. ISBN 3319050222.
[42] Směrnice Evropského parlamentu a rady 97/66/ES ze dne 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikace, dále také i jako „směrnice 97/66/ES".
[43] Směrnice Evropského parlamentu a rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikace, dále také i jako „směrnice 2002/58/ES".

služby elektronické komunikace. Provozovatel veřejné komunikační sítě je podle směrnice 2002/58/ES povinen provozní údaje vymazat nebo anonymizovat, jakmile již nejsou potřebné pro přenos sdělení. Je oprávněn je zpracovávat pouze pro účely účtování a stanovení plateb za propojení. Lokalizační údaje, které nejsou údaji provozními, lze pak zpracovávat pouze za předpokladu, že byly anonymizovány, anebo po předchozím souhlasu uživatele. Směrnice dále zakazuje používání elektronické pošty, faxu a automatických telefonických přístrojů pro přímý marketing, pokud uživatel neposkytl předchozí výslovný souhlas. Nevyžádané sdělení lze posílat pouze zákazníkovi, jehož emailová adresa byla získaná v souvislosti s prodejem výrobku nebo služby, a za předpokladu, že má zákazník vždy možnost vyjádřit nesouhlas se zasíláním nevyžádaného sdělení.

Další směrnice, která byla přijata ve spojitosti s elektronickou komunikací byla směrnice 2006/24/ES[44], která upravuje dobu uchování údajů. Ačkoliv doba uchování údajů byla uvedena výše ve spojitosti se zpracováním provozních a lokalizačních údajů, směrnice 2002/58/ES ve svém článku 15 umožňuje členským státům přijmout právní opatření umožňující zadržení údajů na omezenou dobu z důvodu zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému. Odůvodnění směrnice 2006/24/ES vyjadřuje podporu k uchovávání osobních údajů k výše zmíněným účelům. Navíc konstatuje, že právní opatření přijatá členskými státy se značně liší, a že je proto nutné touto směrnicí přijmout harmonizační úpravu, která bude v souladu s právními předpisy Evropské unie. Směrnice 2006/24/ES podrobně popisuje kategorie uchovávaných údajů a stanovuje dobu uchování na nejméně šest měsíců a nejvýše dva roky ode dne komunikace[45].

1.4.5. Reforma ochrany osobních údajů v Evropské unii

Od přijetí směrnice 95/46/ES, která se stala základním právním nástrojem ochrany osobních údajů v Evropské unii, uplynula dlouhá doba. Během tohoto období se z důvodu zlepšení technologií a zvýšené úrovně globalizace exponenciálně zvětšilo množství zpracovávaných

[44] Směrnice Evropského parlamentu a rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, dále také i jako „směrnice 2006/24/ES“.
[45] Směrnice 2006/24/ES byla v roce 2014 Soudním dvorem Evropské unie prohlášena za neplatnou z důvodu překročení zásady proporcionality u čl. 7, 8 a čl. 52 odst. 1 Listiny základních práv Evropské unie. Spojené věci C-293/12 a C-594/12, Rozsudek Soudního dvora Evropské unie ze dne 8. dubna 2014, ECLI:EU:C:2014:238.

osobních údajů. Jako první na tuto situaci reagovala WP29 společně s pracovní skupinou pro policii a justici. 1. prosince 2009 zveřejnily studii s názvem „Future of Privacy", ve které upozorňují Komisi na potřebnost přijetí nové právní úpravy v oblasti ochrany osobních údajů. Komise pak v návaznosti na tuto studii předkládá v listopadu 2010 strategii o posílení předpisů EU o ochraně údajů, ve které jsou obsaženy návrhy na posílení práv jednotlivců. Komise upozorňuje například na potřebu zajistit „právo být zapomenut". Dále je ve strategii vyjádřen cíl zajistit vysokou úroveň ochrany údajů předávaných za hranice EU a potřeba revidovat právní předpisy týkající se ochrany údajů v oblasti policie. Komise také konstatuje, že z důvodu rozdílnosti prováděcích právních předpisů EU o ochraně údajů není často zcela jasné, jaké předpisy jsou platné. Dochází tak podle Komise ke zbytečné administrativní zátěži podniků a zároveň nejsou zajištěny rovnocenné podmínky jednotného trhu[46]. Jinými slovy je tedy podle Komise potřeba jak reforma, tak i harmonizace oblasti ochrany osobních údajů. Z těchto důvodů předložila Komise 25. ledna 2012 návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů[47]. Za nejvhodnější právní nástroj nepovažuje Komise tentokrát směrnici, ale nařízení. Na základě přímé použitelnosti nařízení podle článku 288 SFEU se zamezí právní nejednotnosti a zavedením harmonizovaného souboru pravidel se zvýší právní jistota.[48] Nicméně je nutné dodat, že GDPR předpokládá určité derogační klauzule v adaptačních zákonech.

Evropský parlament vyjádřil podporu návrhu GDPR v březnu v roce 2014, když přijal upravený návrh GDPR v prvním čtení. [49] Následovalo přijetí návrhu Radou EU v červnu v roce 2015 a začala fáze vyjednávání v rámci trialogu mezi Evropskou komisí, Radou EU a Evropským parlamentem. Finální verze GDPR byla dohodnuta 15. prosince 2015 a následně schválena Radou EU a Evropským parlamentem během dubna stejného roku. GDPR bylo publikováno v úředním věstníku Evropské unie 4. května a stalo se účinné 25. května 2018. Podrobnější informace o GDPR jsou zmíněny v následujících kapitolách této diplomové práce.

[46] IP/10/1462, strategie, jak posílit předpisy EU o ochraně údajů ze dne 4. listopadu 2010.
[47] 2012/0011 (COD), Proposal for a regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), dále jen „GDPR".
[48] Tamtéž, Str. 5.
[49] Návrh GDPR dosáhl při plenárním zasedání Evropského parlamentu velké podpory s 621 hlasy pro a pouze 10 proti (22 poslanců se zdrželo hlasování).

GDPR není jediným nařízením, které si klade za cíl zvýšit ochranu osobních údajů v Evropské unii. Neméně důležité je také nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích[50], které ruší směrnici 2002/58/ES. Směrnice 2002/58/ES upravovala ochranu osobních údajů v rámci elektronické komunikace, ale i přes její novelizaci v roce 2009[51] nedrží tato směrnice krok se současným technologickým vývojem v této oblasti. Konkrétně jde například o moderní formy komunikace, jako je třeba Messenger, WhatsApp nebo Skype, které v době přijetí směrnice buď vůbec neexistovaly, anebo nebyly používány v takovém rozsahu, v jakém jsou používány dnes. Novelizace z roku 2009 přinesla však velmi důležitou změnu ve vztahu k ukládání cookies v zařízeních uživatele. Dle novelizace je před uložením cookies vždy nutný souhlas uživatele, což zavádí tzv. opt-in režim a opouští opt-out režim, který byl zaveden směrnicí 2002/58/ES. Nutné je však dodat, že Česká republika tuto změnu v implementačním zákoně nereflektovala a zachovala režim opt-out[52]. Směrnice jako norma evropského práva neplatí přímo a přímý účinek nebyl dovozen, a tak v České republice nejsou správci v tuto chvíli nuceni zavádět opt-in režim, který je pro ně mnohem méně příznivý. Čeští správci tak sice nyní používají tzv. „cookies oznámení“, ale v rámci něj ukládání cookies pouze uživateli oznamují a nedávají mu možnost s ukládáním nesouhlasit. Nařízení má na rozdíl od směrnice přímý účinek a s účinností E-privacy bude tak i pro české správce platit opt-in režim. V členských státech, kde byla novelizace implementována správně a opt-in režim byl zaveden, byl uživatel nicméně v podobné situaci. Správci stačilo, aby podmínil vstup na své webové stránky souhlasem s ukládáním cookies a uživatel tak neměl možnost se v případě potřeby danou stránku navštívit svobodně rozhodnout. Ze schváleného znění návrhu e-Privacy vyplývá, že uživatelé by měli mít možnost si v nastavení každého internetového prohlížeče vybrat, s jakým uchováním cookies souhlasí a s jakým už nikoliv. Otázkou je, jestli takováto právní úprava nepovede ze strany správců k zavedení nového druhu oznámení nebo vyskakovacích oken, ve kterých budou své návštěvníky žádat o udělení výjimky pro jejich stránky. Souhlas s uchováváním cookies už nebude moci být podle nové úpravy podmíněný možností návštěvy dané stránky a vzhledem k důležitosti uchovávání cookies, například pro oblast online

[50] Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES, dále jen „ePrivacy“.
[51] Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009.
[52] Čl. 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů.

marketingu, se dá podle mého názoru očekávat, že přesně k výše uvedenému jednání ze strany správců dojde. Původní ambice pro e-Privacy byla, že vstoupí v účinnost společně s GDPR, tedy 25. května 2018. V době odevzdání diplomové práce však Evropský parlament a Rada EU nedospěla k finálnímu znění a je tedy očividné, že e-Privacy vstoupí v účinnost nejdříve v roce 2019, ale vzhledem k předpokládané delší legisvakanční lhůtě spíše i později.

GDPR stanovuje novou úroveň ochrany osobních údajů a na tuto úroveň musí být uvedeny i unijní předpisy upravující ochranu osobních údajů. Samotné znění GDPR předpokládá, že nařízení 45/2001 bude uzpůsobeno zásadám a pravidlům zavedeným GDPR.[53] Komise vydala v lednu 2017 návrh nového nařízení, které uvádí zpracování osobních údajů v orgánech a institucích EU v souladu s GDPR. V listopadu 2017 se tento návrh dostal do fáze trialogu a v době odevzdání této diplomové práce nebylo nařízení ve finálním znění ještě schváleno. Instituce Evropské unie tedy opět nepůjdou příkladem a přísnější úprava ochrany osobních údajů pro ně bude účinná minimálně několik měsíců po účinnosti GDPR.

[53] Odůvodnění 17 GDPR.

2. Nová úprava ochrany osobních údajů v pojetí GDPR

GDPR by se bezpochyby dalo označit za doposud nejambicióznější právní úpravu ochrany osobních údajů v Evropě. GDPR vychází sice ze zásad a povinností upravených ve směrnici 95/46/ES, ale zavádí i celou řadu pravidel nových, která ve svém souhrnu zaručují subjektům údajů mnohem větší kontrolu nad svými osobními daty, než tomu bylo doposud. Na druhé straně GDPR ukládá správcům a zpracovatelům mnohem více povinností, které pro ně znamenají větší administrativní a finanční zátěž. V případě porušení povinností hrozí správcům a zpracovatelům výrazně vyšší sankce než za úpravy původní, a to bez ohledu na to, jsou-li velkou korporací se zpracováváním osobních údajů ve velkém rozsahu, nebo zdali jsou malým e-shopem s malou databází. Evropská unie tedy vydává jasný signál, že ochrana osobních údajů fyzických osob je důležitým právem, které si vyžaduje přísnější úpravu. Na následujících stránkách budou popsány vybrané nejdůležitější změny ochrany osobních údajů a srovnány s úpravou ve směrnici 95/46/ES. Vzhledem k rozsahu diplomové práce jsem vybral změny, které se mi zdály být před účinností GDPR velmi diskutované, a také ty, které byly vhodné k srovnání s původní úpravou.

2.1. Pojem osobní údaj a jeho vymezení

Vymezení samotného pojmu osobní údaj je pro novou úpravu klíčové, protože GDPR je aplikovatelné pouze na ty údaje, které spadají pod její definici. Definice osobního údaje byla široká již v původní úpravě ve směrnici 95/46/ES a GDPR toto pojmové vymezení převzalo a dále rozšířilo. GDPR přejalo základní vymezení, které říká, že osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Fyzickou osobu je možno považovat za identifikovanou, pokud ji správce nebo zpracovatel sám dokáže přímo odlišit od ostatních osob, a to za využití údajů, které má k dispozici. Identifikovatelnou osobou je fyzická osoba tehdy, pokud ji buď správce či zpracovatel nebo kdokoliv další dokáže identifikovat za využití dalších údajů, které má v držení on sám, které jsou veřejně dostupné, nebo které má k dispozici další subjekt[54]. GDPR rozšiřuje identifikátory, na základě kterých lze identifikovatelnou fyzickou osobu identifikovat. Konkrétně identifikátory rozšiřuje o lokační

[54] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, Str. 78-79. ISBN 978-80-7552-765-3.

údaje a síťový identifikátor. Mezi zvláštní kategorie údajů[55] pak nově zahrnuje genetické, biometrické a osobní údaje dětí.

2.1.1. Lokační údaje

Lokační údaje jsou sice v GDPR zahrnuty nově v definici osobních údajů, nejedná se ale ve skutečnosti o žádnou novinku. V první kapitole této diplomové práce bylo zmíněno, že směrnice 2002/58/ES upravující ochranu osobních údajů elektronických komunikací, zavedla ochranu lokalizačních údajů. Lokalizační údaje se s lokačními údaji v GDPR sice shodují, ale vztahují se na zpracování údajů pouze v rámci elektronické komunikace. Nicméně lokační data ze své podstaty vždy souvisí s identifikovanou nebo identifikovatelnou fyzickou osobou a jsou tedy osobními údaji, a to jak v rámci GDPR, tak již podle původní definice směrnice 95/46/ES[56]. Ve spojitosti s lokačními údaji bude podle mého názoru největší změnou přísnější udělení souhlasu se zpracováním dat a s novými povinnostmi plynoucími z nových práv subjektu údajů. Mnohé mobilní aplikace například sledují zařízení automaticky bez předchozího souhlasu, což už podle GDPR nebude dále možné. Správci budou muset do nastavení svých aplikací také promítnout právo na výmaz, což může být pro mnohé technologicky náročné.

2.1.2. Síťový identifikátor

GDPR ve svém znění nezavádí definici tohoto nového pojmu, ale jeho vymezení je přiblíženo v odůvodnění 30, které za síťové identifikátory zmiňuje například adresy internetového protokolu, cookies, nebo jiné identifikátory využívající rádiovou frekvenci. Obecně nám toto odůvodnění říká, že o síťový identifikátor půjde tehdy, zanechá-li za sebou subjekt údajů na síti stopy, jež mohou být pomocí jedinečného identifikátoru využity k jejich profilování a identifikaci. Opět je nutné zmínit, že síťové identifikátory nebyly zcela neznámé i původní úpravě. Rozsudek *Breyer*[57] rozšířil definici osobních údajů směrnice 95/46/ES i na dynamické IP adresy. Soudní dvůr Evropské unie v tomto rozsudku došel k závěru, že ačkoliv provozovatel webové stránky nemůže sám o sobě identifikovat subjekt údajů pouze na základě IP adresy, je

[55] V českém právním řádu je používán výraz citlivý údaj, ale v rámci zachování pojmosloví GDPR bude v této diplomové práci používán výraz zvláštní kategorie osobních údajů.
[56] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion on the use of location data with a view to providing value-added services, November 2015, Str. 3.
[57] C-213/15, Rozsudek Soudního dvora Evropské unie ze dne 19. října 2016, Patrick Breyer proti Spolkové republice Německo, ECLI:EU:C:2016:779.

dostačující, že ho může identifikovat za pomoci součinnosti poskytovatele internetových služeb. Kontaktování poskytovatele služeb považoval tedy soud v tomto rozhodnutí za rozumnou a reálnou možnost, jak subjekt údajů bez většího úsilí identifikovat.[58]

Zpracování dat získaných pomocí cookies je momentálně upraveno směrnicí 2002/58/ES a nově bude regulováno nařízením e-Privacy, které bude vůči GDPR zvláštní právní úpravou. Zahrnutí cookies mezi osobní údaje znamená aplikaci přísnější úpravy GDPR, což bude v praxi pro správce internetových stránek znamenat přísnější požadavky na získávání souhlasu. Pro správce tak bude například složitější získávat souhlas k shromažďování informací z koncových zařízení koncových uživatelů, včetně informací o softwaru a hardwaru[59].

