ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

DIPLOMOVÁ PRÁCE

Ochrana osobních údajů v České republice a EU

Vojtěch Hulinský

Plzeň 2019

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: **2018/2019**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vojtěch HULINSKÝ**
Osobní číslo:	**R14M0137P**
Studijní program:	**M6805 Právo a právní věda**
Studijní obor:	**Právo**
Název tématu:	**Ochrana osobních údajů v České republice a EU**
Zadávající katedra:	**Katedra ústavního a evropského práva**

Zásady pro vypracování:

Téma ochrany osobních údajů:
- základní terminologie, základní přehled právní úpravy
- reflexe právní historie
- reflexe současného digitálního informačního rozmachu

Osobní údaje:
- ochrana osobních údajů z pohledu lidských práv jako nejdůležitějších hodnot právního státu
- osobní údaje ve světle obecně závazných právních norem
- identifikace základních subjektů na poli ochrany osobních údajů, jejich funkce, dílčí role
- úprava v rámci EU, zejména analýza Obecného nařízení Evropského parlamentu a Rady (EU) 2016/679, General Data Protection Regulation (GDPR) - vlastní názory Na situaci v období legisvakance (duben 2016 - květen 2018)

Rozsah grafických prací:

Rozsah kvalifikační práce: **103**

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury: **viz příloha**

Vedoucí diplomové práce: **Doc. JUDr. Monika Forejtová, Ph.D.**
Katedra ústavního a evropského práva

Datum zadání diplomové práce: **28. března 2018**

Termín odevzdání diplomové práce: **31. března 2019**

Doc. JUDr. Jan Pauly, CSc.
děkan

L.S.

Doc. JUDr. Monika Forejtová, Ph.D.
vedoucí katedry

V Plzni dne 28. června 2018

Příloha zadání diplomové práce

Seznam odborné literatury:

- NULÍČEK, Michal; DONÁT, Josef; NONNEMANN, František; LICHNOVSKÝ, Bohuslav;
- TOMÍŠEK, Jan. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Praha: Wolters Kluwer ČR, 2017, 544 s. ISBN 978-80-7552-765-3.
- NAVRÁTIL - GDPR pro praxi. Praha: Aleš Čeněk ČR, 2018, 340 s, ISBN 978-80-7380-689-7.
- KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů. Komentář. 1. vyd. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0.
- MORÁVEK - Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům. Praha: Wolters Kluwer ČR, 2016, 360 s, ISBN 978-80-7552-018-0
- Vybrané články o tématu GDPR a ochraně osobních údajů Bulletin advokacie
- Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
- Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
- Výkladová stanoviska, vodítka a články Pracovní skupiny 29 Working Party 29
- Výkladová stanoviska, vodítka a články ÚOOÚ
- Vybrané odborné články na téma ochrany osobních údajů a GDPR

Prohlášení autora

„Prohlašuji, že jsem tuto diplomovou práci zpracoval zcela samostatně, a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal způsobem ve vědecké práci obvyklým.”

Plzeň, březen 2019 Vojtěch Hulinský

Poděkování

Rád bych tímto poděkoval doc. JUDr. Monice Forejtové, Ph.D., za vedení mé diplomové práce, za odbornou pomoc a cenné rady jež mi k jejímu zpracování poskytla. Dále mé rodině a přítelkyni za neopomenutelnou podporu při celém vysokoškolském studiu.

Obsah

1 Úvod

Ochrana osobních údajů je jedním z nejdynamičtěji se rozvíjejících právních institutů posledních let a zároveň jedním z nejmladších. Zajištění jejich dostatečné ochrany je dle autora jedním ze zásadních výzev, se kterou se musí společnost v prvních desetiletích 21. století vypořádat, a to zvláště z důvodu globálního rozsahu této problematiky. Historie dokazuje, že význam ochrany osobních údajů byl širokou veřejností velice podceňován, někdy až znehodnocován, přestože se jedná o jednu z nejdůležitějších hodnot, kterou lze k jednotlivci vázat. Právo na soukromí, ze kterého ochrana osobních údajů jako právní institut vychází je jedním ze základních lidských práv a jako takové je zakotveno v právních předpisech nejvyšší právní síly většiny demokratických právních států. V České republice je právo na soukromí garantováno v rámci ústavního pořádku v Listině základních práv a svobod. Samotná Evropská unie přikládá ochraně osobních údajů bezesporu veliký význam, a to nejen proto, že právo na ochranu osobních údajů je v Listině základních práv Evropské unie upraveno jako jedno ze základních práv, ale také vytvořením úpravy ochrany osobních údajů v podobě nařízení, tedy nejzávaznějším právním aktem Evropské unie.

