

**UNIVERZITA KARLOVA  
PRÁVNICKÁ FAKULTA**

Mgr. Klára Havlíčková

**PODOBA SOUHLASU SE ZPRACOVÁNÍM  
OSOBNÍCH ÚDAJŮ VE SVĚTLE OBECNÉHO  
NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ**

Rigorózní práce

Vedoucí práce: doc. Dr. iur. Harald Christian Scheu, Mag. phil., Ph.D.

Tematický okruh: Katedra evropského práva

Datum vypracování práce (uzavření rukopisu): 17.2.2019

### **Prohlášení**

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

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 232 910 znaků včetně mezer.

V Praze dne \_\_\_\_\_

Mgr. Klára Havlíčková

## **Poděkování**

Děkuji doc. Dr. iur. Haraldu Christianu Scheuovi, Mag. phil., Ph.D., za odborné vedení a laskavou pomoc při vedení této práce. Dále také děkuji svým nejbližším za pomoc a podporu během mého studia.

## Obsah

Úvod.....	1
1 Terminologický a historický úvod do problematiky ochrany osobních údajů 5	
1.1 Ochrana soukromí.....	5
1.2 Pojem soukromí.....	7
1.3 Relevantní právní předpisy.....	9
1.4 Pracovní skupina WP29.....	15
2 Nedostatky Směrnice 95/46/ES.....	18
2.1 Věcná působnost Směrnice 95/46/ES.....	21
2.2 Územní působnost Směrnice 95/46/ES.....	26
2.3 Kritika vymezení územní působnosti Směrnice 95/46/ES.....	29
2.4 Osobní údaj dle Směrnice 95/46/ES.....	32
2.5 Způsob transpozice Směrnice 95/46/ES do českého právního řádu..	33
2.6 Vybraná rozhodnutí SDEU.....	34
2.7 Důvody pro přijetí GDPR.....	41
3 Nová koncepce GDPR oproti původní úpravě.....	44
3.1 Působnost GDPR.....	44
3.1.1 Věcná působnost GDPR.....	45
3.1.2 Územní působnost GDPR.....	49
3.2 Vymezení pojmu „osobní údaj“.....	51
3.2.2 IP adresa jako osobní údaj.....	52
3.2.3 Cookies.....	54
3.3 Zrušení oznamovací povinnosti a nové povinnosti správců.....	56
4 Aspekty souhlasu subjektu údajů dle GDPR.....	58
4.1 Podmínky vyjádření souhlasu.....	62
4.2 Právo na opravu.....	64
4.3 Právo být zapomenut (právo na výmaz).....	65
4.3.1 Aspekty „práva být zapomenut“.....	66
4.3.2 Legislativní zakotvení „práva být zapomenut“.....	68
4.3.3 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González C-131/12.....	70

4.3.4	Úprava „práva být zapomenut“ v GDPR .....	82
4.4	Právo na omezení zpracování .....	84
4.5	Právo na přenositelnost údajů .....	85
4.6	Právo vznést námitku.....	88
4.7	Souhlas se zpracováním osobních údajů dítěte .....	89
4.8	Podoba souhlasu se zpracováním osobních údajů .....	92
5	Adaptační zákony členských států .....	95
5.1	Česká republika .....	97
5.1.1	Působnost adaptačního zákona .....	99
5.1.2	Výjimka z povinnosti posuzování slučitelnosti účelů .....	101
5.1.3	Věková hranice dítěte pro udělení souhlasu se zpracováním osobních údajů .....	102
5.1.4	Výjimka z povinnosti posouzení vlivu zpracování osobních údajů na ochranu osobních údajů.....	103
5.1.5	Povinnost jmenovat pověřence pro ochranu osobních údajů a výklad pojmu veřejný subjekt .....	104
5.1.6	Zpracování prováděné pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu.....	105
5.1.7	Výše sankcí pro veřejnoprávní subjekty .....	107
5.1.8	Souhlas se zpracováním osobních údajů .....	108
5.1.9	Trestání a odpovědnost.....	109
5.2	Slovenská republika.....	111
5.3	Rakouská republika .....	113
	Závěr.....	115
	Seznam zkratk.....	121
	Seznam použitých zdrojů .....	122
	Podoba souhlasu se zpracováním osobních údajů ve světle Obecného nařízení o ochraně osobních údajů .....	132
	Abstrakt .....	132
	Klíčová slova:.....	133

## Úvod

V dubnu 2016 byl na půdě Evropské unie přijat nový právní předpis o ochraně osobních údajů v právní formě nařízení, které nabylo účinnosti dne 25. května 2018. Ke dni účinnosti tohoto nařízení se zároveň zrušil dosavadní právní předpis EU upravující danou problematiku, Směrnice 95/46/ES<sup>1</sup>, která v posední době čelila silné vlně kritiky zejména kvůli své nejednotnosti a nepružnosti s ohledem na rozvoj nových technologií. Nové nařízení „General Data Protection Regulation“ (GDPR)<sup>2</sup> má i s ohledem na svou přímou použitelnost v členských státech EU tyto nežádoucí vlastnosti eliminovat a napomoci tak vzniku jednotného souboru pravidel a tím i k posílení právní jistoty v oblasti ochrany osobních údajů, a dále k posílení samotného digitálního trhu.

GDPR v zásadě primárně principy zrušované úpravy zachovává a dále je rozvíjí, obsahově výraznější změny je tak třeba spatřovat zj. v upraveném vymezení územní působnosti GDPR, v rozšíření práv subjektů údajů, v zavedení nových povinností pro správce osobních údajů, případně zpracovatelů, včetně jmenování tzv. *data protection officera*, nebo-li pověřence pro ochranu osobních údajů, která vychází ze Směrnice 95/46/ES, v rámci níž bylo možné jmenovat pověřence pro ochranu osobních údajů jako náhradu za obecnou oznamovací povinnost. GDPR s sebou přináší i hrozbu nových sankcí, které mohou být

---

<sup>1</sup> Směrnice Evropského parlamentu a Rady (EU) č. 95/46/ES ze dne 24.10.1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

<sup>2</sup> 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/ES.

vypočítávány z ročního obratu společnosti. Dále GDPR např. zrušil informační povinnosti správce vůči dozorovému úřadu. Nebude tak nadále třeba před zahájením zpracování osobních údajů oznamovat dozorovému úřadu např. to, v jakém rozsahu a za jakým účelem budou osobní údaje zpracovávány, informace specifikující subjekty údajů, specifikace zpracovatele a další náležitosti přihlášky.

Cílem této rigorózní práce je upozornit na nedostatky Směrnice 95/46/ES včetně dílčího výzkumu problematiky její územní působnosti, vlivu Směrnice 95/46/ES na vývoj práva o ochraně osobních údajů mimo území EU/EHP a vymezení zpracování osobních údajů pro osobní potřebu. Autorka v úvodní části této práce zkoumá i vztah Listiny základních práv a svobod EU s GDPR. Dále má tato práce za cíl vymežit důvody pro přijetí GDPR včetně posouzení nezbytnosti jeho přijetí a důvodnosti nařízení jako formy nové právní úpravy. Práce má v neposlední řadě také za cíl analyzovat práva subjektů údajů spolu s podmínkami udělení platného souhlasu se zpracováním osobních údajů včetně kritického zhodnocení stávající praxe obchodníků a otázky platnosti souhlasu se zpracováním osobních údajů uděleného konkludentně a problematiky ověřování souhlasu se zpracováním dítěte schváleného nebo vyjádřeného osobou vykonávající rodičovskou zodpovědnost k dítěti.

Vzhledem k tomu, že Česká republika nedokázala včas přijmout adaptační zákon, autorka v poslední kapitole práce upozorňuje na rizika vyplývající z této situace, kdy se v mezičase do účinnosti adaptačního zákona aplikuje GDPR v plném rozsahu (včetně např. výše sankcí). Dále se v této kapitole autorka věnuje možnému postupu Evropské komise proti státům, které nepřijaly adaptační zákon včas a rozboru vybraných ustanovení návrhu adaptačního zákona včetně ustanovení, která dle GDPR umožňují

odlišnou národní úpravu, a kterou český zákonodárce nevyužil. V této kapitole autorka také zkoumá věcnou působnost návrhu českého zákona a právní úpravu Slovenské a Rakouské republiky, když tyto dva státy použily odlišné možnosti adaptace zákona.

S ohledem na vymezení cílů, je práce členěna do sedmi kapitol, kdy první je věnována úvodu do historie a právních pramenů ochrany osobních údajů včetně vymezení pojmu soukromí a dílčí výzkumné otázky vztahu GDPR s Listinou základních práv svobod. Druhá kapitole se zabývá analýzou jednotlivých nedostatků Směrnice 95/46/ES včetně kritického zhodnocení územní působnosti tohoto právního předpisu a jeho vlivu na vývoj práva ochrany osobních údajů mimo prostor EU/EHP a zodpovězením otázky ohledně nezbytnosti přijetí nové právní úpravy. Další čtyři kapitoly jsou věnovány právní úpravě GDPR, včetně analýzy práv subjektů údajů spolu s dílčím výzkumem výkladu ustanovení čl. 12 písm. b) Směrnice 95/46/ES v souvislosti s analýzou a kritickým zhodnocením soudního rozhodnutí Google Spain, náležitostí souhlasu se zpracováním osobních údajů a dílčí výzkumné otázky, za jakých podmínek lze IP adresu a soubory cookies považovat za osobní údaje podléhající právní úpravě GDPR a dále analýzou podmínek výkonu práva na přenositelnost údajů, nového práva, které GDPR zavádí. Poslední kapitola se zabývá adaptačními zákony České, Slovenské a Rakouské republiky, kdy každý stát přijal prováděcí zákon v odlišném rozsahu. Autorka se v této kapitole také zabývá diskuzí nad vzniklým stavem, kdy se v ČR do doby účinnosti nového zákona na ochranu osobních údajů použije GDPR v plném rozsahu.

Při zpracování zvoleného tématu vycházela autorka především z primárních pramenů, judikátů a poznatků nauky. Zvolila přitom analytickou metodu zkoumání relevantních institutů, norem a procesů. Pro samotný



koncept práce pak byly důležité odborné publikace domácí i zahraniční provenience.

# 1 Terminologický a historický úvod do problematiky ochrany osobních údajů

## 1.1 Ochrana soukromí

Ochrana osobních údajů se jako samostatná právní disciplína postupně vyčlenila z obecnější problematiky ochrany soukromí, a to v souvislosti s technologickým pokrokem probíhajícím od druhé poloviny 20. století. Ochrana soukromí tak z historického hlediska představuje materiální východisko pro vznik ochrany osobních údajů. Obě tyto právní disciplíny mají společný účel, a to ochranu jednotlivce před zásahy do jeho soukromí. Ochrana osobních údajů však cílí pouze na takové zásahy do soukromí, ke kterým dochází specifickým způsobem a jako taková se nachází ve vztahu speciality k pojmu ochrany soukromí.

První zmínku o právu na soukromí najdeme ve článku „The Right to Privacy“ od autorů S.D.Warrena a L.D.Brandeise vydaném v roce 1890 v Harvard Law Review,<sup>3</sup> ve kterém bylo právo na soukromí poprvé definováno jako samostatná právní disciplína. V článku se jeho autoři vyslovili pro zajištění práva na nerušený duševní klid, neznepokojování a nerušení člověka v jeho příbytku v okruhu jeho nejbližších, před vnějším zasahováním. Právo na soukromí bylo v tomto tradičním chápání pojímáno jako „právo být ponechán o samotě“ („*the right to be let alone*“).<sup>4</sup>

---

<sup>3</sup> WARREN, S. D., BRANDEIS, L. D. *The Right to Privacy*. In Harvard Law Review 4/1890, č. 5. [online] [cit. 2017-10-17]. Dostupné z [http://faculty.uml.edu/sgallagher/harvard\\_law\\_review.htm](http://faculty.uml.edu/sgallagher/harvard_law_review.htm).

<sup>4</sup> NOVÁK, D. *Problémy ochrany soukromí a osobních údajů v právu EU*. Disertační práce. Právnická fakulta Masarykovy univerzity. 2010/2011. Dostupné z: [https://is.muni.cz/th/52154/pravf\\_d/disertacni\\_prace.pdf](https://is.muni.cz/th/52154/pravf_d/disertacni_prace.pdf).

Na evropském kontinentu můžeme vznik práva na soukromí v moderním smyslu zasadit do devatenáctého století, kdy existovalo především v podobě jeho dílčího práva, a to práva na ochranu osobní cti.<sup>5</sup> Z roku 1920 pak pochází československý ústavní zákon č. 293/1920Sb., o ochraně svobody osobní, domovní a tajemství listovního, jehož účelem bylo poskytnout ochranu individuálních zájmů proti přehmatům orgánů veřejné moci.<sup>6</sup>

Zájem o ochranu soukromí pak vzrostl po zkušenostech s totalitárními a autoritativními režimy dvacátého století, zj. po druhé světové válce, kdy docházelo k masovému zneužívání registrů obsahující data i náboženské příslušnosti občanů. Požadavek na ochranu soukromí byl spojen i s všeobecným lidsko-právním hnutím prosazujícím se po druhé světové válce, kdy toto právo (na soukromí) začalo být pojímáno jako jedno ze základních lidských práv. Pozdějším mocným impulsem k vyzdvihnutí významu ochrany soukromí ve společnosti byl rozvoj informačních a komunikačních technologií.<sup>7</sup> Důležitý mezník ve vývoji pak z formálního hlediska představuje přijetí Evropské úmluvy o ochraně lidských práv z roku 1950, která v článku 8 zakotvila právo každého na respektování soukromého a rodinného života, obydlí a korespondence.

V českém právním řádu byla v době komunistického režimu existence práva na soukromí dovozována právní doktrínou s odkazem na všeobecnou klauzuli ochrany osobnosti,<sup>8</sup> kdy bylo poukazováno na nezbytnost jeho zajištění, jakožto předpokladu rozvoje člověka a možnosti jeho sociálního uplatnění. Samotný ideál totalitní společnosti představovala názorově monolitická společnost.

---

<sup>5</sup> MATES, P. *Ochrana soukromí ve správním právu. 2. aktualizované a podstatně přepracované vydání*. Praha: Linde Praha, a.s., 2006. 314 s. ISBN: 80-7201-589-3.

<sup>6</sup> MALÝ, K., SOUKUP, L. *Československé právo a právní věda v meziválečném období a jejich místo ve střední Evropě*. Praha: Karolinum, 2010. ISBN: 978-80-246-1718-3.

<sup>7</sup> MILLER, A. *The Assault on Privacy: Computers, Data Banks and Dossiers*. Ann Arbor: University of Michigan Press, 1971. [online]. [cit. 23-10-17]. Dostupné z: <http://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2880&context=caselrev>.

<sup>8</sup> Zákon č. 40/1964 Sb., občanský zákoník obsahoval poměrně komplexní úpravu osobnostních práv, avšak v jeho původním znění nebylo právo na soukromí v rámci demonstrativního výčtu osobnostních práv v §11 výslovně uvedeno.

Totalitní stát proto z těchto důvodů nemohl mít zájem na výslovném deklarování práva na soukromí, jehož uplatnění v praxi by mohlo vést k formování odlišných myšlenkových proudů. Až do přijetí Listiny základních práv a svobod v roce 1991 náš režim proto ochranu soukromí prakticky nepřipouštěl.<sup>9</sup>

## 1.2 Pojem soukromí

Pojmy soukromí a svoboda jsou vzájemně podmíněny a dle Elišky Wagnerové „*kde má být svoboda, tam musí být soukromí*“.<sup>10</sup> Samotný pojem soukromí je těžké jednoznačně definovat, protože jeho chápání je velmi subjektivní a zároveň odvisí na faktoru místa a času.

Evropský soud pro lidská práva zdůraznil v případě Niemietz versus Německo,<sup>11</sup> že nepokládá za možné ani vhodné formulovat vyčerpávající definici soukromí ani jejích složek. Své rozhodnutí odůvodnil tak, že v jeho pojetí je soukromí dynamickou kategorií, která se vyvíjí a může se obohacovat o další složky vzhledem k době, prostředí, společenské situaci, kultuře a dalším objektivním prvkům a souvislostem, v níž daná osoba žije. Konkrétní podoba soukromí je pak zpravidla určena judikaturou soudů v jednotlivých případech. Z těchto důvodů bývá právo na soukromí či soukromý život charakterizováno jako právo soudní, vzhledem k tomu, že jeho obsah je určován hlavně judikaturou soudů, a to především ústavních a mezinárodních.<sup>12</sup> Soukromí by ale dle autorky

---

<sup>9</sup> MATES, P. *Ochrana soukromí ve správním právu. 2. aktualizované a podstatně přepracované vydání*. Praha: Linde Praha, a.s., 2006. 314 s. ISBN: 80-7201-589-3.

<sup>10</sup> WAGNEROVÁ, E. *Právo na soukromí: kde má být svoboda, tam musí být soukromí*. IN: ŠIMÍČEK, V. *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011, s. 54-59. ISBN 978-80-210-5449-3.

<sup>11</sup> Rozhodnutí Evropského soudu pro lidská práva ze dne 16. 12. 1992 ve věci Niemietz vs. Německo, stížnost č. 13710/88 nebo dále např. rozhodnutí Evropského soudu pro lidská práva ze dne 28. 1. 2003 ve věci Peck v. Spojené království, stížnost č. 44647/98.

<sup>12</sup> NUTILOVÁ H., *Ochrana osobních údajů*. Dizertační práce. Právnická fakulta Univerzity Karlovy. 2012. Dostupné z: <https://is.cuni.cz/webapps/zzp/detail/68996/26915763/?q=%7B%22searchform%22%3A%22nutilov%5Cu00e1%22%2C%22searchform%22%3A%22butsearch%22%3A%22>

mohlo být vymezeno obecnou definicí prostoru v životě jednotlivce, kam nikdo nesmí zasahovat bez jeho souhlasu, ledaže jde o zákonný důvod opřený o objektivní společenský zájem. Úřad pro ochranu osobních údajů pojem soukromí vymezil jako osobní, intimní sféru člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského tvora. Pojem soukromí obsahuje rovněž hmotný i myšlenkový prostor jednotlivce, součástí soukromého života je i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.<sup>13</sup>

Ochrana soukromí je materiálně vzájemně provázána s problematikou osobnostních práv, když právo na soukromí zahrnuje např. právo na ochranu občanské cti a lidské důstojnosti, právo na ochranu listovního tajemství, právo na rodinný život a jeho ochranu. Tato souvislost je ostatně vystižena systematickým zařazením osobnostních práv a práva na soukromí v článku 10 Listiny základních práv a svobod České republiky.<sup>14</sup> Ústavní soud ČR ve svém rozhodnutí ve věci návrhu skupiny poslanců Poslanecké sněmovny Parlamentu České republiky na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů a na zrušení vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání<sup>15</sup> zároveň uznal jako jeden z aspektů ochrany soukromí i možnost jednotlivce svobodně rozhodovat, které osobní informace z jeho života budou zveřejněny. Ústavní soud judikoval, že „*Právo na respekt*

---

[Vyhledat%22%2C%22\\_facetform\\_facets\\_faculty%22%3A%5B%2211220%22%5D%2C%22PNzppSearchListbasic%22%3A1%7D&lang=cs.](#)

<sup>13</sup> Stanovisko Úřadu pro ochranu osobních údajů č. 6/2009. Ochrana soukromí při zpracování osobních údajů. [cit. 2017-10-11]. Dostupné z <https://www.uoou.cz/stanovisko-c-6-2009-ochrana-soukromi-pri-zpracovani-osobnich-udaju/d-1519>.

<sup>14</sup> Usnesení č. 2/1993Sb. Usnesení předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky.

<sup>15</sup> Viz Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, 94/2011Sb.

*k soukromému životu zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení zda, popř. v jaké rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení, výslovně garantovaný čl. 10 odst.3 Listiny. Právo na informační sebeurčení je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu."*

Dle autorky lze uzavřít, že koncept soukromí je velmi specifický, neboť jeho vnímání je subjektivní pro každého jednotlivce i celé společnosti a současně proměnlivé v čase. Soukromí *de facto* představuje svazek určitých dílčích práv a svobod, jež chrání osobnost člověka, přičemž se jedná o časově proměnlivou hodnotu.

### **1.3 Relevantní právní předpisy**

Po druhé světové válce se do středu zájmu mezinárodního společenství dostala otázka ochrany lidských práv, a to zejména v souvislosti se založením a vznikem Organizace spojených národů (dále jen jako „OSN“) a posléze s přijetím **Všeobecné deklarace lidských práv a svobod z roku 1948**, která mimo jiné ve svém článku 12 stanoví, že „*nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst, každý má právo na zákonnou ochranu proti takových zásahům nebo útokům*“.

Za základní kámen evropské právní úpravy ochrany osobních údajů lze označit **Evropskou úmluvu o ochraně lidských práv a svobod** z roku 1950,

když v článku 8 stanoví, že „každý má právo na respektování svého soukromí a rodinného života, obydlí a korespondence“ a dále v článku 10 týkajícího se práva svobody projevu uvádí, že „každý má právo na svobodu projevu. Toto právo zahrnuje svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování státních orgánů a bez ohledu na hranice“.

Během 60. a 70. let 20. století se v souvislosti s rozvojem informačních technologií nabízela stále silněji otázka, zda-li je tehdejší úroveň ochrany osobních údajů postačující, a zda není potřeba právní úpravu revidovat. Průzkum provedený na základě žádosti Parlamentního shromáždění Rady Evropy v evropských státech potvrdil skutečnost, že dosavadní mezinárodní úprava neposkytuje soukromí jednotlivce dostatečnou míru ochrany.<sup>16</sup>

Z roku 1981 pak pochází **Úmluva č. 108** na ochranu osob se zřetelem na automatické zpracování osobních údajů („Úmluva 108“), která ve své preambuli uvádí jako jeden ze svých cílů „rozšířit ochranu práv a základních svobod každého, zejména právo na soukromý život, se zřetelem k zesílenému toku automatizovaně zpracovávaných údajů přes hranice“. K Úmluvě 108 byl pak v roce 2001 přijat Dodatkový protokol.<sup>17</sup>

Úmluva 108 měla za cíl reagovat na technický vývoj a rozvoj moderních metod zpracování a uchovávání osobních údajů a je koncipována jako určitý minimální základ pro právní úpravu v oblasti ochrany osobních údajů, když se tato úmluva vztahovala pouze na automatizované zpracování dat. Smluvní strany mají dle Úmluvy 108 ale možnost rozšířit její aplikovatelnost i na neautomatizované zpracování osobních údajů. Následující vývoj v oblasti

---

<sup>16</sup> KUČEROVÁ A., BARTÍK V., PECA J., NEWIRT K., NEJEDLÝ J., *Zákon o ochraně osobních údajů. Komentář*. 1.vyd., Praha: C.H. Beck, 2003.

<sup>17</sup> Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice ze dne 8.11.2001, publikovaný jako Sdělení Ministerstva zahraničních věcí č. 29/2005 Sb.m.s.

zpracování osobních údajů však ukázal, že omezení ochrany osobních údajů podle použitého technického prostředku zpracování je takto regulováno nevyhovujícím způsobem, neboť některým subjektům, resp. u některých zpracování, umožňovalo vyhnout se právní regulaci zvolením neautomatizovaného zpracování (bylo-li to pro správce výhodné). Proto se s ohledem na charakter Úmluvy 108, která je mezinárodní smlouvou, tento stav částečně modifikoval teprve prostřednictvím dodatkových protokolů. Díky této zkušenosti se jevílo jako nebytné přijmout a stanovit působnost Směrnice 95/46/ES<sup>18</sup> stejně jako následně českého zákona o ochraně osobních údajů<sup>19</sup> na jakékoliv zpracování bez ohledu na využití prostředky. Na tento vývoj reagovala také Česká republika jako signatář Úmluvy 108, která svým prohlášením podle čl. 3 odst. 2 písm. c) této úmluvy rozšířila její působnost i na zpracování neautomatizované.<sup>20 21</sup>

Úmluva 108 pak ve své výsledné podobě představuje ucelený mezinárodní dokument, neboť vymezuje základní pojmosloví jako např. osobní údaj, subjekt osobních údajů, správce osobních údajů, automatizovaný soubor dat, automatizované zpracování či citlivý osobní údaj. Dále pak jsou v této úmluvě zakotveny základní zásady zpracování osobních údajů, jež byly později promítnuty do Směrnice 98/46/ES. Konkrétně se jedná o požadavky na kvalitu shromažďovaných a zpracovávaných osobních údajů (např. zásada legality a legitimacy, přiměřenosti, zásada shromažďování osobních dat pouze pro stanovené účely), požadavky na zajištění ochrany údajů před jejich zneužitím, práva náležejícím subjektům údajů (právo na opravu či výmaz nepřesných nebo nepravdivých údajů) a zásady pro předávání osobních údajů přes hranice, kdy

---

<sup>18</sup> Srov. čl. 3 odst. 1 a bod odůvodnění 27 Směrnice 95/46/ES.

<sup>19</sup> S výjimkami dále uvedenými v §3 odst. 3 a 4 zákona č. 101/2000 Sb. o ochraně osobních údajů.

<sup>20</sup> Srov. Sdělení Ministerstva zahraničních věcí č. 8/2005 Sb. m. s.

<sup>21</sup> KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů*. Komentář. 1. vydání. Praha: C. H. Beck, 2012, 536 s.



bylo principiálně stanoveno pravidlo, že přijímající stát musí zajistit adekvátní úroveň ochrany srovnatelnou s úrovní ochrany ve smluvních státech. Kritérii pro hodnocení zajišťované úrovně ochrany jsou pak především úroveň kvality národní vnitrostátní právní úpravy či existence nezávislého kontrolního orgánu dozoru. Úmluva 108 nerozlišuje, na rozdíl od předpisů EU, sektorové oblasti zpracování a zahrnuje jak civilní, tak policejní nebo justiční či zpravodajské zpracování.

Na Úmluvu 108 pak navázala doporučení<sup>22</sup> Rady Evropy vládám pro nakládání s osobními údaji pro specifické oblasti (např. oblast direct marketingu)<sup>23</sup>. Úmluva se dle článku 3 odst. 1 vztahuje na automatizované systémy jak ve veřejném, tak i v soukromém sektoru. Z důvodu této omezené působnosti tak nemohla úmluva pokrýt veškeré oblasti potenciálních zásahů do soukromí. Na tento nedostatek (mimo jiné) tak na evropské úrovni zákonodárce reagoval přijetím Směrnice 95/46/ES.

Dne 1. prosince 2009 nabyla platnosti **Listina základních práv Evropské unie**. Listina je po vstupu v platnost Lisabonské smlouvy právně závazným dokumentem, který má stejnou právní sílu jako zakládací smlouvy EU.<sup>24</sup> Listina se stala součástí legislativy Evropské unie a je tak důležitým dokumentem nejen z interpretačního hlediska, ale i z hlediska její přímé aplikace.<sup>25</sup> V článku 7 Hlavy II se uvádí, že „každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace“. Článek 8 je pak speciálním ve vztahu k tomuto ustanovení, když stanoví, že „každý má právo na ochranu osobních údajů, které se ho týkají“ a „tyto údaje musí být zpracovány

---

<sup>22</sup> Tzv. *recommendations*.

<sup>23</sup> Doporučení č. r (85) Výboru ministrů členským státům o ochraně osobních údajů používaných pro účely přímého marketingu ze dne 25. října 1985. Dostupné z: <https://www.uouu.cz/doporuzeni-c-r-85-20-vyboru-ministru-clenskym-statum-o-ochrane-osobnich-udaju-pouzivanych-pro-ucely-primeho-marketingu/ds-1825/archiv=2&p1=1659>.

<sup>24</sup> Viz článek 6 odst. 1 Smlouvy o Evropské unii.

<sup>25</sup> Blíže viz např. ŠTURMA, P. *Lisabonská smlouva a závaznost Listiny základních práv EU pro Českou republiku vzhledem k tzv. výjimce (opt-out)*. [Právní rozhledy 6/2010, 191-194 s].

*korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem“ a „na dodržování těchto pravidel dohlíží nezávislý orgán“.* Právo na ochranu soukromí a právo na ochranu osobních údajů se tak stává základním právem zakotveným přímo v právu Evropské unie. Orgány, instituce a jiné subjekty Evropské unie stejně jako členské státy při aplikaci práva EU musí tato práva dodržovat.

Přijetí Lisabonské smlouvy představuje zásadní mezník ve vývoji evropského práva na ochranu osobních údajů, nejenom z důvodu právní závaznosti Listiny jako primárního pramene práva EU. Článek 16 SFEU obsahuje jako obecně použitelné ustanovení práva EU *právo každého na ochranu osobních údajů, které se ho týkají*. Toto ustanovení také obsahuje zmocnění Evropského parlamentu a Rady k přijetí legislativního aktu týkajícího se ochrany osobních údajů institucemi EU. Článek 16 SFEU tak představuje právní základ nového, komplexního přístupu evropského práva k ochraně osobních údajů, pokrývající veškeré pravomoci EU včetně policejní a justiční spolupráci v trestních věcech. Toto ustanovení se tak stalo právním základem pro přijetí GDPR a pro přijetí tzv. trestněprávní směrnice.<sup>26 27</sup> GDPR je tedy *de facto* prováděcím předpisem Listiny, když provádí její příslušný článek a státy jsou tak povinny při aplikaci GDPR, případně při aplikaci adaptačních zákonů jednat v souladu s Listinou.

Základním principem ochrany osobních údajů v EU deklarované Listinou je zásada legality zpracování osobních údajů, jež vyžaduje zpracování osobních údajů za legitimním a předem stanoveným účelem a v neposlední řadě Listina

---

<sup>26</sup> Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

<sup>27</sup> European agency for fundamental rights: *Handbook on European data protection law* – 2018 edition, s. 28. Dostupné z: <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law>.

požaduje existenci kontrolního mechanismu ve vztahu k dodržování pravidel na ochranu osobních údajů prostřednictvím nezávislého kontrolního orgánu, působícího jak na horizontální, tak na vertikální úrovni právních vztahů.

Článek 52 odst. 1 Listiny zároveň zakotvuje podmínky pro omezení výkonu práva na ochranu osobních údajů, když dle rozhodovací praxe SDEU právo na ochranu osobních údajů se neprojevuje jako absolutní výsada, ale musí k němu být přihlédnuto ve vztahu k jeho funkci ve společnosti.<sup>28</sup> Dané ustanovení stanoví, že *každé omezení výkonu práv a svobod uznaných touto listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.*

Čl. 52 odst. 3 Listiny formuluje minimální standard ochrany odkazující na Evropskou úmluvu o lidských právech. Tam, kde práva obsažená v Listině odpovídají právům zaručeným Evropskou úmluvou o lidských právech, jsou jejich obsah a smysl stejné jako ty, které jim příkládá Evropská úmluva. To ale nebrání tomu, aby právo EU poskytlo v některých případech širší ochranu, než je garantována Evropskou úmluvou. Listina tak představuje „nadstavbu“ ve vztahu k dosavadnímu primátu Evropské úmluvy o lidských právech v oblasti právního zakotvení lidských práv.<sup>29</sup>

---

<sup>28</sup> Viz např. Rozsudek SDEU ze dne 9. 11. 2010, ve spojených věcech Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen, C-92/09 a C-93/09, para 48.

<sup>29</sup> NUTILOVÁ H., *Ochrana osobních údajů*. Dizertační práce. Právnická fakulta Univerzity Karlovy. 2012. Dostupné z: <https://is.cuni.cz/webapps/zzp/detail/68996/26915763/?q=%7B%22searchform%22%3A%22nutilov%5Cu00e1%22%2C%22searchform%22%3A%22Vyhledat%22%2C%22facetform%22%3A%5B%2211220%22%5D%2C%22PNzzpSearchListbasic%22%3A1%7D&lang=cs>.

Pro úplnost autorka dodává, že ustanovení Listiny jsou určena v první řadě orgánům, institucím a jiným subjektům Evropské unie. Členskými státy jsou určena v případech, kdy uplatňují právo EU, nikoliv v případě, kdy jednají čistě ve sféře vnitrostátního práva.<sup>30</sup>

**Směrnice 95/46/ES** obsahově navazuje na Úmluvu 108, ale její pravidla dále rozšiřuje, neboť se již neomezuje pouze na oblast osobních údajů zpracovávaných automaticky. Směrnice 95/46/ES ve svém bodu č. 10 odůvodnění přímo navazuje na úpravu ochrany lidských práv založenou Evropskou úmluvou o lidských právech, když stanoví, že „*předmětem vnitrostátních právních předpisů o zpracování osobních údajů je chránit základní práva a svobody, zejména právo na soukromí uznané v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod i v obecných zásadách práva Společenství.*“

#### **1.4 Pracovní skupina WP29**

Dle čl. 29 Směrnice 95/46/ES byl zřízen nezávislý poradní orgán, tzv. pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů (tzv. WP29).<sup>31</sup> Pracovní skupina měla být dle Směrnice 95/46/ES složena z vrcholných představitelů orgánů zabezpečujících ochranu osobních údajů v jednotlivých členských zemích, konkrétně ji tvořili zástupci orgánů dozoru v jednotlivých členských státech, zástupce úřadu evropského inspektora ochrany osobních údajů a konečně zástupce Komise.

Pracovní skupina měla dle článku 30 Směrnice 95/46/ES za úkol posuzovat veškeré otázky týkající se uplatňování vnitrostátních předpisů přijatých

---

<sup>30</sup> Viz čl. 51 odst. 1 Listiny základních práv EU.

<sup>31</sup> Zkratka vzniklá spojením anglického „working party“ a příslušného článku Směrnice 95/46/ES, na jehož základě byla zřízena.

k provedení Směrnice 95/46/ES a to s cílem přispívat k jejímu jednotnému uplatňování; zaujímat pro Komisi stanovisko o úrovni ochrany v Evropské unii a ve třetích státech; poskytovat Komisi poradenství o všech návrzích změn Směrnice 95/46/ES a dále o všech návrzích opatření v Evropské unii, která by měla být přijata pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů a zaujímat stanovisko ke kodexům chování vypracovaných na úrovni Evropské unie.<sup>32 33</sup> Ačkoliv tato pracovní skupina neměla rozhodující vliv na tvorbu předpisů týkajících se ochrany osobních údajů (měla toliko pouze oprávnění vydávat nezávazná doporučení a stanoviska pro Komisi), byl její význam nepopiratelný z toho důvodu, že pro její prestižní obsazení byla její stanoviska a doporučení Komisí zpravidla respektována. Význam skupiny dále spočíval i v jednotném výkladu aktů evropského práva v oblasti ochrany osobních údajů. Pracovní skupina WP29 dále vypracovávala výroční zprávu o stavu úrovně ochrany osob v souvislosti se zpracováním osobních údajů ve Společenství a ve třetích zemích, která byla adresována Evropskému parlamentu, Radě a Komisi a byla i zveřejňována.<sup>34</sup>

Ke dni účinnosti GDPR se tato pracovní skupina WP29 změnila na Evropský sbor pro ochranu osobních údaj jakožto nejvyššího dozorového orgánu. Tento nový orgán se od stávající WP29 liší především rozšířením svých pravomocí, kdy nově může rozhodovat spory mezi dozorovými úřady nebo rozhodovat o postupech v naléhavých případech a v těchto případech má pravomoc vydávat

---

<sup>32</sup> Úkoly pracovní skupiny WP29 jsou popsány jednak v článku 30 Směrnice 95/46/ES a v článku 15 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, dle kterého WP29 plní i úkoly týkající se záležitostí upravených touto směrnicí, zejména co se týká ochrany základních práv a svobod a oprávněných zájmů v odvětví elektronických komunikací.