2.1.3 Biometrické a genetické údaje

Biometrické a genetické údaje nebyly sice ve směrnici 95/46/ES označeny explicitně za osobní údaje, ale vzhledem k jejich podstatě nebylo jejich zařazení mezi osobní údaje nikdy rozporováno. GDPR zahrnuje biometrické a genetické údaje mezi zvláštní kategorie osobních údajů a zároveň je i definuje[60]. Český zákon o ochraně osobních údajů[61] již biometrické a genetické údaje mezi zvláštní kategorie zahrnuje, ale vzhledem k přísnější úpravě zpracování zvláštních kategorií osobních údajů v GDPR bude mít tato změna pro správce své důsledky. U zvláštních kategorií osobních údajů není například možné využít právního titulu oprávněného zájmu, bude tedy v praxi nejčastěji vyžadován právní titul souhlasu. Zaměstnavatel tak může například zpracovávat běžné osobní údaje za účelem evidence docházky na základě oprávněného zájmu, ale k zpracovávání biometrických údajů, například pro kontrolu vstupu na pracoviště, už bude potřebovat souhlas[62]. Pro správce může zpracovávání těchto údajů také znamenat, že se na ně vztáhne nová povinnost vypracovat posouzení vlivu na ochranu

[58] Soudní dvůr Evropské unie vycházel v tomto rozhodnutí z odůvodnění 26 směrnice 95/46/ES. Obsah tohoto odůvodnění byl převzat i v GDPR shodně v odůvodnění 26.
[59] Čl. 8 odst. 1 písm. b), Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES
[60] Čl. 4, odst. 13 a 14 GDPR.
[61] Zákon č. 101/2000 Sb. O ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, dále i jako „zákon o ochraně osobních údajů".
[62] FRANTIŠEK NONNEMANN a MICHAELA SKÁCELOVÁ, Zpracování biometrických údajů ve světle obecného nařízení o ochraně osobních údajů (GDPR) [online], 2017, dostupné z: https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-ve-svetle-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-106028.html

osobních údajů[63], a to i v případě, že nedochází k rozsáhlému zpracování[64]. DPIA je obecně nutné vypracovat, když je pravděpodobné, že zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Podle pokynů WP29 představuje zpracování zvláštních kategorií vysoké riziko a vypracování DPIA by se mělo ve spojitosti s ostatními kritérii vždy zvážit[65]. Zahrnutí biometrických a genetických údajů mezi zvláštní kategorie osobních údajů tedy není pro český právní řád novinkou, ale ve spojení s novou úpravou v GDPR z toho vyplývají pro správce opět nové povinnosti.

2.2. Extrateritoriální působnost

Ze znění směrnice 95/46/ES upravující místní působnost je zřejmé, že zákonodárce EU měl primárně v úmyslu vztáhnout ochranu osobních údajů na zpracování, ke kterým dochází na území některého ze členských států. Je však nutné podotknout, že extrateritoriální působnost GDPR opět není pro ochranu osobních údajů v Evropské unii úplně nová. Článek 4 odst. 1 písm. a) stanovuje, že se směrnice 95/46/ES použije na každé zpracování, které bude prováděno v rámci činností provozovny správce na území členského státu. Evropský soudní dvůr v kontroverzním rozsudku *Google Spain vs. Costeja*[66] ale svým rozhodnutím došel k extenzivnímu výkladu. V něm judikoval, že dceřiná společnost Google Spain, zaměřující se na podporu lokálního prodeje reklam, pod toto ustanovení spadá vzhledem k tomu, že činnost provozovatele vyhledávače a činnost jeho provozovny umístěné v dotčeném členském státě jsou neoddělitelně spojeny[67].

Již u původní úpravy byla tedy extrateritoriální působnost dovozena judikaturou a GDPR ji nově pouze explicitně zahrnuje do samotného ustanovení o místní působnosti. GDPR se podle nového ustanovení vztahuje i na správce a zpracovatele, kteří nejsou usazeni na území EU, pokud jimi prováděné zpracování souvisí buď s nabídkou zboží nebo služeb subjektům údajů v EU nebo pokud dochází k monitorování jejich chování na území EU.

[63] V anglickém překladu jako Data protection impact assessment, dále jen „DPIA“.
[64] Čl. 35 odst. 2 písm. b) GDPR.
[65] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, adopted on 4 April 2017, Str. 11.
[66] C-131/12, Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 13. května 2014 Google Spain SL, Google Inc. proti Agencia Espanola de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317.
[67] Tamtéž, odůvodnění 56.

K oběma těmto případům stanovuje GDPR a judikatura Evropského soudního dvora vodítka. Základem pro určení, zda správce nebo zpracovatel usazený mimo Unii nabízí zboží nebo služby subjektům údajů v EU, je zjištění okolností, za jakých své zboží nebo služby nabízí. V případě, že je na základě těchto skutečností patrný zjevný úmysl zboží nebo služby nabízet subjektům údajů v Unii, pak se na správce nebo zpracovatele působnost GDPR vztahuje. Odůvodnění 23 GDPR uvádí za konkrétní případ zjevného úmyslu používání jazyka nebo měny obecně používaných v jednom nebo více členských státech spolu s možností objednat zboží a služby v tomto jiném jazyce. Další vodítka pak mohou být nalezena v rozsudku Soudního dvora EU[68] z roku 2010, který i když v odlišném kontextu, rozhodoval o tom, co je považováno za přímou činnost podniku v členském státě a co už nikoliv. Za indicie považoval například uvedení telefonického spojení s mezinárodním předčíslím, vynaložení nákladů na službu sponzorovaných odkazů na internetu, použití cizí domény prvního řádu nebo i jen zmínku o mezinárodní klientele složené ze zákazníků s bydlištěm v jiném členském státě. Dále je zajímavé zmínit, že se jedná o nabízení zboží nebo služeb bez ohledu na to, jestli jsou placené nebo zadarmo. Samotné GDPR nedefinuje pojem zboží ani služby, ale u prvně zmíněného lze předpokládat, že bude pojem vykládán v souladu s definicí uvedenou ve směrnici upravující práva spotřebitelů[69]. Vzhledem k tomu, že GDPR nevylučuje žádné typy zboží ani služeb, mělo by se výše zmíněné vztahovat i na takové služby, kterou nejsou zákonné nebo regulované a bez ohledu na to, zdali jsou nabízeny příležitostně nebo nepřetržitě[70].

Druhým případem aplikace extrateritoriální působnosti je situace, kdy správce nebo zpracovatel bude v rámci činnosti zpracování monitorovat chování subjektů údajů na území Unie. Nařízení neuvádí definici monitorování, ale opět aspoň v rámci odůvodnění[71] poskytuje základní vodítka. Odůvodnění se zmiňuje o monitorování ve vztahu ke sledování subjektu

[68] Spojené věci C-585/08 a C-144/09, Rozsudek soudního dvora EU (velkého senátu) ze dne 7. prosince 2010 Peter Pammer proti Reederei Karl Schlüter GmbH & Co. KG a Hotel Alpenhof GesmbH proti Oliver Heller, EU:C:2010:740.

[69] Směrnice Evropského parlamentu a Rady 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů, čl. 2 odst. 3.

[70] ANNI-MARIA TAKA, Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications, Master's Thesis, Uppsala Universitet, 2017, str. 48 citace z JAY, Rosemary. Data protection: law and practice. 4th ed. London: Sweet & Maxwell, 2012. Str. 75. ISBN 0414024966.

[71] Odůvodnění 24 GDPR.

údajů na internetu. Ze systematického výkladu[72] lze vyvodit, že nejde jen o monitorování v prostředí internetu, ale i o monitorování fyzické. K monitorování chování v internetovém prostředí dochází zejména prostřednictvím cookies, IP adresy připojení, MAC adresy zařízení, ze kterého se k internetu přistupuje, nebo geolokačních údajů[73]. Aby však šlo o monitorování, musí podle odůvodnění dojít zároveň k následnému zpracování osobních údajů za účelem profilování nebo behaviorálního marketingu.

Extrateritoriální působnost by se tedy podle výše zmíněného měla aplikovat i na všechny webové stránky, které využívají cílenou reklamu například pomocí trackovacího kódu Pixel od Facebooku nebo jiného obdobného kódu. Z prohlášení ochrany osobních údajů Facebooku je zřejmé, že obdržení souhlasu pro cílenou reklamu bude odpovědností každého správce: "Každá společnost má vlastní zodpovědnost zajistit, aby splňovala obecné nařízení o ochraně údajů a vůbec dodržovala veškeré zákony, které se na ni vztahují. "[74] Povinnosti z GDPR se tedy budou vztahovat na všechny provozovatele webových služeb, kteří využívají cílenou reklamu.

Na závěr je k extrateritoriální působnosti nutné říci, že navzdory ambiciózním širokému vymezení působnosti je zřejmé, že vynutitelnost povinností bude u správců a zpracovatelů usazených mimo území Unie velmi obtížná, ne-li nemožná. Lze podle mého názoru očekávat, že větší společnosti budou novou úpravu GDPR do svého fungování začleňovat ze strachu z vysokých pokut a z obav o svou reputaci. Některé společnosti možná dokonce udělají z GDPR svoji konkurenční výhodu a zlepší dosažením souladu s GDPR svoji image. Nelze však reálně předpokládat, že vymahatelnost bude proveditelná například u menších asijských správců nebo zpracovatelů, kteří o GDPR a možných pokutách ani nebudou vědět.

[72] Pojem monitorování se nevyskytuje pouze v čl. 3 ve vztahu k místní působnosti, ale vyskytuje se například i v čl. 35 (upravující posouzení vlivu na ochranu osobních údajů) a v čl. 37 (upravující pověřence pro ochranu osobních údajů). Z těchto článků je zřejmé, že se nejedná pouze o monitorování na internetu.
[73] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, Str. 72. ISBN 978-80-7552-765-3.
[74] Dostupné z: https://www.facebook.com/business/gdpr

2.3. Princip odpovědnosti

Princip odpovědnosti[75] není v oblasti ochrany osobních údajů ničím revolučním. Poprvé byl explicitně zmíněn v souvislosti s ochranou osobních údajů již v pravidlech OECD vydaných v roce 1980, konkrétně v článku 14. Tento článek říká, že správce by měl být odpovědný za soulad s opatřeními, která provádí principy v těchto pravidlech uvedené. Směrnice 95/46/ES explicitně princip odpovědnosti nezavádí, ale lze jej vyvodit implicitně z povinností stanovených v rámci jednotlivých zásad. GDPR nově princip odpovědnosti explicitně zavádí, a navíc jeho pojetí rozšiřuje, když po správci nově vyžaduje také doložení souladu se všemi povinnostmi. Správce by měl v rámci dodržování zásad především zavést vhodná technická a organizační opatření, dodržovat zásady záměrné a standardní ochrany, a je-li to potřeba, měl by také jmenovat pověřence pro ochranu osobních údajů či provést posouzení vlivu na ochranu osobních údajů. Vzhledem k tomu, že je správce nově povinen tento soulad doložit, bude pro všechny výše vyjmenované složky ochrany klíčová jejich dokumentace. GDPR tak sice ruší povinnou oznamovací činnost zpracování osobních údajů dozorovému úřadu, ale v rámci principu odpovědnosti a povinnosti doložit soulad, ukládá správci novou a mnohem náročnější administrativní povinnost, v rámci níž musí v souvislosti se zpracováním vše dokumentovat. Demonstrace souladu se bude u správců lišit vzhledem k povaze a rizikovosti zpracování, ale bude provázet každého správce. Z výše uvedeného navíc vyplývá, že soulad s principem odpovědnosti nebude pro správce jednorázovou činností, jako tomu bylo za současné úpravy, ale bude se od něj vyžadovat proaktivní a systematický přístup v rámci celé doby zpracovávání osobních údajů. Cílem GDPR je garantovat subjektům údajů větší ochranu, což by bez proaktivního přístupu k plnění principu odpovědnosti nebylo možné vzhledem k tomu, jak dynamickou činností může zpracování v praxi být. Nelze tedy dle mého názoru ani uvažovat o porušení principu proporcionality[76].

2.3.1. Záměrná a standardní ochrana osobních údajů

Záměrná ochrana osobních údajů[77] je nedílnou součástí principu odpovědnosti a v unijním právu nově zavedený koncept ochrany osobních údajů[78]. V rámci záměrné ochrany je správce

[75] Čl. 5 odst. 2 GDPR.
[76] Čl. 5 odst. 4, SFEU.
[77] V anglickém překladu jako „data protection by design".
[78] Čl. 25 odst. 1 GDPR.

povinen k povaze zpracování přijmout vhodná technická a organizační opatření i v přípravné fázi, kdy ještě k samotnému zpracování nedochází. Každý správce by si tedy měl v rámci záměrné ochrany před započetím zpracování rozmyslet, jakým způsobem bude přistupovat k ochraně osobních údajů a jaká technická a organizační opatření bude implementovat. Ve směrnici 95/46/ES záměrná ochrana nebyla zakotvena a mohlo tedy docházet k situacím, kdy správce začal zpracovávat osobní údaje a až následně se začal zabývat vhodnými bezpečnostními opatřeními, což znamenalo, že osobní údaje nebyly v mezidobí vůbec zabezpečeny. V horším případě mohla nastat situace, kdy správce začal se zpracováním, a až pak zjistil, že vhodná ochrana není dosažitelná, a vzhledem k vynaloženým nákladům pokračoval ve zpracování bez vhodného zabezpečení.

Při zavedení technických a organizačních opatření by měl správce přihlížet k řadě faktorů, především k účelu, povaze, kontextu a rozsahu zpracování, stejně tak jako ke stavu techniky a i k nákladům na provedení. V souvislosti se záměrnou ochranou uvádí GDPR jako příklad pouze pseudonymizaci a další opatření je nutné vyvozovat ze základních zásad[79]. V praxi tedy správce musí přijmout taková organizační a technická opatření, aby: a) zpracovával osobní údaje pouze na základě právního titulu, b) byly subjekty údajů o zpracování náležitě informovány, c) nezpracovával více údajů, než je nezbytně nutné, d) zpracovával pouze přesné údaje, e) neuchovával osobní údaje po dobu delší, než je nezbytně nutné, případně aby osobní údaje po uplynutí této doby anonymizoval. Nakonec by měl správce zajistit, že osobní údaje budou chráněny před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením[80]. V rámci principu odpovědnosti by pak správce měl být opět schopen doložit, že při provedení záměrné ochrany zohlednil všechny své povinnosti.