Není pochyb o tom, že význam ochrany osobních údajů v 21. století masivně vzrostl vlivem globálního rozšíření užívání nových technologií. Užívání počítačů a internetu na denní bázi se stalo naprostou samozřejmostí pro většinu společnosti, což jak naznačuje momentální trend, způsobuje stále větší otevřenost a transparentnost chování uživatelů v informačním prostředí internetu. Většina jednotlivců si dle názoru autora stále neuvědomuje jak význam osobních údajů, tak nebezpečí plynoucí z jejich neobezřetného sdílení a předávání. Jejich zneužití může totiž vést k závažnému zásahu do soukromí jednotlivce jak ze strany poskytovatelů služeb informačních společností, tak i jinými uživateli či státu.

Stejně tak nelze přehlížet ekonomické využití osobních údajů. V České republice začalo docházet k častějšímu zpracovávání osobních údajů s přechodem na systém tržního hospodářství, jelikož velké množství subjektů začalo osobní údaje zpracovávat v rámci podnikatelské činnosti. Celosvětově je pak zpracování

osobních údajů nezbytným předpokladem pro realizaci obchodních transakcí, cíleného marketingu za účelem oslovování většího množství potencionálních zákazníků, reklamy jako takové apod. Vlivem těchto skutečností se osobní údaje se staly postupem času lákavým obchodním artiklem, dřívější běžnou praxí byl obchod s databázemi osobních údajů tisíců subjektů, není tedy divu, že bývají často označovány za *ropu internetu.*

Současně vlivem nejdynamičtěji rostoucího odvětví informačních technologií a jeho významu z hlediska ochrany osobních údajů, je nutné na tento vývoj neustále reagovat. Pro zákonodárce z toho vyplývá poměrně nelehký úkol, a to sledovat jak aktuální stav, tak potenciál pro stav budoucí a zajistit osobním údajům odpovídající ochranu.

Ochranu osobních údajů je dle autora třeba sledovat v kontextu jí příbuzných institutů a na jejich vývoj by se rád zaměřil nejen prostřednictvím formálních právních pramenů, ale taktéž právních pramenů v pojetí materiálním, tedy okolností jejich vzniku, společenských a hospodářských poměrů a historických faktorů. Jedním z cílů této diplomové práce tedy bude analyzovat vývoj ochrany osobních údajů a pro ni stěžejních institutů pomocí nejvýznamnějších milníků a událostí, za účelem poznání materiálního pojetí těchto pramenů.

Vzhledem k tomu, že úprava ochrany osobních údajů na území Evropské unie prošla v posledních letech nebývalou změnou, považuje autor za účelné popsat její aktuální podobu právě ve světle nové unijní právní úpravy, a to *Obecného nařízení o ochraně osobních údajů* neboli *General Data Protection Regulation,* známé také jako *GDPR.*

Autor by také rád ve stručnosti zhodnotil situaci v období legisvakance před účinností Obecného nařízení o ochraně osobních údajů, jelikož atmosféru, kterou přijetí tohoto právního předpisu v České republice vytvořilo lze přirovnat ke společenské hysterii.

2 Vývoj ochrany osobních údajů ve světle stěžejních institutů

První část této diplomové práce bude věnována vývoji ochrany osobních údajů. Jelikož se jedná z historického pohledu o poměrně mladý institut, k jehož dynamickému rozvoji dochází vlivem mnoha faktorů až v několika posledních letech a jehož samotná existence vychází z dalších, historicky starších institutů, bude tento vývoj popisován v jejich kontextu. Autor se pokusí provést jakousi analýzu vývoje dnes již ústavně chráněného práva na soukromí, stejně tak prvopočátků práva na informační sebeurčení a ochrany osobních údajů jako takové. Dle názoru autora je popis vývoje těchto institutů dobrým vodítkem pro poznání kontextu ochrany osobních údajů, jelikož jako takové vznikali v souvislosti s okolnostmi a mimoprávními skutečnostmi daného období jejich vzniku. Cílem této části bude tedy nastínit historický vývoj stěžejních institutů pro ochranu osobních údajů, tedy co jí předcházelo a z čeho jako taková vlastně vznikla, a to pomocí nejdůležitějších milníků a událostí, které postupně vedli, či přispěli k poskytování ochrany osobních údajů a její jednotné úpravě na úrovni Evropské unie.