<sup>33</sup>Např. Stanovisko č.4/2010 k evropskému kodexu chování FEDMA pro používání osobních údajů v přímém marketingu. Přijaté dne 13. července 2010.

<sup>34</sup> Např. Sixteen Report of the Article 29 Working Party on Data Protection Covering the year 2012. Dostupný z: [http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/files/2014/16th\\_annual\\_report\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/files/2014/16th_annual_report_en.pdf).

závazná rozhodnutí. Dalšími jeho úkoly je zejména zajišťovat jednotné uplatňování GDPR a za tímto účelem monitorovat jeho uplatňování a vydávat pokyny, doporučení a osvědčené postupy týkající se postupů pro výmaz odkazů, kopií nebo replikací osobních údajů z veřejně dostupných komunikačních služeb, dále poskytovat poradenství Komisi ve veškerých záležitostech souvisejících s ochranou osobních údajů v Evropské Unii včetně jakýchkoli navrhovaných změn GDPR.<sup>35</sup>

---

<sup>35</sup> Srov. čl. 70 GDPR.

## 2 Nedostatky Směrnice 95/46/ES

Směrnice č. 95/46/ES byla v roce 1995 přijata jako nástroj harmonizace evropské úpravy ochrany osobních údajů. Pro její přijetí hlasovaly všechny členské státy až na Velkou Británii, která se hlasování zdržela. Směrnici také přijaly i tři nečlenské státy EU<sup>36</sup> (Island<sup>37</sup>, Lichtenštejnsko<sup>38</sup> a Norsko<sup>39</sup>). Směrnice 95/46/ES prostřednictvím povinnosti transpozice předurčuje obsah základních právních předpisů vydaných členskými státy, které se týkají ochrany osobních údajů a vychází z tehdejších čl. 94 a čl. 95 Smlouvy o ES<sup>40</sup> a objevují se názory, že hlavní hybnou silou na poli harmonizace ochrany osobních údajů byla Spolková republika Německo, jejíž právní řád zahrnoval nejpropracovanější systém pravidel ochrany osobních údajů, který současně komplikoval svými vysokými požadavky obchodní aktivity německých firem.<sup>41</sup>

---

<sup>36</sup> Jedná se o státy Evropského hospodářského prostoru (EHP). EHP je prostorem, ve kterém dohoda o EHP zaručuje svobodu pohybu zboží, osob, služeb a kapitálu uvnitř Evropského jednotného trhu, Vznikl 1. ledna 1994 na základě dohody uzavřené mezi Evropským sdružením volného obchodu (ESVO/EFTA) a Evropskou unií v roce 1992. Dohoda o EHP specifikuje, že jeho členství je otevřeno pro členy EU a ESVO a rozšířila na celém území EHP platnost čtyř základních svobod (volný pohyb zboží, osob, služeb a kapitálu), jaké platí na území EU. Podmínkou rozšíření těchto svobod pro občany na území Islandu, Norska a Lichtenštejnska je zejména zavádění vymezených částí legislativy EU do právních řádů těchto států. Státy EHP mají tedy povinnost implementovat směrnice EU do svého právního řádu. GDPR tak bude v těchto státech také přímo použitelné a nahradí dosud přijatou Směrnicí 95/46/ES.

<sup>37</sup> Island Směrnicí 95/46/ES implementoval prostřednictvím zákona na ochranu osobních údajů z roku 2000 (Act on the Protection of Individuals with Regard to the Processing of Personal data No.77/2000, Republic of Ireland).

<sup>38</sup> Lichtenštejnsko Směrnicí 95/46/ES implementovalo prostřednictvím zákona na ochranu osobních údajů z roku 2002 (Data Protection Act of 14 March 2002).

<sup>39</sup> Norsko Směrnicí 95/46/ES implementovalo prostřednictvím zákona na ochranu osobních údajů z roku 2000 (Personal Data Act LOV-2000-04-14-31).

<sup>40</sup> srov. čl. 114 a 115 SFEU.

<sup>41</sup> NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související*. 1. vydání. Praha: Wolters Kluwer, 2014. 504 s. ISBN: 9788074786655, s.41.

Mezi hlavní cíle přijetí Směrnice patřily: (i) ochrana soukromí jednotlivců v souvislosti se zpracováním osobních údajů a (ii) harmonizace právní úpravy ochrany osobních údajů členských států EU.<sup>42</sup> Za tímto účelem Směrnice 95/46/ES stanoví zj. zákonné podmínky zpracování osobních údajů, práva subjektů údajů a požadavky na kvalitu zpracovávaných osobních údajů. Směrnice 95/46/ES usilovala o dosažení srovnatelné úrovně ochrany osobních údajů ve všech členských státech za účelem usnadnění přenosu osobních údajů přes hranice členských států Evropské unie (zj. tedy snaha o to, aby členské státy neomezovaly či nezakazovaly volný pohyb osobních údajů mezi členskými státy s odkazem např. na rozdílný standard ochrany v cílové zemi).<sup>43</sup>

Profesoři Solove a Schwartz ji označili za důležitý legislativní akt stanovující základní právní rámec zpracování osobních údajů v rámci Evropské unie a zároveň uvádí, že Směrnice 95/46/ES měla celosvětový vliv na vývoj práva o ochraně osobních údajů.<sup>44</sup> Protože dle jejího článku 25 mohou být osobní údaje předávány do třetích zemích pouze v případě, pokud dotyčná třetí země zajistí odpovídající úroveň ochrany, měla implementace Směrnice 95/46/ES vliv nejenom na vnitrostátní předpisy členských států EU, ale zároveň ovlivnila i přijetí vhodných metod ochrany soukromí ve třetích zemích, např. přijetí zákona o ochraně osobních údajů v Argentině z listopadu roku 1998.<sup>45</sup> Argentinský zákon mimo jiné vyžaduje výslovné udělení souhlasu před shromážděním, uchováním, zpracováním nebo předáním daných osobních údajů, stanovuje podmínky pro

---

<sup>42</sup> CAREY, P. *Data Protection A Practical Guide to UK and EU Law*. 4.vydání. Oxford: Oxford university press, 2015. s.6.

<sup>43</sup> Viz čl. 1 směrnice 95/46/ES/ES: „Členské státy zajišťují v souladu s touto směrnicí ochranu základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů“, odst. 1. „Členské státy nemohou omezit ani zakázat volný pohyb osobních údajů mezi členskými státy z důvodů ochrany zajištěné podle odstavce 1“, odst. 2.

<sup>44</sup> SOLOVE, D. a SCHWARTZ, P. *Information privacy law*. 5. vydání, New York: Wolters Kluwer, 2015. s.688.

<sup>45</sup> S. 577/98, Ley de Protección de los Datos Personales, 26. listopadu. 1998.



nakládání s citlivými osobními údaji a umožňuje přeshraniční předávání osobních údajů pouze v případě, že dotyčná země zajišťuje odpovídající úroveň ochrany. Dále např. zákon o ochraně osobních údajů<sup>46</sup> přijatý v roce 1995 v Hong Kongu obsahuje stejné podmínky pro předávání osobních údajů do třetích zemí jako Směrnice 95/46/ES, také jeho požadavek na informování subjektu údajů o možnosti zvolení režimu opt-out v případě přímého marketingu vychází z evropské právní úpravy.<sup>47</sup> Z požadavků zakotvených ve Směrnici 95/46/ES dále vychází i Turecký zákon na ochranu osobních údajů č. 6698 ze dne 7. dubna 2016 (jedná se např. o požadavek shromažďování osobních údajů pro stanovené účely, výslovně vyjádřené a legitimní; požadavek na korektní, zákonné a přiměřené zpracování osobních údajů pouze po dobu nezbytnou pro uskutečnění cílů, pro které jsou data shromažďována nebo zpracována či o informační povinnost vůči subjektu údajů o totožnosti správce, účely zpracování či o jednotlivých právech subjektu údajů).<sup>48</sup>

Jako další přínos Směrnice 95/46/ES lze také označit vymezení její věcné působnosti, kdy na rozdíl od dříve přijaté Úmluvy 108 se Směrnice 95/46/ES dotýká nejen automatizovaného, ale i manuálního zpracování osobních údajů. Směrnice 95/46/ES dále stanovuje technické požadavky na bezpečnost zpracování a povinnost členských států pověřit alespoň jeden orgán dozoru,

---

<sup>46</sup> Personal Data (Privacy) Ordinance.

<sup>47</sup> BANISAR, D. and Davies, S., *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments* (August 30, 2012). John Marshall Journal of Computer & Information Law, Vol. XVIII, No. 1, Fall 1999. [online] [cit. 03-02-2018]. Dostupné z: <https://ssrn.com/abstract=2138799>. s. 48.

<sup>48</sup> BURAK ÖZDAĞISTANLI: *Data protection in Turkey: overview*. [online] [cit. 09-02-2018]. Dostupné z: [https://uk.practicallaw.thomsonreuters.com/Document/I02064fb01cb611e38578f7ccc38dcbee/View/FullText.html?transitionType=CategoryPageItem&contextData=\(sc.Default\)&navId=A702EEBF2A7AF6A067738D04222CB4F7&comp=pluk#co\\_anchor\\_a795431](https://uk.practicallaw.thomsonreuters.com/Document/I02064fb01cb611e38578f7ccc38dcbee/View/FullText.html?transitionType=CategoryPageItem&contextData=(sc.Default)&navId=A702EEBF2A7AF6A067738D04222CB4F7&comp=pluk#co_anchor_a795431).

který bude dohlížet na dodržování předpisů přijatých členskými státy na základě této směrnice.

Za hlavní nedostatek Směrnice 95/46/ES tak autorka, na základě výše uvedeného, považuje samotnou formu tohoto legislativního aktu, který již z povahy věci nemůže zajistit zcela jednotnou úpravu ochrany osobních údajů v jednotlivých členských státech a dále jistou zastaralost této právní úpravy, kdy Směrnice 95/46/ES byla přijímána v době neexistence sociálních sítí, jako např. Facebook či cloudových úložišť. Za problematické také autorka považuje vymezení územní působnosti Směrnice 95/46/ES, kdy touto problematikou se bude zabývat dále.

## **2.1 Věcná působnost Směrnice 95/46/ES**

Věcná působnost Směrnice 95/46/ES byla vymezena v článku 3 a dle jeho prvního odstavce se vztahovala na zcela nebo částečně automatizované zpracování osobních údajů, které jsou obsaženy v rejstříku nebo do něj mají být zařazeny. Toto vymezení působnosti představovalo posun oproti vymezení věcné působnosti Úmluvy 108, kdy ta byla omezena výhradně na osobní údaje zpracovávané automaticky. Tento posun je jistě třeba vnímat pozitivně, a to z důvodu poskytnutí záruk ochrany osobních údajů dopadající na rozmanitější rozsah činností, a navíc tak byla úpravou ve Směrnici 95/46/ES vyloučena možnost obcházení právního režimu ochrany osobních údajů zaváděním ryze manuálního zpracování v praxi.<sup>49</sup>

---

<sup>49</sup> K výkladu pojmu „zpracování“ srov. rozhodnutí ESD ze dne 6. listopadu 2003, C-101/01 ve věci Lindqvist. V tomto rozhodnutí soud judikoval, že pojem „zpracování“ takových údajů, použitý v čl. 3 odst. 1 směrnice 95/46, zahrnuje v souladu s definicí obsaženou v čl. 2 písm. b) této směrnice „jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů“. Posledně uvedené ustanovení obsahuje několik příkladů takových úkonů, včetně sdělení prostřednictvím přenosu, šíření nebo jakéhokoli jiného zpřístupnění. Z toho vyplývá, že za takové zpracování je třeba považovat i úkon spočívající v uvedení osobních údajů na internetové stránce.

Druhý odstavec pak obsahoval dvě výjimky, na které se Směrnice 95/46/ES nevztahovala a to:

- (i) na zpracování osobních údajů *prováděné pro výkon činností, které nespádají do oblasti působnosti práva Společenství a jsou uvedeny v hlavě V<sup>50</sup> a VI<sup>51</sup> Smlouvy o Evropské unii, a v každém případě na zpracování, které se týká veřejné bezpečnosti státu [...] a činnosti státu v oblasti trestního práva;*

V souvislosti s tím bod odůvodnění č. 16 Směrnice 95/46/ES dále upřesňoval a rozváděl: *... tato směrnice se nevztahuje na zpracování údajů tvořených zvuky či obrazy, jako například údajů zjištěných při dohledu pomocí videokamer, pokud byly zavedeny pro zajištění veřejné bezpečnosti [...] nebo pro výkon jiných činností, které nespádají do oblasti působnosti práva Společenství.*

- (ii) a dále se Směrnice 95/46/ES nevztahuje na zpracování osobních údajů *prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností.*<sup>52 53</sup>

Směrnice 95/46/ES ze své působnosti tedy výslovně vyloučila zpracování osobních údajů pro osobní nebo domácí účely (např. korespondence, vedení adresáře), neboť v daném případě osobní údaje zpracovává zpravidla sám

---

<sup>50</sup> „Mezinárodní smlouvy“.

<sup>51</sup> „Vztahy Unie s mezinárodními organizacemi a třetími zeměmi a delegace Unie“.

<sup>52</sup> Srov. § 3 odst. 3 zákona č. 101/2000Sb., o ochraně osobních údajů. Dle kterého se tento zákon nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu. Srov. důvodovou zprávu k českému zákonu o ochraně osobních údajů, podle níž se se předpis dle svého §3 odst. 4 nevztahuje na osobní údaje, *kteře jsou shromážděny nahodile, bez prvků systematickosti, jsou vedeny manuálně a nejsou nijak dále zpracovány.*

<sup>53</sup> K výjimkám z věcné působnosti Směrnice 95/46/ES srov. např. rozhodnutí ESD ze dne 16. prosince 2008, C-73/07 ve věci Tietosuojaaluttettu. ESD k těmto výjimkám z působnosti Směrnice 95/46/ES uvedl, že *činnosti, uváděné příkladmo v první odrážce tohoto ustanovení, jsou v každém případě činnostmi vlastními státům nebo státním orgánům a nesouvisejícími s oblastmi činnosti jednotlivců. Jsou určeny k vymezení rozsahu působnosti výjimky stanovené v uvedeném ustanovení, takže se tato výjimka uplatní pouze na činnosti, které tam jsou takto výslovně zmíněny nebo které mohou být zařazeny do téže kategorie.* A dále ve svém rozhodnutí uvedl, že *druhá výjimka musí být vykládána tak, že se vztahuje výhradně na činnosti spadající do rámce soukromého či rodinného života jednotlivců.*

subjekt údajů a současně při tom nedochází ke zveřejňování údajů, jehož prostřednictvím by mohlo dojít potenciálně k zásahu do jeho soukromí. Účelem takového zpracování (pro osobní potřebu) může být vzdělávání se, koníčky apod. Například pokud si někdo vede deník obsahující detailní popis průběhu každého jeho dne včetně osobních údajů lidí, se kterými byl v nějaké „sociální interakci“, bylo by jistě zcela neúčelné, kdyby bylo takovéto zpracování předmětem plnění povinností správce osobních údajů, např. informační povinnost vůči subjektům údajů. Lze mít za to, že ale i v takovém případě by osoba zpracovávající osobní údaje výlučně pro osobní potřebu měla věnovat alespoň základní pozornost zabezpečení takových údajů, a to nikoli s ohledem na plnění povinností stanovených právním předpisem na ochranu osobních údajů, ale kvůli možné občanskoprávní žalobě v případě, že by některé osobní údaje nebo jiné projevy osobní povahy, které si takto shromažďuje, byly zpřístupněny neoprávněným osobám.

V souladu s citovaným textem čl. 3 odst. 2 Směrnice 95/46/ES lze osobní potřebu chápat širěji, než jak by mohlo vyplývat z pouhého jazykového výkladu tohoto pojmu, jako potřebu soukromou, a tu pak, s odkazem na judikaturu českého Ústavního soudu,<sup>54</sup> podle kterého v sobě soukromí zahrnuje i sféru rodinného života, nejen jako potřebu fyzické osoby samotné, ale i jejích blízkých, členů rodiny a osobních přátel. Naplnění osobní potřeby je svojí povahou specifickým účelem zpracování osobních údajů a jako takové musí být legální (zákonné) a legitimní. Za osobní potřebu tak nelze považovat zpracování osobních údajů v souvislosti s trestnou činností fyzické osoby pro soukromé účely, nebo zpracování osobních údajů získaných neoprávněně, protiprávně, např. krádeží dat z informačního systému jiného subjektu. Osobní potřebou nebude ani takové zpracování, při kterém dochází k neoprávněnému zásahu

---

<sup>54</sup> Nález Ústavního soudu ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99, N 32/17 SbNU 229.

do práv jiných osob, typicky zveřejňováním osobních údajů. Překročí-li zpracování tento limit, nelze na takový účel již pohlížet jako na osobní potřebu ve smyslu zákona, a tedy na zpracování, které je z pravidel zákona vyjmuté. Tento závěr vychází i z judikatury Evropského soudního dvora, podle kterého není osobní potřebou takové jednání, kdy dochází ke zveřejnění údajů původně získaných v rámci osobní potřeby nebo osobních činností, vůči neurčitému počtu subjektů např. prostřednictvím internetu.<sup>55</sup>

V souvislosti s využitím internetu je třeba zmínit novodobé fenomény, jako jsou Facebook či YouTube. Tyto internetové servery obsahují bezpochyby řadu osobních údajů nejen svých uživatelů, ale i třetích osob. Naskytá se tedy otázka, zda se v těchto případech jedná o zpracování osobních údajů, případně zda lze taková zpracování podřadit pod výjimku z působnosti Směrnice 95/46/ES. WP 29 se k této problematice vyjádřila ve svém stanovisku č. 5/2009 k internetovým sociálním sítím. Podle něj jsou ve většině případů uživatelé služeb sociálních sítí považováni za subjekty údajů. V některých případech se však na činnosti uživatele nemusí vztahovat výjimka pro domácí použití a lze mít za to, že uživatel přebírá určité odpovědnosti správce údajů. Je tomu tak tehdy, kdy je například sociální síť použita jako platforma pro spolupráci určitého sdružení nebo společnosti. Pokud uživatel jedná jménem společnosti či sdružení nebo používá síť převážně jako platformu na podporu obchodních, politických nebo charitativních cílů, výjimka domácího použití neplatí. Pokud přístup k údajům z profilu přesahuje kontakty podle vlastního výběru, je-li například přístup k profilu umožněn všem členům v rámci služeb sociální sítě nebo jsou-li údaje indexovatelné vyhledávači, přístup přesahuje osobní nebo domácí oblast. Stejně tak v případě, že uživatel přijme informované rozhodnutí o rozšíření přístupu mimo přátele podle vlastního výběru, nabývají platnosti odpovědnosti správce údajů. Závěrem k obsahu výše uvedeného stanoviska lze

---

<sup>55</sup> Viz rozsudek ESD ze dne 6. 11. 2003, C-101/01, ve věci Lindqvist.

zdůraznit, že uplatnění výjimky pro domácí použití je omezeno rovněž nutností zaručit práva třetích stran, zejména co se týká citlivých údajů.

Jako další příklad pro přiblížení záměru zpracovávat osobní údaje pro svou osobní potřebu lze uvést stále více se rozšiřující využívání kamerových systémů pro ochranu majetku, a to nejen v případě obchodních společností, ale také pro ochranu majetku fyzických osob. Existuje jistě řada případů, ve kterých se majitel rodinného domu rozhodne zvýšit svůj pocit bezpečí instalací kamer kolem domu. Takový postup lze primárně považovat za činnost pro osobní potřebu spočívající v ochraně majetku. Přesto je nezbytné, aby byly zkoumány ještě některé další aspekty, především to, zda záběry kamer neoprávněně nezasahují do soukromí jiných osob, např. sousedů této fyzické osoby tím, že kamera zabírá mimo jiné i prostor sousedních pozemků, příp. veřejné prostranství. Takový postup by nebyl v souladu s právními předpisy, a tedy by se z povahy věci nemohlo jednat ani o naplnění podmínek výjimky zpracování pro osobní potřebu, neboť by nebyla splněna podmínka legality.<sup>56</sup> K této výjimce SDEU v rozsudku C-212/13 ze dne 11.12.2014 ve věci Ryneš proti Úřadu pro ochranu osobních údajů uvedl, že tato musí být vykládána striktně, což v dané věci vedlo k rozhodnutí, dle kterého se Směrnice 95/46/ES *nevztahuje na zpracování údajů prováděné při výkon nikoli prostě osobních či domácích činností, nýbrž „výlučně“ osobních či domácích činností.*<sup>57</sup> Zpracovávání osobních údajů formou kamerového systému nainstalovaného z důvodu ochrany vlastního majetku, který ale zabírá (a ukládá) záběry i z veřejných prostranství bylo proto SDEU ohodnoceno jako zpracování, které pod výjimku uvedenou ve

---

<sup>56</sup> KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů*. Komentář. 1. vydání. Praha: C. H. Beck, 2012, 536 s.

<sup>57</sup> Bod 30 rozhodnutí ve věci C-212/13.

druhé odrážce druhého odstavce článku 3 Směrnice 95/46/ES spadat nebude.<sup>58</sup>

59

S tím, že zásady vytyčené Směrnicí 95/46/ES platí i za účinnosti GDPR, koresponduje vymezení věcné působnosti GDPR, kdy do ní nadále spadá automatizované zpracování osobních údajů anebo neautomatizované zpracování osobních údajů spojené s vedením evidencí s výjimkami týkajícími se výlučně osobních či domácích činností zpracování při výkonu činností nespádajících do působnosti práva EU, zpracování zahrnutých v hlavě V kapitole 2 Smlouvy o EU nebo zpracování za účelem potírání trestné činnosti a ochrany veřejné bezpečnosti. Zde je ovšem nutno doplnit, že paralelně s GDPR byla vydána i směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů.<sup>60 61</sup>

## 2.2 Územní působnost Směrnice 95/46/ES

Územní působnost Směrnice 95/46/ES byla upravena článkem 4, který obsahoval tuto kolizní normu:

*„1. Každý členský stát použije na zpracování osobních údajů vnitrostátní*

---

<sup>58</sup> Bod 35 rozhodnutí ve věci C-212/13.

<sup>59</sup> K vymezení věcné působnosti Směrnice 95/46/ES také např. v rozsudcích SDEU ze dne 20.5.2003 ve věci Österreichischer Rundfunk a další ve spojených věcech C-465/00, C-38/01 a C-139/01, rozsudek SDEU ze dne 6.11.2003 Lindqvist C-101/01 a rozsudek SDEU ze dne 16.12.2008 Satakunnan Markkinapörssi y Satamedia C-73/03.

<sup>60</sup> Směrnice Evropského parlamentu a Rady 2016/680 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

<sup>61</sup> Úkolem členských států EU bude provedení transpozice této směrnice do vnitrostátních právních řádů nejpozději k 6. 5. 2018. V rámci ČR tedy prakticky půjde především o revizi příslušných ustanovení zákona č. 273/2008 Sb., o Policii České republiky.

*ustanovení, která přijme na základě této směrnice, pokud:*

*a) zpracování je prováděno v rámci činností provozovny správce na území členského státu; pokud je stejný správce usazen na území několika členských států, musí přijmout opatření nezbytná pro dodržování povinností stanovených použitelným vnitrostátním právem každou ze svých provozoven;<sup>62</sup>*

*b) správce není usazen na území členského státu, ale v místě, kde se vnitrostátní právní předpisy daného členského státu uplatňují na základě mezinárodního práva veřejného;*

*c) správce není usazen na území Společenství a používá za účelem zpracování osobních údajů prostředků, automatizovaných či nikoli, umístěných na území zmíněného členského státu, ledaže jsou tyto prostředky použity pouze pro účely tranzitu přes území Společenství.*

*2. V případě uvedeném v odst. 1 písm. c) správce musí určit zástupce usazeného na území zmíněného členského státu, aniž je tím dotčena možnost podniknout právní kroky proti správci samotnému.“*

Článek 4 odst. 1 písm. a) Směrnice 95/46/ES upravoval situaci umístění provozoven správce osobních údajů, v nichž dochází ke zpracování osobních dat v několika členských státech Evropské unie současně. Požadavek zajistit, aby se každá z těchto provozoven řídila právní úpravou platnou v zemi, v níž sídlí, vycházela z faktu, že na základě Směrnice 95/46/ES byla ve všech členských státech osobním údajům zajištěna obdobná ochrana, přičemž bylo ale současně nutné respektovat národní odlišnosti jednotlivých právních aktů přijatých členskými státy.<sup>63</sup>

Zároveň bod odůvodnění č. 20 Směrnice 95/46/ES obsahoval požadavek na zajištění stejné míry ochrany všem údajům zpracovávaným na území Evropské

---

<sup>62</sup> Srov. znění bodu odůvodnění č. 18 a bodu odůvodnění č. 19 Směrnice 95/46/ES.

<sup>63</sup> Odlišnosti národních úprav vycházejí z povahy zvolené formy legislativního aktu, tedy směrnice, upravující danou problematiku. K tomu blíže viz kapitola „Důvody pro přijetí GDPR“.



unie anebo dat odsud pocházejících bez ohledu na faktickou lokalizaci správce a jejím účelem tedy bylo zajištění odpovídající ochrany osobních údajů a umožnění řádného výkonu práv subjektů údajů i vůči správcům dat sídlícím mimo území Evropské unie. V opačném případě – při absenci obdobných institutů by mohlo v důsledku působení správců osobních dat ze třetích zemí nebo přesídlování správců do lokalit s žádnou nebo jen fragmentární úpravou ochrany osobních údajů docházet k citelnému snížení úrovně této ochrany v rámci evropského prostoru, kde je úprava této oblasti plně rozvinuta (včetně ochrany poskytované právům subjektu údajů). Současně se jednalo o vyjádření jednoho ze základních principů evropské spolupráce, a to volného pohybu osobních údajů v rámci Evropské unie. Správce osobních údajů usazený v členském státě EU tak může provádět zpracování i v jiné členské zemi, aniž by byl jakkoliv administrativně omezován nebo měl povinnost zajistit zpracování v této zemi prostřednictvím zde usazeného zpracovatele.<sup>64</sup>

V případě písm. c) citovaného článku Směrnice 95/46/ES se mohlo jednat o případy, kdy např. správce osobních údajů nesídlil na území Evropské unie, ale na jejím území zpracovával určitá osobní data, resp. správce osobních údajů v rámci daného zpracování dat realizoval jen některé, anebo i všechny úkony na území některého ze států Evropské unie a využíval k tomu např. zdejší pracovní sílu či výpočetní techniku.<sup>65</sup> Podmínkou aplikace tohoto ustanovení čl. 4 odst. 1 písm. c) Směrnice 95/46/ES dále bylo, že na území některého ze států Evropské unie nedocházelo k pouhému tranzitu dat z místa jejich shromáždění do místa jejich dalšího zpracování (např. není pouze využíván server na území daného

---

<sup>64</sup> KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů*. Komentář. 1. vydání. Praha: C. H. Beck, 2012, 536 s.

<sup>65</sup> Příkladem může být shromažďování osobních údajů v rámci marketingových nebo farmaceutických výzkumů pro nadnárodní společnosti nebo sběr dat pro projekt Street View, kde docházelo ke shromažďování osobních údajů na území České republiky pro potřeby společnosti Google Inc. sídlící v USA; v současné době je situace v případě Street View již jiná, neboť zahraniční správce osobních údajů – společnosti Google Inc. – pověřil zpracováním osobních údajů zpracovatele sídlícího v Irsku, tedy v Evropské Unii.

státu), ale byla zde prováděna některá z operací odpovídající definici zpracování osobních údajů uvedené v článku 2 písm. b) Směrnice 95/46/ES.<sup>66</sup> Zároveň je třeba upřesnit, že tranzitem dat je myšleno výhradně časově omezené předání určité zprávy (např. elektronické pošty) anebo časově limitovaný fyzický pobyt údajů na území některého státi (např. v rámci přepravy listin z jedné společnosti do druhé např. z dceřiné společnosti v České republice do mateřské společnosti v Německu).<sup>67</sup>

### 2.3 Kritika vymezení územní působnosti Směrnice 95/46/ES

Jak vyplývá z výše uvedeného, územní působnost Směrnice 95/46/ES a vnitrostátních prováděcích předpisů vyplývala buď z umístění provozovny správce, nebo z umístění prostředků nebo zařízení, které se používají v případě usazení správce mimo Evropskou unii, resp. Evropský hospodářský prostor.

Pracovní skupina WP29 ve svém stanovisku č. 8/2010 k použitelnému právu ze dne 16.12.2010<sup>68</sup> uvádí, že *vzhledem k absenci jednotné implementace a také interpretace ustanovení Směrnice 95/46/ES týkajících se pravidel pro určení rozhodného práva je nutné přesně vyložit a vyjasnit smysl těchto ustanovení, aby tím byl zajištěn jejich jednotný výklad pro každodenní aplikaci*. Pracovní skupina v tomto svém stanovisku uvedla, že pro určení práva rozhodného pro konkrétní zpracování osobních údajů není rozhodující místo, ve kterém jsou osobní údaje zpracovávány, ani národnost subjektů údajů, ale místo, ve kterém se nachází

---

<sup>66</sup> Dle tohoto ustanovení se „zpracováním osobních údajů“ rozumí *jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace*.

<sup>67</sup> KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů*. Komentář. 1. vydání. Praha: C. H. Beck, 2012, 536 s.

<sup>68</sup> ARTICLE 29 WORKING PARTY. *Opinion 8/2010 on applicable law*. [cit. 2018-08-20]. Dostupné z [https://ec.europa.eu/justice/article-29/documentation/opinion\\_recommendation/files/2010/wp179\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2010/wp179_en.pdf).

provozovna správce, v rámci jejíž činnosti ke zpracování osobních údajů dochází. Koncept „rámce činností provozovny správce“ pak primárně nesměřuje k právnímu řádu členského státu, v němž je správce usazen, ale k právu toho členského státu, v němž je umístěna relevantní provozovna správce.<sup>69</sup>

S pojmem „provozovna“ je třeba připomenout bod 19 odůvodnění Směrnice 95/46/ES, dle kterého usazení na území členského státu předpokládá efektivní a skutečný výkon činnosti prostřednictvím stálého zařízení, a že právní forma takové provozovny, ať jde o pobočku nebo dceřinou společnost s vlastní právní subjektivitou není rozhodující. Tento bod odůvodnění kromě toho upřesňoval, že pokud je stejný správce usazen na území několika členských států, musí zajistit, aby všechny provozovny plnily povinnosti stanovené vnitrostátními právními předpisy, které se vztahují na jejich činnost, zejména s cílem vyloučit jejich obcházení. Jak uvedl ve svém stanovisku generální advokát v bodech 28 a 32 až 34 ve věci *Weltimmo*<sup>70</sup>, *pojem usazení má být vykládáno materiálně, nikoliv formálně. Striktně formální výklad by vedl k tomu, že za místo usazení by bylo výlučně považováno místo zápisu obchodní společnosti. Za účelem určení, zda obchodní společnost (správce údajů) má provozovnu ve smyslu Směrnice 95/46/ES v jiném členském státě, než je členský stát, nebo třetí země, v nichž je zapsána, je třeba posoudit jak míru stability zařízení, tak skutečný charakter výkonu činnosti v tomto jiném členském státě, s přihlédnutím ke konkrétní povaze dotčených hospodářských činností a poskytovaných služeb. To platí obzvláště pro podniky, které poskytují služby výlučně prostřednictvím internetu.*<sup>71</sup> Zároveň je třeba mít za to, že pojem

---

<sup>69</sup> BAIER, J. a KRAMOLIŠ, O. *Mezinárodněprávní aspekty zpracovávání osobních údajů a nesprávná transpozice směrnice v zákoně o ochraně osobních údajů*. [Právní rozhledy 11/2012, s. 385].

<sup>70</sup> Rozhodnutí SDEU ze dne 1. 10. 2015, C-230/14 *Weltimmo s.r.o. proti Nemzeti Adatvédelmi és Információszabadság Hatóság* [cit. 2017-05-04]. Dostupné z <http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=CS>.

<sup>71</sup> Srov. bod 29 rozhodnutí ve věci *Weltimmo*.

„provozovna“ ve smyslu tohoto ustanovení Směrnice 95/46/ES zahrnoval jakoukoliv efektivní a skutečnou činnost, i minimální, vykonávanou prostřednictvím stálého zařízení.<sup>72</sup> Přítomnost jediného zástupce pak mohla za určitých okolností dostačovat k takové existenci stálého zařízení v dotčeném členském státě, jestliže tento zástupce jednal s dostatečnou mírou stability, s pomocí prostředků nezbytných k poskytování předmětných konkrétních služeb v dotčeném členském státě. SDEU ve svém rozhodnutí Google Spain konstatoval, že čl. 4 odst. 1 písm. a) Směrnice 95/46 nevyžaduje, aby dotčené zpracování osobních údajů bylo prováděno samotnou dotčenou provozovnou, ale pouze aby bylo prováděno „v rámci činnosti“ provozovny,<sup>73</sup> kdy tento pojem nelze, s ohledem na předmět Směrnice 95/46/ES, vykládat restriktivně.<sup>74</sup>

Aby mohla být Směrnice 95/46/ES použitelná i na společnosti usazené mimo EU, resp. EHP (které nesplňují „use of equipment test“ zakotvený v článku 4 odst. 1, písm. c) Směrnice 95/46/ES), musel být naplněn požadavek tzv. neoddělitelné spojitosti („an inextricable link“) mezi společnostmi usazenou na území třetího státu a společnostmi vykonávajícími na území EU zpracování osobních údajů. Pokud by byla taková neoddělitelná spojitost prokázána (byť by měla mít „pouze“ hospodářský rozměr)<sup>75</sup>, použila by se Směrnice 95/46/ES i na správce usazené mimo EU (resp. EHP).<sup>76</sup>

Oproti tomu nová úprava GDPR obsahuje ustanovení, dle kterého se GDPR vztahuje na všechna zpracování osobních údajů subjektů údajů, kteří se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud

---

<sup>72</sup> Viz bod 31 rozhodnutí ve věci Weltimmo.