Standardní ochrana osobních údajů[81] je v GDPR upravena ve stejném článku[82] jako ochrana záměrná a její podstata ze záměrné ochrany vychází. Každý správce je bez ohledu na rizikovost zpracování vždy povinen dodržovat obě tyto zásady. Správce by měl v rámci standardní ochrany přijmout technická a organizační opatření, která zaručí, že budou zpracovávány pouze osobní údaje nezbytně nutné pro daný účel. V tomto ohledu se nejedná

[79] Čl. 5 GDPR.
[80] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, Str. 260. ISBN 978-80-7552-765-3.
[81] V anglickém překladu jako „protection by default“.
[82] Čl. 25 odst. 2 GDPR.

o žádnou novinku, jelikož i směrnice 95/46/ES stanovila, že osobní údaje musí být přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány. GDPR v tomto ohledu zvolilo pouze přísnější formulaci a zaměnilo zpracování nepřesahující míru s ohledem na účely za omezení zpracování pro nezbytný rozsah ve vztahu k účelu. K aplikaci standardní ochrany budou relevantní ustanovení e-Privacy, která ale v době odevzdání této diplomové práce neměla schválenou finální podobu, a tak se zde v souvislosti se standardní ochranou omezím pouze na zmínku o ní.

2.4. Souhlas

GDPR stejně jako původní směrnice 95/46/ES upravuje celkem 6 právních titulů, na základě kterých lze zpracovávat osobní údaje, a souhlas je jedním z nich. Podmínky pro získání souhlasu v souladu se směrnicí 95/46/ES nebyly náročné, a tak i přesto, že směrnice žádný právní titul přímo neupřednostňovala, se souhlas stal nejpoužívanějším právním titulem. Zajímavostí navíc je, že zákon o ochraně osobních údajů, který v České republice transponoval směrnici 95/46/ES, zvolil poměrně nešťastnou formulaci, která mohla vyvolat dojem, že je souhlas upřednostňovaným právním titulem a že ostatní tituly jsou spíše zbytkové[83]. I když se za účinnosti směrnice 95/46/ES jednalo o nejpoužívanější právní titul, s příchodem GDPR se situace otáčí a právní titul už nebude kvůli přísnější úpravě využíván tak často jako doposud. Správce by měl vždy zvolit právní titul, který nejvíce odráží skutečnou povahu svého vztahu se subjektem údajů a účelem zpracování. Pokud je souhlas složitý, je to často proto, že je vhodnější jiný právní titul[84].

GDPR nově stanovuje, že souhlas musí být udělen prohlášením či jiným zjevným potvrzením své vůle se zpracováním svých osobních údajů. U udělení souhlasu by nikdy nemělo být pochyb, že byl souhlas skutečně udělen. GDPR nově také ve svém odůvodnění zmiňuje, že mlčení, předem zaškrtnutá políčka nebo nečinnost nelze považovat za platný souhlas. I když směrnice 95/46/ES explicitně nezmiňuje, že mlčení nemůže znamenat souhlas, nejedná se o úplně novou věc. Již v roce 2010 vyjádřila WP29 totožný názor ve vztahu ke směrnici 95/46/ES a ke stejnému názoru dospěla také v roce 2004 ve vztahu k udělení

[83] §5 odst. 2. zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
[84] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017, Právo pro praxi. Str. 134, ISBN 978-80-271-0668-4.

souhlasu pro přímý marketing[85]. Vzhledem k tomu, že pokyny WP29 mají pouze povahu doporučení, je toto pravidlo pevně ustanoveno až v GDPR.

Další zásadní změnou v úpravě souhlasu je vymezení pojmu svobodný souhlas. Směrnice 95/46/ES sice vyžaduje, aby byl souhlas svobodný, ale už dále nerozvádí, co se pod svobodným souhlasem myslí. Článek 7 odst. 4 GDPR nově správci stanovuje povinnost zohlednit skutečnost, zda plnění smlouvy či poskytnutí služby není podmíněno souhlasem, který není k plnění nutný. Jinými slovy by správce měl pro každé své zamýšlené zpracování s odlišným účelem získat samostatný souhlas. Správce by tedy neměl například podmiňovat uzavření smlouvy souhlasem k zasílání obchodního sdělení. Dále dle odůvodnění[86] GDPR by souhlas neměl být považován za svobodný, bude-li mezi správcem a subjektem údajů nerovné postavení. GDPR jako příklad takového postavení uvádí vztah mezi subjektem údajů a orgánem veřejné moci. Dalším častým nerovným postavením bude vztah zaměstnavatele a zaměstnance. GDPR nevylučuje použití souhlasu v nerovném postavení, ale implicitně doporučuje, aby byl zvolen vhodnější právní titul. Subjekt údajů může podle GDPR svůj souhlas kdykoliv odvolat a nesmí mu to být na újmu. Zaměstnavatel by se při odvolání souhlasu zaměstnancem mohl dostat do nelehké situace, a proto by měl spíše zvážit oprávněnost použití opravného zájmu.

Nové povinnosti plynou pro správce i z ustanovení, která požadují, aby byl souhlas informovaný. Opět se nejedná o zcela novou povinnost, ale pouze o její upřesnění. Stejně jako směrnice 95/46/ES blíže neuvedla, co se myslí svobodným vyjádřením souhlasu, tak ani informovaný souhlas dále neupřesnila[87]. GDPR považuje za informovaný takový souhlas, který je poskytnut ve srozumitelném a snadno přístupném znění za použití jasného a jednoduchého jazyka[88]. Správce je povinen informovat subjekt údajů o všech skutečnostech tykajících se zpracování. Zejména by měl subjekt údajů informovat o své totožnosti, účelu zpracování a o možnosti souhlas odvolat. Zároveň by měl být souhlas oddělen od ostatních obchodních podmínek, což nebylo za účinnosti původní úpravy běžnou praxí. Odůvodnění GDPR ukládá správcům povinnost obdržet souhlasy subjektů znovu v případě, kdy jejich získaní nebylo

[85] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 15/2011 on the definition of consent, 13 July 2011 and Opinion 5/2004 on unsolicited communications for marketing purposes under article 13 of Directive 2002/58/EC.
[86] Odůvodnění 43 GDPR
[87] Směrnice 95/46/ES používá místo pojmu informovaný vědomý souhlas.
[88] Odůvodnění 42 GDPR.

v souladu s novými povinnostmi podle GDPR[89]. Správce tedy mohl splnit všechny povinnosti pro obdržení souhlasu podle směrnice 95/46/ES, a přesto se teď bude muset obracet na subjekt údajů se žádostí o souhlas nový. Z tohoto samotného ustanovení lze demonstrovat, jakou důležitost Evropská unie nově klade na ochranu fyzických osob v souvislosti se zpracováním osobních údajů.

Úprava souhlasu v GDPR neobsahuje úplně nové povinnosti, ale rozpracovává původní ustanovení a ve svém souhrnu zcela mění pojetí a využitelnost tohoto právního titulu.

2.5. Práva subjektu údajů

GDPR rozšiřuje ochranu osobních údajů fyzických osob také pomocí posílení práv subjektu údajů, kterému umožní mít nad svými údaji mnohem větší kontrolu. GDPR navazuje na práva subjektů upravená směrnicí 95/46/ES, která konkretizuje a zároveň zavádí práva úplně nová. Subjekt údajů má při jakémkoliv zpracování především právo být o zamýšleném zpracování náležitě informován. Do této povinnosti se promítá zásada transparentnosti, v jejímž rámci musí správce splnit informační povinnost. Úprava této povinnosti se pro správce od úpravy ve směrnici 95/46/ES moc neliší a GDPR ji pouze upřesňuje. Správce byl měl poskytovat informace subjektu údajů stručným, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků[90]. Informace, které jsou správci povinni subjektu údajů poskytnout, se stejně jako za původní úpravy rozdělují do dvou skupin, a to na informace získané přímo od subjektu údajů a na informace získané nepřímo.[91]

K dalšímu posílení došlo u práva na přístup. GDPR musí nově od původní úpravy poskytnout subjektu údajů také informace o zamýšlené době uložení osobních údajů, o existenci některých jeho práv, o možnosti podat stížnost k dozorovému orgánu a o zdroji osobních údajů subjektu, není-li jím samotný subjekt. Ve spojitosti s právem na přístup je vhodné podotknout, že GDPR nově umožňuje správci neposkytnout informace či nevykonat jiné právo subjektu údajů v případě, že existuje důvodná pochybnost o totožnosti osoby. Toto ustanovení by mělo pomoci zabránit neoprávněnému přístupu k osobním údajům cizí osobou, avšak vzhledem k formulaci ustanovení jako pouhé možnosti, a ne povinnosti lze pochybovat

[89] Odůvodnění 171 GDPR.
[90] Čl. 12 GDPR.
[91] Čl. 13 a 14 GDPR.

o jeho využitelnosti. Ověření totožnosti ve vztahu k výkonu subjektu údajů by mělo být podle mého názoru v GDPR explicitně stanoveno. Uplatnění práva na přístup k jiným, než svým osobním údajům se jeví jako možné a přísnější formulace by byla vhodná. Správce by mohl například v rámci informační povinnosti subjektu údajů sdělit, jakým způsobem bude jeho totožnost ověřovat, a aspoň tímto způsobem výkon práv zabezpečit.

Právo na výmaz („právo být zapomenut“) zakotvené v článku 17 GDPR se stalo před účinností nařízení často diskutovanou věcí navzdory tomu, že to zcela nové právo není. Směrnice 95/46/ES neupravuje právo na výmaz zvlášť, ale zahrnuje ho do práva na přístup v článku 12 odst. 2. V něm říká, že má subjekt údajů právo získat od správce podle daného případu opravu, výmaz nebo blokování údajů, jejichž zpracování není v souladu se směrnicí, zejména z důvodu neúplné nebo nepřesné povahy údajů. Ze samotného znění je tedy zřejmé, že toto právo existovalo i za původní úpravy, ale nebylo příliš široké. Aplikaci článku 12 však dále rozšířil výklad Soudního dvora Evropské unie v rozsudku *Google Spain vs. Costeja*[92] z roku 2014, ve kterém Soudní dvůr zaujal postoj k širšímu výkladu. Rozsudek stanovil, že článek 12 musí být vykládán v souvislosti s článkem 6, který mimo jiné říká, že osobní údaje musí být přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou zpracovávány. Žalobce se v kauze *Google Spain vs. Costeja* dovolával práva na výmaz stránek na španělské verzi vyhledavače Google, které obsahovaly informace o veřejné dražbě jeho majetku. Soudní dvůr Evropské unie došel k závěru, že zveřejněné informace o dražbě měly sloužit k tomu, aby na ni zájemci mohli přijít. Následná difamace žalobce je tedy v rozporu s účelem zpracování a žalobce tak má právo na výmaz těchto informací. GDPR závěr z tohoto rozsudku převzala a explicitně stanovila, že subjekt údajů má právo na výmaz v případě, kdy jeho osobní údaje již nejsou potřebné pro účely, pro něž byly shromážděny nebo jinak zpracovány. Kromě výše zmíněného pak GDPR upravuje i další důvody, na základě kterých je subjekt údajů oprávněn právo na výmaz použít. Jde o případ, kdy subjekt údajů svůj souhlas odvolá, osobní údaje jsou zpracovány protiprávně nebo má-li správce právní povinnost vyplývající z práva EU nebo z práva členského státu. GDPR ukládá také správci povinnost vyhovět žádosti na výmaz v případě, kdy zpracovává osobní údaje dětí v souvislosti s nabídkou informačních služeb. Subjekt údajů má na výmaz právo i poté, co hranici zletilosti překročil. Toto právo se týká i

[92] C-131/12, Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 13. května 2014 Google Spain SL, Google Inc. proti Agencia Espanola de Protección de Datos (AEPD), Mario Costeja González.

údajů, které o něm správce shromáždil, když byl ještě nezletilý.[93] GDPR tedy kromě stanovení zvláštních podmínek pro udělení souhlasu v článku 8 i tímto způsobem garantuje zvláštní ochranu dětí. Posledními případy práva subjektu údajů podat žádost o výmaz jsou situace, kdy subjekt údajů vznese námitku proti zpracování a správce nemá ke zpracování oprávněný důvod a kdy správce zpracovává osobní údaje za účelem přímého marketingu.

Právo vznést námitku není opět nové právo, které by směrnice 95/46/ES neznala, GDPR ale toto právo značně posiluje. Jak směrnice 95/46/ES, tak i GDPR dává subjektu údajů právo vznést námitku proti zpracování, pokud probíhá na základě právního titulu veřejného nebo oprávněného zájmu. Obě úpravy ukládají správci povinnost přestat se zpracováním osobních údajů, je-li žádost subjektu údajů oprávněná. V rámci původní směrnice měl lepší postavení správce, jelikož to byl subjekt údajů, který musel prokazovat oprávněnost své vznesené námitky. S účinností GDPR se situace změnila a důkazní břemeno nyní nese správce. Správce musí dokázat, že má oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon a obhajobu právních nároků[94]. Tato změna bude obzvláště citelná pro správce, kteří využívají právní titul oprávněného zájmu. K jeho dokázání by měli totiž disponovat tzv. balančním testem. Správce je povinen pozastavit zpracování do doby, než dokáže své oprávněné důvody.

Omezení zpracování a právo na omezení není ve směrnici 95/46/ES nijak explicitně zakotveno, ale je obsaženo nepřímo v rámci úpravy práva na přístup. Zde je stanoveno, že subjekt údajů má právo na blokaci[95] svých údajů v případě nesouladu zpracování se směrnicí, a to především v případě, kdy jsou osobní údaje neúplné nebo nepřesné. Zákon o ochraně osobních údajů toto právo transponoval do českého právního řádu velmi obecnou formulací, podle které může subjekt údajů požadovat právo na blokaci tehdy, domnívá-li se, že jeho osobní údaje jsou zpracovány v rozporu s ochranou jeho soukromého a osobního života nebo v rozporu se zákonem[96]. GDPR v tomto ohledu zvolilo podle mého názoru lepší přístup, když právo na omezení zpracování upravilo odděleně v samostatném článku a vyjmenovalo i

[93] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, Str. 211. ISBN 978-80-7552-765-3.
[94] Čl. 21 odst. 1 GDPR.
[95] Pojem blokace není ve směrnici 95/46/ES definován, ale je obsažen v zákoně č. 101/2000 Sb., o ochraně osobních údajů v článku 4 písm. h), který za blokování považuje soustavu operací, kterými se na stanovenou dobu omezí způsob nebo prostředky zpracování osobních údajů, s výjimkou nezbytných zásahů.
[96] §21 odst. 1. zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

konkrétní případy využití tohoto práva. Vzhledem k širokému uplatnění tohoto práva v praxi, kdy například subjekt údajů nebude chtít nutně všechny své údaje vymazat, ale pouze omezit zpracování ke konkrétnímu účelu, jde o účinný prostředek, který umožňuje subjektu údajů mít větší kontrolu nad svými osobními údaji.