2.1 Právo na soukromí

Právo na soukromí a jeho ochranu patří mezi základní lidská práva přirozeně právní povahy, náleží tedy každému člověku již od jeho narození. V některých aspektech náleží i osobám právnickým, a to již od jejího vzniku, zejména v oblasti dobrého jména právnické osoby.

2.1.1 The Right to Privacy

Nejvýznamnější institut, ze kterého osobní údaje a jejich ochrana jako taková pramení je právo na soukromí a jeho ochranu, které se ve světě začalo prosazovat a vyvíjet ve Spojených státech amerických a které se tak staly jakousi kolébkou tohoto práva. Pro téma ochrany soukromí je stěžejním základem velmi rozšířený článek s názvem The Right to Privacy[1] - *"Právo na soukromí"*, který byl

[1] WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. *Harvard Law Review,* 1890, roč. IV, č. 5, s. 193 – 220.

publikován v roce 1890 v časopise Harvard Law Review, a to autory Samuelem D. Warrenem a Louisem D. Brandeisem, kteří v něm formulovali svoji tezi *"right to be left alone".* Tedy právo být ponechán o samotě či právo být ponechán sebou samým a tím v té době vlastně vystihli a popsali termín soukromí. Zajímavostí je, že byť je článek starý téměř 130 let, autoři se ochranou soukromí zabývali tak, jak ji víceméně známe v dnešní době a článek je tedy stále aktuální. Je to také z důvodu, že autoři ve svém článku reagovali na tehdejší technologický pokrok a prosazování médií, což se sice dělo v nesrovnatelně užším měřítku a pomocí jiných prostředků než nyní, nicméně princip zůstal zachován. Aktuálnost tohoto článku vystihuje následující úryvek: "*Nejnovější vynálezy a obchodní metody, upozorňují na další kroky, které je potřeba přijmout k ochraně osobnosti a k zabezpečení jednotlivce tím, co soudce Cooley nazývá právem být o samotě. Novinářské koncerny a fotografové najednou napadly posvátné prostory soukromého a domácího života a užíváním jejich technických zařízení hrozí předpovědí, že to, co bude šeptáno doma ve skříni, bude vyhlášeno z vrcholu domu. Již celé roky panuje pocit, že právo musí poskytnout určitou náhradu na neoprávněné rozšiřování podobizen osob. Určité zlo plynoucí z narušování soukromí jednotlivce novinami a fotografy již bylo pocítěno a následně se o něm začalo i diskutovat."*[2]

2.1.2 Všeobecná deklarace lidských práv

O necelých 60 let déle, byla Organizací spojených národů v roce 1948 přijata Všeobecná deklarace lidských práv, která obsahuje nejznámější katalog lidských práv a tím se stala základem pro další rozvoj v oblasti lidských a sociálních práv. Tento dokument obsahuje celkově 30 článků, včetně článku číslo 12 věnovanému právu na soukromí, který prohlašuje, 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 takovým zásahům nebo útokům."*[3]

[2] WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. *Harvard Law Review,* 1890, roč. IV, č. 5, s. 193 – 220. STRANA 195 (Volný překlad autora)
[3] Všeobecná deklarace lidských práv, článek 12

2.1.3 Úmluva o ochraně lidských práv a základních svobod

O dva roky později je nově vzniklou Radou Evropy přijata nejdůležitější lidskoprávní úmluva, kterou je Úmluva o ochraně lidských práv a základních svobod, jež se stala základem pro regionální mezinárodněprávní ochranu lidských práv na území celé Evropy. Byla podepsána v Římě a vstoupila v platnost 4. listopadu 1950, účinnosti nabyla 3. září 1953.
Úmluva obsahuje právo na soukromí ve svém Článku 8 v odstavci 1 - Právo na respektování rodinného a soukromého života, který zní: *"Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence."*[4]

Tato Úmluva je dle článku 10 Ústavy České republiky vyhlášena s ratifikací Parlamentu jako mezinárodní smlouva, je součástí našeho právního řádu a jako taková má aplikační přednost před vnitrostátní úpravou.