<sup>73</sup> Viz bod 52 rozhodnutí ve věci Google.

<sup>74</sup> Viz bod 53 rozhodnutí ve věci Google.

<sup>75</sup> Za naplnění podmínky „neoddělitelné spojitosti“ lze dle SDEU považovat případ, kdy je daná provozovna určena k tomu, aby v daném členském státě zajišťovala podporu prodeje správce usazeného mimo EU, kdy tento prodej slouží k zajištění výnosnosti služby nabízené daným správcem usazeným mimo EU.

<sup>76</sup> Srov. bod 55 a bod 56 rozhodnutí ve věci Google.

činnosti zpracování souvisí s nabídkou zboží nebo služeb těmto subjektům údajů nebo s monitorováním jejich chování, ke kterému dochází v rámci Unie.

Nově tak není třeba v každém jednotlivém případě posuzovat naplnění podmínky neoddělitelné spojitosti tak, jak ji dovodila judikatura Evropského soudu.<sup>77</sup>

## 2.4 Osobní údaj dle Směrnice 95/46/ES

Směrnice 95/46/ES ve svém článku 2 písm. a) obsahovala definici subjektu údajů, dle které byly osobními údaji *veškeré informace o identifikované nebo identifikovatelné osobě*. Tato fyzická osoba, subjekt údajů, se považovala za určenou či určitelnou, pokud ji lze přímo nebo nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro některou složku její osobnosti. Směrnice 95/46/ES pak v bodu odůvodnění č. 26 k této definici upřesňovala, že pro určení, zda je člověk identifikovatelný či nikoliv, je třeba přihlídnout ke všem prostředkům, které mohou být rozumně, ne tedy pouze teoreticky či při vynaložení extrémních nákladů, využity, a to ať už správcem, který tyto údaje v dané chvíli zpracovává, nebo kýmkoliv dalším.<sup>78</sup>

Požadavek, aby se tyto údaje vztahovaly k identifikovatelné osobě podle Směrnice 95/46/ES znamená, že osobní údaje představují soubor takových údajů, které mohou být spojeny s určitou osobou. K tomu, aby informace představovala osobní údaj tedy nemusí obsahovat označení osoby jménem, ale postačuje vymezení souboru charakteristik, které na konkrétní osobu poukážou. Toto široké vymezení osobních údajů vedlo k vyvratitelné domněnce, že údaj, který svým obsahem má potenciál být osobní, jím také je, neboť se předpokládá identifikovatelnost osoby na jeho podkladě. Toto také zohlednila WP29

---

<sup>77</sup> Srov. rozhodnutí SDEU ve věci *Weltimmo* a ve věci *Google*.

<sup>78</sup> NONNEMANN, F. *IP adresa jako osobní údaj*, [Právní rozhledy 3/2017, s. 88].

následujícím konstatováním: „Leč není možné ve všech případech uživatele internetu identifikovat, tento dokument vychází z předpokladu, že možnost takové identifikace v mnoha případech existuje“ (a tudíž jde o zpracování osobních údajů).<sup>79</sup> Toto vymezení osobního údaje převzalo i GDPR.

## 2.5 Způsob transpozice Směrnice 95/46/ES do českého právního řádu

Transpozice Směrnice 95/46/ES do právních řádů členských států měla být dokončena do dne 24.10.1998. Česká republika ji implementovala zákonem č. 101/2000Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen jako „zákon o ochraně osobních údajů“), který byl ještě před přistoupením České republiky k Evropské unii vícekrát novelizován a dále změnou a harmonizací ostatní legislativy, jež souvisí s oblastí ochrany osobních dat. Hodnotícími dokumenty týkajícími se implementace byly Přístupové partnerství (*Accession Partnership*), roční pravidelné zprávy (*Regular Report*) i závěry mise expertů „Peer Review“<sup>80</sup>, kterými nebyly vůči výsledkům procesu implementace, jakož i činnosti tehdy nově ustanoveného Úřadu pro ochranu osobních údajů vzneseny výhrady.<sup>81</sup>

Zákon o ochraně osobních údajů mimo jiné prováděl základní lidské právo stanovené v čl. 10 odst. 3 Listiny základních práv a svobod České republiky, tedy právo každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Účelem zákona o ochraně osobních údajů bylo zajistit ochranu osobních údajů, stanovit

---

<sup>79</sup> ARTICLE 29 WORKING PARTY. *Privacy on the Internet – An integrated EU Approach to On-line Data Protection* [cit. 2017-04-28]. Dostupné z [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf).

<sup>80</sup> Evropská Komise v roce 2002 vyslala do některých přístupujících států zvláštní hodnotící misi (tzv. Peer Review), která měla na místě prověřit činnost dozorových orgánů pro oblast ochrany dat.

<sup>81</sup> NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související*. 1. vydání. Praha: Wolters Kluwer, 2014. 504 s. ISBN: 9788074786655, s.41.

podmínky, za kterých je zpracování osobních údajů přípustné, stejně tak podmínky pro přenos údajů do zahraničí a regulovat vztahy, které vznikají v souvislosti se zpracováním osobních údajů.

## 2.6 Vybraná rozhodnutí SDEU

Přijetí nové právní úpravy dále ovlivnila i judikatura SDEU (dříve ESD), kdy autorka níže uvede některá významná rozhodnutí:

(i) rozhodnutí „**Lindqvist**“ ze dne 6. listopadu 2003.<sup>82</sup> Bodil Lindqvist ve funkci katechetky ve švédské farnosti vytvořila ve svém bydlišti na svém osobním počítači internetové stránky s cílem umožnit farníkům připravujícím se na biřmování snadno získat potřebné informace. Na její žádost zajistil správce internetových stránek Švédské církve propojení mezi těmito stránkami a stránkami B. Lindqvist. Zmíněné stránky obsahovaly informace o B. Lindqvist a jejich osmnácti kolezích z farnosti, včetně jejich úplného jména, případně jen jejich jména křestního. B. Lindqvist dále lehce humornou formou popsala funkce zastávané jejími kolegy a jejich záliby. V několika případech byl zmíněn i jejich rodinný stav, telefonní číslo a další informace. Krom toho zde uvedla, že jedna z jejích kolegyně se zranila na noze a čerpá částečné volno z důvodu nemoci. Bodil Lindqvist své kolegy neinformovala o existenci těchto stránek, neopatřila si jejich souhlas ani své počínání neohlásila Datainspektion (veřejnoprávní instituce na ochranu údajů předávaných elektronickou cestou). Jakmile se dozvěděla, že někteří z jejích kolegů stránky neschvalují, tyto stránky odstranila.

SDEU v tomto případě mimo jiné judikoval, že pojem „zpracování“ osobních údajů ve smyslu ustanovení čl. 3 odst. 1

---

<sup>82</sup> Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, Bodil Lindqvist.

Směrnice 95/46/ES zahrnuje i úkony spočívající v uvedení osobních údajů na internetové stránce, a že údaj o tom, že se určitá osoba zranila na noze a čerpá částečné volno z důvodu nemoci je citlivým osobním údajem ve smyslu čl. 8 Směrnice 95/46/ES;

(ii) rozhodnutí „**Digital Rights Ireland**“ ze dne 8.4.2014<sup>83</sup>, jehož výsledkem bylo kompletní zrušení Směrnice 2006/24/ES o uchovávání údajů vytvořených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, jejímž předmětem byla úprava plošného uchovávání provozních a lokalizačních údajů o elektronických komunikacích pro účely vyšetřování závažných trestných činů a terorismu. Zrušena byla s účinky *ex tunc* a to pro rozpor s Listinou základních práv EU, konkrétně pro překročení požadavku proporcionality zákonodárcem, když tuto směrnici přijal. Směrnice 2006/24/EC byla přijata v reakci na teroristické útoky v Madridu v roce 2004 a v Londýně v roce 2005<sup>84</sup> a ve svých člancích 5 a 6 požadovala uchovávání údajů potřebných k dohledání a identifikaci osob – např. telefonních čísel, e-mailové komunikace na dobu nejméně šesti měsíců a nejvýše dvou let ode dne komunikace<sup>85</sup> a to za účelem dostupnosti takových dat pro případné vyšetřování závažných trestných činů definovaných v členských státech národní legislativou, navíc bez nutnosti konkrétního podezření na spáchání takového trestné činnosti daným subjektem údajů.<sup>86</sup>

---

<sup>83</sup> Rozsudek Soudního dvora ze dne 8. dubna 2014, C-293/12, Digital Rights Ireland Ltd.

<sup>84</sup> BURRI, M. a SCHÄR, R. *Thereform of the EU Data protection Framework: Outlining key changes and assessing their fitness for a data-driven economy* [online]. Journal of Information Policy, Vol. 6 (2016), s.479-511. [cit. 31-03-2017]. Dostupné z: [https://www.researchgate.net/publication/306119725\\_The\\_Reform\\_of\\_the\\_EU\\_Data\\_Protection\\_Framework\\_Outlining\\_Key\\_Changes\\_and\\_Assessing\\_Their\\_Fitness\\_for\\_a\\_Data-Driven\\_Economy](https://www.researchgate.net/publication/306119725_The_Reform_of_the_EU_Data_Protection_Framework_Outlining_Key_Changes_and_Assessing_Their_Fitness_for_a_Data-Driven_Economy). s. 484.

<sup>85</sup> Viz článek 5 a 6 Směrnice 2006/24/ES.

<sup>86</sup> BURRI, M. a SCHÄR, R. *Thereform of the EU Data protection Framework: Outlining key changes and assessing their fitness for a data-driven economy* [online]. Journal of Information Policy, Vol. 6 (2016), s.479-511. [cit. 31-03-2017]. Dostupné z:



SDEU ve svém rozhodnutí výslovně upozornil na nebezpečí spojená s plošným shromažďováním osobních údajů – např. že je z těchto údajů jako celku možné vyvodit velmi přesné závěry o soukromém životě osob, jejichž údaje byly uchovány<sup>87</sup> a dále uvedl, že takovéto uchovávání dat může mít dopad i na výkon svobody projevy uživatelů daných komunikačních prostředků zaručené článkem 11 Listiny základních práv Evropské Unie.<sup>88</sup>

SDEU dále v rozhodnutí zaujal opačné stanovisko oproti stanovisku generálního advokáta, tedy že musí existovat alespoň nějaká (i nepřímá) vazba mezi takovým uchováváním osobních údajů a závažnou trestnou činností. SDEU zmiňuje jako možnost zeměpisné kritérium. Je proto otázkou, zda by vnitrostátní orgány mohly nařídit uchovávání údajů například z celého území měst či širších aglomerací s vyšší hrozbou teroristických útoků. Zajímavý je i výslovný apel uvedený v rozsudku na to, že pokud je k uchovávaným údajům poskytnut přístup orgánům členského státu, musí se to dotčená osoba následně dozvědět.<sup>89</sup>

(iii) třetím rozhodnutím, které ovlivnilo evropské právo na ochranu osobních údajů je rozhodnutí „Schrems“ ze dne 6. října 2015<sup>90</sup>, ve kterém Soudní dvůr prohlásil za neplatné rozhodnutí Evropské Komise, v němž bylo konstatováno, že Spojené státy zajišťují odpovídající úroveň ochrany předávaných osobních údajů.

SDEU v tomto případě řešil předběžnou otázku ohledně oprávnění komisaře pro lidská práva členského státu (jednalo se konkrétně o Irsko) zabývat se stížnostmi ohledně přezkumu úrovně ochrany osobních dat v USA,

---

[https://www.researchgate.net/publication/306119725\\_The\\_Reform\\_of\\_the\\_EU\\_Data\\_Protection\\_Framework\\_Outlining\\_Key\\_Changes\\_and\\_Assessing\\_Their\\_Fitness\\_for\\_a\\_Data-Driven\\_Economy](https://www.researchgate.net/publication/306119725_The_Reform_of_the_EU_Data_Protection_Framework_Outlining_Key_Changes_and_Assessing_Their_Fitness_for_a_Data-Driven_Economy).s. 484.

<sup>87</sup> Bod 27 rozhodnutí.

<sup>88</sup> Bod 28 rozhodnutí.

<sup>89</sup> VLÁČIL, J. *Soudní dvůr EU – prosinec 2016* [Soudní rozhledy 2/2017, s. 61].

<sup>90</sup> Rozsudek Soudního dvora Evropské unie ze dne 6. října 2015, C-362/14, Schrems.

tedy systému Safe Harbor, schválených rozhodnutím Evropské komise.<sup>91</sup> SDEU ve svém rozhodnutí dospěl k závěru, že národní úřady osobních údajů mají pravomoc a zároveň i povinnost na základě stížnosti dotčené osoby přezkoumávat, zda určitý stát poskytuje, odpovídají úroveň ochrany osobních údajů. Tuto povinnost mají navzdory tomu, že náležitá úroveň byla pro daný stát deklarována rozhodnutím Komise. V případě, že by národní úřad dospěl k závěru, že v dané zemi odpovídající úroveň ochrany osobních údajů dána není, musí mít možnost předložit národnímu soudu, který se musí obrátit na SDEU s předběžnou otázkou, protože pouze on má pravomoc rozhodovat o platnosti rozhodnutí Komise;

(iv) rozhodnutí „**Google Spain**“<sup>92</sup>, kterému se budu autorka detailně věnovat v kapitole vztahující se k „právem být zapomenut“.

Uvedenými rozhodnutími SDEU naznačil potřebu nové právní úpravy, která by již např. explicitně upravovala právo na výmaz jako jedno z práv subjektů údajů. Autorka podmínky pro uplatnění tohoto práva, tak jak je upravené v GDPR, rozebírá v samostatné podkapitole této práce. Dále v rozhodnutí Google Spain SDEU naznačil potřebu nové, širší úpravy územní působnosti ochrany osobních údajů. Nově tak dle GDPR není třeba v každém jednotlivém případě posuzovat naplnění podmínky neoddělitelné spojitosti mezi společností usazenou na území třetího státu a společností vykonávající na území EU zpracování osobních údajů.<sup>93</sup>

Rozhodnutí Digital Rights Ireland přineslo nutnost nové úpravy plošného shromažďování osobních údajů, když jím SDEU zrušil

---

<sup>91</sup> Blíže k pojmu Safe Harbor např. viz [https://www.uouu.cz/VismoOnline\\_ActionScripts/File.ashx?id\\_org=200144&id\\_dokumenty=3002](https://www.uouu.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002).

<sup>92</sup> Rozsudek SDEU ze dne 29. 1. 2008, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU.

<sup>93</sup> Detailněji se autorka problematice „neoddělitelné spojitosti“ věnuje v samostatné podkapitole.

směrnici 2006/24/ES. Státy se tak např. v případě uchování provozních a lokalizačních údajů musí řídit režimem stávající e-privacy směrnice,<sup>94</sup> včetně její výjimky stanovení čl. 15 odst. 1, dle které se státy mohou od omezení zakotvených v e-privacy směrnici odchýlit v případech, kdy je to nutné k zajištění prevence, vyšetřování nebo odhalování trestné činnosti. Vzhledem k tomu, že byla zrušena směrnice, která přikazovala státům údaje uchovávat, nedochází tedy k návratu pravomocí národním státům, ale národní právní úpravy se "přesouvají" pod režim směrnice 2002/58/ES. SDEU ve svém rozhodnutí tedy nejen zrušil směrnici 2006/24/ES, ale zároveň stanovil, jaká omezení musí státy respektovat při transpozici e-privacy směrnice. Není tak na libovůli států, jakým způsobem data retention upraví, ale musí se stát tak, aby úprava respektovala omezení, která pro národní úpravy výjimka zakotvená v čl. 15 odst. 1 této směrnice stanoví. Přičemž rozhodnutí SDEU je pro výklad toho, co lze považovat za "*nezbytné, přiměřené a úměrné opatření*" ve smyslu § 15 odst. 1 e-privacy směrnice klíčové.<sup>95</sup> V současné době probíhá legislační proces ohledně přijetí nového e-privacy nařízení,<sup>96</sup> které má směrnici 2002/58/ES nahradit.

V souvislosti s extraterritoriální působností GDPR je v rozhodnutí Schrems naznačena kontroverzní pravomoc Evropské komise rozhodovat o zajištění dostatečné úrovně ochrany ve třetích státech. GDPR posiluje „test“ ohledně zajištění této dostatečné úrovně ochrany, když stanoví, že *Komise by měla při svém hodnocení určité třetí země zohlednit skutečnost, jak tato třetí země dodržuje zásady právního státu a přístupu ke spravedlnosti, jakož i*

---

<sup>94</sup> Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

<sup>95</sup> VOBORĪL, J. *Jaké budou dopady zrušení směrnice o data retention?* [online]. Dostupné z: <https://www.epravo.cz/top/clanky/jake-budou-dopady-zruseni-smernice-o-data-retention-94415.html>.

<sup>96</sup> Návrh nařízení dostupný online: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM:2017:10:FIN>.

*mezinárodní normy a standardy v oblasti lidských práv včetně právních předpisů týkajících se veřejné bezpečnosti, obrany a národní bezpečnosti, jakož i veřejného pořádku a trestního práva.*<sup>97</sup> V případě neexistence takového rozhodnutí ze strany Komise mohou správce nebo zpracovatel předávat osobní údaje do třetí země nebo mezinárodní organizace pouze pokud správce nebo zpracovatel poskytl vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektu údajů.<sup>98</sup> Dle GDPR by v opačném případě předávání osobních dat do zahraničí mohl umožnit např. institut souhlasu subjektu údajů, který vědomě (náležitě poučen) akceptuje rizika vyplývající ze zahraniční právní úpravy.

GDPR se dle výjimky uvedené v článku 2 nebude vztahovat na zpracování osobních údajů prováděné *fyzickou osobou v průběhu výlučně osobních či domácích činností*. Tato výjimka pak dle bodu odůvodnění č. 18 zahrnuje korespondenci a vedení adresářů a nově, oproti Směrnici 95/46/ES zahrnuje i využívání sociálních sítí a internetu v souvislosti s činnostmi osobní povahy nebo s činnostmi v domácnosti. GDPR tak rozšiřuje tuto výjimku oproti rozhodnutí v případě Bodil Lindqvist, ve kterém SDEU uvedl, že *tato výjimka tedy musí být vykládána tak, že se týká pouze činností v rámci soukromého nebo rodinného života jednotlivců, což zjevně neplatí pro zpracování osobních údajů, jež spočívá v jejich zveřejnění na internetu tak, že se zpřístupní neomezenému počtu osob.*<sup>99</sup> Nadto autorka uvádí, že GDPR se použije pro správce a zpracovatele, kteří „pouze“ poskytnou prostředky pro zpracování osobních údajů spadající pod výjimku čl. 2 odst. 1 písm. c).

---

<sup>97</sup> Viz bod 103 a 104 odůvodnění GDPR.

<sup>98</sup> Viz článek 46 odst. 1 GDPR.

<sup>99</sup> Viz bod 47 rozhodnutí ve věci Bodil Lindqvist.

V době přijetí Směrnice 95/46/ES již několik členských států vnitrostátní úpravu ochrany osobních dat přijalo.<sup>100</sup> Potřeba harmonizace právních úprav členských států pak byla nezbytná s ohledem na zajištění vnitřního trhu s volným pohybem dat, který nemohl být realizován bez toho, aniž by se účastníci tohoto trhu mohli spolehnout na jednotnou vysokou úroveň ochrany osobních údajů. Ačkoliv Směrnice 95/46/ES stanovila podrobná a ucelená pravidla ochrany osobních údajů v EU, nebylo možné skrze směrnici jako právní formou této úpravy, zajistit totožnou úpravu ve všech členských státech, když směrnice pro aplikovatelnost požaduje vnitrostátní transpozici. Dále postupem času došlo ke změnám v informačních technologiích, než které tato směrnice v době svého vzniku v polovině 90 let upravovala.

---

<sup>100</sup> Spolková země Hesensko přijala jako první na světě zákon na ochranu osobních údajů v roce 1970, tento zákon se uplatnil pouze vůči státu. Švédsko přijalo „*Bundesdatenschutzgesetz*“ v roce 1976 a v roce 1977 Francie přijala „*Loi relatif à l'informatique, aux fichiers et aux libertés*“. Velká Británie přijala v roce 1984 „*the Data Protection Act*“ a nakonec Nizozemsko v roce 1989 přijalo „*the Wet Persoonregistraties*“.

## 2.7 Důvody pro přijetí GDPR

Dne 27. dubna 2016 bylo přijato Obecné nařízení o ochraně osobních údajů s plánem dosažení jednotné právní úpravy ochrany osobních údajů v členských státech Evropské unie.<sup>101</sup> Nařízení jako typ sekundárního právního aktu má dle čl. 288 SFEU obecnou působnost a je závazné v celém rozsahu a přímo použitelné ve všech členských státech. Jedná se tedy o obecně závazný normativní právní akt, který se podobá vnitrostátnímu zákonu, protože upravuje konkrétní skutkové situace pro abstraktně určené adresáty. Mezi jeho základní znaky patří (i) závaznost ve všech svých částech a (ii) přímá použitelnost v každém členském státě. Nařízení tak automaticky zakládá práva a povinnosti v právním řádu členských států a zároveň SFEU nařízení výslovně přiznává přímou použitelnost.

Přijetí nového GDPR tak představuje významnou změnu právní formy evropského předpisu upravujícího ochranu osobních údajů ze směrnice na nařízení. Směrnici lze oproti nařízení označit jako specifický nástroj harmonizace předpisů členských států, kdy dle čl. 288 SFEU je směrnice závazná pro každý stát, kterému je určena, pokud jde o výsledek, jehož má být dosaženo, přičemž volba formy a prostředků se ponechává vnitrostátním orgánům. Mezi specifické znaky směrnice patří: (i) adresáty směrnice jsou členské státy, (ii) závaznost zamýšleného výsledku, (iii) uvážení členských států co do volby formy a prostředků transpozičního předpisu, (iv) určení lhůty k dosažení účelu stanoveného směrnici a (v) jako důsledek neprovedení (či nedostatečného provedení) směrnice jsou např. možná přímá použitelnost

---

<sup>101</sup> GDPR bylo přijato na základě ustanovení článku 16 odst. 2 SFEU, které zmocňuje Evropský parlament a Radu ke stanovení pravidel o ochraně fyzických osob při zpracování osobních údajů a pravidel o volném pohybu těchto údajů, za účelem zajištění soudržné a vysoké úrovně ochrany fyzických osob a odstranění překážek bránících pohybu osobních údajů v rámci Unie.

ustanovení směrnice, možnost jednotlivce podat žalobu na náhradu škody proti členskému státu před vnitrostátními soudy a možnost podání žaloby na porušení Smluv.<sup>102</sup>

GDPR nabylo účinnosti dne 25.5.2018 a k tomuto dni byla rovněž zrušena i Směrnice 95/46/ES. Tato směrnice doposud „pouze“ harmonizovala úpravu ochrany osobních údajů a nebylo tak možné zabránit rozdílům při její implementaci v jednotlivých členských státech. Hlavními důvody pro jeho přijetí je tedy odstranění roztržitosti ochrany osobních údajů a dále zajištění soudržné a vysoké úrovně ochrany osobních údajů fyzických osob.

Přijetí GDPR tak představuje reakci na dosavadní roztržitost ochrany osobních údajů v rámci států EU zapříčiněnou zj. právě zvolenou formou právní úpravy, kdy směrnice nemůže zaručit jednotné provádění ochrany osobních údajů na území všech států EU, ani zamezit rozdílům při zpracování osobních údajů v členských státech, jež mohou bránit volnému pohybu osobních údajů v rámci EU a mohou tak představovat překážku pro výkon hospodářských činností na úrovni EU. Zároveň bylo nezbytné dosáhnout nového soudržnějšího rámce vymahatelných pravidel, který by, ačkoli se zdůrazňuje technologická neutralita, měla nová právní úprava umožnit rozvoj digitální ekonomiky na celém vnitřním trhu. Jako další důvod pro přijetí nové právní úpravy lze tak uvést nutnost reflexe technologického rozvoje. Potřeba dosáhnout vyšší úrovně unifikace právních řádů a reakce na rozvoj digitálních technologií<sup>103</sup> tedy představovali i jeden z hlavních důvodů pro to, aby nový instrument ochrany osobních údajů měl formu nařízení a výběr této formy je sám o sobě přidanou

---

<sup>102</sup> Předmětem porušení může být nejen primární právo EU, ale i právo sekundární, včetně rozhodnutí SDEU i porušení mezinárodního práva. IN: SVOBODA, P. *Úvod do evropského práva*. 5. vyd., Praha: C.H.BECK, 2013. s. 190.

<sup>103</sup> Generální advokát ve svém stanovisku ve věci *Google Spain* výslovně uvedl, že je to poprvé, kdy byl SDEU požádán k výkladu Směrnice 95/46/ES v kontextu internetového vyhledávače.

hodnotou oproti předchozímu zakotvení pravidel ochrany osobních údajů prostřednictvím směrnice.<sup>104</sup>

---

<sup>104</sup> MAŠTALKA, J. *Nové GDPR EU o ochraně osobních údajů a některé záležitosti spojené s jeho aplikací v ČR*. [Právní rozhledy 21/2016, s. 737].



### 3 Nová koncepce GDPR oproti původní úpravě

GDPR jakožto nový právní předpis ochrany osobních údajů na evropské úrovni oproti zrušené úpravě mimo jiné přináší i rozšíření práv subjektů údajů, jejichž osobní údaje jsou zpracovávány. Výslovně je již v GDPR upraveno „právo být zapomenut“, právo na přenositelnost údajů k jinému správci, či vznést námitku proti zpracování osobních údajů včetně profilování. Mezi další novinky, které GDPR přináší je dále např. to, že již nepočítá s registrační povinností zpracovatelů, ale ukládá naproti tomu povinnost vést interní záznamy o činnostech zpracování, které má zpracovatel povinnost na vyžádání předložit dozorovému orgánu. Dále je nově jak pro správce, tak i pro zpracovatele zakotvena povinnost hlásit případy porušení zabezpečení osobních údajů. V neposlední řadě GDPR stanovuje vyšší sankce v případě jeho porušení, a to v závislosti na závažnosti takového porušení. Sankce může dosáhnout do výše až 20 mil. eur, nebo jedná-li se o podnik, až do výše 4 % celkového celosvětového ročního obrátu za předchozí rozpočtový rok, podle toho, která z těchto dvou uvedených hodnot bude vyšší.<sup>105</sup>

Ačkoliv nová právní úprava přináší novinky naznačené výše, je jedním ze základních znaků ochrany osobních údajů podle GDPR kontinuita se zrušenou právní úpravou a GDPR tak navazuje ve sledovaných cílech a obsahových zásadách zpracování a ochrany osobních údajů na Směrnici 95/46/ES.

#### 3.1 Působnost GDPR

Články 1 až 3 GDPR upravují předmět GDPR a jeho věcnou a místní působnost. GDPR je základem pro volný pohyb osobních údajů v rámci EU a stanoví podmínky, na jejichž základě se GDPR použije i pro zpracování

---

<sup>105</sup> Viz článek 83 GDPR.

osobních údajů, ke kterému dochází mimo území EU. Věcná působnost GDPR vymezuje zpracování, která podléhají požadavkům GDPR, a dále stanoví výjimky z věcné působnosti a také upravuje vztah ke směrnici o elektronickém obchodu,<sup>106</sup> když explicitně uvádí, že nijak nenarušuje dosavadní zvláštní režim vyloučení odpovědnosti poskytovatele služeb informační společnosti spočívající v tom, že v případě dodržení stanovených pravidel nemůže těmto poskytovatelům vzniknout odpovědnost za činnost jejich uživatelů. Ve vztahu k místní působnosti GDPR reflektuje judikaturu SDEU a oproti dosavadní úpravě rozšiřuje dosah GDPR i na správce a zpracovatele nacházející se mimo EU, pokud zpracovávají osobní údaje subjektů, které se nacházejí na území EU. Mělo by tak dojít k odstranění situací, ve kterých nebude dostatečně zajištěna ochrana osobních údajů.<sup>107</sup>

### 3.1.1 Věcná působnost GDPR

Věcná působnost GDPR je v prvním odstavci článku 2 vymezena pozitivně, dle kterého se GDPR *vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny*. Z tohoto vymezení zároveň vyplývá, že není rozhodné, jaký prostředek zpracování se při automatizovaném zpracování použije. Ochrana fyzických osob obsažená v GDPR je tak technologicky neutrální. Důvodem pro přijetí tohoto přístupu je vyjádřením snahy zákonodárců EU zajistit, aby ochrana poskytovaná GDPR nemohla být obcházena použitím různých technik zpracování osobních údajů.<sup>108</sup>

---

<sup>106</sup> Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu.

<sup>107</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné GDPR o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s. 55.

<sup>108</sup> Viz bod odůvodnění č. 15 GDPR.

Druhý odstavec článku 2 pak obsahuje negativní vymezení věcné působnosti GDPR, když stanoví, na která zpracování osobních údajů se nevztahuje, a to na zpracování osobních údajů prováděné:

- a. *při výkonu činností, které nespádají do oblasti působnosti práva EU;* mezi tyto činnosti pak patří činnosti týkající se národní bezpečnosti a zpracování osobních údajů členskými státy při výkonu činností v rámci společné zahraniční a bezpečnostní politiky EU,<sup>109</sup>
- b. *členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V Kapitoly 2 Smlouvy o EU;* toto ustanovení dopadá na ustanovení vztahující se k společné zahraniční a bezpečnostní politice EU;
- c. *fyzickou osobou v průběhu výlučně osobních či domácích činností;* tedy zpracování prováděné bez jakékoliv souvislosti s profesní nebo obchodní činností, např. využívání sociálních sítí bez souvislosti s obchodní činností nebude pod ochranu GDPR spadat. GDPR se ale vztahuje na správce nebo zpracovatele, kteří pro tyto činnosti osobní povahy či činnosti v domácnosti poskytují prostředky pro zpracování osobních údajů.<sup>110</sup> Důvody, proč se GDPR nemá vztahovat na osobní či domácí činnosti je zřejmý,<sup>111</sup> nicméně je třeba mít na paměti výše uvedený striktní výklad SDEU této výjimky z věcné působnosti;
- d. *příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;* tyto činnosti jsou upraveny zvláštním právním předpisem EU, konkrétně směrnicí

---

<sup>109</sup> Viz bod odůvodnění č. 16 GDPR.

<sup>110</sup> Viz bod odůvodnění č. 18 GDPR.

<sup>111</sup> Autorka je toho názoru, že neexistuje žádný důvod, proč by na tyto případy mělo GDPR dopadat, a to z důvodu nízkého rizika potenciálního porušení, když jednotlivci se při těchto činnostech nebudou s největší pravděpodobností na jakékoliv formě zpracování osobních údajů podílet.

Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, která nabude účinnosti dne 25. května 2018.<sup>112</sup>

Třetí odstavce článku 2 GDPR stanoví, že *na zpracování osobních údajů orgány, institucemi a jinými subjekty Unie se vztahuje Nařízení (ES) č.45/2001*<sup>113</sup>. Toto ustanovení ale zároveň vyžaduje, aby Nařízení (ES) č.45/2001 a další právní akty Unie týkající se takového zpracování osobních údajů byly uzpůsobeny zásadám a pravidlům dle čl. 98 GDPR. Dle tohoto článku v případě vhodnosti Komise předloží legislativní návrhy s cílem změnit jiné právní akty Unie v oblasti ochrany osobních údajů s cílem zajistit tak jednotnou a soudržnou ochranu fyzických osob v souvislosti se zpracováním osobních údajů, zj. stanovení pravidel pro zpracování osobních údajů subjekty EU a dále pravidel týkající se volního pohybu těchto údajů. Důvodem tohoto ustanovení je skutečnost, že Evropský parlament předpokládá určité nesrovnalosti mezi GDPR a Nařízením (ES) č.45/2001<sup>114</sup> a článkem 98 GDPR tak má být zajištěno, že případná změna Nařízení (ES) č.45/2001 bude provedena tak, aby nebyla ohrožena harmonizace předpisů EU na ochranu osobních údajů. Už v tuto chvíli je ale zřejmé, že Nařízení (ES) č.45/2001 bude třeba s ohledem na přijetí GDPR pozměnit, min. s ohledem na provázanost

---

<sup>112</sup> Viz bod odůvodnění č. 19 GDPR.

<sup>113</sup> GDPR Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.

<sup>114</sup> 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.

těchto dvou předpisů. Jako konkrétní případ by autorka uvedla článek 8 tohoto nařízení, který odkazuje na Směrnici 95/46/ES.

GDPR nemá dle odst. 4 článku 2 vliv na uplatňování směrnice o elektronickém obchodu,<sup>115</sup> která upravuje určité aspekty služeb informačních společností a dále také zavádí zvláštní pravidla týkající se elektronického obchodu, jako je např. zasílání obchodních sdělení. Tato směrnice byla do českého právního řádu transponována prostřednictvím zákona o některých službách informační společnosti.<sup>116</sup> Toto ustanovení GDPR výslovně vylučuje jakékoliv omezení článků 12 až 15 směrnice o elektronickém obchodu, kdy tyto články upravují zvláštní režim vyloučení odpovědnosti poskytovatele služeb informační společnosti (ISP) poskytujících služby informační společnosti typu mere conduit,<sup>117</sup> caching<sup>118</sup> a hosting<sup>119</sup>. Tento zvláštní režim vyloučení odpovědnosti ISP zaručuje, že v případě dodržení stanovených pravidel nemůže těmto ISP vzniknout odpovědnost za činnost jejich uživatelů. Jako příklad lze uvést provozovatele populární služby YouTube, který dosud dodržuje vyloučení odpovědnosti pro poskytovatele hostingu, a nemůže být tedy činěn odpovědným za obsah vložený uživateli služby, a to nejen v rovině soukromoprávní, ale také v rovině trestněprávní či správněprávní. Provozovatel takové služby proto např. nemůže být činěn odpovědným za neoprávněné zpracování osobních údajů neoprávněně zveřejněných v rámci videa vloženého uživatelem, pokud provozovatel (např. YouTube) dodržel podmínky vyloučení odpovědnosti (zejména na konkrétní a adresnou výzvu oprávněné osoby takový obsah

---

<sup>115</sup> Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu.

<sup>116</sup> Zákon č. 480/2004Sb., o některých službách informační společnosti a o změně některých zákonů.

<sup>117</sup> Služby spočívající v přenosu informací poskytnutých uživatelem.

<sup>118</sup> Služby spočívající v automatickém mezi ukládání.