Z výše zmíněného je zřejmé, že práva subjektu údajů byla rozšířena především posílením již stávajících práv. GDPR ale zavádí i právo pro původní úpravu neznámé, a to právo na přenositelnost, tzv. právo na portabilitu[97]. Cílem tohoto práva je poskytnout subjektu údajů větší kontrolu nad svými osobními údaji a podpořit volný pohyb osobních údajů v Evropské unii a soutěž mezi správci.[98] V rámci práva na portabilitu má subjekt údajů od správce právo získat své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu. V tomto ohledu se může právo na portabilitu podobat právu na přístup, které směrnice 95/46/ES, jak bylo uvedeno výše, již upravovala. Správce má však při plnění žádosti na přístup právo si vybrat formát, v jakém informace subjektu údajů předá. Právo na portabilitu formu zkonkretizovalo s cílem umožnění rychlého a snadného předávání osobních údajů mezi správci. GDPR tímto chce předcházet situacím, kdy se subjekt údajů mohl cítit upoután například na svého poskytovatele služeb internetu z důvodu neexistence či obtížnosti převodu svých osobních údajů na platformu jiného poskytovatele. Bohužel ale GDPR již blíže neurčuje, o jaké konkrétní podoby formátů by mělo jít. Podle vydaných pokynů WP29 se budou vhodné formáty podle povahy zpracování lišit a správce by měl obecně vybrat takový formát, který zachová hlavní smysl tohoto práva, jímž je přenositelnost[99]. Za špatný formát uvádějí pokyny soubor pdf pro elektronickou poštu. Tento typ souboru totiž neobsahuje meta data, která jsou pro převod elektronické pošty potřebná. Je zcela zřejmé, že pro velké společnosti, jako je Facebook nebo Google, které zpracovávají velké množství různorodých kategorií osobních údajů, bude povinnost poskytnout údaje v strukturovaném formátu obrovská administrativní a technická zátěž. Subjekt údajů může žádat od správce své osobní údaje, které mu sám poskytl, ale i údaje, které služba nebo zařízení získala sama od subjektu ze samotného používání. Subjekt údajů tak podle pokynů může například od poskytovatele streamované hudby zjistit, jaké písničky si přehrával nejčastěji. Co už ale subjekt údajů vyžadovat nemůže,

[97] Čl. 20 GDPR.
[98] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability adopted on 13 December 2016, Str.3.
[99] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability adopted on 13 December 2016, Str.18.

jsou tzv. odvozená data, což jsou údaje zjištěné správcem například pomocí analýz nebo profilování[100]. Na konkrétním příkladu by subjekt údajů mohl od Facebooku vyžadovat například údaje ze svých příspěvků, ale už by nemohl vyžadovat údaje, na základě kterých mu byla zobrazena konkrétní reklama. Právo na portabilitu nebude podle mého názoru znamenat pro správce pouze přítěž, ale zároveň i příležitost. Pro některé společnosti bude toto právo představovat možnost, jak přetáhnout zákazníky konkurenčních společností. Za původní úpravy mohly nastat případy, kdy zákazník nebyl se službami svého poskytovatel spokojen, ale i přesto u něj setrvával z důvodu komplikovanosti přechodu k jinému poskytovateli. Právo na portabilitu přesně tenhle problém řeší a bude tak přínosem jak pro samotné subjekty údajů, tak i pro správce.

Kromě výše zmíněných změn u práv subjektu údajů došlo také ke změnám procesním. Správce má povinnost reagovat na žádosti subjektu údajů bez zbytečného odkladu a měl by nejpozději do jednoho měsíce poskytnout žadateli informace o přijatých opatřeních, v odůvodněných případech do dvou měsíců. Směrnice 95/46/ES sama neupravovala lhůtu pro vyřízení žádostí a každý stát si v transpozičním předpise určil lhůtu vlastní. Současný zákon o ochraně osobních údajů žádnou lhůtu nezvolil a použil obecnou formulaci bez zbytečného odkladu. Posouzení, co znamená poskytnout informaci bez zbytečného odkladu, bude záviset zejména na rozsahu a množství informací, a tedy na možnostech správce požadovanou informaci vyhledat; v zásadě by se mělo jednat o lhůtu v řádech dnů.[101] Lze tedy říci, že lhůta na vyřízení žádosti bude podle nové úpravy GDPR pro správce příznivější, než tomu bylo doposud. Další procesní změna nastala ve finanční stránce vyřizování žádosti. Směrnice 95/46/ES měla ve spojitosti s výkonem práv subjektu údajů stanoveno, že k vyřízení žádosti by mělo dojít bez zbytečných nákladů. GDPR nově zavádí bezplatný výkon práv s možností přiměřeného zpoplatnění v případě, že je žádost zjevně nedůvodná nebo nepřiměřená.

2.6. Odpovědnost a sankce

Podle znění směrnice 95/46/ES měl subjekt údajů právo na náhradu utrpěné škody pouze od správce a už nikoliv od zpracovatele. Zákon o ochraně osobních údajů však odpovědnost

[100] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability adopted on 13 December 2016, Str.9.
[101] A. KUČEROVÁ A KOL., Zákon o ochraně osobních údajů: komentář. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. Str. 221. ISBN 978-80-7179-226-0.

rozšířil i na zpracovatele, a dokonce ustanovil i přísnou solidární odpovědnost. Došlo-li při zpracování osobních údajů k porušení povinností uložených zákonem u správce nebo u zpracovatele, odpovídali za ně společně a nerozdílně[102]. Pokud se tedy na zpracování podílel zpracovatel, odpovídal za porušení povinností se správcem solidárně, a to bez ohledu na to, zda své povinnosti porušil, nebo zda je porušil pouze sám správce. Zákon o ochraně osobních údajů zpracovateli umožnil se zprostit solidární odpovědnosti v případě, kdy zjistil, že správce porušuje své zákonné povinnosti, a na porušení ho upozornil a zpracování zároveň ukončil. Zajímavostí je, že toto ustanovení nepředpokládalo žádnou oznamovací povinnost dozorovému úřadu, což mi vzhledem k důležitosti předcházení újmy připadá jako velký nedostatek.

GDPR stanovuje objektivní odpovědnost jak správců, tak i zpracovatelů. Zpracovatel je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené nařízením pro zpracovatele nebo že jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi[103]. V takovém případě je zpracovatel odpovědný solidárně se správcem. Další změnou je, že GDPR na rozdíl od směrnice 95/46/ES vymezuje náhradu škody jako náhradu jak za majetkovou, tak i za nemajetkovou újmu. Nicméně i když směrnice 95/46/ES ve svém znění hovořila pouze o náhradě za škodu, stanovisko WP29 dovodilo zahrnutí i nemajetkové újmy[104].

Ukládání správních pokut a jejich výše doznala v GDPR od původní úpravy značných změn. Směrnice 95/46/ES sama výši správních pokut neupravovala a ponechala jejich úpravu na uvážení členských států. Zákon o ochraně osobních údajů upravoval odděleně správní pokuty pro fyzické a právnické osoby. Jejich výše se odvíjela podle závažnosti a nejvyšší pokuta činila 5 milionů Kč pro fyzické osoby a 10 milionů pro právnické osoby. Je ale nutné podotknout, že v praxi Úřad pro ochranu osobních údajů ukládal na základě principu přiměřenosti pokuty podstatně nižší[105]. GDPR nově explicitně stanovuje výši správních pokuty podle závažnosti porušení povinností, nejvýše však do 20 milionů EUR a u podniků až do výše

[102] §21 odst. 4. zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
[103] Čl. 82 odst. 2 GDPR.
[104] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, Str. 479. ISBN 978-80-7552-765-3.
[105] Historicky nejvyšší pokuty byly uloženy společnosti T-mobile v roce 2016 za nedostatečné zabezpečení osobních údajů (3,6 milionu Kč) a společnosti Eurydikapol za zasílaní nevyžádaného sdělení (4.2 milionu Kč)

4% celkového celosvětového ročního obratu, a to podle toho, která hodnota je vyšší. Členské státy mají možnost tyto částky upravit pouze pro správní orgány, nikoliv pro fyzické a právnické osoby[106]. GDPR dále umožňuje členským státům uložit i jiné sankce. Jedná se především o porušení, na které se nevztahují správní pokuty. Zejména půjde o ukládání trestních sankcí za porušení povinností GDPR, včetně porušení vnitrostátních pravidel. Ukládání sankcí však vždy musí dodržet zásadu ne bis in idem.[107]

K ukládání pokut je také vhodné zmínit zveřejněný přístup Úřadu pro ochranu osobních údajů. Český dozorový úřad prohlásil, že se v období před přijetím adaptačního zákona zaměří především na zvyšování povědomí správců o vhodné ochraně údajů. V rámci dozorové činnosti bude vyzývat a vést k nápravě, nikoliv tedy primárně trestat za méně závažná a nedbalostní pochybení[108].

[106] Podle neschváleného návrhu českého adaptačního zákona je výše pokuty pro správní orgány stanovena na maximální částku 10 milionů Kč.
[107] Odůvodnění 149 GDPR.
[108] Úřad pro ochranu osobních údajů, Přístup Úřadu k pokutování [online], 2018, dostupné z: https://www.uoou.cz/pristup-uradu-k-nbsp-pokutovani/d-31044

3. Právní úprava institutu pověřence pro ochranu osobních údajů v GDPR a jeho komparace s německou úpravou

Pověřenec pro ochranu osobních údajů[109] je pro unijní právo nový institut, který má za cíl posílit ochranu osobních údajů u rizikovějších zpracování. Je zřejmé, že sám správce nebude vždy dostatečně rozumět GDPR a jiným relevantním předpisům, aby byl schopen plnit bez cizí pomoci všechny své povinnosti. GDPR proto zavádí institut pověřence jako nový prvek ochrany, který bude předcházet pochybením správců. Některé národní úpravy členských států Evropské unie měly tento prvek ochrany zavedený již mnoho let před účinností GDPR. Nutné je však dodat, že většina těchto úprav nestanovovala jmenování pověřence jako povinnost a k jmenování docházelo dobrovolně na základě úvahy správce[110]. Státy upravující pověřence jako nepovinný institut byly například Slovensko[111], Francie[112], Španělsko[113] či Švédsko[114]. Vyskytovaly se však i státy, které upravovaly povinnost jmenovat pověřence pro určité druhy zpracování. Těmito státy bylo Německo[115] a Maďarsko[116]. Německo má s institutem pověřence dlouholeté zkušenosti, neboť někteří správci jsou zde povinni jmenovat pověřence již od roku 1977[117]. Německá úprava demonstrovala, že jmenování pověřence je pro ochranu osobních údajů vhodným institutem, který snížil potřebu zásahů dozorového úřadu[118]. GDPR se inspirovala ze základního konceptu povinného jmenování pověřence a z předchozí německé federativní úpravy[119]. Právě federativní úprava bude proto z tohoto důvodu použita i ke komparaci s úpravou pověřence v GDPR.

[109] Dále také i jako “pověřenec” či “DPO”.
[110] Jmenování pověřence není při naplnění podmínek GDPR povinností vztahující se pouze na správce, ale také na zpracovatele. Kde je v kapitole ve vztahu k pověřenci zmíněn pouze správce, je též myšlen i zpracovatel.
[111] Ve slovenském jazyce jako ”zodpovedná osoba”, zákon č. 122/2013 o ochrane osobných údajov v znení zákona č. 84/2014 Z. z.
[112] Ve francouzském jazyce jako ”le Correspondant informatique et libertés”, ACT N°78-17, Amended by the ACT OF 6 August 2004.
[113] Ve španělském jazyce jako ”responsible de seguridad”, Ley Orgánica 15/1999, de protección de datos de character personal; Real Decreto 1720/2007.
[114] Ve švédském jazyce jako ”personuppgiftsombudet”, Personal Data Act of April 29, 1998 (Personuppgiftslag)
[115] V německém jazyce jako ” datenschutzbeauftragter”, Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) in the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66). Dále pouze jako “BDSG”.
[116] V maďarském jazyce jako ”belsö adatvédelmi felelös”, Act LXIII of 1992.
[117] Taylor Wessing, The compliance burden under the GDPR - Data Protection Officers [online], dostupné z https://www.lexology.com/library/detail.aspx?g=37cd2a6d-9bbf-4db0-a66e-05d74a22291c

[118] tamtéž
[119] Německý adaptační zákon pro GDPR byl přijat již 27. dubna 2017.

3.1. Povinnost jmenovat pověřence

Správce není povinen jmenovat pověřence vždy, ale pouze při naplnění podmínek GDPR, které jsou vymezeny v čl. 37 odst. 1. Obecně by šlo říci, že správce je povinen jmenovat pověřence u těch zpracování, která pro svoji povahu či rozsah představují větší riziko pro subjekty údajů. Na rozdíl však od povinnosti provést DPIA není povinnost jmenovat pověřence výslovně spojena s každým zpracováním, které by mohlo mít za následek vysoké riziko pro práva a svobody fyzických osob, a váže se výslovně pouze na podmínky stanovené ve výše zmíněném čl. 37 odst. 1.

Pověřence je nutné jmenovat vždy, když zpracování provádí orgán veřejné moci či veřejný subjekt, který není soudem jednajícím v rámci svých soudních pravomocí[120]. Pojem orgánu veřejné moci či veřejného subjektu není v GDPR vymezen a dle pokynů WP29 by si tento pojem měl každý členský stát stanovit sám svými vnitrostátními právními předpisy[121]. Návrh českého adaptačního zákona[122] vymezuje pojem veřejný subjekt v §13, který říká, že se za veřejný subjekt považuje orgán zřízený zákonem nebo na základě zákona v oblasti práva veřejného, který plní zákonem stanovené úkoly ve veřejném zájmu. K tomuto vymezení je nutné vzít v potaz i doporučení WP29[123]. To ukládá subjektům jmenovat pověřence i tehdy, když veřejné úkoly vykonává fyzická nebo právnická osoba veřejného nebo soukromého práva.

Správce je také povinen jmenovat pověřence vždy, když jeho hlavní činnost spočívá v takových operacích, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů[124]. Pojem hlavní činnosti přibližuje GDPR ve svém odůvodnění, ve kterém říká, že v soukromém sektoru souvisí hlavní činnost správce s jeho základními činnostmi a nevztahuje se na zpracování osobních údajů jakožto pomocnou činnost[125]. Hlavní činnost nejde tedy bez zpracování osobních údajů vůbec vykonávat, protože je s hlavní činností neoddělitelně spjato. K tomuto ještě pokyny WP29[126]

[120] Čl. 37 odst. 1. písm. a) GDPR.
[121] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016, Str. 8.
[122] Návrh adaptačního zákona ve znění ke dni 21.6. 2018.
[123] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016, Str. 8.
[124] Čl. 37 odst. 1 písm. b) GDPR.
[125] Odůvodnění 97 GDPR.
[126] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016, Str. 9.

dodávají, že se nejedná o taková zpracování osobních údajů, která jsou nutná pro výkon všech činností, jako je například vyplácení mezd. Pojem rozsáhlost není v GDPR definován. O vymezení se pokusil Úřad pro ochranu osobních údajů ve svém doporučení[127], avšak toto vymezení není právně závazné. Vzhledem k různorodosti druhů zpracování nešlo dle mého názoru ani uvažovat o stanovení konkrétního rozsahu daného hodnotou a zákonodárci EU zde neměli jinou možnost, než zvolit takto neurčitý pojem. Pokyny WP29[128] sice nevylučují možnost stanovení postupů pro určení konkrétních hodnot u jednotlivých druhů zpracování, lze ale jen polemizovat, jestli bude Evropský sbor pro ochranu osobních údajů chtít o něco takového usilovat. Pojem monitorování byl již zmíněn ve spojitosti s extrateritoriální působností. Odůvodnění GDPR[129] přibližuje však pojem monitorování výslovně ve vztahu k extrateritoriální působnosti a lze tedy pouze předpokládat, že je toto odůvodnění aplikovatelné i pro vymezení zpracování pro účely stanovení povinnosti jmenovat pověřence.