2.1.4 Právo na soukromí v České republice

V Českém právním řádu se samotná ochrana soukromí jednotlivce v podobě, v jaké ji známe nyní objevila až v devadesátých letech dvacátého století. V první Československé ústavě z roku 1920, byla upravena pouze nedotknutelnost soukromého vlastnictví a Ústavním zákonem přijatým téhož roku, byla upravena svoboda osobní, domovní a listovní tajemství a ve kterém bylo právo na soukromí určitým způsobem upraveno v patnácti paragrafech.
Ani po roce 1948, přijetím nové Ústavy nedošlo k výrazným změnám. Naopak vlivem socialistických idejí, pozdější právní nauka soukromí jednotlivce vůbec neuznávala a spíše ho popírala, jelikož dle tehdejších tezí nebyla potřeba poskytovat tomuto nehmotnému statku ochranu.

V roce 1989 se na našem území odehráli významné politické změny pozitivního charakteru, které měli za následek i změny v oblasti práva. Tyto změny se silně projevily i v souvislosti s ochranou soukromí. V lednu roku 1991 byla přijata Listina základních práv a svobod pro Českou a Slovenskou Federativní republiku a po rozdělení na samostatné státy byla vyhlášena i pro samostatnou Českou republiku.

[4] Evropská úmluva o ochraně lidských práv, článek 8 odst. 1

LZPS ve svém článku 7 odst. 1 stanovuje: *"Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem."* a zároveň v článku 10 odst. 2 *"Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života."* odst. 3 *"Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě"*.[5] Tímto se právo na soukromí a jeho ochranu dostalo do ústavněprávní roviny.

2.2 Právo na svobodný přístup k informacím

2.2.1 Freedom of Information Act

Vývoj tohoto institutu započal opět ve Spojených státech amerických, a to v roce 1967. Toho roku, 4. července se stal účinným zákon přijatý americkým Kongresem, tzv. Freedom of Information Act (FOIA) - Zákon o svobodném přístupu k informacím, který lze s jistotou označit za první právní předpis upravující toto právo, a který se zároveň stal stavebním kamenem a signálem pro přijetí obdobné úpravy dalšími vyspělými státy.

Institut práva na svobodný přístup k informacím je do jisté míry také stěžejní pro následný vývoj ochrany osobních údajů, jelikož FOIA ve svém znění vymezil několikero druhů informací, na které ho nelze aplikovat. Tedy informace, které nelze zveřejnit na základě podané žádosti. Jednalo se například o různé druhy utajovaných skutečností, obchodní tajemství, údaje o vyšetřování, geologické a geofyzikální údaje a pro nás nejdůležitější, osobní a zdravotní údaje.[6] Tím vlastně osobním údajům jednotlivce poskytl základní formu ochrany.

Po přijetí tohoto zákona ve Spojených státech amerických, následovala zákonná úprava tohoto práva například ve Francii v roce 1978, v Austrálii, Novém Zélandě a v Kanadě v roce 1982 a postupně ve většině vyspělých zemích světa.

[5] Usnesení předsednictva České národní rady č. 2/1993 Sb. o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.
[6] The Freedom of Information Act, section (b)

2.2.2 Právo na svobodný přístup k informacím v České republice

Jak bylo uvedeno výše, základem pro úpravu práva na svobodný přístup k informacím se stala americká úprava v podobě zákona FOIA a z jako takového fakticky další následující úpravy vycházeli.