<sup>119</sup> Služby spočívající v ukládání informací poskytnutých uživatelem.

odstranil).<sup>120</sup>

### 3.1.2 Územní působnost GDPR

GDPR oproti Směrnici 95/46/ES nově obsahuje přístup, který spojuje územní působnost unijních předpisů s veřejností, na kterou je činnost zaměřená, když ve svém článku 3 stanoví, že [GDPR] (i) *se vztahuje na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii bez ohledu na to, zda zpracování probíhá v Unii či mimo ni [...]*. Přičemž „provozovna“ pak dle bodu odůvodnění číslo 22 GDPR předpokládá účinný a skutečný výkon činnosti prostřednictvím stálého zařízení a její právní forma není rozhodující.<sup>121</sup> Dle tohoto vymezení se dále GDPR použije i na správce, který působí v EU, ale data zpracovává mimo její území. GDPR tak obsahuje princip, že „ochrana putuje s osobními údaji“; a dále stanoví, že [GDPR] (ii) *se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí: (a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba; nebo (b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie*. GDPR se tak uplatní i na správce ze třetích zemí, kteří nejsou v Unii usazeni, ale kteří nabízejí své zboží a/nebo služby subjektům údajů usazeným v Unii.

Nabídkou zboží nebo služeb podle ustanovení odst. 2 písm. a) článku 3 GDPR dle bodu č. 23 odůvodnění GDPR rozumí úmysl správce nebo zpracovatele nabízet zboží nebo služby subjektům údajů, které se nacházejí v EU. Pro určení aplikovatelnosti GDPR dle této normy je proto třeba posoudit, zda je zjevné, že správce nebo zpracovatel má úmysl cílit svou nabídku na

---

<sup>120</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné GDPR o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s.69.

<sup>121</sup> Srov. bod 29 rozhodnutí ve věci *Weltimmo*.

subjekty údajů v EU. Takové posouzení bude záležet na okolnostech konkrétního případu. Bod č. 23 odůvodnění GDPR však uvádí seznam okolností, ze kterých lze zacílení na fyzické osoby dovozovat. Mezi ně mohou patřit používání jazyka nebo měny některého členského státu, možnost objednat si zboží nebo služby v jazyce členského státu. Naopak pouhá dostupnost webových stránek, e-mailové adresy nebo jiných kontaktních údajů v členském státě nebo používání jazyka obecně používaného ve třetí zemi, v níž je správce usazen (byť je současně jazykem členského státu), o takovém zacílení nevyovídá. Z judikatury SDEU<sup>122</sup> lze dovozovat i další činnosti správce nebo zpracovatele, které tzv. zacílení zakládají. Jde o nabízení zboží nebo služby prostřednictvím domény členského státu, případně cílenou reklamu zobrazovanou na základě geolokačních údajů pouze subjektům údajů v EU. Není přitom důležité, zda je za zboží či služby požadována platba, pod působnost GDPR spadá i provozování služeb, které jsou pro dotčené osoby zdarma, např. bezplatné online služby provozovatelů mimo území EU, které však na osoby na území EU cílí svou aktivitu.<sup>123</sup>

Monitorováním chování subjektu údajů, kteří se nacházejí v EU, se podle ustanovení odst. 2 písm. b) článku 3 GDPR rozumí jakékoli sledování aktivity těchto subjektů údajů, ke kterému nejčastěji dochází v prostředí internetu, kde může být sledována a jako osobní údaj zpracovávána jejich aktivita. K monitorování chování v internetovém prostředí dochází zejména prostřednictvím souborů cookies, IP adresy připojení či prostřednictvím MAC adresy zařízení, ze kterého se k internetu přistupuje, nebo prostřednictvím

---

<sup>122</sup> Rozsudek SDEU ze dne 7. prosince 2010 Peter Pammer v. Reederei Karl Schlüter GmbH & Co.KG a HOTEL Alpenhof GesmbH proti Oliver Heller, spojené věci C-585/08 a C-144/09. [cit. 2017-12-20]. Dostupné z <http://curia.europa.eu/juris/liste.jsf?language=cs&num=C-585/08>.

<sup>123</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s. 72.

geolokačních údajů. I údaj o prohlížených webových stránkách může být osobním údajem, ke kterému může poskytovatel internetového připojení získat přístup. Otázkou vymezení pojmu „osobní údaj“ v úpravě GDPR se autorka věnuje níže. V přijatém znění GDPR není obsažen požadavek na bydliště monitorovaných subjektů údajů na území EU. Lze tak mít za to, že se GDPR vztahuje na všechny subjekty údajů, které se na území EU nacházejí, byť jen na omezenou dobu.

Otázkou ale samozřejmě zůstává tato aplikovatelnost GDPR, resp. vymáhání povinností z něj plynoucích na správcích údajů usazených mimo EU, kteří v EU nemají zastoupení, ale do EU distribuují např. služby, v praxi. Jako důvod podřízení se těchto správců GDPR by ale mohla být např. otázka zachování dobré pověsti dané společnosti před svými zákazníky v obchodním styku.

### **3.2 Vymezení pojmu „osobní údaj“**

Definici „osobního údaje“ obsažené ve Směrnici 95/46/ES GDPR rozšiřuje, když stanoví, že fyzická osoba je identifikovatelná zejména s odkazem na určitý identifikátor, nově například jméno, lokační údaje či síťový identifikátor. Zároveň osobní údaje v nové právní úpravě, stejně jako v úpravě Směrnice 95/46/ES, nejsou omezeny na údaje přímo identifikující nějaký subjekt. Právní definice osobních údajů nemůže být výčtová, protože počet druhů osobních údajů je z podstaty neuzavřený a osobní údaje vznikají neomezeně nejen jako hodnoty vztažené k novým konkrétním subjektům údajů, ale také s novými technologiemi zpracování osobních údajů, jako jsou např. internetové technologie. Zároveň bod č. 30 odůvodnění GDPR stanoví, že *fyzickým osobám mohou být přiřazeny síťové identifikátory, které využívají jejich zařízení, aplikace, nástroje a protokoly, jako například adresy internetového protokolu či identifikátory cookies, nebo jiné identifikátory, jako jsou štítky pro identifikaci na základě rádiové frekvence. Tímto způsobem mohou být zanechány*



*stopy, které mohou být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají, použity k profilování fyzických osob a k jejich identifikaci.* Nově je tak za osobní údaj výslovně označena i IP adresa či cookies (a to za splnění níže uvedených podmínek).

### 3.2.2 IP adresa jako osobní údaj

IP adresy obecně jsou řady čísel, které jsou přiděleny počítačům připojeným na internet, aby mezi sebou mohly v této síti komunikovat. V závislosti na typu tohoto připojení může být IP adresa dynamická nebo statická. Pakliže je IP adresa dynamická, vytváří se při každém připojení k internetu (při každém novém připojení k internetu se tedy mění), v ostatních případech je přiřazena pro všechna připojení ta samá (statická). Na rozdíl od statických IP adres, neumožňují dynamické IP adresy spojit prostřednictvím veřejně přístupných souborů daný počítač s fyzickým připojením k síti používané poskytovatelem internetového připojení.

Otázkou charakteru IP adresy, jakožto osobního údaje se zabýval SDEU deset let před účinností GDPR. Ve svém rozsudku ze dne 29.1.2008 ve věci *Promusicae*<sup>124</sup> nepřímo podpořil zahrnutí i dynamické IP adresy mezi osobní údaje, a to v případě, je-li spojena s časovými údaji o připojení. Statická IP adresa byla tedy dle názoru SDEU za osobní údaj považována vždy a v případě dynamické adresy pouze v kombinaci s dalšími údaji o připojení.

Dynamickými IP adresami (dočasnými IP adresami, jež jsou přidělovány při každém internetovém připojení a nahrazovány při dalších připojeních), jakožto osobním údajem se mimo jiné SDEU dále zabýval ve svém rozhodnutí *Breyer proti Německu*,<sup>125</sup> ve kterém výslovně dynamickou IP adresu za osobní údaj

---

<sup>124</sup> Rozsudek ze dne 29. 1. 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*; bod 45.

<sup>125</sup> Rozsudek SDEU ze dne 19. října 2016, C-582/14, *Patrick Breyer vs. Bundesrepublik Deutschland* [cit. 2017-04-28]. Dostupné z

označil.<sup>126</sup> <sup>127</sup> Jako zdůvodnění uvedl, že IP adresu je třeba za osobní údaj považovat z důvodu jejího charakteru velmi specifické informace ve vztahu k soukromí jednotlivci a to s ohledem na úzké provázání IP adresy zařízení, jako je např. osobní počítač nebo mobilní zařízení se svým vlastníkem. Je obvyklé, že osobní počítač používá právě jedna osoba a pokud někde existuje informace, která může IP adresu doplnit tak, aby identifikovala konkrétní zařízení a tím samotnou fyzickou osobu, je také dynamickou IP adresu nutné považovat za osobní údaj.<sup>128</sup> Tento závěr jistě neplatí absolutně, důležité je vzít při posuzování v potaz, zda-li je dynamická IP adresa v daném případě přiřazena nástroji, který ke komunikaci využívá fyzická osoba, nebo pouze věci, která komunikuje do velké míry či zcela samostatně. Jako příklad lze uvést různé senzory, čidla nebo jiná zařízení, která prostřednictvím internetu posílají informace, jež se netýkají konkrétních lidí, ale např. teploty, tlaku či vlhkosti v průmyslových prostorech. I tato zařízení musí mít pro možnost komunikovat na internetu přiřazenu dynamickou IP adresu, nicméně o osobní údaj se v tomto případě vzhledem k absenci vazby na konkrétní osobu jednat nebude.<sup>129</sup>

Dynamická IP adresa bude tedy za osobní údaj považována tehdy, pokud je provozovatel internetové stránky schopen identifikovat uživatele (konkrétní osobu), byť pouze „nepřímo“ – např. v situaci, kdy provozovatel uživatele

---

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=1403270>.

<sup>126</sup> SDEU IP adresu za osobní údaj označil i v rozsudku ze dne 24. 11. 2011, C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), bod 51.

<sup>127</sup> V bodě 49 rozhodnutí ve věci Patrick Breyer vs. Bundesrepublik Deutschland SDEU uvádí, že *pro poskytovatele on-line mediálních služeb představuje [dynamická IP adresa] osobní údaj [...] pokud má k dispozici právní prostředky, které mu umožňují nechat identifikovat subjekt údajů díky dalším informacím, kterými disponuje poskytovatel internetového připojení tohoto subjektu.*

<sup>128</sup> K objektivnímu a subjektivnímu pojetí pojmu osobní údaj srov. Harašta, J., Míšek, J. *IP adresy v kybernetické bezpečnosti*. [Revue pro právo a technologie, 12/ 2015].; Nonnemann, F. *Objektivní, či subjektivní pojetí osobních údajů*. [Právní rozhledy, 12/ 2015].

<sup>129</sup> NONNEMANN, F. *IP adresa jako osobní údaj*, [Právní rozhledy 3/2017, s. 88].

identifikuje prostřednictvím internetového připojení,<sup>130</sup> resp. IP adresa bude osobním údajem vždy, když se vztahuje k určené nebo určitelné osobě, a to od prvního použití IP adresy v provozu.

### 3.2.3 Cookies

Cookies neboli textové soubory, které server umístí do počítače uživatele webových stránek a které následně odesílají informace o jeho chování zpět na příslušný server, nacházejí v poslední době široké využití při tzv. cílenou reklamu. Cookies nejsou přímo vázány na naše jméno ani e-mailovou adresu, často ale obsahují naše přihlašovací údaje do systému. Jsou společné pro jednu instalaci prohlížeče. Směrnice Evropského parlamentu a Rady 2009/136/ES, která novelizovala čl. 5 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací („e-Privacy směrnice“), došlo k posílení ochrany uživatelů internetu, neboť bylo nově vyžadováno poskytnutí informací a získání souhlasu uživatele ještě před tím, než bude cookies<sup>131</sup> uložena či bude získán přístup k již uchovaným informacím v počítači uživatele. E-Privacy směrnice tedy vyžaduje zavedení tzv. opt-in režimu pro používání cookies, kdy uživatel webových stránek musí aktivně udělit souhlas s používáním

---

<sup>130</sup> K tomu SDEU v bodě 44 svého rozhodnutí ve věci Patrick Breyer vs. Bundesrepublik Deutschland uvedl, že: *Skutečnost, že další informace potřebné k identifikaci uživatele internetové stránky nemá k dispozici poskytovatel on-line mediálních služeb, nýbrž poskytovatel internetového připojení tohoto uživatele, tedy nemůže vyloučit, že dynamické IP adresy uchovávané poskytovatelem online mediálních služeb představují pro tohoto poskytovatele osobní údaje ve smyslu čl. 2 písm. a) směrnice 95/46/ES.*

<sup>131</sup> Podle dnes platné legislativy je možné odlišit dva druhy cookies. Mandatorní, které jsou nezbytné k funkčnosti internetových stránek, a které lze používat i bez souhlasu uživatele internetu před vstupem na dané stránky a cookies, které slouží provozovatelům (mimo jiné) ke sběru osobních dat, a které vyžadují předchozí souhlas uživatele internetu s jejich používáním. Dle e-Privacy směrnice byly členské státy zavázány přijmout právní úpravu vyžadující předchozí souhlas s používáním druhé jmenované skupiny cookies.

cookies ještě před samotným uložením cookies v uživatelském zařízení.<sup>132</sup> Tato úprava byla v českém právním řádu zohledněna novelou zákona o elektronických komunikacích zákonem č. 468/2011 Sb. Tento zákon sice stanoví pro provozovatele internetových stránek povinnost jejich uživatele předem prokazatelně informovat o rozsahu a účelu zpracování dat získaných pomocí cookies, ale již nevyžaduje souhlas uživatele před uložením cookies na uživatelský počítač. Podle zákona postačuje, aby provozovatel internetových stránek nabídl uživateli pouze možnost používání cookies odmítnout. Provozovatelé internetu v České republice tak mohou v současné chvíli zpracovávat informace o uživatelských stránkách bez jejich souhlasu. Transpozice byla tedy provedena nesprávně.<sup>133</sup>

V současné době se zároveň dokončuje i návrh nového nařízení respektování soukromého života a ochrany osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) (dále jako „nařízení e-privacy“), které stanoví jednotný právní rámec pro ochranu soukromí v elektronických komunikacích v EU. Dohled nad dodržováním pravidel nařízení e-privacy má být svěřen dozorovým úřadům pro ochranu osobních údajů a na evropské úrovni Evropskému sboru pro ochranu osobních údajů. Návrh nové právní úpravy přináší i modifikaci v právním režimu cookies. Podle stávajícího návrhu by například měla být dána možnost vyjádřit souhlas se zpracováním cookies „hromadně“ prostřednictvím nastavení

---

<sup>132</sup> Některé cookies lze podle e-privacy směrnice používat i bez předchozího souhlasu uživatele (tedy v režimu opt-out) – např. tzv. session cookies, které se smažou, jakmile uživatel zavře prohlížeč. U všech cookies však musí provozovatel webových stránek splnit informační povinnost vůči uživateli.

<sup>133</sup> V případě, že členské státy řádně a včas netransponují evropskou směrnici, může mít taková směrnice přímý účinek vertikální, který se uplatní v situaci, kdy se jednotlivec dovolává svých práv vyplývajících pro něho ze směrnice. Naopak přímo ze samotné směrnice nemohou pro soukromého jednotlivce vyplývat žádné povinnosti. V současné chvíli tak ani na základě tzv. nepřímého účinku e-Privacy směrnice, ani eurokonformním výkladem zákona o elektronických komunikacích nelze dovést povinnost provozovatele webových stránek zpracovávat cookies v režimu opt-in.

prohlížeče. Vzhledem k různému přístupu koncových uživatelů k ochraně svého soukromí se v rámci příprav nařízení e-privacy diskutuje také o možnostech nastavování stupňů ochrany soukromí samotnými uživateli. Uživatelé by si tak sami mohli při instalaci nového software zvolit stupeň ochrany soukromí – kupříkladu povolit či zakázat přijímání cookies, nebo zakázat jen některá cookies, například cookies třetích stran.<sup>134</sup>

GDPR výslovně v článku 4 jako osobní údaj uvádí také síťové identifikátory či lokační údaje, kam nepochybně cookies spadají. Nicméně bod 30 odůvodnění GDPR vychází z toho, že samotné elektronické (síťové) identifikátory (včetně cookies) nemusí být vždy považovány za osobní údaje. Lze mít za to, že v případě, kdy by cookies byly podle GDPR osobními údaji, tedy v případě, kdy by provozovatel webových stránek byl schopen na jejich základě a případně na základě i dalších údajů identifikovat konkrétní fyzickou osobu, vztahoval by se na jejich používání režim opt-in.

Provozovatel webových stránek si tedy v takovém případě bude muset vyžádat předchozí informovaný souhlas uživatele s ukládáním cookies do jeho počítače obsahující informace o tom, jaké údaje jsou v souvislosti s používáním cookies zpracovávány, dále v jakém rozsahu a za jakým účelem jsou zpracovávány, kým jsou zpracovávány a jakým způsobem lze zpracování údajů odmítnout. Takový souhlas může být udělen například zakliknutím odkazu v pop-up oknu, které se zobrazí při spuštění webových stránek.

### **3.3 Zrušení oznamovací povinnosti a nové povinnosti správců**

GDPR nově ruší oznamovací povinnosti správce vůči dozorovému orgánu před zahájením automatizovaného zpracování ve smyslu ustanovení článku 18

---

<sup>134</sup> KADLECOVÁ, G.: *Několik poznámek k návrhu nařízení ePrivacy* [online]. Dostupné z <https://www.epravo.cz/top/clanky/nekolik-poznamek-k-navrhu-narizeni-eprivacy-107820.html>.

Směrnice 95/46/ES. Není tak tedy třeba před zahájením zpracování osobních údajů oznamovat dozorovému orgánu např. to, v jakém rozsahu a za jakým účelem budou osobní údaje zpracovávány, informace specifikující subjekty údajů, specifikace zpracovatele.<sup>135</sup> Na druhou stranu, GDPR přináší pro správce osobních údajů nové povinnosti, mimo jiné povinnost před zahájením zpracování osobních údajů vypracovat posouzení vlivu zpracování údajů na subjekty údajů z hlediska hrozících rizik při hodnocení povahy, rozsahu, kontextu a účelů zpracování<sup>136</sup> a povinnost předchozí konzultace dle článku 36 GDPR<sup>137</sup>, které do jisté míry představují náhradu za zrušenou oznamovací povinnost dle Směrnice 95/46/ES. Další „novou“<sup>138</sup> povinností je i povinnost jmenování pověřence pro ochranu osobních údajů (DPO). Účelem tohoto institutu je zvýšit a zkvalitnit ochranu osobních údajů u „exponovaných“ zpracování. Tomu odpovídá i stanovení oblastí zpracování vymezených článkem 37 GDPR, který stanoví, v jakých případech správce a zpracovatel musí pověřence pro ochranu osobních údajů mít.<sup>139</sup>

---

<sup>135</sup> Viz ustanovení § 16 zákona č. 101/2000Sb., o ochraně osobních údajů a o změně některých zákonů.

<sup>136</sup> Ustanovení článku 35 GDPR demonstrativně vyjmenovává případy, kdy takové posouzení vlivu bude nutné učinit; posouzení vlivu na ochranu osobních údajů bude nutné zejména v těchto případech: (i) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad; (ii) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo (iii) rozsáhlé systematické monitorování veřejně přístupných prostorů.

<sup>137</sup> Dle tohoto ustanovení správce konzultuje před zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů podle článku 35 vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.

<sup>138</sup> Formálně se jedná o novou povinnost, nicméně již v současnosti ve firmách či organizacích figurují pracovníci zodpovědní za zpracování osobních údajů.

<sup>139</sup> Bude se jednat o případy, kdy: (i) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou osudů jednajících v rámci svých soudních pravomocí; (ii) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo

#### 4 Aspekty souhlasu subjektu údajů dle GDPR

Souhlas se zpracováním osobních údajů je jedním z právních důvodů pro jejich zpracování. Dle čl. 4 odst. 11 GDPR se jím rozumí *jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů*. Definice obsažená v GDPR tak rozšiřuje vymezení souhlasu se zpracováním osobních údajů, jak bylo uvedeno v čl. 2 Směrnice 95/46/ES.<sup>140</sup>

Základním znakem souhlasu je dobrovolnost jeho udělení. Při posuzování svobody udělení souhlasu je pak dle čl. 7 odst. 4 GDPR zohledňována skutečnost, zda je plnění smlouvy (poskytnutí služby) podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné. Za svobodně udělený souhlas se zpracováním osobních údajů bude považován takový projev vůle, u kterého měl subjekt údajů skutečnou volbu ho (ne)udělit bez negativních dopadů, např. v podobě neuzavření smlouvy v případě jeho neposkytnutí. Souhlas se zpracováním osobních údajů pak nebude možné považovat za svobodně udělený v případě, kdy subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen. GDPR tato obecná pravidla nově doplňuje o příklady tří situací, kdy je svoboda souhlasu kompromitována a souhlas v nich, proto nebude s velkou pravděpodobností považován za svobodně udělený.<sup>141</sup>

---

(iii) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 10.

<sup>140</sup> Dle písmena h) článku 2 Směrnice 95/46/ES je souhlas subjektu údajů vymezený jako *jakýkoliv svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování*.

<sup>141</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s.146.

V prvním případě popsaném v bodě odůvodnění č. 43 GDPR jde o situace, kdy existuje jasná nerovnováha mezi subjektem údajů a správcem (bod odůvodnění č. 43 GDPR výslovně jako příklad uvádí vztah mezi orgánem veřejné moci jako správcem, nicméně se může jednat i o jiné postavení subjektů, ve kterém bude existovat nerovnováha nebo prvek podřízenosti jako např. mezi zaměstnavatelem a zaměstnancem) a je tedy nepravděpodobné, že souhlas byl udělen svobodně.

Druhým případem, který je také popsán v bodě odůvodnění č. 43 GDPR, je situace, kdy subjekt údajů nemá možnost vyjádřit souhlas s jednotlivými operacemi zpracování, i když je to v daném případě možné a vhodné. Taková situace může nastat např. při zpracováních prováděných mobilními aplikacemi. Subjekt údajů zde často musí souhlasit se zpracováním osobních údajů pro všechny operace zpracování dohromady, přičemž mnohé operace zpracování jsou vyžadovány pro funkce aplikace, které vůbec nevyužívá ani využívat nechce. V takovém případě má mít subjekt údajů možnost udělit tzv. členěný souhlas (*granular consent*). Subjekt údajů má mít v takovém případě možnost odsouhlasit jednotlivé operace, které chce provádět, a to zpravidla v okamžiku, kdy je chce aplikace provést poprvé. Takovýmto postupem se snižuje pravděpodobnost, že takto udělený souhlas bude vyhodnocen jako nesvobodný.<sup>142</sup>

Třetím případem je pak situace, kdy je plnění smlouvy, včetně poskytnutí služby, učiněno závislým na souhlasu, i když to pro plnění není nezbytné.

Souhlas je tedy možné považovat za svobodný jen tehdy, když má subjekt údajů skutečnou možnost volby a neexistuje žádné riziko klamání, zastrasování, nátlaku či podstatných negativních důsledků, jestliže souhlas neudělí. Pokud by

---

<sup>142</sup> Stanovisko WP29 č.02/2013 ze dne 27.2.2013 *k aplikacím na chytrých zařízeních*, WP 202, s. 15.



důsledky (ne)udělení souhlasu ohrožovaly svobodu volby jednotlivců, souhlas není možné považovat za svobodný.

Aby byl souhlas konkrétní, musí být udělen pro konkrétní účel či účely zpracování. Nelze obecně prohlásit, že se souhlas uděluje pro „všechny legitimní účely“, popř. blíže nespécifikované „marketingové účely“ správce.<sup>143</sup>

K naplnění požadavku informovanosti souhlasu subjektu údajů bod odůvodnění č. 42 GDPR uvádí, že by subjekt údajů *měl znát alespoň totožnost správce a účely zpracování, k nimž jsou jeho osobní údaje určeny*. Subjekt údajů musí být zároveň dle ustanovení čl. 7 odst. 3 GDPR informován o svém právu jednou udělený souhlas se zpracováním kdykoliv odvolat a musí být splněny požadavky poskytování informací zajišťující transparentní zpracování ve smyslu ustanovení čl.12 až 14 GDPR.<sup>144</sup>

Aby byl projev vůle „jednoznačný“ musí zde (při udělení souhlasu se zpracováním) existovat jednoznačná indikace toho, že subjekt údajů souhlasí s takovým zpracováním. Tedy nemělo by být pochyb o tom, že určitou akcí subjekt údajů skutečně směřuje k udělení svolení se zpracováním. To může být relativně snadné prokázat v případě udělení souhlasu k jednomu konkrétnímu účelu (např. přihlášení k odebírání newsletteru), ale bude pravděpodobně těžší v situaci zpracovávání osobních údajů pro více účelů. V daném případě nesmí být pochyb o tom, že určitou akcí subjekt údajů skutečně směřuje k udělení souhlasu se zpracováním. Nejednoznačné to může být např. tehdy, činí-li v elektronické komunikaci spolu s udělením souhlasu subjekt údajů i jiné úkony, přičemž udělení souhlasu nebude jasně označeno. Udělení souhlasu musí být vždy nezpochybnitelné. Aby byla jednoznačnost projevu vůle zachována, požaduje GDPR, aby byl souhlas udělen formou prohlášení nebo jiným zjevným

---

<sup>143</sup> Stanovisko WP29 č. 15/2011 ze dne 13.7.2011 *k definici souhlasu*, WP 187, s.17.

<sup>144</sup> ANNERAU, S. *Understanding consent under the GDPR* [online] [cit. 17-05-2017]. Dostupné z: <https://www.taylorwessing.com/globaldatahub/article-understanding-consent-under-the-gdpr.html>.

potvrzením. Za platně udělený souhlas nebude možné považovat souhlas udělený mlčením, předem zaškrtnutým políčkem, zahrnutím souhlasné formulace do smluvních podmínek nebo nečinností. V praxi tedy nebude možné, aby byl souhlas se zpracováním osobních údajů pouze součástí např. obchodních podmínek či přímo v těle adhézní smlouvy.

Z platného znění GDPR ale není zcela jasné, zda-li může být za platný považován i souhlas se zpracováním udělený konkludentně. Pokud by bylo z úkonu subjektu údajů zcela jasné, že musel vědět, že na základě těchto úkonů dává svolení ke zpracování svých osobních údajů, lze mít za to, že i v takovém případě se jedná o platně udělený souhlas, byť konkludentním způsobem.

Dle GDPR se tedy jedná o aktivně <sup>145</sup> projevenou vůli subjektu údajů, který může mít podobu (i) konstituujícího právního titulu, kdy zakládá oprávnění zpracovávat osobní údaje nebo se může jednat o (ii) „nastavbu“ nad zpracováním, které již na základě jiného právního titulu, ke kterému není souhlasu potřeba, probíhá, ale správce chce dané osobní údaje ještě zpracovávat nad tento rámec. Souhlas je následně platný pouze pro operace zpracování, které jsou nezbytné a přiměřené k naplnění účelu, pro který byl udělen v souladu se zásadou účelového omezení.

Vzhledem k tomu, že subjekt údajů může jednou udělený souhlas se zpracováním kdykoliv odvolat, lze tento právní titul zpracování považovat za nestálý, nestabilní. Odvoláním souhlasu správce ztrácí právní základ pro zpracování subjektu údajů a vzniká jím nárok na uplatnění práva na výmaz dle čl. 17 GDPR. Odvolání souhlasu však nemá zpětné účinky, a nebude se tak dotýkat zpracování, které bylo na základě platného souhlasu učiněno až do okamžiku jeho odvolání. Zpracování od okamžiku udělení souhlasu do jeho

---

<sup>145</sup> Dle bod odůvodnění č. 32 GDPR *mlčení, předem zaškrtnutá políčka nebo nečinnost neměla být považována za souhlas se zpracováním osobních údajů.*

odvolání bude zákonné. Na tuto skutečnost musí být subjekt údajů před udělením souhlasu upozorněn.

V neposlední řadě klade GDPR požadavky i na formu souhlasu, kdy dle bodu odůvodnění č. 42 by prohlášení o souhlasu navržené správcem mělo být srozumitelné, ve snadno přístupném znění za použití jasného a jednoduchého jazyka a nemělo by obsahovat nepřiměřené podmínky.

Jeli zpracování osobních údajů založeno na právním titulu souhlasu, bude mít i vliv na práva tohoto jednotlivce. Subjekt údajů může v takovém případě uplatnit práva upravená v článcích 16 až 20 GDPR.

#### **4.1 Podmínky vyjádření souhlasu**

Článek 7 GDPR ve svých odstavcích 1 až 3 výslovně stanovuje podmínky vyjádření souhlasu subjektu údajů se zpracováním jeho osobních údajů, kdy tyto se v GDPR poměrně výrazně zpřísnují. Podmínky pro udělení souhlasu vyplývají z definice souhlasu tak, jak ji autorka uvedla výše.

Jsou jimi:

(i) podmínka doložitelnosti udělení souhlasu se zpracováním ze strany správce (v případě písemné formy se pak bude jednat o uchování příslušného dokumentu, uchování IP adresy u souhlasu uděleného elektronicky či záznam hovoru v případě telefonicky uděleného souhlasu). V zájmu ověřitelnosti by tedy správci měli k získávání souhlasu v zásadě vždy, kdy je to možné, používat písemnou formu. Stejně tak však bude možné zaznamenávat udělené souhlasy elektronicky, např. pomocí příznaků v databázi. Bez ohledu na formu udělení souhlasu by měl správce vždy zajistit záznamy o tom, kdo souhlas udělil, kdy jej

udělil, o čem všem byl subjekt údajů před udělením souhlasu informován, jak byl souhlas udělen a údaj o tom, zda byl souhlas odvolán;<sup>146</sup>

(ii) jasná odlišitelnost udělení souhlasu od jiných skutečností a jeho srozumitelnost;

(iii) právo subjektu údajů svůj souhlas se zpracováním kdykoliv odvolat včetně informační povinnosti o tomto právu před udělením souhlasu se zpracováním osobních údajů, kdy odvolání souhlasu musí být stejně snadné jako jeho poskytnutí.

V praxi tak toto ustanovení bude mít vliv na zavedenou praxi uzavírání smluv ze strany společností, kdy souhlas se zpracováním osobních údajů často bývá součástí obchodních podmínek a v případě, kdy ho subjekt údajů nechce udělit, musí v těchto obchodních podmínkách přeškrtnout jejich příslušnou pasáž jako výraz svého nesouhlasu se zpracováním osobních údajů. Obchodní společnosti by tedy mohli ke smlouvě přikládat např. samostatný list obsahující pouze prohlášení o udělení souhlasu se zpracováním osobních údajů a ten samostatně archivovat spolu se smlouvou. Takovýto samostatný list pak také může snadno plnit důkazní prostředek o udělení souhlasu se zpracováním ve smyslu první věty bodu odůvodnění č. 42 GDPR, dle kterého *by správce měl být schopen prokázat, že subjekt údajů vyjádřil s danou operací zpracování souhlas.* Důkazní břemeno při sporu o platnost udělení souhlasu dle GDPR (stejně jako dle současné právní úpravy) leží na správci.

Bod odůvodnění č. 171 GDPR pak zakotvuje pravidlo pro použitelnost souhlasů se zpracováním osobních údajů získaných v době účinnosti Směrnice 95/46/ES, dle kterého není nutné, aby subjekt údajů znovu udělil svůj

---

<sup>146</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s.150.

souhlas, pokud je způsob jeho udělení daného souhlasu v souladu s podmínkami GDPR. Z odkazovaného bodu odůvodnění je ve vodítku WP29 k souhlasu<sup>147</sup> mj. dovozováno, že neodpovídá-li souhlas se zpracováním osobních údajů kritériím a podmínkám plynoucím z GDPR, je třeba do dvou let ode dne účinnosti GDPR zajistit nový souhlas se zpracováním osobních údajů.

Použitelné po 25. květnu 2018 tedy jsou pouze ty souhlasy, které splňují podmínky jejich udělení popsané výše. Při posuzování toho, zda doba platnosti souhlasu již vypršela, je vždy nutné hledět na rozumná očekávání subjektu údajů při jeho udělování.

## 4.2 Právo na opravu

Dle ustanovení článku 16 GDPR má subjekt údajů právo na to, aby *správcem bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají*. A dále subjektu údajů přísluší (s přihlédnutím k účelům zpracování) právo *na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení*. V případě neúplnosti osobních údajů má subjekt údajů dle tohoto ustanovení právo na jejich opravu/ úpravu, a to na základě dodatečných informací poskytnutých tímto subjektem údajů. Dle gramatického výkladu tohoto ustanovení lze zároveň dospět k závěru, že užití slovního spojení „i poskytnutím“ znamená, že oprava/ doplnění neúplných osobních údajů není omezena pouze na poskytnutí dodatečných informací subjektem údajů. Toto dodatečné prohlášení subjektu údajů představuje pouze jeden z více „opravných prostředků“, které GDPR subjektům údajů poskytuje. Mezi další takovéto

---

<sup>147</sup> ARTICLE 29 WORKING PARTY. *Guidelines on consent under Regulation 2016/679*. [cit. 2018-07-16]. Dostupné z [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=623051](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051).

„opravné prostředky“ by bylo možné zařadit i právo subjektu údajů vznést námitku, právo na výmaz či omezení zpracování osobních údajů.

### 4.3 Právo být zapomenut (právo na výmaz)

Právo být zapomenut neboli právo na výmaz dává subjektům údajů při splnění daných podmínek právo požadovat vůči správci, aby zlikvidoval jeho osobní údaje a dále je neuchovával. Toto právo bylo dovozováno již za účinnosti Směrnice 95/46/ES z práva na opravu, výmaz nebo blokování údajů dle čl. 12 a práva na námitku dle čl. 14 Směrnice 95/46/ES. Toto právo bylo v českém zákoně o ochraně osobních údajů implementováno v ustanovení §21 jako obecná žádost o vysvětlení a odstranění nežádoucího stavu ve spojení s ustanovením §20, který v případě žádosti dle §21 ukládá správci za určitých podmínek povinnost osobní údaje zlikvidovat.<sup>148</sup>

„Právo být zapomenut“ je možné vymezit jako právo každého jednotlivce na odstranění jeho osobních údajů po uplynutí určité doby. Bývalá místopředsedkyně Evropské komise a komisařka pro spravedlnost Vivien Reding „právo být zapomenut“ popsala jako povolení jednotlivce odstranit jeho osobní údaje ze systému správce v případě zániku legitimního důvodu jejich uchování.<sup>149</sup> Belgičan Jef Ausloos pak rozeznává dvě formy tohoto práva a to jednak (i) v podobě práva na výmaz ve vztahu k údajům, které jejich subjekt poskytl pasivně a v (ii) podobě práva podobnému francouzskému *droit à l'oubli* (právu na zapomnění) judikované např. v soudním rozhodnutí X vs. Journal de

---

<sup>148</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s.209.