V posledním případě je správce povinen jmenovat pověřence tehdy, když v rámci své hlavní činnosti rozsáhle zpracovává zvláštní kategorie údajů či údaje týkající se rozsudků v trestních věcech a trestných činů[130]. Zvláštní kategorie údajů a údaje týkající se rozsudků v trestních věcech a trestných činů jsou dobře identifikovatelné vzhledem k tomu, že je výčet této kategorie vymezen taxativně[131]. I u tohoto bodu je však otázkou, co bude považováno za rozsáhlé zpracování.

BDSG nestanovuje stejně jako GDPR povinnost jmenovat pověřence pro všechny druhy zpracování. BDSG však na rozdíl od GDPR nevztahuje povinnost jmenovat pověřence pouze na povahu zpracování, ale také na počet osob, které mají k osobním údajům přístup a údaje zpracovávají. Dle BDSG[132] byl správce povinen jmenovat pověřence tehdy, když zaměstnával více jak 9 lidí, kteří automatizovaně zpracovávali osobní údaje. V případě neautomatizovaného zpracování pak musel správce zaměstnávat minimálně 20 zaměstnanců, aby se na něj tato povinnost vztahovala. Správce musel jmenovat pověřence vždy bez ohledu na počet zaměstnanců, když zpracovával osobní údaje, které vyžadovaly tzv. předchozí kontrolu[133],

[127] viz kapitola 4 této práce.
[128] tamtéž
[129] Odůvodnění 24 GDPR.
[130] Čl. 37 odst.1 písm. c) GDPR.
[131] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, Str. 254, ISBN 978-80-7380-689-7.
[132] §4f odst. 1. BDSG
[133] V anglickém jazyce jako “prior checking”.

nebo když údaje zpracovával automatizovaně a komerčně pro účely jejich převodu, průzkumu trhu nebo výzkumu veřejného mínění. Veřejný subjekt byl povinen jmenovat pověřence vždy bez ohledu na počet zaměstnanců, když docházelo k jakémukoliv automatizovanému zpracovávání osobních údajů.

Z výše zmíněného je zřejmě, že Německo mělo upraveno jmenování přísněji než GDPR a že za předchozí úpravy BDSG musel správce jmenovat pověřence častěji. Není tedy překvapující, že německý adaptační zákon zvolil přísnější úpravu pro jmenování pověřence, než je úprava v GDPR. Dle adaptačního zákona musí povinně jmenovat pověřence každý správce, který zaměstnává více než 10 zaměstnanců a zpracovává osobní údaje jako trvalou a hlavní činnost. Pověřence musí povinně jmenovat i ti správci, kteří jsou povinni provést DPIA nebo pokud komerčně zpracovávají osobní údaje pro účely jejich převodu, průzkumu trhu nebo výzkumu veřejného mínění[134]. Německo se tedy rozhodlo si svoji původní přísnější úpravu ponechat a je zřejmé, že institut pověřence byl důležitou součástí německé úpravy ochrany osobních údajů již před účinností GDPR. Vzhledem k povaze nařízení je však téměř jisté, že Evropská komise nebude německé odchýlení akceptovat a že zahájí řízení o porušení unijního práva[135]. Německá přísnější úprava pověřence jde mimo rámec přípustných derogačních klauzulí obsažených v GDPR, které umožňují členským státům stanovit si vlastní pravidla, a je tak zjevným porušením unijního práva. Nezahájením řízení Evropskou komisí by došlo k popření úsilí harmonizovat ochranu osobních údajů v Evropské unii.

3.2. Funkce a povinnosti pověřence

Pověřenci jsou důležitým aspektem principu odpovědnosti, jejichž povinností je zajištění souladu s GDPR bez zásahu dozorového úřadu[136]. GDPR sice vymezuje v čl. 39 povinnosti každého pověřence, ale jedná se pouze o povinnosti minimální a správce si může s pověřencem ujednat i povinnosti jiné. Za minimální povinnosti považuje GDPR poskytování informací a poradenství, a to jak vůči správcům, tak případně také vůči správcovým

[134] Nový německý zákon o ochraně osobních údajů [online], 2017, dostupné z: http://www.gdprbezobav.cz/novy-nemecky-zakon-ochrane-osobnich-udaju/, BDSG, §38 odst.1.
[135] OLIVER SÜME, Data Protection: Does the German Implementation Act (BDSG-E) undermine the GDPR?, [online], dostupné z: https://privacylawblog.fieldfisher.com/2017/data-protection-does-the-german-implementation-act-bdsg-e-undermine-the-gdpr
[136] LINKLATERS, GDPR booklet [online], Str.36, dostupné z: https://lpscdn.linklaters.com/-/media/files/linklaters/pdf/mkt/london/tmt_data_protection_survival_guide_singles.ashx?rev=5ef6afd7-f614-4423-9145-0a9d0a60a452

zaměstnancům. Poradenství se netýká pouze GDPR, ale i dalších předpisů EU či členských států[137]. Pověřenec by měl tedy být obeznámen kromě GDPR i s adaptačními předpisy a měl by mít přehled o všech unijních předpisech upravujících ochranu osobních údajů. Další povinností pověřence dle GDPR je monitorování souladu se všemi výše zmíněnými předpisy. Úkolem pověřence je dohled nad souladem s GDPR a řádné vedení dokumentace včetně výpomoci správci s vedením záznamů o činnostech zpracování dle čl. 30[138]. Další minimální povinností pověřence je poskytování poradenství ohledně DPIA[139], a to na požádání správce. Správce je povinen si vyžádat od pověřence posudek k DPIA[140], což dle mého názoru může vyvolat nejistou situaci v případě, když si správce posudek od pověřence nevyžádá. Pověřenec je dle výše zmíněného povinen poskytovat správci poradenství a monitorovat soulad s nařízením, k čemuž se poskytování poradenství ohledně provedení DPIA či pouhé posouzení nutnosti provedení DPIA určitě vztahuje. Vyjasnění této situace je důležité pro případnou povinnost pověřence na náhradu škody, ke které by došlo z důvodu nesplnění jeho povinností. Pověřenec sice dle GDPR nemůže být pro výkon svých povinností propuštěn ani sankcionován, to ale nevylučuje jeho odpovědnost za škodu[141]. Vzhledem k tomu, že je povinnost poskytovat na požádání poradenství ohledně DPIA upravena samostatně, lze dle mého názoru dovodit, že pověřenec není povinen správce na provedení DPIA upozornit. Poslední minimální povinností pověřence je dle čl. 39 povinnost komunikační. V rámci této povinnosti pověřenec spolupracuje za správce s dozorovým úřadem a slouží pro dozorový úřad jako kontaktní místo[142]. Pověřenec nemusí být trvale přítomen na místě, kde se nacházejí nebo zpracovávají osobní údaje, musí však být rychle dosažitelný alespoň prostřednictvím telefonu, či jiného elektronického spojení[143]. K minimálním povinnostem pověřence je ještě nutné dodat, že se nenacházejí pouze v čl. 39, ale i v článcích jiných. Subjekt údajů se například může dle čl. 38 odst. 4 obrátit na pověřence ve všech záležitostech souvisejících se zpracováním svých osobních údajů a výkonem svých práv.

[137] Čl. 39 odst. 1 písm. a) GDPR.
[138] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017, Právo pro praxi. Str. 167, ISBN 978-80-271-0668-4.
[139] Čl. 39 odst. 1 písm. c).
[140] Čl. 35 odst.2 GDPR.
[141] EVA ŠKORNIČKOVÁ, Musíte mít pověřence? A jak ho vybrat? [online], Dostupné z: https://www.gdpr.cz/blog/vyber-poverence
[142] Čl. 39 odst. 1 písm. d) a e) GDPR.
[143] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, Str. 257, ISBN 978-80-7380-689-7.

Německá federativní úprava[144] stanovovala povinnosti pověřence v §4g a stejně jako GDPR tyto minimální povinnosti upravovala a umožňovala jejich smluvní rozšíření. Stejně jako v GDPR byla i v BDSG hlavním úkolem pověřence povinnost monitorovat soulad s právní úpravou. V případě potřeby konzultoval pověřenec dle BDSG zpracování s dozorovým úřadem a taktéž jako GDPR ukládala BDSG povinnost pověřenci poskytovat poradenství správci a jeho zaměstnancům. BDSG upravovala na rozdíl od GDPR předchozí kontrolu pověřencem u všech automatických zpracování, která by mohla mít vysoká rizika pro práva a svobody subjektů údajů[145]. Pověřenec byl dle BDSG povinen provést kontrolu před započetím každého takového zpracování a v případě nejistot byl povinen konzultovat dozorový úřad[146]. V tomto ohledu je předchozí federativní úprava přísnější než GDPR. GDPR vyžaduje sice u rizikovějších zpracování provedení DPIA, ke kterému má správce povinnost si vyžádat od pověřence posudek (je-li pověřenec jmenován), avšak v rámci BDSG byl správce povinen si vyžádat kontrolu od pověřence vždy.

3.3. Kvalifikace a jmenování

GDPR upravuje požadovanou kvalifikaci pověřence velmi obecným způsobem. Pověřenec by měl být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39[147]. Odůvodnění k tomu dodává, že potřebná odborná znalost se bude lišit podle ochrany, která se vyžaduje pro osobní údaje zpracovávané správcem nebo zpracovatelem[148]. GDPR nestanovuje podmínku vysokoškolského právního vzdělání pro výkon funkce pověřence a ani nepředpokládá žádnou povinnou certifikaci. Správce tedy může přijmout jakoukoliv osobou s dostatečnou odbornou znalostí pro konkrétní zpracování. Správce by měl u pověřence hledat nejen odborné právní znalosti, ale i orientaci v IT technologiích. Pověřenec by totiž měl pro zajištění řádné ochrany osobních údajů rozumět prováděným operacím zpracování, jakož i informačním systémům, aby mohl správci navrhnout vhodné technické opatření pro každý

[144] V diplomové práci se pracuje pro účely srovnání s již neúčinným zněním zákona BDSG z 14. srpna 2009.
[145] BDSG uvádí demonstrativně za taková zpracování v §4d odst. 5 profilování a zpracování zvláštních kategorií údajů, ke kterým dochází automatizovaně.
[146] §4d odst. 6 BDSG.
[147] Čl. 37 odst. 5 GDPR.
[148] Odůvodnění 97 GDPR.

druh zpracování[149]. Pověřenec by se zároveň měl konstantně vzdělávat v nových technologiích a rizicích z nich plynoucích pro ochranu osobních údajů[150].

Pověřenec může být zaměstnancem správce nebo může výkon funkce vykonávat na základě smlouvy o poskytování služeb[151]. Český občanský zákoník však neupravuje přímo smlouvu o poskytování služeb a ani jiný typ smlouvy se nejeví jako vhodný. Proto by se smlouva s pověřencem mohla řídit ustanovením § 1746 odst. 2 jako smlouva nepojmenovaná[152]. Rozhodnutí správce, zdali mít pověřence jako zaměstnance či ho mít pouze externě, by mělo záviset především na povaze a složitosti zpracování. Obecně by se dalo říci, že u komplexnějšího zpracování bude pro správce lepší varianta pověřence zaměstnávat a u méně náročného zpracování bude naopak pro správce lepší využívat služeb externího pověřence. Zaměstnanec správce bude totiž u komplexnějšího zpracování lépe obeznámen s vnitřním chodem organizace a se zavedenými postupy, což mu výkon funkce značně usnadní[153].

Dle BDSG může vykonávat funkci pověřence pouze spolehlivá osoba s nezbytnými odbornými znalostmi pro výkon povinností pověřence[154]. Za spolehlivou osobu lze považovat takovou osobu, u které nedochází ke střetu zájmů, dodržuje povinnost mlčenlivosti a zaručuje záruky osobní odpovědnosti[155]. Výše nezbytných odborných znalostí se dle BDSG liší především podle rozsahu zpracování. GDPR má tedy téměř identické kvalifikační požadavky pro pověřence jako německá federativní úprava, pouze je maličko upřesňuje. BDSG stejně jako GDPR umožňovala jmenování externího pověřence[156].

---

[149] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016, Str. 13.
[150] THOMAS SHAW, What skills should your DPO absolutely have? [online], dostupné z: https://iapp.org/news/a/what-skills-should-your-dpo-absolutely-have/
[151] Čl. 37 odst. 6 GDPR.
[152] EVA ŠKORNIČKOVÁ, Musíte mít pověřence? A jak ho vybrat? [online], dostupné z: https://www.gdpr.cz/blog/vyber-poverence/
[153] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, Str. 340. ISBN 978-80-7552-765-3.
[154] §4f odst. 2 BDSG.
[155] Data protection officer according to German law [online], dostupné z: https://www.activemind.legal/law/de-data-protection-officer/

[156] Tamtéž.

3.4. Závěr komparace institutu pověřence s německou úpravou

Institut pověřence je dle mého názoru jednoznačným přínosem pro zaručení větší ochrany osobních údajů. Určité druhy zpracování by bezpochyby měly mít větší bezpečnostní záruky a jmenování nezávislé specializované osoby se dle německých zkušeností osvědčilo. Není reálné očekávat, že každý správce bude mít dostatečnou právní a technickou odbornost, která je u rizikovějších zpracování zapotřebí. Jmenovat pověřence je správce povinen podle vzoru německé úpravy pouze ve stanovených případech a nejedná se tedy o plošnou povinnost pro všechny správce. GDPR se sice německou úpravou inspirovalo, ale nepřijalo ji doslovně. Dle mého názoru je správné, že GDPR nezvolilo stejné podmínky pro povinné jmenování pověřence jako německá úprava, podle které je povinné jmenování pověřence vcelku častá záležitost. Správce je totiž povinen jmenovat pověřence u všech automatizovaných zpracování citlivých údajů, a to bez ohledu na rozsah, jak je tomu u GDPR. Zaručení větší ochrany subjektů údajů je sice cílem GDPR, ale mělo by ho být dosaženo proporcionálně ve vztahu k možnostem jednotlivých správců. Jmenování pověřence je jak finanční, tak i administrativní zátěží, která by mohla být pro mnohé správce likvidační. Vyžadovat jmenování pověřence u správce s databází pouhých 50 lidí by nebylo dle mého názoru správné a je dobře, že to GDPR reflektovalo. I když v tomto případě šlo GDPR svojí vlastní cestou, v případě povinnosti jmenovat pověřence u orgánů veřejné moci zvolilo úpravu totožnou a pověřence musí mít všechny orgány veřejné moci. V tomto ohledu se domnívám, že inspirace německou úpravou vhodná nebyla a že měla obsahovat výjimky. Jmenování pověřence bude pro určité veřejné orgány, jako jsou například menší školy, nepřiměřenou zátěží, a to především finanční. Školy mají i bez této nové povinnosti většinou dost napjaté rozpočty. V tomto ohledu na to GDPR pamatuje pouze tak, že obsahuje derogační klauzuli[157] pro vlastní úpravu pokut pro veřejné orgány. V době odevzdání diplomové práce stanovoval návrh českého adaptačního zákona omezenou pokutu pro veřejné orgány s vrchní hranicí 10 milionů Kč[158]. GDPR si mělo dle mého názoru zvolit pro povinné jmenování pověřence u veřejných orgánů vlastní úpravu, která by se bezpodmínečně nevztahovala na všechny veřejné orgány. Navzdory tomu bych závěrem

[157] Čl. 83 odst. 7 GDPR.