Co se týče tuzemské úpravy, byla stejně jako u práva na soukromí provedena až koncem dvacátého století. Do roku 1989 byla totiž myšlenka svobodného šíření informací spíše nežádoucí a v rozporu s politikou bývalého režimu.
Tento institut se dostal přijetím LZPS do ústavní roviny, jelikož samotná listina ve svém článku 17 zaručuje spolu se svobodou projevu i právo na informace: *"Svoboda projevu a právo na informace jsou zaručeny."*[7]

Nicméně bylo třeba vypracovat prováděcí předpis v podobě zákona, jelikož bylo nutné jasně strukturovat a vymezit oblast informací, osoby povinné tyto informace poskytovat a specifikovat informace chráněné, které nelze zveřejnit. Také jasně stanovit podmínky, dle kterých mají žadatelé a povinné osoby postupovat. Jelikož se tímto právem otvírají státní instituce a orgány hospodařící s veřejnými prostředky občanovi, bylo nemožné ponechat postavení státu v souvislosti s poskytováním informací nejasné. 1. ledna 2000 tedy nabyl účinnosti zákon č. 106/1999 Sb., o svobodném přístupu k informacím, který byl od svého přijetí již pětkrát novelizován a jeho současná podoba svými principy prakticky odpovídá tehdejší americké úpravě, ze které určitým způsobem také vychází.

2.3 Právo na informační sebeurčení

2.3.1 Volkszählungsurteil aneb rozhodnutí o sčítání lidu

V roce 1983, konktrétně 15. prosince toho roku, dospěl Německý Spolkový Ústavní soud k zásadnímu rozhodnutí, které je považováno na velice důležitý

[7] Usnesení předsednictva České národní rady č. 2/1993 Sb. o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, článek 17

milník na poli ochrany osobních údajů.[8] Rozhodnutí *"Volkszählungsurteil"*[9], neboli *"Rozhodnutí o sčítání lidu",* se týkal věci posouzení souladu zákonné úpravy procesu sběru a uchování dat za účelem sčítání lidu s *"Grundgesetz",* tedy spolkovou Ústavou. V tomto rozhodnutí bylo také poprvé definováno *"právo na informační sebeurčení",* které je bezpochyby také jedním ze stěžejních institutů pro následný vývoj ochrany osobních údajů.

V tomto rozhodnutí bylo mimo jiné uvedeno: *"V moderní společnosti, která je charakterizována také obrovským nárůstem informací a dat, musí být ochrana jednotlivce před neomezeným sběrem, uchováváním, zveřejňováním a užitím dat o jeho osobě a soukromí poskytována v rámci obecnějšího, ústavně garantovaného práva jednotlivce, práva na soukromí. Pokud jednotlivec nebude mít garantovanou možnost určitým způsobem hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež jsou předmětem zveřejňování, uchovávání a nebo užití k jiným než původním účelům, nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potencionálního komunikačního partnera a případně tomu přizpůsobit i své jednání, poté zcela jistě dochází k omezení, dokonce potlačování jeho práv a svobod, a nelze tak již nadále hovořit o svobodné a demokratické společnosti. Právo na informační sebeurčení je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, ale také pro ustavení svobodného a demokratického komunikačního řádu."*[10] Z textu rozhodnutí je patrná vzájemná souvislost nadřazeného institutu práva na soukromí a z něj vycházející právo na informační sebeurčení, které zároveň souvisí s osobními údaji a jejich ochranou.

2.3.2 Právo na informační sebeurčení v České republice

V České republice bylo právo na informační sebeurčení definováno poměrně nedávno. Tento institut vymezil Ústavní soud ve svém nálezu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, právě jako součást institutu práva na soukromí,

[8] A brief history of data protection: How did it all start? | Cloud Privacy Check (CPC). *Homepage | Cloud Privacy Check (CPC)* [online]. Dostupné z: https://cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/
[9] Rozsudek Spolkového ústavního soudu SRN ze dne 15. prosince 1983, sp. zn. BVerfGE 65, 1.
[10] Volkszählungsurteil in englischer Sprache: Census Act [online]. Dostupné z: https://freiheitsfoo.de/census-act/

na jehož základě *„právo na respekt 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 jakém 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.“*[11]
Právě článek 10. odst. 3 LZPS, upravuje ochranu práva na informační sebeurčení tím, že *“Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.”*[12]

Právo na informační sebeurčení je tedy v České republice upraveno na úrovni ústavního pořádku a znamená právo každého jednotlivce rozhodnout, zda a které informace poskytne ostatním subjektům. Také znamená právo na ochranu před sledováním subjektů disponující veřejnou mocí, pokud takové sledování není v souladu s testem proporcionality.[13]