<sup>149</sup> Viviane Reding, Vice President and Comm'r for Justice, Fundamental Rights, and Citizenship, Eur. Comm'n, Keynote at the DLD12 Conference: All You Need Is...Data?: The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age (Jan. 22, 2012) [cit. 6.3.2017]. Dostupné z: [http://europa.eu/rapid/pressrelease\\_SPEECH-12-26\\_en.htm](http://europa.eu/rapid/pressrelease_SPEECH-12-26_en.htm).

Genève,<sup>150</sup> ve kterém byl přiznán nárok na náhradu újmy pachateli trestného činu z důvodu zveřejnění jeho jména v souvislosti s jeho předchozím odsouzením v trestním řízení vedeném proti jeho bývalému spolupachatelovi.<sup>151</sup> Američan Jeffrey Rosen pak „právo být zapomenut“ označuje jako největší hrozbu svobody vyjadřování na internetu pro následující desetiletí.<sup>152</sup>

Dle autorky zákonodárce výstižně nazval článek 17 jako Právo na výmaz („právo být zapomenut“), když v dnešní digitální době není reálně možné přimět někoho skutečně „zapomenout“.

#### 4.3.1 Aspekty „práva být zapomenut“

Profesor Toulouské univerzity Gregory Vosse rozeznává tyto hlavní aspekty „práva být zapomenut“:

- **právo na rehabilitaci** v souvislosti se zahlazením odsouzení v trestněprávní rovině, kdy tento institut umožňuje (při splnění zákonných podmínek) odstranit nepříznivé důsledky odsouzení (např. podmínka bezúhonnosti pro výkon celé řady povolání atd.) – pachatel je tak ve svém občanském životě v zásadě postaven na roveň osobám netrestaným, neboť se na něj hledí, jako by nebyl odsouzen;<sup>153</sup>

---

<sup>150</sup> Soudní rozhodnutí ve věci *A* v *Journal de Geneve et de la Gazette de Lausanne* ze dne 23.10.2003, 5C156-2003IN: Franz Werro, ‘*The Right to Inform v The Right to be Forgotten: A Transatlantic Clash*’, in Aurelia Colombi Ciacchi, Christine Godt, Peter Rott and Leslie Jane Smith (eds), *Liability in the Third Millennium* (Nomos, 2009) 285, 290-291. [online] [cit. 2017-06-05]. Dostupné z: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1401357](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357).

<sup>151</sup> BUNN, A. *The curious case of the right to be forgotten*. *Computer Law & Security Review*. 31 (3): strana 4. [online] [cit. 05-06-2017]. Dostupné z: [https://espace.curtin.edu.au/bitstream/handle/20.500.11937/25286/229675\\_229675.pdf?sequence=2&isAllowed=y](https://espace.curtin.edu.au/bitstream/handle/20.500.11937/25286/229675_229675.pdf?sequence=2&isAllowed=y).

<sup>152</sup> ROSEN, J. *The Right to Be Forgotten*, *Stanford Law Review* [online] [cit. 2017-06-01]. Dostupné z: <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>.

<sup>153</sup> JELÍNEK J. a kol. *Trestní právo procesní*. 4. vydání. Praha: Leges, s.r.o., 2016.

- **právo na výmaz** ve smyslu předpisů na ochranu osobních údajů,<sup>154</sup> obsažené např. v Úmluvě Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat, Listině základních práv Evropské unie, či ve Smlouvě o fungování Evropské unie, která ve svém ustanovení článku 16 odst. 2 obsahuje závazek přijetí [...] *pravidel o ochraně fyzických osob při zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy [...] a pravidla o volném pohybu těchto údajů* [...];
- **právo být zapomenut v digitálním kontextu** vychází z odůvodnění, že jednotlivec má mít právo vykonávat efektivní kontrolu nad jeho on-line zveřejněnými osobními údaji,<sup>155</sup> které zahrnuje (i) právo na výmaz osobních údajů uchovávaných v digitálním prostředí jako výsledků vyhledávání odkazů na osobní údaje fyzické osoby; (ii) právo na nezřetelnost<sup>156</sup> v tom smyslu, že dané osobní údaje nejsou snadno dostupné pro všechny. Toto „právo na nezřetelnost“ však neznamená, že osobní údaje jsou fakticky vymazány či uzamčeny, ale spíše že jsou na základě určitých faktorů hůře dostupné (např. požadavek identifikace vyhledávající osoby na internetu); (iii) právo na výmaz osobních údajů shromážděných informačními společnostmi v digitálním prostředí ve smyslu ustanovení článku 17 odst. 1 písm. f) GDPR.<sup>157</sup> V tomto případě pak dle Vosse není výmaz takových údajů nutné podmiňovat prokázáním

<sup>154</sup> Rozsah přijímání této legislativy ve světě [cit. 9.3.2017]. Dostupný z <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=AO>.

<sup>155</sup> BUNN, A. *The curious case of the right to be forgotten*. Computer Law & Security Review. 31 (3): strana 6. [online] [cit. 05-06-2017]. Dostupné z: [https://espace.curtin.edu.au/bitstream/handle/20.500.11937/25286/229675\\_229675.pdf?sequence=2&isAllowed=y](https://espace.curtin.edu.au/bitstream/handle/20.500.11937/25286/229675_229675.pdf?sequence=2&isAllowed=y).

<sup>156</sup> right to obscurity.

<sup>157</sup> VOSS, G. W.; CASTETS-RENARDS, C. Proposal for international taxonomy on the various forms of the „right to be forgotten“: a study on the convergence of norms SSRN European Public Law: EU eJournal [online]. 2016 [cit. 2017-04-20]. Dostupné z: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2800742](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800742).



jejich nemístnosti, nezákonnosti či zastaralosti. Může se jednat např. o oprávnění odstranit data shromažďovaná sociální sítí Facebook.

Namísto snahy o komplexní definici tohoto práva na zapomenutí je dle autorky možné přijetí faktu, že existuje několik hledisek, resp. aspektů tohoto práva, jak je uvádí výše, které se mohou do jisté míry překrývat.

#### 4.3.2 Legislativní zakotvení „práva být zapomenut“

V evropském právu „právo být zapomenut“ vychází z koncepce základních lidských práv, konkrétně z práva na respektování soukromého a rodinného života tak, jak jej obsahuje čl. 8 Evropské úmluvy o ochraně lidských práv a základních svobod,<sup>158</sup> dále z článku 7 (respektování soukromého a rodinného života) a z článku 8 (ochrana osobních údajů) Listiny základních práv Evropské unie.<sup>159</sup>

Profesor Rolf Weber<sup>160</sup> uvádí, že ačkoliv „právo být zapomenut“ v dnešním digitálním věku je relativně nové, jeho koncept byl předmětem debat již v minulosti, například „právo být zapomenut“ v podobě práva na „zahazení odsouzení“ v trestním právu.<sup>161</sup> Nicméně v souvislosti s přijetím GDPR hovoříme o „právu být zapomenut“ v kontextu digitalizace a internetu a v tomto kontextu je na úrovni evropské legislativy<sup>162</sup> zásadním okamžikem přijetí Směrnice 95/46/ES a její implementace členskými státy.

Samotné „právo být zapomenut“ nebylo před jeho explicitním zakotvením v GDPR v právních předpisech EU výslovně upraveno. Do jisté míry bylo možné toto právo odvodit z povinnosti správce uchovávat údaje pouze

---

<sup>158</sup> Evropská úmluva o lidských právech a základních svobodách ze dne 4.11.1950.

<sup>159</sup> Listina základních práv Evropské unie 2012/C 326/02 ze dne 7.12.2000.

<sup>160</sup> Profesor soukromého, obchodního a Evropského práva, University of Zurich.

<sup>161</sup> WEBER, H., R. *The right to be forgotten: More than a Pandora's box?* [online] [cit. 2017-06-01]. Dostupné z: <https://www.jipitec.eu/issues/jipitec-2-2-2011/3084>.

<sup>162</sup> Přijetí Směrnice 95/46/ES na půdě EU předcházela např. francouzský zákon o ochraně osobních údajů Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et eux libérés.

po dobu nezbytnou pro dosažení účelu zpracování zakotvené ve Směrnici 95/46/ES.<sup>163</sup> Dle stanoviska generálního advokáta ve věci Google Spain<sup>164</sup> Směrnice 95/46/ES neupravovala všeobecné právo být zapomenut v tom smyslu, že dotčená osoba má nárok na omezení nebo ukončení zpracování, svých osobních údajů pouze tehdy, pokud je to pro ni dle jejího tvrzení škodlivé, nepříjemné nebo to jinak odporuje jejím zájmům.<sup>165</sup> Generální advokát rovněž konstatoval, že pokud by toto právo mělo být uplatněno, tak ne proti provozovateli internetového vyhledávače, ale vůči vydavateli (správci) původní, zdrojové internetové stránky, který napadenou informaci jako první zveřejnil. Soudní dvůr se ale s touto argumentací generálního advokáta neztotožnil. Na základě soudního rozhodnutí pak společnost Google uveřejnila formuláře, na kterých může jednotlivec požádat o uplatnění svého „práva být zapomenut“.<sup>166</sup> V dubnu 2016 společnost Google obdržela 699.560 žádostí o výmaz, na základě kterých společnost odstranila 706.134 výsledků vyhledávání z celkového počtu 1.932.339 zkoumaných webových adres.<sup>167</sup> Soudnímu rozhodnutí Google Spain se bude autorka věnovat detailněji dále, zde by pouze uvedla, že Soudní dvůr Evropské unie v tomto případě „právo být zapomenut“ aplikoval a to tak, že společnosti Google uložil povinnost odstranit odkaz na určité webové stránky.

Český zákon o ochraně osobních údajů<sup>168</sup> upravoval „právo být zapomenut“ v případě, kdy určité zpracování osobních údajů bylo nepřiměřené

---

<sup>163</sup> Článek 6 odst. 1 písem. e) Směrnice 95/46/ES.

<sup>164</sup> Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González C-131/12.

<sup>165</sup> NONNEMANN, F. *Základní analýza rozhodnutí Soudního dvora EU ve věci internetového vyhledávače Google*, [Právní rozhledy 13-14/2014, s. 479].

<sup>166</sup> Žádost o odstranění z vyhledávání na základě evropských předpisů o ochraně údajů [cit. 6.3.2017]. Dostupné z: [https://support.google.com/legal/contact/lr\\_eudpa?product=websearch](https://support.google.com/legal/contact/lr_eudpa?product=websearch).

<sup>167</sup> Žádost o odstranění z vyhledávání na základě evropských předpisů o ochraně údajů [cit. 6.3.2017]. Dostupné z: [https://support.google.com/legal/contact/lr\\_eudpa?product=websearch](https://support.google.com/legal/contact/lr_eudpa?product=websearch).

<sup>168</sup> Zákon č. 101/2000Sb., o ochraně osobních údajů.

svému účelu a neadekvátním způsobem zasahovalo do soukromého a osobního života daného člověka.<sup>169</sup> Subjekt údajů tedy dle ustanovení §21 zákona o ochraně osobních údajů mohl v případě, že se domníval, že dochází k nezákonnému zpracování jeho osobních údajů, požadovat po správci údajů vysvětlení, případně odstranění nezákonného stavu.<sup>170</sup>

#### 4.3.3 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González C-131/12

„Právo být zapomenut“ SDEU judikoval ve svém rozhodnutí z roku 2012, a to na základě ustanovení článku 12 písm. b) Směrnice 95/46/ES, dle kterého *Členské státy zaručí každému subjektu údajů právo získat od správce podle daného případu opravu, výmaz nebo blokování údajů, jejichž zpracování není v souladu s touto směrnicí, zejména z důvodů neúplné nebo nepřesné povahy údajů.*

V březnu roku 2010 španělský státní příslušník s bydlištěm ve Španělsku podal stížnost k Agencia Española de Protección de Datos (dále jen „AEPD“) proti společnosti La Vanguardia Ediciones SL, vydavatele vysoko nákladového deníku (dále jen „La Vanguardia“), jakož i proti společností Google Spain a Google Inc. Tato stížnost se zakládala na skutečnosti, že se po zadání jména pana M. Costeja González do internetového vyhledávače skupiny Google (dále jen „Google Search“) objevoval odkaz na dvě strany deníku La Vanguardia ze

---

<sup>169</sup> Ustanovení §21 zákona o ochraně osobních údajů upravovalo právo na námitku, tedy právo subjektu údajů požádat vysvětlení nebo zastavení zpracování v případě, kdy se domníval, že zpracování jeho údajů je v rozporu s ochranou jeho soukromého či osobního života nebo v rozporu se zákonem a v ustanovení §5 odst.2 písm. d), které upravovalo principu testu proporcionality při dalším zpracování oprávněně zveřejněných osobních údajů, když nedílnou součástí tohoto právního titulu ke zpracování údajů bylo i respektování práva na ochranu soukromého a osobního života subjektu údajů.

<sup>170</sup> MÍŠEK, J.; HARAŠTA, J. *Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain*. [online] Bulletin-advokacie.cz [cit. 08-03-2017]. Dostupné z: <http://www.bulletin-advokacie.cz/analiza-prakticky-ch-dopadu-rozhodnuti-soudniho-dvora-eu-ve-veci-google-spain>.

dne 19. ledna 1998 a ze dne 9. března 1998, na kterých bylo oznámení uvádějící jméno pana M. Costeja Gonzáleze v souvislosti s dražbou nemovitostí zabavených v důsledku dluhů na sociálním zabezpečení. Touto stížností pan Gonzáles požadoval, aby bylo vydavateli La Vanguardia nařízeno odstranit nebo opravit zveřejněné informace tak, aby se jeho osobní údaje nezobrazovaly nebo aby použil nástroje, které vyhledávače poskytují k ochraně jeho osobních údajů. Zároveň usiloval o to, aby společnosti Google Spain a společnosti Google Inc. byla uložena povinnost zrušit či skrýt jeho údaje tak, aby se přestaly objevovat ve výsledcích vyhledávání a přestaly být propojeny s odkazy na deník La Vanguardia. V červenci roku 2010 AEPD vyhověl stížnosti proti společnostem Google Spain a Google Inc. a vyzval je, aby přijaly opatření nezbytná k odstranění údajů z jejich indexů<sup>171</sup> a znemožnily přístup k těmto údajům v budoucnu, avšak zamítl stížnost proti vydavateli deníku s tím, že zveřejnění údajů bylo právně odůvodněno. Společnosti Google Spain a Google Inc. podaly k předkládajícímu soudu opravné prostředky, v nichž požadovaly zrušení rozhodnutí AEPD. Vnitrostátní soud přerušil řízení a položil Soudnímu dvoru mimo jiné předběžnou otázku týkající se toho, zda lze právo na námitku pro zpracování osobních údajů a právo na výmaz a blokování osobních údajů vykládat jako právo na odstranění na internetu dostupných osobních údajů z výsledků vyhledávání. Podstatou této (třetí) předběžné otázky tedy bylo to, zda článek 12 písm. b) a článek 14 první pododstavec písm. a) směrnice 95/46/ES musí být vykládány v tom smyslu, že umožňují subjektu údajů požadovat od

---

<sup>171</sup> Stěžejní úlohu při vyhledávání na internetu plní procesy označované jako „procházení“ a „indexace“. Procházení má za úkol nalezení dostupných webových stránek, indexace pak zastupuje proces shromažďování, analýzy a ukládání dat s cílem zajistit rychlé a přesné získávání informací. Internetové vyhledávače na podkladě indexace generují rejstříky s hesly s jejich umístěním. Podstata vyhledávání tak *de facto* spočívá v soustavném procházení existujících dat po zadání dotazu. Samotný proces indexace mohou rovněž ovlivnit vlastníci webových stránek za použití např. tzv. souborů „robots.txt“, které umožňují znemožnění indexace některých stránek, které se po zadání dotazu ve vyhledávači neobjeví.

provozovatele vyhledávače, aby vymazal ze zobrazeného seznamu výsledků vyhledávání provedeného na základě jména tohoto subjektu odkazy na webové stránky legálně zveřejněné třetími osobami a obsahující pravdivé informace týkající se tohoto subjektu z důvodu, že ho uvedené informace mohou poškodit nebo protože si přeje, aby uvedené informace byly po určité době „zapomenuty“.

#### 4.3.3.1 Článek 12 písm. b): právo na výmaz

Článek 12 písm. b) Směrnice 95/46/ES stanoví, že:

*Členské státy zaručí každému subjektu údajů právo získat od správce: podle daného případu opravu, výmaz nebo blokování údajů, jejichž zpracování není v souladu s touto směrnicí, zejména z důvodů neúplné nebo nepřesné povahy údajů.*

Již před tímto případem a v souvislosti s ním, byla předmětem diskuzí otázka, zda-li má být znění *zejména z důvodů neúplné nebo nepřesné povahy údajů* vykládáno restriktivně.<sup>172</sup> Jinými slovy, je toto právo omezeno pouze a výhradně na situace, kdy jsou osobní údaje neúplné nebo nepřesné? Rozhodnutí ve věci Google Spain mimo jiné v této souvislosti potvrdilo, že odkaz na neúplnost nebo nesprávnost osobních údajů je pouze příkladným, nikoliv taxativním výčtem, takže nedodržení ostatních podmínek zákonnosti zpracování osobních údajů stanovených Směrnicí 95/46/ES bude mít za následek nezákonnost takového zpracování, včetně práva subjektu údajů domáhat se opravy či vymazání těchto osobních údajů ve smyslu ustanovení článku 12 písm. b) Směrnice.<sup>173</sup>

---

<sup>172</sup> BUNN, A. *The curious case of the right to be forgotten*. Computer Law & Security Review. 31 (3): strana 10. [online] [cit. 05-06-2017]. Dostupné z: [https://espace.curtin.edu.au/bitstream/handle/20.500.11937/25286/229675\\_229675.pdf?sequence=2&isAllowed=y](https://espace.curtin.edu.au/bitstream/handle/20.500.11937/25286/229675_229675.pdf?sequence=2&isAllowed=y).

<sup>173</sup> Viz bod 70 rozhodnutí dle kterého *nesplnění požadavků stanovených v čl. 6 odst. 1 písm. d) směrnice 95/46/ES je příkladné, a nikoli vyčerpávající, z čehož vyplývá, že nesoulad zpracování, který může dotčené osobě zpřístupnit právo zaručené v čl. 12 písm. b) uvedené směrnice, může*

SDEU dále ve svém rozhodnutí uvedl, že subjekt údajů má právo požadovat opravu či výmaz osobních údajů, jestliže proces jejich zpracování nenaplnuje zásady pro kvalitu údajů zakotvených v článku 6 Směrnice 95/46/ES, nebo pokud nesplňuje zásady pro oprávněné zpracování údajů dle článku 7 Směrnice 95/46/ES. Důležité je, že toto právo se uplatní vůči jakémukoli správci údajů, který osobní údaje zpracovává v rozporu se Směrnicí 95/46/ES. Proto i tehdy, kdy je zveřejňování osobních údajů zákonné (v tomto případě oznámení o dražbě nemovitostí), další zpracování těchto údajů (jako např. odkazy ve výsledcích vyhledávání) už v souladu se Směrnicí 95/46/ES být nemusí. Jinými slovy SDEU judikoval, že v případě, kdy je v návaznosti na žádost subjektu údajů na základě článku 12 písm. b) Směrnice 95/46/ES konstatováno, že zahrnutí odkazů na webové stránky legálně zveřejněné třetími osobami a obsahující pravdivé informace týkající se jeho osoby do zobrazeného seznamu výsledků vyhledávání provedeného na základě jeho jména, je za současného stavu neslučitelné s článkem 6 odst. 1 písm. c) až e) (kdy dle ustanovení článku 6, písm. a) Směrnice 95/46/ES *členské státy stanoví, že osobní údaje musejí být zpracovány korektně a zákonným způsobem* a dále stanoví, že osobní údaje musejí být *shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely*, a že osobní údaje musejí být *přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány a/nebo dále zpracovávány*),<sup>174</sup> protože uvedené informace se s ohledem na všechny okolnosti daného případu zdají být nepřiměřené, irelevantní nebo již irelevantní

---

*plynout rovněž z porušení ostatních podmínek právoplatnosti uložených uvedenou směrnicí pro zpracování osobních údajů.*

<sup>174</sup> Viz bod 93 rozhodnutí, dle kterého *z uvedených požadavků stanovených v čl. 6 odst. 1 písm. c) až e) směrnice 95/46/ES vyplývá, že i zpracování přesných údajů, které bylo původně v souladu se zákonem, se časem může stát neslučitelným s uvedenou směrnicí, jestliže již uvedené údaje nejsou nezbytné pro účely, pro které byly shromažďovány nebo zpracovány. To platí zejména v případě, že se zdají nepřiměřenými, jsou nepodstatné nebo již nepodstatné nebo přesahují míru s ohledem na uvedené účely a uplynulý čas.*

nebo přesahující míru s ohledem na účely dotčeného zpracování provedeného provozovatelem vyhledávače.<sup>175</sup> Na základě výše uvedeného SDEU rozhodl, že dotčené informace a odkazy musí být z uvedeného seznamu výsledků vymazány.

Na druhou stranu, subjekt údajů nebude oprávněn požadovat výmaz spojení mezi jeho osobními údaji v internetovém vyhledávači pouze z důvodu, že uchování takových osobních údajů již není nezbytné pro uskutečnění cílů, pro které byly shromážděny nebo dále zpracovány jiným správcem osobních údajů. Posouzení přiměřenosti, relevantnosti, adekvátnosti, přesnosti či úplnosti zpracování osobních údajů musí být vždy učiněno s ohledem na účel, za kterým byly osobní údaje shromážděny správcem osobních údajů, proti kterému subjekt údajů právo na výmaz uplatňuje.<sup>176</sup> SDEU nerozhodl v tom smyslu, že údaje, jakožto výsledky vyhledávání vztahující se k panu Gonzálesovi by byly nepřiměřené, irelevantní, neadekvátní nebo nepřesné ve vztahu k účelu, za kterým byly společností Google shromážděny. SDEU pouze uvedl, že informace a odkaz na ní musí být smazány v případě, kdy je takový stav neslučitelný se Směrnicí 95/46/ES a to zj. z důvodu nepřiměřenosti či irelevantnosti takových informací. Google, či jiný obdobný vyhledávač by tak pravděpodobně mohl tvrdit, že téměř veškeré osobní údaje jsou relevantní pro účely zpracování tímto vyhledávačem, kterými jsou vyhledávání a umožnění přístupu k informacím, které jsou veřejně dostupné na internetu.<sup>177</sup>

Právo subjektu údajů na výmaz ve smyslu ustanovení článku 12 písm. b) je zároveň uplatnitelné v případech, kdy zpracování takových osobních údajů není v souladu s článkem 7 Směrnice 95/46/ES, dle kterého *členské státy stanoví, že zpracování osobních údajů může být provedeno, pouze pokud subjekt*

---

<sup>175</sup> Viz bod 94 rozhodnutí.

<sup>176</sup> Takovýto závěr rovněž uvedl Generální advokát Niila Jääskinena ve svém stanovisku, viz bod 98 stanoviska.

<sup>177</sup> Viz bod 98 stanoviska Generálního advokáta.

*údaje k takovému zpracování nezpochybnitelně udělil souhlas, nebo je zpracování nezbytné pro splnění smlouvy, kde je subjekt údajů jednou ze stran, nebo pokud je nezbytné ve smyslu ustanovení článku 7, písm. d) - f).* SDEU v rozhodnutí uvedl, že veškeré zpracování osobních údajů musí být ve smyslu článku 7 odůvodněno po celou dobu provádění zpracování těchto osobních údajů.<sup>178</sup>

V posuzovaném případě nedošlo k udělení souhlasu se zpracováním ze strany pana Gozálese ve smyslu článku 7 písm. a) a ani není možné na toto zpracování aplikovat ustanovení tohoto článku písm. b) až e). Právním titulem pro zpracovávání osobních údajů bylo ale v tomto případě ustanovení článku 7 písm. f), dle kterého zpracování osobních údajů může být provedeno, pokud je nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem nebo základní práva a svobody subjektu údajů, které vyžadují ochranu podle článku 1 odst. 1.

Za těchto okolností bylo v posuzovaném případě pro SDEU rozhodující, zda-li právo pana Gonzálese na odstranění odkazů na dané informace dostupných na veřejných webových stránkách zobrazovaných ve výsledcích vyhledávání převyšuje legitimní zájmy Googlu a jeho uživatelů, kteří by mohli mít zájem na přístup k výše uvedeným informacím. SDEU k tomu uvedl, že za daných okolností nemůže pouze hospodářský zájem provozovatele vyhledávače (společnosti Google) ospravedlnit zásah do práva na soukromí a do práva na ochranu osobních údajů jednotlivce, kdy tato by mohla být předmětným zpracováním dotčena. SDEU judikoval, že výše uvedená práva subjektu údajů chráněná články 7 a 8 Listiny základních práv EU obecně převažují nad zájmy uživatelů internetu. Je nicméně nutné každý jednotlivý případ posuzovat s ohledem na povahu dotčené informace a její citlivost v souvislosti se soukromím subjektu údajů, jakož i s ohledem na zájem veřejnosti mít k této

---

<sup>178</sup> Viz bod 95 rozhodnutí.



informaci přístup, jež se může lišit zejména v závislosti na úloze, kterou subjekt údajů ve veřejném životě má.<sup>179</sup>

Jinými slovy, subjekt údajů může se svými základními právy na základě článků 7 a 8 Listiny požadovat, aby dotčená informace již nebyla nadále poskytována široké veřejnosti prostřednictvím zahrnutí do seznamu výsledků vyhledávání, a lze mít v zásadě za to, že tato práva převažují nejen nad hospodářským zájmem provozovatele takového vyhledávače, ale rovněž i nad zájmem veřejnosti nalézt uvedenou informaci při vyhledávání prováděném na základě jména subjektu údajů. Nebude tomu ale tak v případě, kdy se z konkrétních důvodů, jako je např. úloha subjektu údajů ve veřejném životě, jeví, že zásah do těchto základních práv subjektu údajů je odůvodněný převažujícím zájmem veřejnosti mít na základě zahrnutí jména subjektu údajů do výsledků vyhledávání k dotčené informaci přístup.<sup>180</sup>

SDEU v rozhodnutí uvedl, že s ohledem na citlivost zveřejněných informací a také s ohledem na časový úsek šestnácti let mezi jejich zveřejněním, má subjekt údajů právo na to, aby takové informace nebyly v seznamu výsledků vyhledávání nadále spojeny s jeho jménem. V tomto případě tedy neexistovaly konkrétní důvody odůvodňující převažující zájem veřejnosti mít v rámci takového vyhledávání k uvedeným informacím přístup.<sup>181</sup>

#### 4.3.3.2 Článek 14 písm. a): právo na námitku

SDEU se dále zabýval výkladem ustanovení článku 14 písm. a) Směrnice 95/46/ES, dle kterého členské státy přiznávají subjektu údajů právo:

*Alespoň v případech uvedených v čl. 7 písm. e) a f) vznést kdykoli z vážných a legitimních důvodů souvisejících s jeho osobní situací námitku proti*

---

<sup>179</sup> Viz bod 81 rozhodnutí.

<sup>180</sup> Viz bod 97 rozhodnutí.

<sup>181</sup> Viz bod 98 rozhodnutí.

*zpracování osobních údajů, které se ho týkají, ledaže vnitrostátní právo stanoví jinak. Je-li námitka oprávněná, nesmí se zpracování zahájené správcem těchto údajů nadále týkat.*

Směrnice 95/46/ES tak v článku 14 písm. a) upravuje právo subjektu údajů vznést námitku a to tak, že při zpracování osobních údajů v případech, kdy se tak děje pro vykonání úkolu ve veřejném zájmu nebo při výkonu veřejné moci anebo pokud je jejich zpracování nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby, které jsou sdělovány, musí mít dotčená osoba možnost z vážných a legitimních důvodů vznést proti takovému zpracování svých osobních údajů námitku. Je-li námitka oprávněná, nesmí správce ve zpracování nadále pokračovat.

V posuzovaném případě bylo nutné zodpovědět otázku, zda-li toto právo vznést námitku znamená, že dotčená osoba je oprávněná po poskytovateli internetového vyhledávače požadovat odstranění svých osobních údajů z výsledků vyhledávání (resp. zda-li je poskytovatel internetového vyhledávače povinen takové žádosti vyhovět).

Generální advokát Niila Jääskinena ve svém stanovisku uvedl, že uvedené právo na námitku dopadá zejména na situaci, kdy jsou osobní údaje neúplné nebo nepřesné povahy. Směrnice 95/46/ES však podle jeho názoru v žádném případě neupravuje všeobecné právo vznést námitku (a právo být zapomenut) v tom smyslu, že dotčená osoba má nárok na ukončení nebo omezení zpracování svých osobních údajů v případě, kdy je to pro ni škodlivé, nepříjemné, nebo to jinak odporuje jejím zájmům. Generální advokát rovněž uvedl, že toto právo by mělo být případně uplatněno vůči vydavateli (správci) původní zdrojové internetové stránky, který danou informaci první zveřejnil, a ne proti provozovateli internetového vyhledávače.

V rozporu s tímto stanoviskem generálního advokáta SDEU ve svém rozhodnutí uvedl, že právo na námitku svědčí subjektu údajů i proti

provozovateli služeb internetového vyhledávače, který je dle jeho názoru samostatným správcem osobních údajů, který na svoji odpovědnost provádí jejich zpracování, a to i bez ohledu na to, zda se již dříve obrátil na původního správce, který údaje zveřejnil jako první. Provozovatel vyhledávače, případně vnitrozemský orgán (dozorový orgán v oblasti ochrany osobních údajů či soud), pak musí tuto žádost vyřídit individuálně s přihlédnutím ke všem okolnostem a dotčeným zájmům.

#### 4.3.3.3 Kritika rozhodnutí

Rozhodnutí lze kritizovat jednak právě z „nadřazení“ práva jednotlivce nad svobodou vyjadřování a nad právem na přístup k informacím, stejně jako z důvodu zakotvení obecného pravidla, že hospodářské zájmy správce osobních údajů nemohou převážet nad právem jednotlivce na soukromí a na ochranu jeho osobních údajů.<sup>182</sup> Jak ve svém rozhodnutí SDEU uvedl, k takovému závěru ho vedla závažnost zásahu do práv jednotlivce na soukromí a ochranu osobních údajů s ohledem na citlivost zveřejňované informace.<sup>183</sup> SDEU ale již nezdůvodnil, z jakého důvodu považoval zájem správce na zpracování daných osobních údajů výhradně za hospodářský, když Generální advokát ve svém stanovisku uvedl, že zájmy správce (společnosti Google) na zpracování osobních údajů šly nad rámec těch hospodářských, když osobní údaje pana Gonzálese společnost Google zpracovávala z důvodů (i) zlepšení dostupnosti informací pro uživatele internetu a (ii) zefektivnění šíření informací uložených na internetu.<sup>184</sup>

SDEU ve svém rozhodnutí dále uvedl, že práva subjektu údajů chráněná ustanoveními článků 7 a 8 Listiny základních práv EU obecně převažují nad zájmy uživatelů internetu. SDEU pro odůvodnění takového obecného závěru

---

<sup>182</sup> PEERS, S. *The CJEU's Google Spain Judgement Failing to Balance Privacy and Freedom of Expression*, EU Law Analysis [online] [cit. 2017-07-04]. Dostupné z: <http://eulawanalysis.blogspot.cz/2014/05/the-cjeus-google-spain-judgment-failing.html>.

<sup>183</sup> Viz bod 80 a 81 rozhodnutí.

<sup>184</sup> Viz bod 95 a 132 stanoviska Generálního advokáta.

použil argumentaci článkem 1 Směrnice 95/46/ES, dle kterého je *předmětem této směrnice zajištění vysoké úrovně ochrany základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů*.<sup>185</sup> Je otázkou, zda-li je takové odůvodnění dostačující. Lze souhlasit s Generálním advokátem, který ve svém stanovisku uvedl, že právo subjektu údajů na ochranu jeho soukromého života je třeba vyvážit s jinými základními právy, zejména se svobodou projevu a právem na informace.<sup>186</sup> A dále poznamenal, že poskytovatel služeb internetového vyhledávače, který zpřístupňuje nástroje na vyhledávání informací na internetu založené na vyhledávači, legálně vykonává jak svoji svobodu podnikání, tak svoji svobodu projevu. Mimoto, dle stanoviska Generálního advokáta právo uživatele internetu na informace by bylo ohroženo, pokud by jeho vyhledávání informací o určité fyzické osobě nepřineslo výsledky vyhledávání poskytující věrný obraz o relevantních internetových stránkách, ale jejich „bowdlerovanou“ verzi.<sup>187</sup>

Dále lze rozhodnutí vytknout přenesení odpovědnosti ohledně vyvážení práv subjektu údajů a práv veřejnosti na informace a svobodu projevu na soukromoprávní subjekt.<sup>188</sup> Nicméně dle zásad pro oprávněné zpracování osobních údajů je správce osobní údaje oprávněn zpracovávat pouze pokud je to nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem nebo základní práva a svobody subjektu údajů (v případě, že není dán jiný právní titul k oprávněnému zpracování osobních údajů).<sup>189</sup> Správce osobních údajů je tak povinen formálně zpracovat a zdokumentovat postupy, na základě jichž učinil rozhodnutí, že dané zpracování tyto zásady splňuje. V případě vznesení námítky

---

<sup>185</sup> Viz bod 58 a 66 rozhodnutí.

<sup>186</sup> Viz bod 128 stanoviska Generálního advokáta.

<sup>187</sup> Viz bod 131 stanoviska Generálního advokáta.

<sup>188</sup> Viz bod 133 stanoviska Generálního advokáta.

<sup>189</sup> Viz ustanovení článku 7, písm. f) Směrnice 95/46/ES.

proti zpracování osobních údajů, kdy se tato námitka ukáže oprávněnou, správce nesmí dále ve zpracování osobních údajů pokračovat. Rozhodne-li se daná osoba, že si nepřeje dohledatelnost určité stránky prostřednictvím vyhledávače, kontaktuje přímo provozovatele internetového vyhledávače (tedy soukromoprávní subjekt), který však posuzuje i její oprávněnost. Tomu tedy přísluší právo hodnotit adekvátnost, aktuálnost či přesnost daných dat včetně zájmu veřejnosti o nich vědět. Očekává se od něj vyřešení konfliktu mezi oprávněnými zájmy třetích osob na přístup k informacím a zásahem do práva jednotlivce na soukromí. Aplikací principu proporcionality se aktivita provozovatele vyhledávače *de facto* blíží činnosti soudní moci. Za předpokladu oprávněnosti námitky provozovatel ukončí zpracování, respektive odstraní stránku z indexace. V opačném případě je subjekt údajů oprávněn se obrátit na dozorový orgán, případně soud.<sup>190</sup>

Rozhodnutí Soudního dvora bezpochyby staví provozovatele internetových prohlížečů do nelehké role, když je označil za správce osobních údajů, kterým kromě jiného vznikly povinnosti v intencích Směrnice 95/46/ES. SDEU podřadil aktivity internetového vyhledávače (procházení a indexaci) pod pojem zpracování osobních údajů ve smyslu ustanovení článku 2 písm. b) Směrnice 95/46/ES. SDEU jej v případě vyhledávače Google vymezil jako vyhledávání informací zveřejněných nebo umístěných na internetu třetími stranami, automatickou indexací, dočasné ukládání a v neposlední řadě zajištění dostupnosti pro internetové uživatele dle pořadí určité preference.<sup>191</sup> Tomuto závěru SDEU lze ale oponovat argumentem provozovatelů internetových vyhledávačů, kdy aktivita vyhledávání webových

---

<sup>190</sup> Viz čl. 12 písm. b) ve spojení s čl. 14 písm. a) Směrnice 95/46/ES.