[158] §62 vládního návrhu zákona o zpracování osobních údajů předloženého 28.3. 2018.

k pověřenci dodal, že inspirace německou úpravou byla dle mého názoru pro GDPR tím správným východiskem.

4. Posouzení vlivu na ochranu osobních údajů a koncept jejího provedení

Posouzení vlivu na ochranu osobních údajů je v unijním právu taktéž nový institut ochrany osobních údajů, jehož zavedením je sledováno snížení rizik u zpracování osobních údajů, která mohou mít za následek vysoké riziko pro práva a svobody fyzických osob. GDPR ukládá všem správcům obecnou povinnost odpovědnosti, v rámci níž musí správci předcházet rizikům zpracování pomocí přijetí vhodných organizačních a technických opatření. Vypracování DPIA vychází z obecné odpovědnosti správce, avšak ukládá správcům více povinností, které reflektují povahu zpracování s větším rizikem pro práva a svobody fyzických osob. DPIA je proces, jehož cílem je popsat zpracování, posoudit nezbytnost a přiměřenost zpracování a napomoci zvládnutí rizik vyplývajících ze zpracování osobních údajů. Zároveň bude DPIA sloužit jako nástroj k dokazování souladu s GDPR[159].

DPIA je novým institutem v unijním právu, avšak jeho koncept úplně nový není. Čl. 35 GDPR, který DPIA upravuje, je protějškem čl. 20 směrnice 95/46/ES, který upravuje tzv. předběžnou ochranu[160]. V rámci předběžného šetření měly dozorové úřady členských států povinnost prošetřit před započetím všechna svou činností vymezená zpracování, která představovala zvláštní rizika z hlediska práv a svobod subjektů údajů[161]. Této povinnosti dozorového úřadu odpovídala povinnost správce podat dozorovému úřadu oznámení, které zamýšlené zpracování specifikovalo[162]. Jak již bylo dříve zmíněno, GDPR oznamovací povinnost ruší, a tím dochází zároveň k zániku výše zmíněného předběžného šetření podle původní úpravy. Dozorové úřady tak účinností GDPR ztrácejí přehled o všech zpracováních a správcům se naopak zvyšuje odpovědnost a povinnosti. Jednou z těchto povinností je právě provedení DPIA, které správce až na výjimku v čl. 36 nekonzultuje s dozorovým úřadem. Zajímavostí je, že oznamovací povinnost byla kritizována především kvůli administrativní zátěži všech správců

[159] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017, Právo pro praxi. Str. 99, ISBN 978-80-271-0668-4.
[160] BITCOM, Risk assessment & data protection impact assessmen guide [online], dostupné z http://www.digitalestadt.org/bitkom/org/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf, str. 5.
[161] Čl. 20 směrnice 95/46/ES.
[162] Čl. 18 a čl. 19 směrnice 95/46/ES.

a dle navrhovatelů GDPR měla být tato zátěž odbourána[163]. Administrativní zátěž v tomto ohledu odbourána sice byla, ale nikoliv na straně správců, ale na straně dozorových úřadů. O celkovém zvýšení administrativní zátěže v rámci GPDR pro všechny správce bylo již v práci hovořeno. U rizikovějších zpracování je novou zátěží právě vypracování DPIA. Dle mého názoru však ani není možné zaručit u rizikovějších zpracování větší ochranu a zároveň správce nezatížit novými povinnostmi, neboť si to logicky odporuje. Nicméně by šlo polemizovat o tom, kolik správců bude bez oznamovací povinnosti skutečně provádět DPIA a jestli vysoké pokuty budou pro správce dostatečným odstrašujícím prostředkem.

Ve spojitosti k unijní úpravě a DPIA je na místě ještě zmínit doporučení[164] Evropské komise z roku 2009 o ochraně osobních údajů ve vztahu k možné identifikaci pomocí rádiové frekvence[165], ve kterém je předpokládána povinnost vypracovat DPIA pro všechny provozovatele RFID. K doporučení se vyjádřila i WP29[166], která povinnost přijetí DPIA blíže specifikovala, avšak již neobsahovala komplexnější metodologii. Komplexní metodologii k provedení DPIA u provozovatelů RFID publikoval v návaznosti na výše zmíněné až Spolkový úřad pro bezpečnost informační techniky [167].

Mnohé národní úpravy ochrany osobních údajů předpokládají vypracování DPIA nezávisle na unijním právu, ale neukládají vypracování DPIA jako zákonnou povinnost. Ve Spojeném království například dozorový úřad[168] vypracoval podrobnou metodologii k provedení DPIA. Ta má za cíl podpořit správce v procesu implementace vhodných opatření k zajištění ochrany osobních údajů[169]. Podobný přístup zaujal i francouzský dozorový úřad[170].

---

[163] DAVID BURIAN, K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů, [online], dostupné z https://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr

[164] EUROPEAN COMISSION: Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radiofrequency identification. OJ L 122/47 of 16 May 2009.

[165] V anglickém překladu jako radio frequency identification, dále také i jako „RFID".

[166] ARTICLE 29 WORKING PARTY: Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. WP 175 (2010).

[167] Federal Office for Information Security, Privacy Impact Assessment Guideline for RFID Applications, [online], dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1

[168] Information Commissioner's Office, dále také i jako „ICO"

[169] FELIX BIEKER et al., A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Springer International Publishing Switzerland 2016, Str. 2

[170] Tamtéž. Nationale de l'Informatique et des Libert´es, dále také i jako „CNIL"

V německém BDSG byla obsažena obdoba DPIA, jíž je již dříve zmíněná předchozí kontrola. V rámci ní byl pověřenec povinen provést kontrolu před započetím každého automatizovaného zpracování, u kterého docházelo k profilování či zpracování zvláštních kategorií údajů. Cílem předchozí kontroly bylo, stejně jako je tomu u GDPR, zvýšení ochrany u rizikovějších zpracování. Na rozdíl od úpravy v BDSG však v GDPR vypracovává DPIA přímo správce a nikoliv pověřenec[171]. V BDSG byl správce povinen předat pověřenci veškeré informace o zpracování a pověřenec sám následně provedl předchozí kontrolu.[172]

4.1. Povinnost provést DPIA

GDPR stanovuje obecnou povinnost vypracovat DPIA v čl. 35 odst. 1. Toto ustanovení ukládá povinnost vypracovat DPIA pro ty druhy zpracování, u nichž je pravděpodobné, že zejména při využití nových technologií budou mít s přihlédnutím k povaze, rozsahu, kontextu a účelům za následek vysoké riziko pro práva a svobody fyzických osob. Právy a svobodami fyzických osob se myslí především právo na soukromí, ale obsažena mohou být i další základní práva, jako je například svoboda vyjadřování, myšlení či zákaz diskriminace[173]. GDPR dále k tomuto obecnému vymezení demonstrativně uvádí tři příklady takovéto povahy zpracování v čl. 35 odst. 3.

DPIA bude dle čl. 35 nutné vypracovat vždy, bude-li docházet k systematickému a rozsáhlému vyhodnocování osobních aspektů, založeném na automatizovaném zpracování. V rámci něj dochází k rozhodnutím, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají podobný závažný dopad. Co se považuje za systematické zpracování, objasňují pokyny WP29[174] ve vztahu k povinnosti jmenovat pověřence pro ochranu osobních údajů. Ty považují zpracování za systematické tehdy, když k němu dochází na základě předem daného systému či strategie. Pojem vyhodnocování osobních aspektů se překrývá s pojmem profilování, který je vymezen v čl. 4 odst. 4 GDPR[175]. Příkladem takovéhoto zpracování je cílená reklama.

[171] §4d odst. 6 BDSG.
[172] Tamtéž.
[173] ARTICLE 29 DATA PROTECTION WORKING PARTY, Statement 14/EN WP 218 on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014, Str. 4.
[174] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers (‘DPOs’), adopted on 13 December 2016, Str. 9.
[175] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, Str. 316. ISBN 978-80-7552-765-3.

Jako druhý příklad uvádí GDPR rozsáhlé zpracování zvláštních kategorií podle čl. 9 a čl. 10. GDPR neobsahuje vymezení rozsáhlého zpracování, ale dle doporučení Úřadu pro ochranu osobních údajů[176] se za velký rozsah zpracování osobních údajů považuje zpracování od 10 001 subjektu údajů nebo takové zpracování, kdy má přístup k osobním údajům alespoň 20 osob.

DPIA bude podle čl. 35 také nutné vypracovat tehdy, dochází-li k rozsáhlému systematickému monitorování veřejně přístupných prostorů. GDPR ve svém znění nedefinuje pojem veřejného prostoru, ale jeho bližší vymezení obsahují pokyny WP29[177]. Podle pokynů je veřejný prostor jakýkoliv veřejně přístupný prostor, například obchodní centrum, ulice či veřejná knihovna. GDPR pak ve svém odůvodnění[178] zmiňuje, že se za rozsáhlé monitorování veřejně přístupných prostor budou považovat i zpracování, ke kterým dochází za pomocí optických elektronických přístrojů. Příkladem rozsáhlého systematického monitorování veřejně přístupného prostoru tak může být třeba městský kamerový systém nebo Google Street View.

Dozorové úřady dle čl. 35 odst. 4 a 5 sestaví seznamy druhů operací zpracování, která podléhají a nepodléhají požadavku na vypracování DPIA. Tyto seznamy by měly být za podmínek čl. 35 odst. 6[179] vypracovány na principu mechanismu jednotnosti ve vzájemné spolupráci dozorových úřadů a budou předány Evropskému sboru pro ochranu osobních údajů pro dohled nad dodržováním jednotnosti. Ačkoliv by měly tyto seznamy správcům pomoci při posuzování nutnosti provést DPIA, nelze dle mého názoru očekávat, že tyto seznamy budou zahrnovat širší okruh druhů zpracování, omezí se spíše pouze na ty nejběžnější druhy.

[176] Úřad pro ochranu osobních údajů [online], dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003

[177] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017, Str. 8.

[178] GDPR, odůvodnění 91

[179] Dle čl. 35 odst. 6 je vždy nutné postupovat dle mechanismu jednotnosti tehdy, pokud seznamy zahrnují činnosti zpracování související s nabídkou zboží či služeb subjektům údajů nebo s monitorováním jejich chování v několika členských státech, nebo jestliže dané seznamy mohou výrazně ovlivnit volný pohyb osobních údajů v rámci Unie.

WP29 vypracovala ve svých pokynech[180] kritéria, která by měla pomoci dozorovým úřadům při vypracování výše zmíněných seznamů. Jedná se celkem o 9 kritérií[181], která dle WP29 signalizují, že jde o zpracování s vysokým rizikem pro práva a svobody fyzických osob. Tato kritéria obecně neobsahují žádné nové poznatky pro stanovení zhodnocení míry rizika, spíše na jednom místě shrnují důležitá kritéria již obsažená v jednotlivých článcích a odůvodněních GDPR. Pokyny WP29 jsou ale důležité svým postupem pro vyhodnocení povinnosti provést DPIA. Dle WP29 bude ve většině případů nutné splnit minimálně dvě kritéria, aby šlo o zpracování, u kterého je nutné provést DPIA. Čím více kritérií zpracování správce splní, tím je větší pravděpodobnost, že bude nutné DPIA provést. Pokyny ale nevylučují povinnost provést DPIA i v případě splnění pouze jediného kritéria, a tak i tento postup nelze používat bezpodmínečně a vždy bude zároveň nutné vyhodnotit rizika každého zpracování samostatně ve vztahu k možným následkům pro práva a svobody fyzických osob.

Článek 35 odst. 1 stanovuje, že DPIA je nutné provést vždy před zamýšleným zpracováním, což vychází i ze zásady záměrné ochrany osobních údajů. Správce zamýšlející zpracovávat osobní údaje způsobem, na který se vztahuje povinnost provést DPIA, vždy musí nejdříve DPIA provést a zohlednit povinnosti pro něj z toho plynoucí. Správce má zároveň dle čl. 36 odst. 1 povinnost konzultovat zpracování s dozorovým úřadem, když na základě DPIA dojde k závěru, že nelze přijmout vhodná opatření, která by zmírnila možné následky pro práva a svobody fyzických osob. Nelze ale reálně předpokládat, že správci budou vždy postupovat dle čl. 36 odst. 1 a s dozorovým úřadem zpracování konzultovat vzhledem k tomu, že je tato povinnost uložena na základě správcem provedené analýzy rizik. Správce totiž tímto postupem riskuje, že dozorový úřad dojde dle čl. 36 odst. 2 k závěru, že je dostatečné zmírnění rizik nemožné, a tak zpracování v rámci své pravomoci zakáže.

[180] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017, Str. 7-9.

[181] WP29 uvádí těchto 9 kritérií: 1) hodnocení nebo bodování; 2) automatizované rozhodování, které má právní nebo podobně závažný dopad; 3) systematické monitorování; 4) citlivé údaje nebo údaje vysoce osobní povahy, údaje zpracovávané v rozsáhlém měřítku; 5) přiřazování nebo slučování datových souborů; 6) údaje týkající se zranitelných subjektů údajů; 7) nové použití nebo využití nových technologických nebo organizačních řešení; 8) bránění subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy.

Pokyny WP29[182] vyjadřují názor, že provedení DPIA není jednorázovou věcí, kterou by správce udělal a více se k ní nevracel, ale že jde naopak o trvalý proces, u kterého je vyžadována pravidelná aktualizace. Dle usnesení o návrhu nařízení Evropského parlamentu a Rady[183] byla dokonce předpokládána povinnost správce provádět pravidelné přezkumy DPIA, ale toto ustanovení bylo v konečném znění GDPR vypuštěno, a tak je pravidelná aktualizace DPIA uvedena pouze ve výše zmíněných nezávislých pokynech WP29. GDPR pouze výslovně stanovuje povinnost přezkumu DPIA v případě, kdy dojde ke změně rizika, jež představuje operace zpracování[184].