2.4 Právo na ochranu osobních údajů

Pokud se zaměříme na ochranu osobních údajů jako takovou, první předpisy či mechanismy této ochrany se začali formovat v osmdesátých letech dvacátého století. Zde nelze hovořit o tom, že by se s ochranou osobních údajů nějakým způsobem zahálelo, nebyla do té doby zkrátka potřeba a její prvopočátky byli reakcí na stále se rozvíjející užívání nových technologií v širším měřítku, než bylo do té doby zvykem a stále častější výskyt využívání a zneužívání osobních údajů samotných. S historickým odstupem nelze neocenit, že jednotlivé státy včas odhadly charakter téměř neomezeného dosahu osobních údajů a informací obecně, a že ochrana proti jejich zneužití nemůže být postavena na čistě teritoriálním principu v podobě národních úprav. Lze tedy považovat za rozumné, že první úpravy ochrany osobních údajů vznikaly v podobě mezinárodních konvencí, které svým způsobem vytvořili půdu pro jednotné mezinárodní prostředí.

[11] Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, bod 29.
[12] Usnesení předsednictva České národní rady č. 2/1993 Sb. o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, článek 10 odst. 3
[13] *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer Česká republika, 2012. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7357-750-6. Str. 284

2.4.1 OECD

V roce 1980 byli mezivládní organizací OECD, *Organisation for Economic Co-operation and Development* neboli Organizací pro hospodářskou spolupráci a rozvoj, vydány *"pokyny o ochraně soukromí přeshraničních toků osobních údajů"*[14]. Jednalo se o obecné pokyny týkající se nakládání s osobními informacemi ve veřejném i soukromém sektoru, které představovali jakýsi základ pro následně vytváření mechanismů ochrany osobních údajů. Tyto pokyny reagovali na stále rostoucí tendenci využívání počítačů a jiných technických zařízení pro zpracovávání obchodních transakcí. Strukturálně byli rozčleněny do pěti základních částí a dále rozděleny do dvaadvaceti článků. Byť tyto pokyny měly pouze doporučující charakter, svými zcela novými principy a terminologií stanovily základ pro budoucí právní úpravy, které je dostaly na právně závaznou úroveň.

2.4.2 Úmluva 108

Přibližně o rok později, 28. ledna 1981, byla Radou Evropy přijata tzv. Úmluva 108, celým názvem *"Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat".* Jednalo se o první evropský právní nástroj o právní síle mezinárodního právního aktu pro ochranu osobních údajů, který následně výrazně ovlivnil další směřování unijního právního rámce i vývoj v dalších státech. Úmluva je právní akt zavazující pouze signatářské státy jako takové, nikoli subjekty soukromého práva, a těm ukládá, aby podnikly veškerá nutná opatření k ochraně soukromí prostřednictvím vymezení pravidel při automatizovaném zpracování osobních údajů. Zároveň signatářským státům ukládá povinnost umožnění volného pohybu a předávání osobních údajů mezi jednotlivými státy. Poprvé v historii je právo na soukromí a z něj v tomto kontextu vyplývající ochrana osobních údajů na úrovni právního imperativu, je totiž závazná a vynutitelná.[15] Úmluva zavazuje ke dnešnímu dni celkem 51 států.[16]

[14] *OECD.org – OECD Guidelines* [online]. Dostupné z: http://www.oecd.org/internet/ieconomy/37626097.pdf

[15] A brief history of data protection: How did it all start? | Cloud Privacy Check (CPC). *Homepage | Cloud Privacy Check (CPC)* [online]. Dostupné z: https://cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

[16] Modernizace Úmluvy 108, základního nástroje Rady | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html

Jménem České republiky byla Úmluva 108 podepsána dne 8. září 2000 a vstoupila v platnost dne 1. listopadu 2001. Jelikož byla Úmluva připravována v sedmdesátých letech dvacátého století, její obsah odpovídá kontextu tehdejší politické a sociální situace, práva a prostředků na zpracování osobních údajů. Je tedy logické, že situaci okolo osobních údajů, prostředků k jejich zpracování, a hlavně dnešní rozsah zpracování nemohla svou šíří spolehlivě pokrýt. Proto byla vypracována její modernizace, která započala již téměř před deseti lety a první návrh byl předložen v roce 2012. Konečný text modernizované Úmluvy byl zveřejněn 18. května 2018 a jeho smyslem bylo Úmluvu přiblížit novým unijním předpisům. Jedná se samozřejmě o Obecné nařízení o ochraně osobních údajů - *"General Data Protection Regulation"* neboli GDPR, kterému je potřeba věnovat v kontextu ochrany osobních údajů zvýšenou pozornost a samotné nařízení bude předmětem samostatné kapitoly této diplomové práce.