<sup>191</sup> SOMMEROVÁ, K. *Vybrané praktické dopady rozhodnutí Google Spain SL., Google Inc. vs. AEPD, Mario Costeja González*, [online] [cit. 2017-07-18]. Dostupné z: <https://www.epravo.cz/top/clanky/vybrane-prakticke-dopady-rozhodnuti-google-spain-sl-google-inc-vs-agencia-espaola-de-proteccion-de-datos-aepd-mario-costeja-gonzalez1-95363.html>.

stránek probíhá automaticky, nahodile, bez znalosti obsahu indexovaných stránek a s avizovaným dočasným ukládáním na serverech.

Samotné přisouzení role správce osobních údajů provozovatelům internetového prohlížeče je při nejmenší diskutabilní. Podle článku 6 Směrnice 95/46/ES správce údajů zajišťuje zpracování osobních údajů zákonným způsobem. Jejich shromažďování je možné jen v případě specifických, explicitních a legitimních důvodů a nikoli v rozporu s nimi a správce může takové informace shromažďovat pouze po nezbytně dlouhou dobu a pouze k odpovídajícímu účelu. Kromě výše uvedeného je správce povinen zajistit, aby údaje, které tyto požadavky nesplňují, byly smazány, resp. upraveny. K dostání veškerých nároků kladených Směrnicí 95/46/ES na správce se tito neobejdou bez znalosti příslušných webových stránek, což je u internetového vyhledávače z povahy věci vyloučeno. Provozovatel internetového vyhledávače nezná konkrétní obsah webové stránky, zpracovává ji, jak autorka uvedla výše, pouze nahodile.<sup>192</sup>

Striktní označení provozovatele prohlížeče za správce osobních údajů může být zároveň krokem k přísnější regulaci internetu do budoucna, která se promítne do finančního profitu zainteresovaných společností.

Jakkoliv je pochopitelná argumentace převahy ochrany soukromí subjektu údajů nad ekonomickými zájmy provozovatele vyhledávače, bude mít „právo být zapomenut“ dopad též do sféry dalších subjektů např. ve vztahu k provozovateli – vlastníkovi webových stránek. Ve chvíli, kdy se na jeho stránce objeví obsah v rozporu s ochranou osobních údajů, který posléze provozovatel internetového vyhledávače na žádost odstraní z vyhledávání,

---

<sup>192</sup> SOMMEROVÁ, K. *Vybrané praktické dopady rozhodnutí Google Spain SL., Google Inc. vs. AEPD, Mario Costeja González*, [online] [cit. 2017-07-18]. Dostupné z: <https://www.epravo.cz/top/clanky/vybrane-prakticke-dopady-rozhodnuti-google-spain-sl-google-inc-vs-agencia-espaola-de-proteccion-de-datos-aepd-mario-costeja-gonzalez1-95363.html>.

vzniká vlastníkově webových stránek nezanedbatelná škoda ve formě vynaložených nákladů na zprovoznění a podobu těchto webových stránek, ale také např. náklady na optimalizaci webových stránek pro internetové vyhledávače. V této souvislosti vyvstává otázka ohledně uplatnění žaloby na náhradu takto vzniklé škody, např. kdo k ní bude pasivně legitimován – bude se jednat o provozovatele internetového vyhledávače, jenž danou stránku odstraní z indexace, nebo o subjekt osobních údajů, na jehož žádost provozovatel prohlížeče stránku odstraní?

Rozhodnutí Google Spain neukládá povinnost vlastníkově webových stránek předmětnou informaci beze zbytku odstranit. Týká se pouze potenciálního vyhledávání při zadání odkazu do vyhledávače. Informace tedy setrvává stále na stejném místě, pouze se nezobrazí na příkaz prohlížeče, neboť byla vyřazena z indexace a relevantních rejstříků. Pro nalezení zveřejněných dat tak bude zapotřebí jen vynaložit větší množství úsilí a času. Vzhledem k tomu, že SDEU ve svém rozhodnutí aspekty archivace webových stránek toliko neřeší, nezbytvá než očekávat, jaký přístup SDEU, případně soudy členských států dále zvolí.

#### 4.3.4 Úprava „práva být zapomenut“ v GDPR

Ustanovení článku 17 GDPR explicitně upravuje právo subjektu údajů na výmaz jejich správcem. Podstatou tohoto práva je, že osobní údaje mohou být vymazány, je-li dán některý z těchto důvodů: (i) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány; (ii) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány a neexistuje žádný další právní důvod pro jejich zpracování; (iii) subjekt údajů vznesl námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování; (iv) osobní údaje zpracovány protiprávně; (v) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu EU nebo členského státu, které se

na správce vztahuje; (vi) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační povinnosti dítěti ve smyslu článku 8 odst. 1 GDPR.

V případě, kdy správce osobní údaje zveřejnil a je z některého z výše uvedeného důvodu povinen je vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technologických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.<sup>193</sup>

„Právo být zapomenut“ předpokládané GDPR však není právem absolutním. Neuplatní se v případě, pokud je zpracování nezbytné (i) pro výkon práva na svobod projev a informace; (ii) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen; (iii) z důvodů veřejného zájmu v oblasti veřejného zdraví; (iv) pro účely archivace ve veřejném zájmu (např. povinnost organizací archivovat dokumenty obsahující osobní údaje po určitou dobu dle zákona č. 499/2004Sb., o archivnictví a spisové službě a o změně některých zákonů), pro účely vědeckého či historického výzkumu či pro statistické účely nebo (v) pro určení, výkon nebo obhajobu právních nároků.

Právo být zapomenut, resp. právo na výmaz bývá občas prezentováno jako novinka v právech subjektu údajů, kterou GDPR přináší. Opak je ale pravdou, právo bylo již v minulosti dovozováno podle čl. 14 Směrnice 95/46/ES a v českém právním řádu bylo dovozováno na základě zákona o ochraně osobních údajů. Toto právo jednotlivce představuje určitý koncept společenského zapomnění, které dle autorky bude vždy kolidovat s právem veřejnosti na

---

<sup>193</sup> Dle bod odůvodnění č. 59 GDPR by pak výmaz osobních údajů měl být, pokud je to možné, učiněn bezplatně.



informace a svobodou vyjadřování. Je proto otázkou budoucích rozhodnutí příslušných orgánů, jak budou přesné hranice tohoto práva vymezeny.

#### **4.4 Právo na omezení zpracování**

Článek 18 GDPR zakotvuje právo subjektu údajů na omezení zpracování osobních údajů správcem v těchto taxativně stanovených případech: (i) subjekt údajů popírá přesnost osobních údajů, (ii) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití, (iii) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků nebo (iv) subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1 GDPR, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

V případě omezení zpracování z výše uvedených důvodů, mohou být osobní údaje zpracovávány pouze se souhlasem subjektu údajů,<sup>194</sup> nebo z důvodu určení výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu. Subjekt údajů, který takového omezení zpracování dosáhl musí pak být správcem předem upozorněn na to, že bude omezení zpracování zrušeno.<sup>195</sup> Způsoby, jak omezit zpracování osobních údajů, by mohly např. zahrnovat dočasný přesun vybraných údajů do jiného systému zpracování, znepřístupnění vybraných osobních údajů uživatelům nebo dočasné odstranění takových zveřejněných osobních údajů z internetových stránek. V případě systémů automatizovaného zpracování by omezení takového zpracování mělo být v zásadě zajištěno technickými prostředky tak, aby se na osobní údaje již nevztahovaly žádné další

---

<sup>194</sup> Jako výjimku z tohoto ustanovení článku 18, odst. 2 GDPR stanoví „uložení“ takových osobních údajů.

<sup>195</sup> Viz ustanovení článku 18, odst. 3 GDPR.

operace zpracování, a aby nemohly být změněny. Skutečnost, že zpracování osobních údajů je omezeno by pak měla být v příslušném systému jasně vyznačena.<sup>196</sup> Výše uvedené způsoby zpracování uvádí GDPR pouze příkladně, jednotliví správci tedy mohou přijmout i jiné metody omezení zpracování, které nebudou v rozporu s GDPR.<sup>197</sup>

Článek 19 GDPR ukládá oznamovací povinnost správci vůči jednotlivým příjemcům osobních údajů ohledně opravy nebo výmazu osobních údajů nebo v případě omezení zpracování s výjimkou případů, kdy by takové oznámení bylo nemožné nebo by vyžadovalo nepřiměřené úsilí. Smyslem tohoto ustanovení je zajistit účinnost předchozích ustanovení upravujících právo subjektu údajů na opravu, výmaz a omezení zpracování, kdy správce je povinen oznámit uplatnění některého z výše uvedeného práva subjektem údajů vůči dalším příjemcům (zpracovatelům) těchto osobních údajů, aby tito s těmito údaji dále nakládali v souladu s uplatněným konkrétním právem subjektu údajů. Právo subjektu údajů požadovat a být informován o příjemcích jeho osobních údajů pak má zajistit, aby tento subjekt údajů mohl mít přehled o dodržování jím uplatněného práva na opravu, výmaz či omezení zpracování.

#### **4.5 Právo na přenositelnost údajů**

Právo na přenositelnost údajů je jedním ze zcela nových práv, které GDPR zavádí a znamená právo subjektu údajů na získání osobních údajů, které správci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu,<sup>198</sup> kdy tyto údaje může předat jinému správci, aniž by mu v tom správce bránil.

---

<sup>196</sup> Viz bod odůvodnění č. 67 GDPR.

<sup>197</sup> AKINTUNDE, E. S. *An analysis of the General Data Protection Regulation (EU) 2016/679 GDPR* [online] [cit. 18-05-2017]. Dostupné z [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2966210](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2966210).

<sup>198</sup> Skupina WP29 zdůrazňuje, aby správci k poskytovaným údajům připojovali co nejvíce metadat a v reálně dosažitelné rozlišitelnosti zachovávající přesný význam vyměřované informace.

Toto právo má usnadnit přechod subjektu údajů od jednoho poskytovatele služeb ke druhému a také posílit možnost kontroly subjektu údajů nad svými osobními údaji. Subjekt údajů tak může získané osobní údaje od daného správce uchovávat pro další soukromé účely, a to i bez jejich předání dalšímu správci. Může se tak např. jednat o situaci, kdy uživatel online hudební platformy chce získat svůj aktuální playlist, aby zjistil, jakou skladbu a kolikrát si ji přehrál, a aby se na základě toho mohl např. rozhodnout, jakou hudbu si u jiné hudební platformy zakoupí nebo se může jednat např. o žádost poskytnutí informací o nákupech přes věrnostní kartu subjektu údajů.<sup>199</sup>

Druhý odstavec článku 20 GDPR pak výslovně stanoví, že subjekt údajů může dokonce požadovat (je-li to technicky proveditelné), aby byly jeho osobní údaje předány přímo jedním správcem správci druhému. Dle výkladového stanoviska WP29 by toto předání údajů mezi správci mělo být prováděno poskytnutím rozhraní pro programování aplikací<sup>200</sup> (API<sup>201</sup>).

Z tohoto nového práva subjektů údajů ale nevyplývá pro správce údajů povinnost uchovávat dané osobní údaje déle, než je pro účel zpracování nezbytné nebo déle než pro stanovenou dobu zpracování. Pokud tedy správce např. neukládá záznamy o písních přehrávaných uživatelem, tak tyto údaje nemusí ani danému uživateli na žádost předávat. Správcům osobních údajů tedy nevzniká

---

<sup>199</sup> ARTICLE 29 WORKING PARTY. *Guidelines on the right to data portability*. [cit. 2017-02-27]. Dostupné z: [http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc\\_id%3D43822&rct=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwjE14u4qpXUAhWofZoKHf2YCFYQFggUMAA&usg=AFQjCNGBNPz-voEZx1SuSTVO-xQ9UHIGIg](http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D43822&rct=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwjE14u4qpXUAhWofZoKHf2YCFYQFggUMAA&usg=AFQjCNGBNPz-voEZx1SuSTVO-xQ9UHIGIg).

<sup>200</sup> ARTICLE 29 WORKING PARTY. *Guidelines on the right to data portability*. [cit. 2017-02-27]. Dostupné z: [http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc\\_id%3D43822&rct=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwjE14u4qpXUAhWofZoKHf2YCFYQFggUMAA&usg=AFQjCNGBNPz-voEZx1SuSTVO-xQ9UHIGIg](http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D43822&rct=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwjE14u4qpXUAhWofZoKHf2YCFYQFggUMAA&usg=AFQjCNGBNPz-voEZx1SuSTVO-xQ9UHIGIg).

<sup>201</sup>API (Application Programming Interface) označuje rozhraní pro programování aplikací, které představuje soubor podprogramů, protokolů a nástrojů pro tvorbu softwaru a aplikací. Jedná se o rozhraní aplikací nebo webových služeb, které mohou využívat správci, aby se ostatní systémy nebo aplikace dokázaly napojit a pracovat s jejich systémy.

dodatečná povinnost uchovávat osobní údaje pouze pro účely případné žádosti subjektu údajů o přenos údajů dle ustanovení článku 20 GDPR. Na druhou stranu správce údajů, ke kterému budou osobní údaje přeneseny, má povinnost zpracovávat jen údaje relevantní a přiměřené vzhledem k novému zpracování ve smyslu ustanovení čl. 5 odst. 1. písm. c) GDPR. Pokud by tedy byly některé přenášené údaje nadbytečné s ohledem na účel nového zpracování, neměly by tyto údaje vůbec být novým správcem uchovávány a zpracovávány.

Dle prvního odstavce článku 20 GDPR se právo na přenositelnost údajů vztahuje pouze na údaje, které se týkají subjektu údajů (*a contrario* se tedy nevztahuje na anonymní osobní údaje nebo na osobní údaje, které se daného subjektu údajů netýkají). Nicméně se toto právo vztahuje na pseudonymní osobní údaje.<sup>202</sup> V případě, kdy mají být předány osobní údaje, které obsahují i osobní údaje třetích osob (např. v případě přenosu záznamů telefonních hovorů obsahující údaje o třetích osobách účastnících se těchto hovorů) má dle stanoviska skupiny WP29 subjekt údajů právo tyto informace získat a předat je jinému správci, ten však nesmí tyto údaje třetích osob zpracovávat za žádným účelem, kterým by ohrožoval nebo porušoval jejich práva a svobody. Nový správce tak nesmí tyto osobní údaje třetích stran využít pro vlastní účely, např. k marketingu.<sup>203</sup> Další podmínka omezující rozsah uplatnění tohoto práva spočívá v tom, že se musí jednat pouze o data poskytnutá subjektem údajů. Za takové lze považovat data poskytnutá subjektem údajů aktivně a vědomě (např. e-mailová adresa, věk atd.) a zároveň data poskytnutá subjektem údajů na

---

<sup>202</sup> Pseudonymizací se dle článku 4 odst. 5 GDPR rozumí *zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné osobě.*

<sup>203</sup> ARTICLE 29 WORKING PARTY. *Guidelines on the right to data portability.* [cit. 2017-02-27].

Dostupné

z

[http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc\\_id%3D43822&ret=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwjE14u4qpXUAhWoFZoKHf2YCFYQFggUMAA&usg=AFQjCNGBNPz-voEZx1SuSTVO-xQ9UHIGIg](http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D43822&ret=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwjE14u4qpXUAhWoFZoKHf2YCFYQFggUMAA&usg=AFQjCNGBNPz-voEZx1SuSTVO-xQ9UHIGIg).

základě využívání služby nebo zařízení (např. historie vyhledávání), byť subjekt údajů tyto data správci nepředává vědomě nebo aktivně (např. přístupové logy).<sup>204</sup> Naopak do práva na přenositelnost údajů nebudou spadat údaje dovozené nebo odvozené správcem údajů, které správce vytvořil např. v procesu profilování uživatele. Na tyto dovozené nebo odvozené osobní údaje se ale uplatní povinnost správce na žádost subjektu údajů poskytnout potvrzení o tom, zda jsou či nejsou jeho osobní údaje zpracovávány, a pokud jsou, tak má subjekt údajů právo na přístup k těmto údajům. Právo na přenositelnost údajů se dle písm. a) prvního odstavce článku 20 GDPR pak vztahuje pouze na ty osobní údaje, které správce zpracovává na základě souhlasu subjektů nebo pro účely plnění smlouvy uzavřené se subjektem údajů a dle písmene b) stejného ustanovení na osobní údaje, které správce zpracovává automatizovaně. U zpracování údajů na základě jiného důvodu pak toto právo na přenositelnost údajů nevzniká. GDPR výslovně stanovuje, že se právo na přenositelnost neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

#### 4.6 Právo vznést námitku

V případech stanovených GDPR má subjekt údajů právo vznést námitku proti zpracování. Jedná se zejména o situace, kdy subjekt údajů nemohl ovlivnit to, že jsou jeho osobní údaje zpracovávány, a zároveň se nejedná o plnění právní povinnosti nebo životně důležitý zájem, kdy je tato nemožnost ovlivnění obhajitelná. Právo vznést námitku může subjekt zpracování vznést proti: (i) zpracování na základě právního titulu oprávněného zájmu a plnění úkolu

---

<sup>204</sup> ARTICLE 29 WORKING PARTY. *Guidelines on the right to data portability*. [cit. 2017-02-27]. Dostupné z [http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc\\_id%3D43822&ret=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwjE14u4qpXUAhWoFZoKHf2YCFYQFggUMAA&usq=AFQjCNGBNPz-voEZX1SuSTVO-xQ9UHIGIg](http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D43822&ret=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwjE14u4qpXUAhWoFZoKHf2YCFYQFggUMAA&usq=AFQjCNGBNPz-voEZX1SuSTVO-xQ9UHIGIg).

prováděného ve veřejném zájmu nebo při výkonu veřejné moci; (ii) zpracování pro účely přímého marketingu na základě právního titulu oprávněného zájmu a proti (iii) zpracování pro vědecké nebo statistické účely či z důvodu historického výzkumu. Tato úprava GDPR se příliš neliší od zrušené právní úpravy, kdy námitka proti zpracování byla zakotvena v čl. 14 Směrnice 95/46/ES. Zároveň správce má povinnost subjekt údajů výslovně upozornit na toto jeho právo. Upozornění musí provést nejpozději v okamžiku první komunikace se subjektem údajů a musí být uvedeno zřetelně a odděleně od jakýchkoliv jiných informací.<sup>205</sup>

#### 4.7 Souhlas se zpracováním osobních údajů dítěte

Ve srovnání úpravou Směrnice 95/46/ES GDPR vytváří další ochranu tam, kde jsou zpracovávány osobní údaje dětí. Článek 8 GDPR stanoví, že pokud má správce v úmyslu zpracovávat osobní údaje dítěte mladšího 16 let (členské státy mohou tuto věkovou hranici snížit až na 13 let) na základě právního titulu souhlasu se zpracováním dle čl. 6 odst. 1 písm. a) GDPR v souvislosti s nabídkou služeb informační společnosti, musí být tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.<sup>206</sup>

Důvody pro zvýšenou ochranu jsou pak konkretizovány v bodě odůvodnění č. 38 GDPR dle kterého „*Děti zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů.*“ A dále stanoví, že „*tato zvláštní ochrana by se měla zejména vztahovat na používání osobních údajů dětí*

---

<sup>205</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s. 227-230.

<sup>206</sup> Lze mít za to, že pojem „osoba vykonávající rodičovskou zodpovědnost k dítěti“ má být vykládána jako zákonný zástupce. V případě restriktivního výkladu by totiž v takovém případě souhlas vyjadřoval/ schvaloval pouze rodič či osvojitel a už ne např. poručník, který dle občanského práva není nositelem práv a povinností vyplývajících z rodičovské zodpovědnosti.

*pro účely marketingu nebo vytváření osobnostních či uživatelských profilů a shromažďování osobních údajů týkajících se dětí při využívání služeb nabízených přímo dětem.“ Gramatickým výkladem tak lze dovodit, že tato zvláštní ochrana není omezena jen na marketing nebo profilování, ale vztahuje se na širší okruh shromažďování osobních údajů týkajících se dětí.<sup>207</sup>*

Správce je povinen vyvinout přiměřené úsilí k tomu, aby s ohledem na dostupnou technologii ověřil, zda-li tento souhlas skutečně vyjadřuje či schvaluje zákonný zástupce. V praxi bude ale velmi obtížné takové ověření reálně provést, protože děti zpravidla nedisponují žádným dokladem, který by ověření jejich zástupce nějak jednoduše umožňoval, a stejně tak správce nemá přístup do registrů, aby mohl totožnost ověřit. V případě, že služby správce na děti necílí, lze v takovém případě doporučit zahrnout do obchodních podmínek výhradu, že služba není určena dětem mladším 16 let (popř. 13 let v případě snížení věkové hranice členským státem) a ustanovení se tak na správce nebude vztahovat.<sup>208</sup> Po takovém upozornění o vyloučení dětí v obchodních podmínkách by ale měla následovat i technická opatření, která dětem pod zákonným věkovým limitem daný přístup neumožní.

Návrh českého zákona na ochranu osobních údajů tuto hranici snížil na věk 15 let. Autorka se připravovanou českou právní úpravou blíže zabývá v páté kapitole této práce.

Dle ustanovení čl. 8 odst.3 GDPR není odstavcem 1 dotčeno obecné smluvní právo členských států, například pravidla týkající se platnosti, uzavírání

---

<sup>207</sup> WP 29 Guidelines on Consent under Regulation 2016/679.

<sup>208</sup> Dalším možným řešením by bylo čestné prohlášení o schválení daného prohlášení osobou vykonávající rodičovskou zodpovědnost.

nebo účinků smlouvy vzhledem k dítěti. Je tedy nutné brát vždy v úvahu také ustanovení občanského zákoníků, která upravují právní jednání nezletilých.<sup>209</sup>

Pokud tak bude souhlas udělován k nějakému komplikovanému zpracování, u kterého dítě není s ohledem na svůj rozumový vývoj schopno posoudit následky udělení souhlasu, může být takový souhlas neplatný i v případě, že dítě již překročilo stanovenou věkovou hranici.<sup>210 211</sup>

Zároveň WP 29 ve svém doporučení k souhlasu mj. uvádí, že: *„souhlas udělený osobou vykonávající rodičovskou zodpovědnost nebo takovou osobou schválený souhlas se zpracováním osobních údajů dětí vyprší dnem, kdy subjekt údaje dosáhne věku, kdy sám může digitální souhlas dát. Počínaje tímto dnem musí správce získat platný souhlas od samotného subjektu údajů. V praxi to může znamenat, že správce opírající se o souhlas uživatelů jim může pravidelně posílat připomínku, že souhlas v zastoupení dítěte vyprší dnem, kdy dovrší 16 let, a musí být obnoven subjektem údajů osobně.“* Tento princip má být ale aplikován pouze na souhlasy udělované informačním společnostem, když si lze jen velmi těžko v praxi představit, když např. zákonní zástupci dítěte dali souhlas s pořizováním fotografií např. na dětských letních táborech, které jsou pak veřejně dostupné na webové stránce dané organizace.<sup>212</sup>

---

<sup>209</sup> Dle ust. §31 zákona č. 89/2012Sb., občanský zákoník jsou nezletilé osoby způsobilé k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti nezletilých jejich věku.

<sup>210</sup> Za nepřipustný souhlas by tak mohl být např. označen souhlas dítěte s dlouhotrvajícím profilováním, které pro něj může mít negativní důsledky.

<sup>211</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s. 159.

<sup>212</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.



#### 4.8 Podoba souhlasu se zpracováním osobních údajů

Souhlas se zpracováním osobních údajů je jedním, ne jediným právním titulem na základě, kterého vzniká oprávnění ke zpracovávání daných osobních údajů. Jedná se o titul nestálý, lehce odvolatelný, ale i obtížně získatelný a nemusí být jednoduché ho prokázat. Z těchto důvodů se autorka domnívá, že by v konkrétním případě měl správce vždy zvážit, zda-li je praktické a nutné, aby se v daném případě správce spolehal právě na tento titul.<sup>213</sup>

Pokud bude správce chtít zpracovávat právě na základě tohoto titulu, měl by si nejdříve ověřit, že splňuje níže uvedené podmínky:

- žádost o udělení souhlasu musí být jasně odlišitelná a nesmí být součástí obchodních podmínek ani formulářových smluv;
- správce nesmí využívat předem zaškrtnutých políček se souhlasem nebo jiných podobných nastavení;
- při získávání souhlasu musí být použito jasných a srozumitelných jazykových prostředků;
- subjekt údajů musí být informován o tom, z jakého důvodu a za jakým účelem je souhlas vyžadován;
- subjekt údajů má mít možnost souhlasit pouze s některými operacemi zpracování;

---

<sup>213</sup> Právní tituly pro zpracování osobních údajů jsou uvedené v článku 6 GDPR, dle kterého je zpracování zákonné, pouze za předpokladu splnění nejméně jedné z těchto podmínek a pouze v odpovídajícím rozsahu: (i) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů; (ii) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů; (iii) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje; (iv) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby; (v) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce nebo (vi) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

- ze znění souhlasu musí být jasná totožnost správce a totožnost ostatních osob, kterým budou osobní údaje předávány;
- subjektu údajů musí být sděleno, jak může souhlas se zpracováním odvolat;
- správce je zároveň povinen zajistit, že odmítnutím udělení souhlasu nebude subjekt údajů nijak poškozen a udělení souhlasu nesmí být podmínkou poskytnutí služby.

Správce je dále povinen vést záznamy o tom, kdy a jak byl souhlas získán a záznamy o tom, co bylo subjektu údajů při získání souhlasu sděleno.<sup>214</sup>

Samotný dokument „souhlas se zpracováním osobních údajů“ musí obsahovat identifikaci správce, kterému subjekt údajů souhlas uděluje (v případě právnické osoby se tak bude jednat o název, sídlo, IČ a údaj o zápise ve veřejném rejstříku) a případně kontaktní údaje pověřence pro ochranu osobních údajů; dále vyjmenování osobních údajů, které správce bude na základě tohoto souhlasu zpracovávat (např. jméno, příjmení, e-mail a telefonní číslo); stanovení účelu zpracování (např. zasílání newsletteru) a dobu, po kterou budou údaje na základě souhlasu zpracovávány. V případě, že pro správce budou údaje zpracovávat další zpracovatelé, musí být v souhlasu se zpracováním identifikováni.<sup>215</sup> Dále správce poskytne subjektu údajů informace o jeho právech (právo na přístup k osobním údajům, jejich opravu nebo výmaz, popřípadě omezení zpracování a právo na přenositelnost údajů) a poučení o tom, že subjekt údajů má právo podat stížnost u Úřadu pro ochranu osobních údajů. Správce subjekt údajů musí také informovat o použití dat k rozhodnutím čistě na bázi automatizovaného

---

<sup>214</sup> NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3. s. 160.

<sup>215</sup> Dle článku 13 odst. 1 písm. f) GDPR má být subjekt údajů informován o případných příjemcích nebo o kategorii příjemců osobních údajů.

zpracování, včetně profilování a týká-li se souhlas předávání, pak musí být subjekt údajů informován o možných rizicích přenosu dat do třetích zemí a náležitých zabezpečovacích opatřeních.

Z právního jednání subjektu údajů pak musí být zřejmé, že subjekt údajů s daným konkrétním zpracováním souhlasil.<sup>216</sup>

Správci, kteří v současné chvíli zpracovávají osobní údajů na základě souhlasu získaných v souladu s národní legislativou nemusí automaticky své vnitřní procesy zcela měnit z důvodu přijetí GDPR – souhlas, který byl do té doby získán, zůstává v platnosti, pokud odpovídá podmínkám stanoveným v GDPR. GDPR ale zavádí povinnost doložit všechny získané souhlasy subjektů údajů a dále vyžaduje „prohlášení či zjevné potvrzení“ o získání souhlasu. Souhlasy založené na nepřímo vyjádřených, implicitních úkonech subjektů údajů (např. ignorování předem zaškrtnutého políčka) rovněž nebudou dle GDPR platně získané (stejně jako např. souhlasy obsažené v obchodních podmínkách přiložených k podepsané smlouvě zákazníkem).

Také operace a systémy IT mají být revidovány tak, aby bylo možno prokázat, že souhlas byl získán. Zároveň musejí být k dispozici mechanismy umožňující subjektu údajů snadné odvolání souhlasu a poskytující informaci o tom, jak souhlas odvolat. Pokud postupy pro získávání a spravování souhlasu nesplňují standardy GDPR, musí správci získat nový souhlas, který už bude v souladu s GDPR.

---

<sup>216</sup> Jak již autorka uvedla výše, souhlas nelze v žádném případě získat tím samým krokem, kterým dojde k odsouhlasení smlouvy nebo přijetím obchodních podmínek. Paušální odsouhlasení všeobecných obchodních podmínek nelze totiž považovat za jednoznačný projev souhlasu s použitím osobních údajů.

## 5 Adaptační zákony členských států

GDPR, přestože je převážně přímo použitelné, ukládá členským státům upravit vnitrostátním předpisem několik oblastí. Jde zejména o:

- a) volbu orgánu příslušného k akreditaci certifikačních těles,
- b) ustavení nezávislého dozorového orgánu, zajištění jeho činnosti, proceduru jmenování jeho vedení, zajištění nezávislosti vedení i zaměstnanců,
- c) případné doplňující sankce za porušení ochrany osobních údajů (kromě dosud existujících) a
- d) vyvážení svobody projevu a ochrany osobních údajů.

Z povahy věci pak národní legislativy vyžadují také dílčí adaptace tak, aby GDPR přivodily zamýšlený efekt. Národní legislativy mají dílčí specifika v různých oblastech, např. v koncepci správního trestání. Členské státy tak zpravidla spolu s nařízením přijímají adaptační zákony, kterými odstraňují normy, které by byly s nařízením v rozporu (ačkoliv jsou takovéto normy nařízením fakticky nahrazeny, je zachování takovéto derogované právní úpravy v rozporu s principem právní jistoty). Těmito adaptačními zákony jsou pak také prováděny případné dílčí odchylky a doplněny povinnosti, které nařízení umožňuje takovými adaptačními zákony upravit, a případně na nařízení navazují působnost národních orgánů veřejné moci, které nad jeho dodržováním mají vykonávat dozor a propojují je s procesními předpisy.<sup>217</sup> Stejně jako Česká republika nepřijaly ke dni 14. listopadu 2018 adaptační zákon tyto státy: Bulharsko, Estonsko, Finsko, Řecko, Portugalsko a Španělsko.<sup>218</sup> Islandský a Norský zákon na ochranu osobních údajů nabyde účinnosti spolu se začleněním

---

<sup>217</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.

<sup>218</sup> Srov. online mapu států s vyznačením implementace GDPR společnosti Morrison Foerster [online] [cit. 2018-07-12]. Dostupné z: <https://www.mofo.com/special-content/gdpr-readiness-center/gdpr-local-implementation.html>.

GDPR do Dohody o EHP. Lichtenštejnský zákon nabył účinnosti dne 1. ledna 2019.

Evropská komise jako „strážkyně smluv“ prosazuje evropské právo a dohlíží na jeho dodržování, tzn. je zodpovědná za zajištění řádného uplatňování aktů EU ve všech členských státech. Pokud zjistí, že některá členská země neuplatňuje právní předpis EU, zahájí tzv. řízení pro porušení práva, kdy nejprve zašle oficiální dopis dané vládě s odůvodněním svého stanoviska a stanovením lhůty na vysvětlení. Jestliže stát včas nepodá uspokojivé vysvětlení ani nezjedná nápravu, zašle Komise další dopis, v němž stanoví lhůtu, do kdy je třeba situaci napravit. Pokud ani tentokrát členský stát požadavky nesplní, je věc postoupena Soudnímu dvoru, který může svým rozsudkem uložit finanční sankce.<sup>219</sup> Dle sdělení Komise Evropskému parlamentu a Radě ze dne 24.1.2018<sup>220</sup> bude Evropská komise po květnu 2018 pečlivě monitorovat uplatňování GDPR v členských státech a v případě potřeby přijme příslušná opatření, včetně právních prostředků proti jeho porušení. Dle výše uvedeného sdělení Komise rok po vstupu GDPR v platnost uspořádá akci za účelem vyhodnocení zkušeností různých zúčastněných stran z jeho provádění. Toto bude rovněž zahrnuto do zprávy o hodnocení a přezkumu GDPR, kterou má Komise zpracovat do května 2020.

Při zpracování této kapitoly autorka vycházela zejména z důvodové zprávy k návrhu českého zákona o zpracování osobních údajů a z českých a

---

<sup>219</sup> PATNAIK, S.: *Extending the GDPR across the borders of the EU: data protection in the EEA*. [online] [cit. 2018-09-12]. Dostupné z: <https://www.privacyperfect.com/en/blog/data-protection-eea>.

<sup>220</sup> Viz informace, která je dostupná na stránkách Odboru komunikace o evropských záležitostech Úřadu vlády České republiky Dostupné z: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/CS/COM-2018-43-F1-CS-MAIN-PART-1.PDF>.

zahraničních odborných článků (např. od těchto autorů: Jakub Morávek, Alex van der Wolk, Gernot Fritz).

## 5.1 Česká republika

GDPR nenahradilo pouze Směrnicí 95/46/ES, ale v rámci ČR nahradilo také prováděcí zákon o ochraně osobních údajů. Adaptační zákon by měl nově upravovat jen aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho ustavení, organizaci atd.) a některé záležitosti, u kterých GDPR počítá s vnitrostátní úpravou. Jedná se např. o aspekty zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby. Český návrh zákona např. omezuje povinnost zřídit funkci pověřence pro ochranu osobních údajů tam, kde by šlo o ryzí formalitu. Výkladem pojmu „veřejný subjekt“ se předkladatel rozhodl, že pověřenec pro ochranu osobních údajů by nemusel být např. u tzv. servisních příspěvkových organizací. Rovněž sankce vyplývající z nové úpravy zůstávají pro obce a kraje stejné jako doposud. Horní hranice je stanovena na 10 mil. Kč. České právo však vylučuje, aby byly pokuty pro obce likvidační, čemuž odpovídá i dosavadní praxe, protože nejvyšší pokuta uložená obci byla 80 tis. Kč.