Na závěr je k povinnosti provedení DPIA nutné dodat, že za vypracování a správnost DPIA je vždy odpovědný správce, a to i v případě, kdy se správce řídí posudkem pověřence pro ochranu osobních údajů. Zpracovatel má dle GDPR uloženu povinnost být nápomocen správci při provedení DPIA, a to přiměřeně dle povahy zpracování a informací, jež má zpracovatel k dispozici[185]. Zpracovatel tedy může být se správcem solidárně odpovědný za předpokladu, že správci neposkytne součinnost při provedení DPIA.

4.2. Koncept provedení DPIA

GDPR kromě stanovení obecných náležitostí čl. 35 odst. 7 neobsahuje žádné konkrétní pokyny pro provedení DPIA. Pokyny WP29 koncept provedení DPIA také neobsahují a pouze odkazují na obecné rámce vypracované úřady pro ochranu údajů členských států EU[186]. Příkladem těchto rámců je již dříve zmíněná metodologie od ICO a CNIL či od německého dozorového úřadu[187].

4.2.1. Příprava provedení DPIA

Přípravná fáze provedení DPIA vychází ze samotného zhodnocení rizikovosti zamýšleného zpracování a nutnosti DPIA provést. V rámci tohoto zhodnocení by měl správce splnit i první

[182] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017, Str. 13.
[183] LEGISLATIVNÍ USNESENÍ EVROPSKÉHO PARLAMENTU, ze dne 12. března 2014 o návrhu nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů, odůvodnění 74(a).
[184] Čl. 35 odst. 11 GDRP.
[185] Čl. 28 odst. 3 písm. f) GDPR.
[186] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017, Str. 20.
[187] Unabhängiges Landeszentrum für Datenschutz.

povinnou náležitost DPIA, kterou je systematický popis zamýšlených operací zpracování a stanovení účelu zpracování[188]. Aby se správce mohl připravit na možné následky zpracování, musí si být plně vědom jeho rozsahu a toku všech zpracovávaných osobních údajů. V rámci tohoto základního posouzení by se správce měl také ujistit, že zamýšlené zpracování bude splňovat základní zásady zpracování osobních údajů, jakými je například účelové omezení a minimalizace údajů[189]. Správce by měl mít také zmapován okruh osob, které mají nebo budou mít k osobním údajům přístup. Obecně by se správce neměl omezovat pouze na předcházení vnějším rizikům, ale měl by si být zároveň vědom úskalí, ke kterým může dojít v rámci samotného správcova provozu či činnosti.

4.2.2. Posouzení nezbytnosti zpracování

Nedílnou součástí každého DPIA musí být posouzení nezbytnosti a přiměřenosti zpracování z hlediska účelu[190]. Každé zpracování osobních údajů je zásahem do práva na soukromí, a to bez ohledu na oprávněnost zpracování na základě právního titulu. Správce by měl tedy zpracovávat pouze relevantní osobní údaje, a to přiměřeně a omezeně v nezbytném rozsahu ve vztahu k účelu, pro který jsou zpracovávány[191]. Zásada minimalizace osobních údajů je stejně jako ostatní zásady aplikovatelná na veškerá zpracování osobních údajů spadajících do působnosti GDPR. Ve vztahu k provedení DPIA je vzhledem k povaze vysokého rizika zpracování o to důležitější na tuto zásadu nezapomenout a vždy její posouzení v DPIA uvést.

4.2.3. Vymezení rámce ochrany

K efektivnímu zhodnocení rizik zpracování je vhodné si vymezit okruhy povinností, které správci plynou ze znění GDPR a v rámci těchto okruhů stanovit vhodná technická a organizační opatření. Podle německého vzoru lze tyto okruhy povinností vymezit jako tzv. cíle ochrany[192], které jsou používány v rámci IT bezpečnosti. Německá federativní úprava ochrany osobních údajů cíle ochrany používá pro vymezení povinností správců a jejich použití se nabízí jako vhodné i pro zhodnocení rizik v rámci GDPR. Navíc jak již bylo dříve zmíněno, pokyny WP29

[188] Čl. 35 odst. 7 písm. a) GDPR.
[189] FELIX BIEKER et al., A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Springer International Publishing Switzerland 2016, Str. 28

[190] Čl. 35 odst. 7 písm. b) GDPR.
[191] Čl. 5 odst. 1 písm. c) GDPR.
[192] Překlad z německého gewährleistungsziel

odkazují na standardní model pro ochranu údajů[193], který byl vypracovaný právě německým dozorovým úřadem pro ochranu osobních údajů a který cíle ochrany detailně popisuje. Konkrétně tento model rozlišuje celkem šest cílů ochrany a každý z nich vymezuje různé povinnosti správce.

Availability ("dostupnost")

Cíl ochrany dostupnosti vychází v GDPR z článku 32 odst. 1 písm. b) a c) ve vztahu k zabezpečení zpracování. Stanovuje povinnost správce zajistit neustálou dostupnost zpracování a schopnost správce včas obnovit dostupnost osobních údajů a přístup k nim v případě fyzických či technických problémů. Cíl ochrany dostupnosti je dále předpokladem pro realizaci některých práv subjektu údajů, a to především práva na přístup a práva na portabilitu[194]. Model dále zahrnuje pod tento cíl ochrany i zásadu omezení uložení, která stanovuje povinnost ukládat osobní údaje ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány[195].

Integrity ("integrita")

Cíl ochrany integrity vychází v GDPR z článku 5 odst. 1 písm. f)[196]. Stanovuje povinnost osobní údaje náležitě zabezpečit pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Osobní údaje by zároveň měly být vždy přesné a neměly by být neoprávněně měněny.

Confidentiality ("důvěrnost")

Důvěrnost je spojena s povinností mlčenlivosti a s povinností chránit osobní údaje před neoprávněným zpracováním. Osobní údaje by správcem měly být vždy zpracovávány na základě právního titulu a neměly by být neoprávněně předávány třetím stranám. V případě zpracování osobních údajů zpracovatelem je nutné ve zpracovatelské smlouvě stanovit

[193] Unabhängiges Landeszentrum für Datenschutz [online]., Dostupné z: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf
[194] Čl. 15 a 20 GDPR.
[195] Čl. 5 odst. 1 písm. e) GDPR.
[196] Povinnost zachovat integritu je dále stanovena i v čl. 32 odst. 1 písm. b) GDPR.

povinnost mlčenlivosti pro všechny osoby oprávněné ke zpracování[197]. Cíl ochrany důvěrnosti vychází ze stejných ustanovení jako zásada integrity[198].

Unlinkability ("nespojitelnost")

Cíl ochrany nespojitelnosti vychází ze zásady účelového omezení[199], která stanovuje, že osobní údaje mohou zpracovány pouze pro určité, výslovně vyjádřené a legitimní účely, a to pouze na základě jednoho z právních titulů uvedených v článku 6. Správce by tedy měl vždy zpracovávat osobní údaje jen k dosažení účelu konkrétního zpracování a ne již pro účely další.

Transparency ("transparentnost")

Tomuto cíli ochrany odpovídá zásada transparentnosti[200], která prostupuje celým GDPR a všemi povinnostmi správce. Zásada transparentnosti vyjadřuje povinnost správce být otevřený a transparentní ohledně toho, jakým způsobem je s osobními údaji nakládáno, a povinnost chovat se dle rozumného očekávání subjektu údajů ohledně způsobu zpracování[201]. Základním předpokladem pro dodržení zásady transparentnosti je splnění informační povinnosti dle čl. 13 a 14.

Intervenability ("zakročitelnost")

Zakročitelnost se promítá do práva subjektu údajů mít nad svými zpracovávanými údaji přehled a kontrolu. Správce by měl subjektu údajů zaručit uplatnění jeho práv po organizační a technické stránce a toto uplatnění by měl zároveň co nejvíce usnadňovat, což vyplývá i ze zásady transparentnosti.

4.2.4. Zhodnocení a posouzení rizik

K zvolení vhodných technických a organizačních opatření je nutné zhodnotit výši rizik jednotlivých druhů zamýšlených zpracování. Standardní model pro ochranu údajů rozděluje zpracování do kategorií podle toho, zda je nutná "normální", "vysoká" nebo "velmi vysoká" ochrana[202]. Každý správce musí při zpracovávání osobních údajů zhodnotit rizika zpracování, a to bez ohledu na povinnost provést DPIA. Posouzením rizik pro účely provedení DPIA jsou

[197] Čl. 28 odst. 3 písm. b) GDPR.
[198] Čl. 5 odst. 1 písm. e) a čl. 32 odst. 1 písm. b) GDPR.
[199] Čl. 5 odst. 1 písm. b) GDPR.
[200] Čl. 5 odst. 1 písm. a) GDPR.
[201] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, Str. 106. ISBN 978-80-7552-765-3.
[202] UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ, Standard Data Protection Model, 2016, Str. 34.

myšleny zpracování dle čl. 35 odst. 1, tedy taková zpracování, která představují vysoké riziko pro práva a svobody fyzických osob. Vysoké riziko je ale dále nutné kategorizovat a za pomoci dříve zmíněného rámce cílů ochrany k němu přiřadit vhodné technické či organizační opatření.

4.2.5. Výběr vhodného opatření

Ačkoliv čl. 32 odst. 1 uvádí demonstrativně určitá technická a organizační opatření, výběr vhodného opatření je vždy velmi specifický vzhledem ke konkrétnímu zpracování. Standardní model pro ochranu údajů obsahuje výčet typických opatření[203] pro každý z cílů ochrany. I když se ale jedná o výčet těch nejčastějších opatření, pořád by k nim správce měl přistupovat pouze jako k doporučenému vodítku a v případě potřeby by měl implementovat i opatření jiná. Správce by měl dle odůvodnění GDPR vzít v úvahu rizika, která zpracování představuje. Jsou jimi např. náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předaných, uložených nebo jiným způsobem zpracovaných osobních údajů, která by mohla vést zejména k fyzické, hmotné nebo nehmotné újmě[204]. V DPIA musí být uvedena plánovaná opatření řešení rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů[205].

4.2.6. Implementační plán DPIA a dokumentace

Kromě zvolení vhodných technických a organizačních opatření je k úspěšnému provedení DPIA vhodné stanovit i opatření a pravidla samotného provedení DPIA. Měla by být zvolena odpovědná osoba, která DPIA provede a bude konzultovat s pověřencem a dozorovým úřadem. Zvolení odpovědné osoby je důležité především pro řádné dokumentování provedení DPIA a pro případy, kdy zpracovávají osobní údaje společní správci. Dále je vhodné, aby si správce stanovil kritéria, podle nichž bude hodnotit účinnost implementovaných technických a organizačních opatření, a aby určil osobu odpovědnou za vyhodnocení, není-li jí správce sám. V poslední řadě je také důležité, aby se pro jednotlivá opatření stanovila doba jejich implementace[206].

Správce je povinen v souladu s principem odpovědnosti doložit soulad splnění svých povinností, a to obecně ke všem svým povinnostem včetně provedení DPIA. Zdokumentován

[203] UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ, Standard Data Protection Model, 2016, Str. 27-30.
[204] Odůvodnění 83 GDPR.
[205] Čl. 35 odst. 7 písm. d) GDPR.
[206] FELIX BIEKER et al., A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Springer International Publishing Switzerland 2016, Str. 34-35

by měl být celý proces přijetí zahrnující všechny body zmíněné v předešlých odstavcích této kapitoly. Dokumentace by měla obsahovat stanovisko pověřence pro ochranu osobních údajů, které by mělo dle pokynů WP29 řešit následující témata. Těmi jsou: a) zhodnocení povinnosti DPIA provést, b) doporučení pro volbu vhodné metodiky, c) doporučení pro interní či externí provedení DPIA, d) navrhovaná opatření, e) posouzení správnosti provedení DPIA a zhodnocení závěrů[207]. Dle těchto pokynů není správce povinen se posudkem pověřence pro ochranu osobních údajů řídit. V případě, kdy správce s posudkem nesouhlasí a nechce DPIA provést navrhovaným způsobem, musí své rozhodnutí v dokumentaci řádně odůvodnit.

Zdokumentování provedení DPIA je důležité i pro případnou konzultaci s dozorovým úřadem podle čl. 36. V případě povinnosti správce konzultovat s dozorovým úřadem je správce povinen dle stejného článku předložit úřadu provedené DPIA, na základě kterého se vedle jiných věcí bude úřad rozhodovat o uplatnění příslušné pravomoci.

GDPR neukládá správci povinnost DPIA zveřejnit, avšak dle pokynů správce dobrovolným zveřejněním podpoří důvěru ve zpracování a prokáže odpovědnost a transparentnost[208]. Pokyny zdůrazňují, že není nutné zveřejňovat celou dokumentaci DPIA, ale pouze její závěry. Posouzení může obsahovat informace týkající se bezpečnostních rizik či obchodních tajemství, a tak by úplné zveřejnění často nebylo ani možné[209].

4.3. Závěr k provedení DPIA

Povinné provedení DPIA v GDPR pro určité druhy zpracování reflektuje snahu Evropské unie o celkové zvýšení ochrany osobních údajů. Všichni správci bez ohledu na nutnost provést DPIA jsou povinni přijmout vhodná technická a organizační opatření a svůj postup řádně zdokumentovat. Vypracování DPIA je komplexní proces, který vyžaduje po správci provedení důkladnějšího rozboru rizik a zvážení vhodných opatření, převážně z důvodu rizikovější povahy zpracování. Úprava DPIA mohla být podle mého názoru konkrétnější v případě vymezení zpracování s vysokým rizikem pro práva a svobody subjektu údajů. Článek 35 vymezuje

[207] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers (‘DPOs’), adopted on 13 December 2016, Str. 15.
[208] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, adopted on 4 April 2017, Str. 21.
[209] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017, Právo pro praxi. Str. 111, ISBN 978-80-271-0668-4.

zpracování velmi obecným způsobem, a to většinou i bez náležitého vymezení pojmů. Je zřejmé, že cílem čl. 35 bylo ochránit veškeré rizikovější zpracování, což se dle mého názoru podařilo. Na druhou stranu je očividné, že povinnost provedení DPIA nebude pouze záležitostí velkých společností, ale že bude dopadat i na společnosti menší, kterým jejich povinnost provést DPIA nemusí být ze znění GDPR vůbec jasná. Článek 4 GDPR obsahující definice by měl dle mého názoru obsahovat i další pojmy, jako je např. systematické zpracování či rozsáhlé zpracování, vzhledem k tomu, že na základě výkladu těchto pojmů se bude správce často rozhodovat, zda DPIA provést, či nikoliv. Některé pojmy jsou sice dodatečně upřesněny pokyny WP29, avšak vzhledem k jejich nezávaznému charakteru je lze brát spíše jako pomůcku či doporučení než jako závazný právní výklad. Pro efektivní použití tohoto nového unijního institutu bude také důležitý přístup národních dozorových úřadů k plnění jejich povinností sestavit seznamy zpracování, která buď podléhají, nebo nepodléhají[210] povinnosti DPIA provést.