2.4.3 PC Brown, případ z roku 1993

V roce 1993 se odehrál jeden z prvních evidovaných případů, ve kterém pravděpodobně došlo k určité formě zneužití osobních údajů.

Pan Brown byl britský policejní důstojník, který ve snaze pomoci svému příteli vedoucímu agenturu na vymáhání pohledávek (Capital Investigations Ltd), požadoval po svém kolegovi přístup k tzv. Police National Computer, což je počítačový systém značně využívaný ve Spojeném království organizacemi, které vymáhají právo. Chtěl tím získat některé osobní údaje a informace. Neexistovali ale žádné důkazy o tom, že by osobní údaje byly předány nebo zpřístupněny agentuře Capital Investigations Ltd, nebo použity samotným policistou, kromě vyhledání a následného prohlížení. Důstojník byl obviněn dle *"UK Data Protection Act 1984",*[17] z užívání osobních údajů pro jiný účel, než který je popsán v Registru Osobních údajů, nicméně rozhodnutí bylo zrušeno v rámci odvolání. Sněmovna Lordů usoudila, že slovo *"užívání"* má v tomto kontextu svůj specifický význam a že v tomto případě důstojník Brown osobní údaje neužíval, pouze je vyhledal a zobrazil. Kdyby se byl případ odehrál o několik let déle, byl by posuzován dle

[17] *Legislation.gov.uk* [online]. Copyright © [cit. 25.03.2019]. Dostupné z: http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf

následných unijních právních předpisů, ve kterých obsažený výraz *"zpracování"* umožňoval mnohem širší výklad pro své využití v kontextu s osobními údaji a výsledek odvolání by byl nejspíše velmi odlišný.[18]

2.4.4 Směrnice 95/46/ES

Klíčový milník ochrany osobních údajů představoval rok 1995, kdy byla schválena *Směrnice Evropského parlamentu a Rady 95/46/ES, ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.* Tímto se úprava ochrany osobních údajů dostává do úrovně komunitárního práva. Tato směrnice logicky reagovala na vytváření užších vztahů mezi unijními státy a utvoření vnitřního trhu s volným pohybem zboží, z čehož vyplývá i volný pohyb osobních údajů. Zároveň reflektovala i technologický posun v oboru telekomunikačních sítí, které předávání osobních údajů zjednodušovali. Tím, že se ochrana osobních údajů dostala na úroveň zavazující celou Evropskou unii, byly odstraněny překážky v toku osobních údajů, které byly vytvořeny různorodou právní úpravou v jednotlivých členských státech. Respektive dosavadní roztříštěnost této úpravy byla sjednocena, byť měl tento předpis formu směrnice a nikoli nařízení. Ochrana osobních údajů vycházela v právních úpravách jednotlivých členských států zejména ze základních lidských práv, tento krok vedoucí ke sjednocení měl vést ke zvýšení jejich ochrany, jelikož sama směrnice vycházela z článku 8 Listiny základních práv EU.

Do právního řádu České republiky byla tato směrnice implementována prostřednictvím zákona č.101/2000 Sb., o ochraně osobních údajů a změně některých zákonů. Tento zákon působil jako lex generalis pro ochranu osobních údajů v České republice, jelikož zvláštní pravidla pro zpracování osobních údajů lze najít v celé řadě zvláštních právních předpisů.[19] Zároveň implementace této směrnice bylo jednou z podmínek pro kandidátské státy před vstupem do EU.