Jak uvádí důvodová zpráva k návrhu zákona, nevyužívá Česká republika možnosti, které GDPR dává ke stanovení ještě přísnějších podmínek, než GDPR stanovuje. Předkladatel tak např. nevyužívá možnosti stanovit další omezení zpracování některých citlivých údajů ve smyslu čl. 9 odst.4 GDPR, ani možnosti rozšířit skupinu správců povinných jmenovat pověřence ve smyslu čl. 37 odst. 4 ani možnosti vyžadovat další hodnocení dopadů podle čl. 35 odst. 10 GDPR. Předkladatel také nestanoví další sankce podle čl. 84 nad rámec sankcí již nyní stanovených trestním zákoníkem nebo zákonem na ochranu osobních údajů.<sup>221</sup>

---

<sup>221</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského

Český zákonodárce mimo jiné zakotvil detailní nároky na odborné a kvalifikační požadavky na členy vedení ÚOOÚ, když dle ustanovení §50 je mimo jiné podmínkou výkonu předsedy Úřadu i *potřebná úroveň znalostí anglického, německého nebo francouzského jazyka*.

V souvislosti s přijetím GDPR by měla Česká republika přijmout dva adaptační zákony – jednak zákon o zpracování osobních údajů a dále zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů (tzv. změnový zákon). Zákon o zpracování osobních údajů má zejména přizpůsobit právní řád požadavkům GDPR, včetně povolených výjimek a odchylek a má upravovat postavení Úřadu pro ochranu osobních údajů. Změnový zákon by měl upravovat 19 zákonů, jejichž obsah je nutné přizpůsobit (jedná se např. o občanský soudní řád, trestní řád, zákon o organizaci a provádění sociálního zabezpečení). Až 21. března 2018 vláda schválila návrh „nového“ zákona o ochraně osobních údajů a „nový“ zákon o zpracování osobních údajů tak nebyl doposud Českou republikou přijat.

Nepřijetí adaptačního zákona včas bude představovat problém zejména pro veřejnou správu, kdy nedošlo ke schválení některých výjimek z povinností dle GDPR a omezení pokut, které by se na zpracování osobních údajů při výkonu veřejné moci měly vztahovat. Oproti tomu má autorka za to, že na soukromoprávní subjekty nemá nepřijetí vnitrostátního zákona do dne účinnosti GDPR téměř žádný dopad.

Na rozdíl od směrnice, nařízení nepředpokládá a ani neumožňuje, aby se provedlo v rámci národní legislativy, pokud tak není v nařízení přímo umožněno. Zákon o ochraně osobních údajů tak bude muset být aplikován

---

parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 48. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

současně s GDPR. Obdobně jako u zrušeného zákona o ochraně osobních údajů platí, že obecná úprava je v tomto předpisu a zvláštní výjimky a postupy jsou dle potřeby v jiných zákonech.<sup>222</sup> S ohledem na přímou použitelnost nařízení nemůže zdvojit vnitrostátní právní úpravu obsaženou v nařízení. Do českého zákona tak nelze opětovně přepisovat definice (správce, zpracovatel, osobní údaj) či jednotlivá práva subjektu údajů apod. GDPR. Zákon o zpracování osobních údajů tak obsahuje pouze tu právní úpravu, kdy GDPR předpokládá, že národní legislativa bude přijata (zj. k využití výjimek, které jsou v GDPR obsaženy). Zákon o zpracování osobních údajů kromě adaptace GDPR transponuje i směrnici 2016/680, která upravuje zpracování osobních údajů justičními a policejními orgány.<sup>223</sup>

Autorka se dále bude zabývat analýzou výjimek GDPR upravených v českém návrhu zákona o zpracování osobních údajů.

#### 5.1.1 Působnost adaptačního zákona

Působnost adaptačního zákona je v ustanovení §4 vymezena takto:

*(1) Ustanovení této hlavy se použijí při zpracování osobních údajů podle nařízení Evropského parlamentu a Rady (EU) 2016/679.*

*(2) Ustanovení této hlavy a nařízení Evropského parlamentu a Rady (EU) 2016/679 se použijí i při zpracování osobních údajů, které mají být nebo jsou zařazeny do evidence, a při zpracování osobních údajů, které probíhá zcela nebo*

---

<sup>222</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 34-35. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

<sup>223</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 60-61. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.



*částečně automatizovaně, nejde-li o zpracování osobních údajů fyzickou osobou v průběhu výlučně osobních nebo domácích činností,*

*a) při výkonu činností, které nespádají do oblasti působnosti práva Evropské unie nebo do působnosti hlavy III nebo IV, nebo*

*b) při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o Evropské unii.*

Věcná působnost je tedy stanovena odlišně a širěji, než jak je vymezena v GDPR, které se (naopak mimo) jiné nepoužije na zpracování prováděné:

- (i) při výkonu činností, které nespádají do oblasti působnosti práva EU;
- (ii) členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU.<sup>224</sup>

Český právní předpis se tak bude vztahovat i na další oblasti zpracování osobních údajů, u kterých by mohly být pochybnosti, zda spadají nebo nespádají do působnosti práva EU (např. ochrana osobních údajů při správě daní, které právo EU neupravuje), popřípadě na která se GDPR ani směrnice 2016/680 zjevně nevztahuje. Takovým zpracováním dle písm. b) bude oblast společné zahraniční a bezpečnostní politiky, na kterou lze pravidla GDPR a adaptačního zákona ve vztahu k českým správčům vztáhnout, neboť EU svou působnost podle čl. 39 SEU nevykonala.<sup>225 226</sup>

---

<sup>224</sup> Srov. článek 2 GDPR.

<sup>225</sup> Srov. čl. 39 GDPR dle kterého *V souladu s článkem 16 Smlouvy o fungování Evropské unie a odchylně od jeho odstavce 2 přijímá Rada rozhodnutí, které stanoví pravidla o ochraně fyzických osob při zpracovávání osobních údajů členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti této kapitoly, a pravidla o volném pohybu těchto údajů. Dodržování těchto pravidel podléhá kontrole nezávislými orgány.*

<sup>226</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 59. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

### 5.1.2 Výjimka z povinnosti posuzování slučitelnosti účelů

V ustanovení §6 využívá zákonodárce možnosti dané bodem odůvodnění 50, návěťím článku 6 odst. 4 a článkem 23 GDPR k tomu, aby se pro zvláště významná zpracování ve veřejném zájmu stanovila možnost dalšího zpracování bez přezkoumávání slučitelnosti účelů původního a následného zpracování, které v jiných případech článek 6 odst. 4 ve spojení se zásadou účelového omezení zakotvené v článku 5 odst. 1 písm. b). Rozšiřuje se tak slučitelnost účelů i na další případy kromě slučitelnosti zpracování pro vědecké nebo historické výzkumné účely, statistické účely a účely archivace ve veřejném zájmu podle samotného článku 5 odst. 1 písm. b) GDPR. Český zákon stanoví výjimky, pokud má správce právním předpisem stanovenou povinnost nebo úkol ve veřejném zájmu, případně pokud je pověřen výkonem veřejné moci. Odstavec 2 pak tyto zájmy uvádí, když jejich výčet odpovídá příslušným důvodům pro výjimky podle čl. 23 odst. 1 GDPR.<sup>227</sup>

---

<sup>227</sup> Dle českého zákona se chráněným zájmem rozumí: (a) obranné nebo bezpečnostní zájmy České republiky, (b) veřejný pořádek a vnitřní bezpečnost, předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkon trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách věcech, (c) jiný důležitý cíl veřejného zájmu EU nebo členského státu EU, zejména důležitý hospodářský nebo finanční zájem EU nebo členského státu EU, včetně záležitostí měnových, peněžních, rozpočtových, daňových a finančního trhu, veřejného zdraví nebo sociálního zabezpečení, (d) ochrana nezávislosti soudů a soudců, (e) předcházení, vyhledávání, odhalování nebo stíhání porušování etických pravidel regulovaných povolání, (f) dohledové, kontrolní nebo regulační funkce spojené s výkonem veřejné moci v případech uvedených v písmenech a, b a e, (g) ochrana práv a svobod osob, nebo (h) vymáhání soukromoprávních nároků.

### 5.1.3 Věková hranice dítěte pro udělení souhlasu se zpracováním osobních údajů

GDPR dává státům možnost upravit odlišně věkovou hranici pro souhlas udělovaný dítětem v souvislosti se službami informační povinnosti oproti v GDPR stanovenému věku 16 let.<sup>228</sup>

Dále v ustanovení §7 návrhu zákona je stanovena věková hranice pro „online souhlasy“ dětí na věk 15let. Ačkoliv GDPR tak přímo nestanoví, lze mít za to, že je-li dítě daného věku způsobilé k udělení souhlasu, je způsobilé i k jeho odvolání, případně k uplatnění dalších práv (právo na výmaz, opravu atd.) týkajících se takového zpracování osobních údajů, ke kterému dalo souhlas.<sup>229</sup>

Není ale jasné zde-li bude po přechodnou dobu mezi účinností GDPR a účinností českého zákona vyžadován souhlas zákonného zástupce nebo jeho svolení v případech, kdy by podle návrhu zákona nebyl potřeba.<sup>230</sup>

Vzhledem k možnosti volby věkové hranice členskými státy může tato hranice oscilovat mezi 13 a 16 lety. Například v Německu nebo na Slovensku je stanovena na 16 let, naopak Rakousko ji stanovilo na věk 14 let. S ohledem na tuto odlišnost si tak provozovatelé webů musí ohlídat, zda-li jsou splněny požadavky té konkrétní země. Zejména problematické může toto být u webových stránek a aplikací dostupných v angličtině – i když provozovatel může cílit např. pouze na britský trh, internet nezná hranic a k takovému webu nebo aplikaci se mohou snadno připojit i děti z České republiky. Odkud se ale

---

<sup>228</sup> Nejnižší věkovou hranici 13 let si stanovilo 11 z 28 států EU včetně např. Polska.

<sup>229</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 62-63. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAOCDZPW5>.

<sup>230</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.

uživatel připojuje může provozovatel webových stránek zjistit z jeho IP adresy a případně se může rozhodnout přístup pro takovou IP adresu blokovat.<sup>231</sup>

#### 5.1.4 Výjimka z povinnosti posouzení vlivu zpracování osobních údajů na ochranu osobních údajů

Ustanovení §10 návrhu zákona stanovuje výjimku z povinnosti posouzení vlivu zpracování osobních údajů na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést. Jedná se o provedení možnosti danou článkem 35 odst. 10 GDPR. Pokud tedy ukládá právní předpis nějakou povinnost, jejíž součástí je i zpracování osobních údajů (např. zaměstnavatel musí zpracovávat osobní údaje pro účely sociálního pojištění), nemusí správce provádět posouzení vlivu na ochranu osobních údajů. Česká republika tedy na základě čl. 35 odst. 10 GDPR další hodnocení nepožaduje.<sup>232</sup>

Bude existovat řada zpracování osobních údajů uložených správci právním předpisem, u kterých by se dle GDPR posouzení vlivu muselo provést (např. zdravotnická dokumentace), dle znění návrhu zákona budou ale tato zpracování vyňata. Není ale jasné, zda-li má být po přechodnou dobu mezi účinností GDPR a účinností českého adaptačního zákona v takových situacích předběžné posouzení vlivu provedeno.<sup>233</sup>

---

<sup>231</sup> VEJVODOVÁ, A. *Facebookový profil a e-mail díky GDPR budou až od 15 let se souhlasem rodičů.* [online] [cit. 2018-11-12]. Dostupné z: <https://pravnicaradce.ihned.cz/c1-66108830-facebookovy-profil-a-e-mail-diky-gdpr-budou-az-od-15-let-se-souhlasem-rodicu>.

<sup>232</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 63-64. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

<sup>233</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.

### 5.1.5 Povinnost jmenovat pověřence pro ochranu osobních údajů a výklad pojmu veřejný subjekt

Návrh zákona o zpracování osobních údajů v ustanovení §14 uvádí, že povinnost jmenovat pověřence pro ochranu osobních údajů mají kromě *orgánů veřejné moci* také *orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu*.<sup>234</sup> Český zákonodárce výkladem pojmu *veřejný subjekt* omezil povinnost jmenování pověřence pro správce spadající sice do veřejného sektoru, kteří se ale zároveň nevyznačují vztahem formální a materiální nerovnováhy mezi subjektem údajů a správcem jako v případě orgánů veřejné moci. Povinnost jmenovat pověřence pro ochranu osobních údajů tak nebude dle důvodové zprávy dopadat např. na divadlo či knihovnu zřízenou obcí jakožto příspěvkovou organizací s běžným rozsahem zpracování osobních údajů. Pokud ale taková organizace bude provádět zpracování ve smyslu ustanovení čl. 37 odst. 1 písm. b) nebo c) GDPR<sup>235</sup> (například zdravotnická nebo pečovatelská zařízení, protože provádějí systematický monitoring subjektů údajů nebo rozsáhlé zpracování citlivých údajů) bude se na ně povinnost pověřence ustanovit vztahovat.

Český zákonodárce vycházel z toho, že někteří správci, tradičně řazení spíše do veřejného sektoru, se nevyznačují podobným vztahem se subjekty údajů jako

---

<sup>234</sup> Srov. výklad pojmu „veřejný subjekt“ WP 29 ve stanovisku k pověřenci pro ochranu osobních údajů, dle kterého: „*veřejné úkoly mohou vykonávat a veřejnou moc uplatňovat nejen orgány veřejné moci a veřejné subjekty, ale také fyzické nebo právnické osoby veřejného nebo soukromého práva, a to v závislosti na vnitrostátní právní úpravě v každém členském státu, v odvětvích jako služby veřejné dopravy, dodávky vody a energie, silniční infrastruktura, veřejnoprávní vysílání a obecní bydlení, nebo disciplinárními orgány pro regulovaná povolání*“.

<sup>235</sup> Dle tohoto ustanovení *Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy: b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.*

orgány veřejné moc. Pokud však takový správce provádí jako svou hlavní činnost zpracování zahrnující rozsáhlé a systematické monitorování nebo rozsáhlé zpracování citlivých osobních údajů nebo údajů o rozsudcích v trestních věcech a trestných činech, pověřence bude muset jmenovat, a to podle článku 37 odst. 1 písm. b) nebo c) GDPR.<sup>236</sup>

S ohledem na nepřijetí adaptačního zákona včas lze také položit otázku, zda-li mají na přechodnou dobu mezi účinností GDPR a účinností adaptačního zákona ustanovit pověřence i subjekty, u nichž by tato povinnost vyplývala z GDPR, nikoliv však podle definice zakotvené v návrhu zákona. Dle autorky lze mít za to, že nikoliv. Na druhou stranu není v tuto chvíli zřejmé, zda-li návrh zákona nebude v tomto ustanovení připomínkován, a zda-li bude opravdu v takovémto znění schválen a přijat.<sup>237</sup>

#### 5.1.6 Zpracování prováděné pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu

Ustanovení článku 85 GDPR ukládá členským státům povinnost uvést prostřednictvím právních předpisů právo na ochranu osobních údajů podle GDPR do souladu s právem na svobodu projevu a informací, včetně zpracování pro novinářské účely a pro účely akademického, uměleckého nebo literárního projevu. Český návrh zákona toto provádí v ustanoveních §16 - §21.

Ustanovení §16 odst. 1 navazuje na čl. 6 odst.1 písm. f) GDPR, dle kterého je zpracování osobních údajů zákonné, pokud je prováděno pro účely oprávněných zájmů správce, ledaže by převažovala práva a zájmy subjektu

---

<sup>236</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 66-68. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAOCDZPW5>.

<sup>237</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.

údajů. Dle důvodové zprávy lze dovodit, že mezi tyto oprávněné zájmy patří i zpracování pro novinářské účely a pro účely akademického, uměleckého a literárního projevu. Návrh zákona pak výslovně tyto účely uvádí jako zákonný titul zpracování. Odst. 2 §16 upravuje podmínky pro zpracování citlivých osobních údajů pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu a je přípustné pouze v případě nezbytnosti takového zpracování k dosažení oprávněného cíle a pouze pokud převažuje oprávněný zájem na tomto zpracování nad oprávněnými zájmy subjektu údajů. Lze mít za to, že oprávněným cílem novináře tak nebude zveřejnění citlivého údaje za účelem senzace a oprávněným zájmem subjektu údajů naopak nebude snaha vyhnout se zveřejnění citlivého osobního údaje významného např. v souvislosti s politickou činností.<sup>238</sup> Ustanovení §16 dále obsahuje zpracování údajů o trestních věcech, když cílem návrhu je v zásadě zachovat dosavadní standard informování o trestních věcech. S ohledem na citlivost informace o potrestání se připouští zpracování osobních údajů jen v případě potřeby použití údajů k dosažení oprávněného cíle a převahy oprávněného zájmu na použití osobních údajů nad zájmy subjektu údajů. Odst. 4 §16 návrhu zákona zakotvuje zákaz cenzury a právo na ochranu zdroje. S ohledem na rozvoj nových technologií se výslovně odkazuje na použitelnost shodných pravidel i pro internetová media. Právo na ochranu zdroje a obsahu informací se z povahy věci bude vztahovat i na informace, věci či prostředky, z nichž by mohl být zdroj či obsah informací určen.<sup>239</sup>

---

<sup>238</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 70. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

<sup>239</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 72. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

Návrh zákona dále v ustanovení §17 počítá s výjimkami z poučovací a informační povinnosti správce při zpracování pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu, když by její naplňování bylo v praxi jen obtížně představitelné a v některých případech by i mohlo mařit novinářskou práci.

Návrh zákona zároveň upravuje pravidla a výjimky potřebné k ochraně zdroje a informací, které by jinak byly normami GDPR prolomeny,<sup>240</sup> zužující výjimku z práva na omezení zpracování osobních údajů<sup>241</sup> a zužující výjimku z povinnosti informovat o opravě nebo výmazu osobních údajů, kdy toto plnění by zejména v on-line prostředí nebylo v praxi reálně proveditelné.<sup>242</sup>

Ustanovení §21 návrhu zákona pak zužuje právo subjektu údajů na podání námítky proti zpracování. Námítka musí být v tomto případě dostatečně konkrétní a musí se týkat konkrétní informace a převaha osobního zájmu nad veřejným musí být alespoň osvědčena. Námítku je zároveň možné podat pouze ohledně již zveřejněných údajů, protože v rámci svobody projevu, resp. svobody tisku, teprve zveřejnění údajů podstatně zasahuje do práv subjektu údajů.<sup>243</sup>

#### 5.1.7 Výše sankcí pro veřejnoprávní subjekty

Dle ustanovení článku 83 odst. 7 GDPR *může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.*

---

<sup>240</sup> Viz ustanovení §18 návrhu zákona o zpracování osobních údajů.

<sup>241</sup> Viz ustanovení §19 návrhu zákona o zpracování osobních údajů.

<sup>242</sup> Dle §20 návrhu zákona o zpracování osobních údajů bude tato povinnost splněna také *uvedením údaje o okamžiku poslední aktualizace obsahu, v němž jsou nebo byly osobní údaje uvedeny.*

<sup>243</sup> Viz důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680, s. 75. Dostupné online na: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.



V souladu s tím český zákonodárce omezuje v §60 odst. 5 návrhu zákona horní hranici správní pokuty pro veřejnoprávní subjekty na 10 mil. Kč, shodně s původní úpravou zákona č. 101/2000Sb. Důvodem tohoto omezení je dle důvodové zprávy k návrhu zákona *snaha smířit odrazující a sankční povahu pokuty s faktem, že finanční prostředky těchto pokutovaných institucí zpravidla plynou z veřejných rozpočtů*. Nadto je třeba upozornit, že český zákonodárce nevyužil možnost vyloučit sankce pro veřejnoprávní orgány zcela.

Ačkoliv uvedený důvod pro zavedení snížených sankcí pro veřejnoprávní orgány je na jednu stranu pochopitelný, má autorka za to, že takovouto diferenciací výše pokut zákonodárcem by bylo možné vykládat i jako sdělení pro občany, že stát není plně připraven chránit jejich soukromí a nechce v této oblasti nést plnou zodpovědnost.

#### 5.1.8 Souhlas se zpracováním osobních údajů

Dle bodu odůvodnění č. 171 GDPR *„zpracování, které již ke dni použitelnosti tohoto nařízení probíhá, by mělo být uvedeno v soulad s tímto nařízením ve lhůtě dvou let ode dne vstupu tohoto nařízení v platnost. Je-li toto zpracování založeno na souhlasu podle směrnice 95/46/ES, není nutné, aby subjekt údajů znovu udělil svůj souhlas, pokud je způsob udělení daného souhlasu v souladu s podmínkami tohoto nařízení, s cílem umožnit správci pokračovat v tomto zpracování i po dni použitelnosti tohoto nařízení.“* V rámci jednání legislativní rady vlády bylo správně poukazováno na to, že pokud má být pravidlo vyplývající z tohoto bodu odůvodnění závazné, musí být součástí nějakého normativního právního aktu, což není. Tato připomínka byla předkladatelem reflektována v ustanovení §64, odst. 7 tohoto znění:

*„Souhlas subjektu údajů udělený podle zákona č. 101/2000 Sb. se považuje za souhlas podle nařízení Evropského parlamentu a Rady (EU) 2016/679, ledaže způsob jeho udělení nebyl v souladu s tímto nařízením.“*

Lze mít za to, že takováto úprava není dostačující, když není českým zákonem stanovena lhůta, dokdy je třeba případně souhlas v kvalitě GDPR získat. S ohledem na fakt, že účinnost zákona je stanovena dnem jeho vyhlášení, měl by být dle gramatického výkladu nový souhlas získán bezprostředně s účinností zákona. Takto stanovená lhůta není, zejména u velkých databází, objektivně možná, proto je i v bodu odůvodnění č.171 lhůta dvou let. Nemá-li být tato právní norma defektní, pak je nutné ji upravit.<sup>244</sup>

#### 5.1.9 Trestání a odpovědnost

S ohledem na rozdílnost v pojetí přestupkového práva v jednotlivých členských státech, nemůže GDPR stanovit univerzální skutkové podstaty deliktů. Členské státy tedy musí reagovat na čl. 83 GDPR a stanovit příslušné skutkové podstaty deliktů. Samotné GDPR stanovuje, jaká jednání by měla být podle národní legislativy trestná a jaké sankce by za ně mělo být maximálně možné uložit s tím, že přímo na základě GDPR není možné trestat. Tak učinil i český zákonodárce v rámci návrhu ustanovení §60 adaptačního zákona.<sup>245</sup> Důvodová zpráva k tomuto ustanovení pak mimo jiné uvádí, že *„smyslem ustanovení nicméně je, aby se na projednání a ukládání sankcí stanovených čl. 83 nařízení 2016/679 úřadem použily předpisy o správním trestání“*.

Dle ustanovení §5 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich (přestupkový zákon) *„Přestupek je společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje*

---

<sup>244</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.

<sup>245</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.

*znaky stanovené zákonem, nejde-li o trestný čin.“ Důvodová zpráva k přestupkovému zákonu pak stanoví, že „Přestupek je vymezen na základě materiálně-formálního pojetí, přičemž ke vzniku odpovědnosti za přestupek bude muset dojít k naplnění všech jeho znaků současně – to znamená, že musí jít o protiprávní společensky škodlivý čin, který je v zákoně za přestupek výslovně označen a zároveň vykazuje znaky stanovené zákonem, tedy obecné znaky přestupku i znaky konkrétní skutkové podstaty přestupku, nejde-li o trestný čin.“*

Vzhledem k neúčinnosti národního adaptačního zákona po 25. květnu 2018 je otázkou, zda-li jednání odporující GDPR bude trestné, když v danou situaci není národní právní předpis, který by takové jednání za přestupek označil. Zároveň není zřejmé, jak bude za těchto okolností nahlíženo na jednání, která naplňovala skutkové podstaty přestupků podle zákona na ochranu osobních údajů, kterých se bude po dni nabytí účinnosti vést správní řízení, nebo o kterých ještě řízení vedeno nebylo, nebo o kterých již bylo rozhodnuto tak, že se o přestupky jedná a v danou chvíli zákonnost rozhodnutí Úřadu pro ochranu osobních údajů přezkoumává správní soud.<sup>246</sup> Lze mít za to, že trestnost takovýchto jednání nebude generálně zachována, a že je nebude možné bez dalšího podřadit pod ustanovení §44 a §45 zákona o ochraně osobních údajů a podle těchto ustanovení trestat. Dle Morávka<sup>247</sup> *jednání spáchaná do 24. 5. 2018 (porušení právních povinností podle zákona č. 101/2000 Sb.) by mohla být dále trestná jedině tehdy, bude-li i nadále existovat hmotněprávní povinnost, která je znakem objektivní stránky přestupku. Tato musí být nutně obsahově shodná. Pokud povinnost existovat dále nebude, odpovědnost zaniká. A Jednání spáchaná po 24. 5. 2018 (porušení právních povinností podle obecného nařízení) by mohla být trestná jedině tehdy, bude-li hmotněprávní povinnost podle nařízení obsahově totožná s povinností podle zákona č. 101/2000 Sb.,*

---

<sup>246</sup> K tomu srov. rozhodnutí NSS sp. Zn. 50 As 104/2013.

<sup>247</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.

*kteřá v §44 nebo §45 zákona na ochranu osobních údajů tvořív objektivní stránku skutkové podstaty přestupku. Tak tomu není např. u povinnosti jmenovat pověřence pro ochranu osobních údajů (čl. 37) a dalších.*

Lze mít tedy za to, že včasné nepřijetí adaptačního zákona českým zákonodárcem přineslo částečnou „přestupkovou“ amnestii v oblasti ochrany osobních údajů.

Včasné nepřijetí adaptačního zákona nemá, s ohledem na přímou použitelnost nařízení EU, vliv na účinnost a použitelnost GDPR. Česká republika tím ale nevyužila možnost aplikovat již od samého počátku vlastní pravidla úpravy tam, kde to GDPR umožňuje. Tak bude nutné do data účinnosti nového zákona používat GDPR v jeho plném rozsahu bez jakýchkoliv výjimek nebo úlev. Zároveň dle Morávka *lze mít za to, že by návrh zákona o zpracování měl být doplněn o určité aspekty, které by vedly ke snížení nedůvodné administrativní zátěže. Takovým doplněním je kupř. zakotvení obecné povinnosti mlčenlivosti odpovídající právní úpravě obsažené v §15 zákona na ochranu osobních údajů.* Ke dni 31. ledna 2019 byl návrh zákona na schůzi Senátu návrh zákona vrácen Poslanecké sněmovně s pozměňovacími návrhy.<sup>248 249</sup>

## **5.2 Slovenská republika**

Slovenský zákon o ochraně osobních údajů č.18/2018Z. z.,<sup>250</sup> kterým se provádív GDPR a související směrnice o ochraně fyzických osob v souvislosti se

---

<sup>248</sup>Viz sněmovní tisky č. 138/0 a 139/0, dostupné na stránkách Poslanecké sněmovny Parlamentu České republiky: <http://www.psp.cz/sqw/tisky.sqw?str=2&O=8&PT=K&N=1&F=N&D=1,2,16&RA=20&iseu=1>.

<sup>249</sup> Viz usnesení Senátu č. 85 z 5. schůze konané dne 30. ledna 2019. Dostupné online z: <https://www.senat.cz/xqw/xervlet/pssenat/htmlhled?action=doc&value=90498>.

<sup>250</sup> Zákon č. 18/2018 Z. z. o ochrane osobních údajov a o zmene a doplneni niektorých zákonov.

zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonů trest, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV nabyt účinnosti dne 25. května 2018. Na rozdíl od českého návrhu je slovenský zákon o ochraně osobních údajů podstatně obsáhlejší, neboť vedle přejímání definic a zásad obsažených v GDPR zavádí i vlastní definice (např. logování) a rovněž blíže upravuje např. proces podávání stížností pro porušení předpisů o zpracování osobních údajů a řízení o těchto stížnostech. Odlišně od českého zákona pak setrvává na věkové hranici 16 let pro udělení souhlasu dítěte v souvislosti se službami informační společnosti a nedefinuje veřejné subjekty.

V jeho ustanovení §78 upravuje možnost zpracovávat osobní údaje bez souhlasu subjektu údajů, a to pro účely akademické, umělecké nebo literární, nebo pokud je takové zpracování nezbytné pro potřeby informování veřejnosti sdělovacími prostředky a pokud takové zpracování vyplývá z předmětu činnosti provozovatele. Uvedené zpracování však nesmí porušovat právo dotčené osoby na ochranu její osobnosti nebo právo na ochranu soukromí a provozovatel by měl podle důvodové zprávy zvážit, zda je dané zpracování skutečně nezbytné.

Dále pro zpracování pro účely archivace, vědecké a statistické účely nebo pro účely historického výzkumu zakotvil slovenský zákonodárce možnost omezení práv dotčené osoby, a to práva na přístup, práva na opravu, práva na omezení zpracování, právo námitky a právo na přenositelnost při zpracování osobních dat pro tyto účely.

Na rozdíl od České republiky, kdy se zákonodárce omezil na nebytné minimum, slovenská verze adaptačního zákona fakticky obsah GDPR opakuje. Toto řešení nelze považovat za vhodné z důvodu chybovosti předpisu a s ohledem na skutečnost, že přetlumočením fakticky dojde k odtržení

normativního textu od úvodních recitálů (bodů odůvodnění), které GDPR uvozují a dávají mu konkrétní smysl.<sup>251</sup>

### 5.3 Rakouská republika

Rakouský zákon na ochranu osobních údajů<sup>252</sup> (dále jen „DSG“) reflektující GDPR byl oficiálně zveřejněn dne 31. července 2017 a dne 25. května 2018 nabyl účinnosti. Rakouský zákonodárce upravil pouze některá ustanovení GDPR umožňující odlišnou národní úpravu.

Dle rakouského práva na ochranu osobních údajů může být subjektem údajů vedle fyzické osoby i osoba právnická. Věková hranice pro udělení souhlasu dítěte v souvislosti se službami informační společnosti je DSG stanovena na věk 14 let. Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů mohou dle DSG zpracovávat i soukromoprávní subjekty, když ustanovení článku 10 GDPR stanoví, že takové údaje mohou být zpracovávány pouze pod dozorem orgánu veřejné moci nebo pokud je takové zpracování oprávnění podle práva EU nebo podle práva příslušného členského státu. Takovou možnost upravuje §4 odst. 3 DSG, který stanoví, že k takovému zpracování může dojít, pokud to je nezbytné pro účely oprávněných zájmů ve smyslu článku 6, písm. f) GDPR. S ohledem na článek 88 GDPR<sup>253</sup> DSG v ustanovení §11 odkazuje na rakouský zákoník práce upravující zpracování v souvislosti se zaměstnáním. Ustanovení §30 DSG stanoví zvláštní pravidla pro vybírání pokut od právnických osob. Pokuty mají být ukládány přímo odpovědné právnické osobě. Kromě toho má rakouský úřad na ochranu osobních údajů pravomoc potrestat i odpovědnou fyzickou osobu (zejména

---

<sup>251</sup> MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14. s.487.

<sup>252</sup> Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).

<sup>253</sup> Dle tohoto ustanovení mohou členské státy stanovit konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, za demonstartivně uvedenými účely.

výkonné ředitele společnosti, nikoliv DPO).<sup>254</sup> První pokuta byla rakouským regulátorem uložena necelé čtyři měsíce ode dne účinnosti DSG, a to ve věci instalace neoznačeného kamerového systému, který mimo jiné zaznamenával i část chodníku – veřejného prostranství. Výše pokuty byla však v tomto případě poměrně nízká – 4 800 EUR.<sup>255</sup> Ustanovení §30 odst. 5 rakouského zákona pak stanoví, že *pokuty nelze uložit orgánům státní moci a veřejným institucím.*<sup>256</sup>

Rakouský DSG je celkově minimalistický a využívá omezený počet možností nabízených GDPR k zakotvení přísnějších nebo odchylných ustanovení. Zvláštní ustanovení o ochraně osobních údajů budou následovat i v dalších právních předpisech, neboť DSG se omezuje toliko na obecná ustanovení (např. oblast finančního a pojišťovacího sektoru).

---

<sup>254</sup> WOLK, A.: *Austria's GDPR Implementation Law*. [online] [cit. 2018-12-12]. Dostupné z <https://www.mofo.com/resources/publications/170918-austria-gdpr-implementation-law.html>.

<sup>255</sup> GERNOT, F.: *First GDPR fine issued by Austrian data protection regulator*. [online]. Dostupné z <https://www.lexology.com/library/detail.aspx?g=7efc00e0-fcaf-4509-b3f8-afa6bf1f2893>.

<sup>256</sup> *Gegen Behörden und öffentliche Stellen können keine Geldbußen verhängt werden.*

## Závěr

Přijaté GDPR reaguje na rozvoj nových technologií, které v době přijetí Směrnice 95/46/ES neexistovaly (jedná se např. rozvoj sociálních sítí a cloudových úložišť) a dále na odlišnou úpravu ochrany osobních dat napříč členskými státy, kdy GDPR má zajistit jednotnou vysokou úroveň jejich ochrany. Autorka v úvodu práce vytyčila níže uvedené cíle včetně dílčích výzkumných otázek.

Upozornit na nedostatky Směrnice 95/46/ES včetně dílčího výzkumu problematiky její územní působnosti. Nad rámec výše uvedeného autorka jako nedostatek identifikovala problematiku územní působnosti této směrnice. Aby mohla být Směrnice 95/46/ES použitelná i na společnosti usazené mimo EU, resp. EHP, musel být naplněn požadavek tzv. neoddělitelné spojitosti („*an inextricable link*“) mezi společnostmi usazenou na území třetího státu a společnostmi vykonávající na území EU zpracování osobních údajů. Oproti tomu GDPR se vztahuje na všechna zpracování osobních údajů subjektů údajů, kteří se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisí s nabídkou zboží nebo služeb těmto subjektům údajů nebo s monitorováním jejich chování, ke kterému dochází v rámci Unie.

Dále se autorka v první části práce věnovala dílčímu výzkumu vlivu Směrnice 95/46/ES na vývoj práva o ochraně osobních údajů mimo území EU/EHP. Zrušovaná Směrnice 95/46/ES ovlivnila vývoj práva na ochranu osobních údajů i mimo území EU, když díky požadavku na zajištění odpovídající úrovně ochrany osobních dat třetí zemí, do které jsou údaje z EU předávány, ovlivnila vnitrostátní předpisy těchto nečlenských států (jedná se např. o Argentinu, Turecko či Hong Kong).