[210] V době dokončování této práce Úřad pro ochranu osobních údajů zveřejnil návrh seznamu zpracování, která nepodléhají DPIA [online], dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30738

Závěr

Rozsah a způsob zpracování osobních údajů se za více než 20 let od přijetí směrnice 95/46/ES výrazně změnil a přijetí nové úpravy, která by tyto změny reflektovala, bylo nutné. GDPR bylo vydáno formou nařízení s cílem harmonizovat úpravu ochrany osobních údajů a zaručit větší ochranu subjektům údajů na území Unie. Ačkoliv neuplynulo od účinnosti GDPR mnoho času, lze dle mého názoru už teď říci, že vyšší ochrany osobních údajů bude přijetím GDPR skutečně dosaženo. GDPR bylo veřejně velmi diskutovaným tématem již od svého schválení v dubnu 2016 a tento stav nadále trvá i po dni jeho účinnosti. Správci, ať už jako jednotlivci či menší, nebo větší organizace, získali povědomí o svých povinnostech ve vztahu k subjektu údajů a byli dostatečně postrašeni nově zavedenými vysokými pokutami.

Nicméně je také nutné dodat, že ačkoliv je harmonizace ochrany osobních údajů v Unii přelomovým momentem, není samotná úprava obsažená v GDPR pro oblast ochrany osobních údajů něčím úplně novým. GDPR vychází z původní směrnice 95/46/ES, kterou v mnohých věcech pouze rozšiřuje či upřesňuje. Některá nová práva a povinnosti nebyly sice výslovně stanoveny ve směrnici 95/46/ES, nebo byly upraveny velmi omezeně, ale nezřídka vyplývaly z judikatury Soudního dvora Evropské unie. Příkladem může být často diskutované právo na výmaz, které nejenže bylo upraveno v omezeném rozsahu již ve směrnici 95/46/ES, ale zároveň bylo později rozšířeno judikaturou Soudního dvora Evropské unie. GDPR obsahuje ale i práva úplně nová, jako je právo na portabilitu, a přináší i mnoho jiných změn a institutů.

Některé nově zavedené instituty byly používány v mnohých členských státech již před účinností GDPR, a to například institut DPIA nebo institut pověřence. Institut pověřence má v oblasti ochrany osobních údajů velmi silnou tradici v Německu, kde úprava povinnosti jmenovat pověřence byla ve federativní podobě přísnější než v GDPR. Institut pověřence se zde osvědčil jako důležitý preventivní prvek ochrany osobních údajů u všech rizikovějších zpracování. V mnohých jiných členských státech byl institut pověřence také zaveden národními úpravami, avšak ve většině států byl pověřenec pouze dobrovolnou funkcí. Povinné jmenování pověřence je tedy pro členské státy výraznou změnou, a to bez ohledu na to, že úprava pověřence není v GDPR tak přísná jako například zmíněná německá federativní úprava.

DPIA je důležitým novým institutem ochrany osobních údajů, který GDPR v unijním právu zavádí. Národní úpravy některých členských států sice tento institut už znají, ale

neupravují provedení DPIA jako samostatnou povinnost. Spíše se jedná o doporučení ve formě vhodného prostředku k implementaci opatření pro zajištění ochrany osobních údajů. Proces provedení DPIA není ve znění GDPR popsán a jako vhodné východisko k jeho provedení se jeví inspirace metodologiemi vydanými dozorovými úřady členských států. Komplexnější proces posouzení rizik a přijetí vhodných opatření u rizikovějších zpracování je dle mého názoru důležitým novým prvkem ochrany, avšak vzhledem k nejednoznačnému vymezení této povinnosti lze očekávat snížení účinnosti tohoto nového institutu.

Nová úprava ochrany osobních údajů v Unii, která by reflektovala technologický pokrok, byla nutná. GDPR zpřísňuje podmínky zpracování osobních údajů a klade na správce i na zpracovatele mnohem více povinností. Subjekty údajů mají nyní silnější postavení a větší kontrolu nad svými osobními údaji. U rizikovějších zpracování nově existují na unijní úrovni dodatečné záruky kvality, obecné nároky na zabezpečení osobních údajů byly posunuty o úroveň výše.

Závěrem lze tedy konstatovat, že GDPR samotnou oblast ochrany osobních údajů neposouvá výrazně obsahově nikam dále, ale pouze rozšiřuje původní unijní úpravu, a k tomu navíc přijímá některé nové, ale pro oblast ochrany osobních údajů již známé instituty. GDPR lze za přelomovou úpravu ochrany osobních údajů považovat v Evropské unii hlavně díky skutečnosti, že bylo přijato formou nařízení, a nikoliv formou směrnice.

Seznam zdrojů

Knižní publikace

A. KUČEROVÁ A KOL., Zákon o ochraně osobních údajů: komentář. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony, ISBN 978-80-7179-226-0.

GONZÁLEZ-FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. New York: Springer, 2014. Law, governance and technology series, ISBN 3319050222.

NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, ISBN 978-80-7380-689-7.

NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017, Právo pro praxi, ISBN 978-80-271-0668-4.

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR), ISBN 978-80-7478-665-5.

NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, ISBN 978-80-7552-765-3.

ANNI-MARIA TAKA, Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications, Master's Thesis, Uppsala Universitet, 2017

Prameny práva a jiné právní dokumenty

a) Právní předpisy a mezinárodní smlouvy

Zákon 101/2000 Sb. O ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů

Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Směrnice evropského parlamentu a rady 97/66/ES ze dne 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikace

Směrnice evropského parlamentu a rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES

Směrnice evropského parlamentu a rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikace

Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009

Úmluva o ochraně lidských práv a základních svobod ze dne 4. listopadu 1950.

Všeobecná deklarace lidských práv ze dne 10 prosince 1948.

Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních údajů ze dne 28. ledna 1981.

Mezinárodní pakt o občanských a politických právech ze dne 19. prosince 1966.

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted on 23 September 1980.

Úmluva k provedení Schengenské dohody ze dne 14. června 1985 mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích

Smlouva o fungování Evropské unie

Legislativní usnesení evropského parlamentu, ze dne 12. března 2014 o návrhu nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů

Vládní návrh zákona o zpracování osobních údajů předložený 28.3. 2018

Federal Data Protection Act (BDSG) in the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66 (Bundesdatenschutzgesetz)

b) Pokyny WP29

ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 adopted on 4 April 2017

ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability adopted on 13 December 2016

ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016

ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion on the use of location data with a view to providing value-added services, November 2015

ARTICLE 29 DATA PROTECTION WORKING PARTY, Statement 14/EN WP 218 on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014

ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011 and Opinion 5/2004 on unsolicited communications for marketing purposes under article 13 of Directive 2002/58/EC.

ARTICLE 29 WORKING PARTY: Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications

c) Sdělení, rezoluce, strategie, white papers

81/679/EEC: Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data

OJ L 122/47: Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radiofrequency identification.

90/C 277/03: Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data

90/C 277/04: Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks

IP/10/1462, strategie, jak posílit předpisy EU o ochraně údajů ze dne 4. listopadu 2010

Úřad pro ochranu osobních údajů, Přístup Úřadu k pokutování, 2018, dostupné z: https://www.uoou.cz/pristup-uradu-k-nbsp-pokutovani/d-31044

d) Soudní rozhodnutí

C-213/15, Rozsudek Soudního dvora Evropské unie ze dne 19. října 2016, Patrick Breyer proti Spolkové republice Německo, ECLI:EU:C:2016:779.

C-131/12, Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 13. května 2014 Google Spain SL, Google Inc. proti Agencia Espanola de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317.

Spojené věci C-585/08 a C-144/09, Rozsudek soudního dvora EU (velkého senátu) ze dne 7. prosince 2010 Peter Pammer proti Reederei Karl Schlüter GmbH & Co. KG a Hotel Alpenhof GesmbH proti Oliver Heller

e) Publikace dozorových úřadů členských států EU

Úřad pro ochranu osobních údajů, k povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA), dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003

Úřad pro ochranu osobních údajů, návrh seznamu zpracování, které nepodléhají DPIA, dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30738

Německý dozorový úřad spolkové země Šlesvicko-Holštýnsko (Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein), dostupné z: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf

Elektronické zdroje

a) Elektronické knižní publikace a příspěvky ve sbornících

Agentura Evropské unie pro základní práva, Příručka evropského práva v oblasti ochrany údajů, Úřad pro publikace Evropské unie 2014, ISBN 978-92-871-9933-1, dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=15363

LINKLATERS, GDPR booklet, dostupné z: https://lpscdn.linklaters.com/-/media/files/linklaters/pdf/mkt/london/tmt_data_protection_survival_guide_singles.ashx?rev=5ef6afd7-f614-4423-9145-0a9d0a60a452

Bird & Bird, Cookies v české republice, dostupné z: http://www.fccps.cz/data/cookies.pdf

Kinast & Partner, DPO in Europe, dostupné z: https://www.kinast-partner.com/wp-content/uploads/2014/09/dpo-in-europe.pdf

BITCOM, Risk assessment & data protection impact assessmen guide [online], dostupné z http://www.digitalestadt.org/bitkom/org/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf

FELIX BIEKER et al., A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Springer International Publishing Switzerland

b) Internetové články

EVA ŠKORNIČKOVÁ, Musíte mít pověřence? A jak ho vybrat?, 2018, dostupné z: https://www.gdpr.cz/blog/vyber-poverence/

Nový německý zákon o ochraně osobních údajů, 2017, dostupné z: http://www.gdprbezobav.cz/novy-nemecky-zakon-ochrane-osobnich-udaju/

Reforma ochrany osobních údajů v eu z pohledu pracovněprávních vztahů, dostupné z: http://www.bulletin-advokacie.cz/reforma-ochrany-osobnich-udaju-v-eu-z-pohledu-pracovnepravnich-vztahu

Zpracování biometrických údajů ve světle obecného nařízení o ochraně osobních údajů (GDPR), dostupné z: https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-ve-svetle-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-106028.html

OLIVER SÜME, Data Protection: Does the German Implementation Act (BDSG-E) undermine the GDPR?, dostupné z: https://privacylawblog.fieldfisher.com/2017/data-protection-does-the-german-implementation-act-bdsg-e-undermine-the-gdpr

Taylor Wessing, The compliance burden under the GDPR - Data Protection Officers, dostupné z: https://www.lexology.com/library/detail.aspx?g=37cd2a6d-9bbf-4db0-a66e-05d74a22291c

Data protection officer according to German law, dostupné z: https://www.activemind.legal/law/de-data-protection-officer/

DAVID BURIAN, K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů, dostupné z https://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr

THOMAS SHAW, What skills should your DPO absolutely have? [online], dostupné z: https://iapp.org/news/a/what-skills-should-your-dpo-absolutely-have/

c) Ostatní

Facebook business, Co je obecné nařízení o ochraně údajů (GDPR)? Dostupné z: https://www.facebook.com/business/gdpr

Federal Office for Information Security, Privacy Impact Assessment Guideline for RFID Applications, [online], dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1

Vybrané otázky aktuální právní úpravy osobních údajů v Evropské unii

Abstrakt

Diplomová práce s názvem „Vybrané otázky aktuální právní úpravy osobních údajů v Evropské unii“ je zaměřena na přiblížení vývoje ochrany osobních údajů v Evropské unii a na aktuální změny v této oblasti unijního práva.

První kapitola je zaměřena na historický vývoj ochrany osobních údajů na evropském kontinentě se zaměřením na vývoj v Evropské unii. V této kapitole je přiblížen postupný vývoj práva na ochranu osobních údajů, které se začalo formovat v rámci práva na soukromí jako důsledek rozvoje technologií. V první kapitole je dále zmíněna ochrana osobních údajů v primárním a sekundárním právu Evropské unie, která se stala základem pro jeho další vývoj.

Druhá kapitola se věnuje komparaci původní unijní úpravy ochrany osobních údajů obsažené ve směrnici 95/46/ES s novou úpravou obsaženou v GDPR. Ke komparaci byly vybrány nejdůležitější změny a společně s nimi ty, které byly před účinností nařízení veřejností často diskutované. Dílčím cílem této kapitoly je vysvětlit čtenáři míru změn, které GDPR do oblasti ochrany osobních údajů skutečně přivádí.

Třetí kapitola podrobně popisuje institut pověřence pro ochranu osobních údajů, který je pro unijní právo zcela novým institutem. Institut pověřence je v třetí kapitole detailně rozebrán a srovnán s německou federativní úpravou, která má s tímto institutem již dlouholeté zkušenosti.

Poslední čtvrtá kapitola se zabývá posouzením vlivu na ochranu osobních údajů. V kapitole je čtenář obeznámen se samotným institutem a zároveň je mu přiblížen samotný koncept provedení posouzení, který není v GDPR dostatečně upraven. K přiblížení provedení posouzení bylo využito metodologie německého dozorového úřadu, která byla zpracována pro aplikaci nejen federativní německé úpravy ochrany osobních údajů, ale také i pro aplikaci GDPR a je tak skvělým východiskem pro lepší pochopení implementace posouzení.

Závěr diplomové práce je věnován celkovému zhodnocení původní unijní úpravy v kontextu s GDPR. Shrnuje na jedné straně potřebnost harmonizace této oblasti v Evropské

unii, ale zároveň poukazuje na to, že po obsahové stránce není GDPR pro oblast ochrany osobních údajů přelomovou úpravou.

Klíčová slova: osobní údaj, GDPR, pověřenec, posouzení vlivu na ochranu osobních údajů

Selected issues of the current legal regulation of protection of personal data in the European Union

Abstract

The thesis „Selected issues of the current legal regulation of protection of personal data in the European Union“ is focused on describing the development of personal data in the European Union and on current changes in this field of European law.

The first chapter is focused on the historical development of the personal data protection on the European continent with the specific aim of looking at the development in the European Union. This chapter describes the progressive development of the right to the protection of personal data which was formed within the right to privacy because of technological developments. The first chapter also talks about personal data protection in primary and secondary legislation which became the foundation for the further development.

The second chapter is devoted to the comparison of the former EU regulation of the personal data protection in the directive 95/46/ES with the new regulation in GDPR. The most important changes were chosen for the comparison together with the ones which were often discussed prior to GDPR coming into effect. The interim goal of this chapter is to explain to the reader the extent of changes which GDPR brings to the field of personal data protection.

The third chapter is focused on the institute of the data protection officer which is a new institute in European law. The institute of the data protection officer is analyzed and compared in detail with the German federative regulation which has long-time experience with this institute.

The final fourth chapter talks about the institute of data protection impact assessment. The reader is familiarized with this institute in this chapter together with the concept of carrying out the assessment which is not sufficiently described in GDPR. Methodology of the German data protection authority was used for the purposes of describing the implementation. This methodology was made not just for the use of the German federative regulation but also for the purposes of GDPR and it is therefore a great base for a better understanding of the implementation.

The closing part is devoted to the overall assessment of the formal regulation in relation to GDPR. It concludes the necessity of harmonization of this field in the European Union but at the same time it points out that GDPR is not revolutionary in the field of personal data protection regarding its content.

Keywords: personal data, GDPR, data protection officer, data protection impact assessment