Dále autorka zkoumala problematiku věcné působnosti Směrnice 95/46/ES, když je z ní vyloučeno „zpracování pro osobní potřebu“. Osobní potřebu je třeba chápat jako potřebu soukromou, a tu pak nejen jako potřebu fyzické osoby samotné, ale i jejích blízkých, členů rodiny a osobních přátel. Naopak za osobní potřebu nelze považovat zpracování osobních údajů v souvislosti s trestnou činností fyzické osoby pro soukromé účely, nebo zpracování osobních údajů získaných neoprávněně, protiprávně, např. krádeží dat z informačního systému jiného subjektu. Osobní potřebou nebude ani takové zpracování, při kterém dochází k neoprávněnému zásahu do práv jiných osob, typicky zveřejňováním osobních údajů.

Ve třetí kapitole se autorka zabývá otázkou důvodnosti a nezbytnosti přijetí nové právní úpravy na poli Evropské unie. Jak již autorka uvedla, GDPR reaguje na rozvoj nových technologií, které v době přijetí Směrnice 95/46/ES neexistovaly a dále, jakožto evropský zákon, má zajistit jednotnou právní úpravu ochrany osobních dat napříč členskými státy. Autorka považuje přijetí GDPR za potřebné a právní formu nařízení za odůvodněnou.

Dalším cílem stanoveným v úvodu práce bylo zodpovězení otázky, za jakých podmínek lze IP adresu a soubory cookies považovat za osobní údaje podléhající právní úpravě GDPR. GDPR výslovně v článku 4 jako osobní údaj uvádí také síťové identifikátory či lokační údaje, kam nepochybně cookies spadají. Nicméně bod 30 odůvodnění GDPR vychází z toho, že samotné elektronické (síťové) identifikátory (včetně cookies) nemusí být vždy považovány za osobní údaje. Lze mít za to, že v případě, kdy by cookies byly podle GDPR osobními údaji, tedy v případě, kdy by provozovatel webových stránek byl schopen na jejich základě a případně na základě i dalších údajů identifikovat konkrétní fyzickou osobu, vztahoval by se na jejich používání režim opt-in.

Ústředním tématem práce je institut souhlasu se zpracováním osobních údajů včetně jeho aspektů, kdy GDPR základní parametry souhlasu upravených Směrnicí 95/46/ES nemění, ale požadavky rozšiřuje. Souhlas se zpracováním osobních údajů dle GDPR musí být svobodný, konkrétní, informovaný a jednoznačný. Zároveň v případě, kdy je souhlas se zpracováním vyjádřen písemným prohlášením, které se týká i jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Není tak možné souhlas se zpracováním osobních údajů „včleňovat“ do obchodních podmínek přikládaných ke smlouvě se zákazníky apod. Lze mít za to, že za platný může být považován i souhlas udělený konkludentně. Pokud by bylo z úkonu subjektu údajů zcela jasné, že musel vědět, že na základě těchto úkonů dává svolení ke zpracování svých osobních údajů, lze mít za to, že i v takovém případě se jedná o platně udělený souhlas, byť konkludentním způsobem. GDPR dále v článku 8 provádí zájem na zvláštní ochranu osobních údajů dětí mladších 16 let. V praxi bude ale velmi obtížné takové ověření udělení/ schválení souhlasu uděleného osobou vykonávají rodičovskou zodpovědnost k dítěti reálně provést, protože děti zpravidla nedisponují žádným dokladem, který by ověření jejich zástupce nějak jednoduše umožňoval, a stejně tak správce nemá přístup do registrů, aby mohl totožnost ověřit.

Autorka ve čtvrté kapitole rozebírá některá práva subjektů údajů, např. právo na výmaz, které GDPR již výslovně zakotvuje. V souvislosti s tím autorka v práci provedla analýzu rozhodnutí SDEU ve věci Google Spain s cílem jeho kritického zhodnocení. Za problematické v tomto judikátu lze označit zj. nadřazení práva jednotlivce nad svobodou vyjadřování a nad právem na přístup k informacím; to že práva subjektu údajů chráněná ustanoveními článků 7 a 8

Listiny základních práv EU obecně převažují nad zájmy uživatelů internetu a dále lze rozhodnutí vytknout přenesení odpovědnosti ohledně vyvážení práv subjektu údajů a práv veřejnosti na informace a svobodu projevu na soukromoprávní subjekt.

GDPR nově upravuje „právo na přenositelnost údajů“, které má usnadnit přechod subjektu údajů od jednoho poskytovatele služeb ke druhému a také posílit možnost kontroly subjektu údajů nad svými osobními údaji. Musí se však jednat pouze o data poskytnutá subjektem údajů. Naopak do práva na přenositelnost údajů nebudou spadat údaje dovozené nebo odvozené správcem údajů, které správce vytvořil např. v procesu profilování uživatele. GDPR výslovně stanovuje, že se právo na přenositelnost neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

Poslední kapitola se zabývá problematikou adaptačních zákonů členských států, když GDPR, ačkoliv je převážně přímo použitelné, ukládá či umožňuje členským státům některé problematiky upravit vnitrostátním předpisem. Ačkoliv Česká republika nepřijala do data účinnosti adaptační zákon, nebrání tato situace přímé aplikovatelnosti GDPR na našem území, když např. hlavní parametry souhlasu se zpracováním osobních údajů jsou upraveny přímo GDPR. Nařízení ale dává v některých místech prostor pro vlastní úpravu členskými státy. Jedná se např. o stanovení věkové hranice dítěte pro udělení „on-line“ souhlasu. Autorka v práci zkoumala jednak návrh českého prováděcího zákona a dále slovenský a rakouský zákon na ochranu osobních údajů. Návrh českého adaptačního zákona má upravovat jen aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho ustavení, organizaci atd.) a některé záležitosti, u kterých GDPR počítá s vnitrostátní úpravou. Autorka dále zkoumala věcnou působnost tohoto zákona, který se má vztahovat i na další oblasti zpracování osobních údajů, u kterých by mohly být pochybnosti, zda

spadají nebo nespadají do působnosti práva EU (např. ochrana osobních údajů při správě daní, které právo EU neupravuje), popřípadě na která se GDPR ani směrnice 2016/680 zjevně nevztahuje. Takovým zpracováním bude oblast společné zahraniční a bezpečnostní politiky, na kterou lze pravidla GDPR a adaptačního zákona ve vztahu k českým správčům vztáhnout, neboť EU svou působnost podle čl. 39 SEU nevykonala.

Na rozdíl od českého návrhu je slovenský zákon o ochraně osobních údajů podstatně obsáhlejší, neboť vedle přejímání definic a zásad obsažených v GDPR zavádí i vlastní definice (např. logování) a rovněž blíže upravuje např. proces podávání stížností pro porušení předpisů o zpracování osobních údajů a řízení o těchto stížnostech. Odlišně od českého zákona pak setrvává na věkové hranici 16 let pro udělení souhlasu dítěte v souvislosti se službami informační společnosti a nedefinuje veřejné subjekty. Oproti tomu rakouský DSG je celkově minimalistický a využívá omezený počet možností nabízených GDPR k zakotvení přísnějších nebo odchylných ustanovení. Věkovou hranici pro on-line souhlas dítěte je rakouským zákonem stanoven na 14 let. S ohledem na tuto odlišnost si tak provozovatelé webů musí ohlídat, zda-li jsou splněny požadavky té konkrétní země. Zejména problematické může toto být u webových stránek a aplikací dostupných v angličtině – i když provozovatel může cílit např. pouze na britský trh, internet nezná hranic a k takovému webu nebo aplikaci se mohou snadno připojit i děti z České republiky. Odkud se ale uživatel připojuje může provozovatel webových stránek zjistit z jeho IP adresy a případně se může rozhodnout přístup pro takovou IP adresu blokovat.

Přijetí nové právní úpravy ochrany osobních dat na území EU/ EHP lze dle autorky považovat za odůvodněné a potřebné, včetně změny právní formy tohoto předpisu. Zároveň se ale autorka domnívá, že se nejedná o „revoluční“ zákon, za který GDPR bývá někdy označován, když základním znakem nové

právní úpravy je kontinuita. GDPR v bodě odůvodnění č. 9 přímo stanoví, že „[...] cíle a zásady Směrnice 95/46/ES nadále platí [...]“. GDPR reaguje na moderní trendy technologického vývoje a globalizaci, podrobněji upravuje práva subjektů údajů a upravuje podmínky pro naplnění transparentnosti zpracování osobních dat a zároveň by mělo podnikatelským subjektům umožnit využití příležitostí, které nabízí jednotný digitální trh. Až praxe ale ukáže, zda nová právní úprava naplní všechna tato očekávání.

## Seznam zkratk

EHP	Evropský hospodářský prostor
EU	Evropská unie
ESD	Evropský soudní dvůr
GDPR	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 zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
SDEU	Soudní dvůr Evropské unie
SEU	Smlouva o Evropské unii
SFEU	Smlouva o fungování Evropské unie
Směrnice 95/46/ES	Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
ÚS	Ústavní soud
Úmluva č. 108	Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28.1.1981, publikovaná jako Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb.m.s.

## Seznam použitých zdrojů

### 1. Monografie, učebnice:

BARTÍK, V., JANEČKOVÁ, E.: *Ochrana osobních údajů v aplikační praxi (vybrané otázky)*. Praha: Linde, 2009, 280 s. ISBN: 978-80-7201-740-9.

BERGER, V. *Judikatura evropského soudu pro lidská práva*. 1. české vydání. Praha: IFEC s.r.o., 2003, 769 s. ISBN: 80-86412-23-7.

BYGRAVE, L. *Data Privacy Law An International Perspective*. Oxford: Oxford university press, 2014. 233 s. ISBN: 978-0-19-967555-5.

CAREY, P. *Data Protection A Practical Guide to UK and EU Law*. 4. vydání. Oxford: Oxford university press, 2015. 820 s. ISBN: 978-0-19-968712-1.

GERLOCH, A., ŠTURMA, P. a kol.: *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2011. 536 s. ISBN: 978-80-87284-23-0.

GERLOCH, A., WINTR., J. *Lisabonská smlouva a ústavní pořádek*. Plzeň: Aleš Čeněk, 2009. 384 s. ISBN: 978-80-7380-192-2.

JELÍNEK J. a kol. *Trestní právo procesní*. 4. vydání. Praha: Leges, s.r.o., 2016. 848 s. ISBN: 978-80-7502-160-1.

MALÝ, K., SOUKUP, L. *Československé právo a právní věda v meziválečném období a jejich místo ve střední Evropě*. Praha: Karolinum, 2010. 1184 s. ISBN: 978-80-246-1718-3.

MATES, P. *Ochrana soukromí ve správním právu*. 2. aktualizované a podstatně přepracované vydání. Praha: Linde Praha, a.s., 2006. 314 s. ISBN: 80-7201-589-3.

MORGAN, R., BOARDMAN, R. *Data Protection Strategy*. Sweet&Maxwell, 2nd edition, 2012, 330 s. ISBN: 9780414026742.

MORAVEK, J. *Přehled judikatur vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Praha: Wolters Kluwer, a.s., 2015. 360 s. ISBN: 978-80-7552-018-0.

NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související*. 1. vydání. Praha: Wolters Kluwer, 2014. 504 s. ISBN: 978-80-7478-665-5.

NULÍČEK, M., DONÁT, J., NONNEMANN F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický*

*komentář*. Praha: Wolters Kluwer ČR, 2017. 544 s. ISBN: 978-80-7552-765-3.

KUČEROVÁ A., BARTÍK V., PECA J., NEWIRT K., NEJEDLÝ J., *Zákon o ochraně osobních údajů. Komentář*. 1.vyd., Praha: C.H. Beck, 2003.

KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck, 2012, 536 s. ISBN: 978-80-7179-226-0.

SOLOVE, D. a SCHWARTZ, P. *Information privacy law*. 5. Vydání, New York: Wolters Kluwer, 2015. 1201 s. ISBN: 978-1-4548-4953-7.

SVOBODA, P. *Úvod do evropského práva*. 5. vydání, Praha: C.H.BECK, 2013. 432 s. ISBN: 9788074004889.

PAVLÍČEK, V., HOFMANNOVÁ, H. a kol. *Občanská a lidská práva v současné době*. Praha: Auditorium, 2014. 308 s. ISBN: 978-8087284-51-3.

TOMÁŠEK, M., TÝČ, V. a kol. *Právo Evropské unie*. Praha: Leges, 2013. 496 s. ISBN: 978-80-8757-653-3.

WAGNEROVÁ, E. *Právo na soukromí: kde má být svoboda, tam musí být soukromí*. IN: ŠIMÍČEK, V. *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. s. 54-59. ISBN: 978-80-210-5449-3.

## 2. Odborné články

AKINTUNDE, E. S. *An analysis of the General Data Protection Regulation (EU) 2016/679 GDPR* [online]. Dostupné z [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2966210](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2966210).

ANNERAU, S. *Understanding consent under the GDPR* [online]. Dostupné z: <https://www.taylorwessing.com/globaldatahub/article-understanding-consent-under-the-gdpr.html>.

BAIER, J. a KRAMOLIŠ, O. *Mezinárodněprávní aspekty zpracovávání osobních údajů a nesprávná transpozice směrnice v zákoně o ochraně osobních údajů*. Právní rozhledy roč. 2012, č. 11.

BANISAR, D. and Davies, S., *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments* (August 30, 2012). John Marshall Journal of Computer & Information Law, Vol. XVIII, No. 1, Fall 1999. [online]. Dostupné z: <https://ssrn.com/abstract=2138799>.



BIRNHACK, M. *The EU Data Protection Directive: An Engine of a Global Regime* (September 16, 2008). 24(6) *Computer Law & Security Report*, 508-520 (2008). [online]. Dostupné z: <https://ssrn.com/abstract=1268744>.

BUNN, A. *The curious case of the right to be forgotten*. *Computer Law & Security Review*. 31 (3): pp. 336-350. [online]. Dostupné z: [https://espace.curtin.edu.au/bitstream/handle/20.500.11937/25286/229675\\_229675.pdf?sequence=2&isAllowed=y](https://espace.curtin.edu.au/bitstream/handle/20.500.11937/25286/229675_229675.pdf?sequence=2&isAllowed=y).

BURAK ÖZDAĞISTANLI: *Data protection in Turkey: overview*. [online]. Dostupné z: [https://uk.practicallaw.thomsonreuters.com/Document/I02064fb01cb611e38578f7ccc38dcbec/View/FullText.html?transitionType=CategoryPageItem&contextData=\(sc.Default\)&navId=A702EEBF2A7AF6A067738D04222CB4F7&comp=pluk#co\\_anchor\\_a795431](https://uk.practicallaw.thomsonreuters.com/Document/I02064fb01cb611e38578f7ccc38dcbec/View/FullText.html?transitionType=CategoryPageItem&contextData=(sc.Default)&navId=A702EEBF2A7AF6A067738D04222CB4F7&comp=pluk#co_anchor_a795431).

BURRI, M. and SCHÄR, R. *Thereform of the EU Data protection Framework: Outlining key changes and assessing their fitness for a data-driven economy* [online]. *Journal of Information Policy*, Vol. 6 (2016), s.479-511. Dostupné z: [https://www.researchgate.net/publication/306119725\\_The\\_Reform\\_of\\_the\\_EU\\_Data\\_Protection\\_Framework\\_Outlining\\_Key\\_Changes\\_and\\_Assessing\\_Their\\_Fitness\\_for\\_a\\_Data-Driven\\_Economy](https://www.researchgate.net/publication/306119725_The_Reform_of_the_EU_Data_Protection_Framework_Outlining_Key_Changes_and_Assessing_Their_Fitness_for_a_Data-Driven_Economy).

JASMONTAITE, L. a DE HERT, P.: *The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet*. *International Data Privacy Law* [online]. 2015, 5(1), 20-33. DOI: 10.1093/idpl/ipu029. ISSN 20443994. Dostupné z: <http://idpl.oxfordjournals.org/cgi/doi/10.1093/idpl/ipu029> s.11.

KADLECOVÁ, G.: *Několik poznámek k návrhu nařízení ePrivacy* [online]. Dostupné z <https://www.epravo.cz/top/clanky/nekolik-poznamek-k-navrhu-narizeni-eprivacy-107820.html>.

KARTNER, M. a PROUZA, J.: *Nářízení EU o ochraně osobních údajů – právo na přenositelnost údajů* [online]. Dostupné z <https://www.epravo.cz/top/clanky/narizeni-eu-o-ochrane-osobnich-udaju-pravo-na-prenositelnost-udaju-105500.html>.

GELLMAN, R. a DIXON, P.: *Decision in Europe: Controversial revival of practical obscurity: Implications of the Google Spain Case*. *World Privacy Forum* [online].

Dostupné z: <https://www.worldprivacyforum.org/2014/05/wpf-analysis-implications-of-the-google-spain-case/>.

GERNOT, F.: *First GDPR fine issued by Austrian data protection regulator*. [online]. Dostupné z <https://www.lexology.com/library/detail.aspx?g=7efc00e0-fcaf-4509-b3f8-afa6bf1f2893>.

GONZÁLEZ-FUSTER, G. *The emergence of personal data protection as a fundamental right of the EU*. New York: Springer, 2014. Law, governance and technology series, v.16. ISBN 3319050222.

MAŠTALKA, J. *Nové nařízení EU o ochraně osobních údajů a některé záležitosti spojené s jeho aplikací v ČR*. Právní rozhledy roč. 2016, č. 21.

MILLER, A. *The Assault on Privacy: Computers, Data Banks and Dossiers*. Ann Arbor: University of Michigan Press, 1971. [online]. Dostupné z: <http://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2880&context=caselrev>.

MÍŠEK, J.; HARAŠTA, J. *Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain*. [online] Bulletin-advokacie.cz Dostupné z: <http://www.bulletin-advokacie.cz/analyza-prakticky-ch-dopadu-rozhodnuti-soudniho-dvora-eu-ve-veci-google-spain>.

MORÁVEK, J.: *Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?* Právní rozhledy, roč. 2018, č.13-14.

NONNEMANN, F. *Adresný marketing a ochrana osobních údajů*. Právní rozhledy, roč. 2013, č. 23-24.

NONNEMANN, F. *Odvolání souhlasu se zpracováním osobních údajů*. Právní rozhledy roč. 2011, č. 24.

NONNEMANN, F. *Náležitosti souhlasu se zpracováním osobních údajů*. Právní rozhledy roč. 2011, č. 14.

NONNEMANN, F. *IP adresa jako osobní údaj*. Právní rozhledy roč. 2017, č. 3.

KOMÍNKOVÁ, M. *Panuje kolem nové ochrany osobních údajů zbytečná panika?* [online]. Dostupné z: <https://www.euroskop.cz/9260/sekce/o-cem-se-mluvi/>.

PADOVA, Y.: *What the European Draft Regulation on Personal Data is going to change for companies*. *International Data Privacy Law* [online]. 2014, 4(1), 39-52 DOI: 10.1093/idpl/ipt031. ISSN 20443994. Dostupné z: <http://idpl.oxfordjournals.org/cgi/doi/10.1093/idpl/ipt031>.

PEERS, S. *The CJEU's Google Spain Judgment Failing to Balance Privacy and Freedom of Expression*, EU Law Analysis [online]. Dostupné z: <http://eulawanalysis.blogspot.cz/2014/05/the-cjeus-google-spain-judgment-failing.html>.

POLČAK, R. *Getting European data protection off the ground*. *International Data Privacy Law* [online]. 2014, 4(4), 282-289 DOI: 10.1093/idpl/ipu019. ISSN 20443994. Dostupné z: <http://idpl.oxfordjournals.org/cgi/doi/10.1093/idpl/ipu019>.

PFEIFLE, S. *Will GDPR Move Age of Consent to 16?* [online]. Dostupné z: <https://iapp.org/news/a/will-gdpr-move-age-of-consent-to-16/>.

ROSEN, J. *The Right to Be Forgotten*, Stanford Law Review [online]. Dostupné z: <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>.

Selfies Now Fulfill COPPA Parental Verification Requirement [online]. Dostupné z: <https://iapp.org/news/a/selfies-now-fulfill-coppa-online-verification-requirement>.

SCANLON, L. *What data protection reform will mean for obtaining 'customer consent'* [online] Pinsent Masons LLP [online]. Dostupné z: <http://www.out-law.com/en/articles/2015/february/what-data-protection-reform-will-mean-for-obtaining-customer-consent/>.

SCHÖNBERGER-MAYER, V. *Omission of search results is not a right to be forgotten or the end of Google*. The Guardian [online]. Dostupné z: <https://www.theguardian.com/commentisfree/2014/may/13/omission-of-search-results-no-right-to-be-forgotten>.

SOMMEROVÁ, K. *Vybrané praktické dopady rozhodnutí Google Spain SL., Google Inc. vs. AEPD, Mario Costeja Gonzáes*. [online]. Dostupné z: <https://www.epravo.cz/top/clanky/vybrane-prakticke-dopady-rozhodnuti-google-spain-sl-google-inc-vs-agencia-espaola-de-proteccion-de-datos-aepd-mario-costeja-gonzalez1-95363.html>.

ŠTURMA, P. *Lisabonská smlouva a závaznost Listiny základních práv EU pro Českou republiku vzhledem k tzv. výjimce (opt-out)*. Právní rozhledy roč. 2010, č. 6.

ŠUCHMAN, J. *Souhlas se zpracováním osobních údajů aneb jak přijímat nabízené koláčky*. EU Právní novinky roč. 2011, č. 10.

VEJVODOVÁ, A. *Facebookový profil a e-mail díky GDPR budou až od 15 let se souhlasem rodičů*. [online]. Dostupné z: <https://pravnicaradce.ihned.cz/c1-66108830-facebookovy-profil-a-e-mail-diky-gdpr-budou-az-od-15-let-se-souhlasem-rodicu>.

VLÁČIL, J. *Soudní dvůr EU – prosinec 2016*. Soudní rozhledy roč. 2017, č. 2.

VOBOŘIL, J. *Jaké budou dopady zrušení směrnice o data retention?* [online]. Dostupné z: <https://www.epravo.cz/top/clanky/jake-budou-dopady-zruseni-smernice-o-data-retention-94415.html>.

VOSS, G. W.; CASTETS-RENARDS, C. *Proposal for international taxonomy on the various forms of the „right to be forgotten“: a study on the convergence of norms*. SSRN European Public Law: EU eJournal [online]. Dostupné z: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2800742](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800742).

WEBER, H., R. *The right to be forgotten: More than a Pandora's box?* [online]. Dostupné z: <https://www.jipitec.eu/issues/jipitec-2-2-2011/3084>.

WARREN, S. D., BRANDEIS, L. D. *The Right to Privacy*. IN Harward Law Review 4/1890, č. 5. [online]. Dostupné z [http://faculty.uml.edu/sgallagher/harvard\\_law\\_review.htm](http://faculty.uml.edu/sgallagher/harvard_law_review.htm).

WERRO, F. 'The Right to Inform v The Right to be Forgotten: A Transatlantic Clash', in Aurelia Colombi Ciacchi, Christine Godt, Peter Rott and Leslie Jane Smith (eds), *Liability in the Third Millennium* (Nomos, 2009) s. 290-291. [online]. Dostupné z: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1401357](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357).

WOLK, A.: *Austria's GDPR Implementation Law*. [online]. Dostupné z <https://www.mofo.com/resources/publications/170918-austria-gdpr-implementation-law.html>.

### 3. Seznam použitých právních předpisů

*Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten* (Datenschutzgesetz – DSGVO).

*Evropská Úmluva o ochraně lidských práv a základních svobod*, publikovaná pod č. 209/1992 Sb.

*Listina základních práv Evropské Unie* 2012/C 326/02 ze dne 7.12.2000.

*Listina základních práv a svobod*, která byla usnesením předsednictva České národní rady ze dne 16. prosince 1992 č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, vyhlášena jako součást ústavního pořádku České republiky.

*Nařízení Evropského parlamentu a Rady (EU) č. 2016/679* ze dne 27.4.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

*Smlouva o Evropské Unii a Smlouva o fungování Evropské Unie 2016/C 202/1.*

*Směrnice Evropského parlamentu a Rady (EU) č. 95/46/ES ze dne 24.10.1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.*

*Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.*

*Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu.*

*Úmluva o ochraně lidských práv a základních svobod ve znění pozdějších protokolů, vyhlášená 4. prosince 1950 Radou Evropy v Římě, (číslo zákona ve sbírce: 209/1992 Sb.).*

*Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních údajů č. 108, která byla vyhlášena pod číslem 115/2001 Sb.m.s.*

*Všeobecná deklarace lidských práv přijatá a vyhlášená Valným shromážděním OSN dne 10. prosince 1948.*

*Zákon č. 18/2018 Z. z. o ochraně osobních údajů a o změně a doplnění některých zákonů.*

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

*Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů.*

#### **4. Seznam použité judikatury**

Nález Ústavního soudu ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99, N 32/17 SbNU 229.

Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, 94/2011Sb. Rozhodnutí NSS sp. Zn. 50 As 104/2013.

Rozsudek ESD ze dne 29. 1. 2008, Productores de Música de España (Promusicae) v. Telefónica de España SAU, C-275/06.

Rozsudek ESD ze dne 16. 12. 2008, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy a Satamedia Oy, C-73/07.

Rozsudek SDEU ze dne 9. 11. 2010, ve spojených věcech Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen, C-92/09 a C-93/09.

Rozsudek SDEU ze dne 7. 12. 2010, ve spojených věcech Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG a HOTEL Alpenhof GesmbH proti Oliver Heller, C-585/08 a C-144/09.

Rozsudek SDEU ze dne 24. 11. 2011, Asociación Nacional de Establecimientos Financieros de Crédito C-468/10 a C-469/10.

Rozsudek SDEU ze dne 8. 4. 2014, Digital Rights Ireland Ltd, C-293/12.

Rozsudek SDEU ze dne 13. 5. 2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González, C-131/12.

Rozsudek SDEU ze dne 11. 12. 2014, Ryneš, C-212/13.

Rozhodnutí SDEU ze dne 1. 10. 2015, Weltimmo s.r.o., C-230/14.

Rozsudek SDEU ze dne 6. 10. 2015, Schrems, C-362/14.

Rozsudek SDEU ze dne 19. 10. 2016, Patrick Breyer vs. Bundesrepublik Deutschland, C-582/14.

Rozsudek ESLP ze dne 16. 12. 1992 ve věci Niemietz v. Spolková republika Německo, stížnost č. 13710/88.

Rozsudek ESLP ze dne 16. 2. 2000 ve věci Amann v. Švýcarsko, stížnost č. 27798/95.

## 5. Seznam ostatních zdrojů

ARTICLE 29 WORKING PARTY. *Privacy on the Internet – An integrated EU Approach to On-line Data Protection*. Dostupné z [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf).

ARTICLE 29 WORKING PARTY. *Guidelines on the right to data portability*. Dostupné z: [http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc\\_id%3D43822&rct=j&frm=1&q=&esrc=s&sa=U&ved=0ahUK EwjE14u4qpXUAhWoFZoKHf2YCFyQFggUMAA&usg=AFQjCNGBN Pz-voEZX1SuSTVO-xQ9UHIGIg](http://www.google.de/url?url=http://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D43822&rct=j&frm=1&q=&esrc=s&sa=U&ved=0ahUK EwjE14u4qpXUAhWoFZoKHf2YCFyQFggUMAA&usg=AFQjCNGBN Pz-voEZX1SuSTVO-xQ9UHIGIg).

ARTICLE 29 WORKING PARTY. *Opinion 15/2011 on the definition of consent*. Dostupné z: <https://www.pdpjournals.com/docs/88081.pdf>.

ARTICLE 29 WORKING PARTY. *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC* of 24 October 1995. Dostupné z [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp114\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf).

ARTICLE 29 WORKING PARTY. *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*. Dostupné z: [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=614109](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109).

ARTICLE 29 WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. Dostupné z [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf).

ARTICLE 29 WORKING PARTY. *Opinion 5/2009 on online social networking*. Dostupné z [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf).

ARTICLE 29 WORKING PARTY. *Opinion 8/2010 on applicable law*. Dostupné z [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf).

ARTICLE 29 WORKING PARTY. *Working Document 02/2013 providing guidance on obtaining consent for cookies*. Dostupné z [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf).

ARTICLE 29 WORKING PARTY. *Guidelines on consent under Regulation 2016/679*. Dostupné z [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=623051](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051).

European agency for fundamental rights. *Handbook on European data protection law* – 2018 edition. Dostupné z: <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law>.

Stanovisko Úřadu pro ochranu osobních údajů č. 6/2009. *Ochrana soukromí při zpracování osobních údajů*. Dostupné z <https://www.uouu.cz/stanovisko-c-6-2009-ochrana-soukromi-pri-zpracovani-osobnich-udaju/d-1519>.

Doporučení č. r (85) 20 Výboru ministrů členským státům o ochraně osobních údajů používaných pro účely přímého marketingu. Dostupné z <https://www.uoou.cz/doporuzeni-c-r-85-20-vyboru-ministru-clenskym-statum-o-ochrane-osobnich-udaju-pouzivanych-pro-ucely-primeho-marketingu/ds-1825/archiv=2&p1=1659>.

NUTILOVÁ H., *Ochrana osobních údajů*. Dizertační práce. Právnická fakulta Univerzity Karlovy. 2012. Dostupné z: [https://is.cuni.cz/webapps/zzp/detail/68996/26915763/?q=%7B%22\\_searchform\\_search%22%3A%22nutilov%5Cu00e1%22%2C%22\\_searchform\\_butsearch%22%3A%22Vyhledat%22%2C%22\\_facetform\\_facets\\_faculty%22%3A%5B%2211220%22%5D%2C%22PN\\_zzpSearchListbasic%22%3A1%7D&lang=cs](https://is.cuni.cz/webapps/zzp/detail/68996/26915763/?q=%7B%22_searchform_search%22%3A%22nutilov%5Cu00e1%22%2C%22_searchform_butsearch%22%3A%22Vyhledat%22%2C%22_facetform_facets_faculty%22%3A%5B%2211220%22%5D%2C%22PN_zzpSearchListbasic%22%3A1%7D&lang=cs).

Důvodová zpráva k novému zákonu o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Návrh zákona je adaptovaný na nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680. Dostupné z: <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

Sdělení Komise Evropskému parlamentu a Radě *Posílená ochrana, nové příležitosti – pokyny Komise týkající se přímého uplatňování obecného nařízení o ochraně osobních údajů ke dni 25. května 2018*. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX%3A52018DC0043&qid=1517578296944&from=EN>.



## **Podoba souhlasu se zpracováním osobních údajů ve světle Obecného nařízení o ochraně osobních údajů**

### **Abstrakt**

Tato rigorózní práce se zabývá problematikou právní úpravy ochrany osobních údajů zakotvené jednak ve zrušené Směrnici 95/46/ES a zejména v nové právní úpravě nařízení GDPR. GDPR reaguje na rozvoj nových technologií, které v době přijetí Směrnice 95/46/ES neexistovaly (jedná se např. rozvoj sociálních sítí a cloudových úložišť) a dále na odlišnou úpravu ochrany osobních dat napříč členskými státy, kdy GDPR, jakožto nařízení, má zajistit jednotnou vysokou úroveň jejich ochrany.

Úvodní část práce je věnována terminologickému a historickému úvodu do problematiky ochrany osobních údajů a nedostatkům zrušené směrnice, kdy za problematiku autorka, nad rámec uvedeného, v práci identifikovala zejména vymezení její územní působnosti. Dále se autorka v této části zabývá vybranými soudními rozhodnutími Lindqvist, Digital Rights Ireland, Schrems a Google Spain, v rámci kterých SDEU naznačil potřebu nové právní úpravy.

Dále se práce zabývá novou koncepcí právní úpravy GDPR. Autorka se na tomto místě zabývá otázkou důvodnosti a nezbytnosti přijetí nové právní úpravy a zodpovězení otázky, za jakých podmínek lze IP adresu a soubory cookies považovat za osobní údaje podléhající právní úpravě GDPR. Ústředním tématem práce je institut souhlasu se zpracováním osobních údajů včetně jeho aspektů dle GDPR, kdy GDPR základní parametry souhlasu upravených Směrnicí 95/46/ES nemění, ale požadavky rozšiřuje. Autorka se v této části práce věnuje i institutu udělení on-line souhlasu dětmi mladšími 16 let. V rámci této části autorka provedla analýzu některých práv subjektů údajů zahrnující mediálně známé „práva na výmaz“ včetně kritického zhodnocení soudního rozhodnutí Google Spain.

Závěr rigorózní práce je pak věnován problematice adaptačních zákonů členských států, když GDPR, ačkoliv je převážně přímo použitelné, ukládá či umožňuje členským státům některé problematiky upravit vnitrostátním předpisem. Autorka provedla nejprve analýzu návrhu českého zákona o zpracování osobních údajů, který v době dokončení této práce nebyl doposud Parlamentem České republiky přijat a dále v rámci této části autorka provedla analýzu odlišných přístupů adaptace GDPR v české, slovenské a rakouské republice. Každá tato právní úprava např. stanovuje odlišně věkovou hranici pro online souhlasy dětí, v praxi tak provozovatelé webů musí ohlídat, zda-li jsou splněny požadavky té konkrétní země.

**Klíčová slova:**

Ochrana osobních údajů

Souhlas se zpracováním osobních údajů

GDPR

## **The consent to the processing of personal data in the light of the General data protection regulation**

### **Abstract**

The work presented considers the data protection law formerly regulated via Directive 95/46/EC and presently regulated by GDPR (General Data Protection Regulation). GDPR was introduced as a response to the development of new technologies, such as growth of social networks and cloud storages, which did not exist when Directive 95/46/EC was enacted. Furthermore, GDPR is a reaction to the variety of data protection acts across the EU member states. Its aim is to consistently guarantee a high level of personal data protection across entire EU.

The introductory part of the thesis is devoted to the terminology, history of personal data protection and shortcomings of the repealed directive. In particular, the territorial scope is identified as problematic. In addition, author in this part made an analyse of selected rulings of CJEU, which indicated the need for a new legal regulation, are discussed.

The second part of the thesis considers the design of GDPR. Here, the question of necessity for such regulation is addressed. Furthermore, the author discusses the circumstances under which the IP address and cookies can be considered personal data which are protected by GDPR. The central theme of the thesis is the consent to the processing of personal data. GDPR does not modify the fundamental parameters of the consent required by Directive 95/46/EC. Instead, it extends these requirements. In particular, the online consent given by individuals under the age of 16 is considered. In addition, selected rights of data subjects under GDPR, e.g. medially known „right to erasure“, are discussed including the critical analysis of the Google Spain ruling.

The final part of the thesis considers the GDPR adaptation by member states. While GDPR is directly applicable at large, it imposes or allows the Member States to adapt some issues via national legislation. The author analysed the proposed data protection law which will be voted on by the Czech Parliament only after the submission of the thesis. In addition, the approaches to GDPR adaptation in the Czech Republic, Slovakia and Austria republic are compared and contrasted. For example each of these states sets a different age for online children's consent. In practice, webmasters must ensure that the requirements of that particular legislation are met.

**Key words:**

Data protection

consent to the processing of personal data

GDPR