[18] Destination GDPR - how did we arrive here? . *Object moved* [online]. Copyright © [cit. 25.03.2019]. Dostupné z: https://sytorus.com/ie/Blog/Article/176?title=destination-gdpr-how-did-we-arrive-here

[19] MATES, Pavel a Karel NEUWIRT. *Právní úprava ochrany osobních údajů v ČR: znění zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů: vybrané předpisy EUpoznámkové vydání se zapracovanou důvodovou zprávou*. Praha: IFEC, 2000. AZ-IUS. ISBN 80-86412-02-4. str. 113-116

Nutno podotknout, že první úpravou ochrany osobních údajů v České republice byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl výše uvedeným zákonem nahrazen.

2.4.5 Směrnice 97/66/ES a 2002/58/ES

Směrnici 95/46/ES po dvou letech účinnost následovala speciální úprava a to *Směrnice 97/66/ES Evropského parlamentu a rady z 15. prosince 1997 o zpracování osobních údajů a ochrany soukromí v sektoru telekomunikací.* Nicméně vlivem stále se zrychlujícího vývoje komerčních a technologických inovací na přelomu milénia a v prvních několika letech 21. století, byla nahrazena po pěti letech směrnicí novou. Jedním z nejrychleji se rozvíjejících odvětví v komerční činnosti, bylo tehdy využívání elektronických médií k propagaci a prodeji výrobků široké veřejnosti. E-mailové adresy a čísla mobilních telefonů jednotlivců se staly hlavní měnou při vedení marketingových a prodejních kampaní, široká veřejnost byla neustále vystavena tlaku v podobě nevyžádané pošty a nevítané reklamy. Právě toto byli důvody, proč evropští zákonodárci považovali za nutné v roce 2002 opět regulovat úpravu ochrany soukromí a důvěrnosti osobních údajů svých občanů. Tentokrát se zaměřili na využívání osobních údajů pro účely marketingu využívaného prostřednictvím elektronických médií.[20] Byla tedy přijata *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 o soukromí a elektronických komunikacích).*

2.4.6 Rozhodnutí komise 2000/520/ES, Safe harbour

Jednotný právní prostor v oblasti ochrany osobních údajů byl v té době na území EU určitým způsobem vytvořen, nicméně vzhledem ke globální povaze předávání osobních údajů, bylo třeba upravit i situace předávání osobních údajů do třetích zemí. Předávání osobních údajů mimo EU bylo možné prostřednictvím schválené žádosti dozorového úřadu, nicméně žádoucí bylo nastavit předávání na podobném principu jako uvnitř EU, aby předávání do třetích států mohlo probíhat

[20] Destination GDPR - how did we arrive here? . *Object moved* [online]. Copyright © [cit. 28.03.2019]. Dostupné z: https://sytorus.com/ie/Blog/Article/176?title=destination-gdpr-how-did-we-arrive-here

bez zbytečné administrativní zátěže. Největším problémem byl paradoxně přístup Spojených států amerických, které obecně zastávají spíše formu samoregulace než centralizovaná pravidla a přístup EU byl jimi vytýkán z hlediska přehnané institucionalizace a byrokratizace problematiky předávání osobních údajů.[21] V roce 2000 bylo dosaženo jistého kompromisu, prostřednictvím *Rozhodnutí Komise z 26. července 2000, č. 2000/520/ES o adekvátnosti ochrany poskytované dle principů bezpečného přístavu,* které mělo zajistit bezpečné předávání osobních údajů do států, kde jim je poskytnuta odpovídající úroveň ochrany.[22] Pojem "*bezpečný přístav"* byl označením pro spolehlivé subjekty z hlediska ochrany osobních údajů. Princip bezpečného přístavu byl poměrně jednoduchý, spočíval v zařazení amerických společností na tzv. Safe Harbor List, které se zavázaly dodržování pravidel dle výše uvedeného rozhodnutí a které navazovalo na Směrnici 95/46/ES.

2.4.7 Směrnice 2006/24/ES

Dalším mezníkem ve vývoji ochrany osobních údajů a jí příbuzných institutů, bylo vydání *Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES,* a to především jako reakce na teroristické útoky v Londýně z roku 2005.

Tato směrnice ukládala tzv. *"data retention"* povinnost, jinými slovy povinnost uchovávání provozních a lokalizačních údajů u poskytovatelů komunikačních služeb, zejména pro účely trestního řízení. Jedná se o uchovávání plošných informací o uskutečněné komunikaci, která zahrnuje telefonní hovory, SMS/MMS zprávy i připojení k internetu. Tyto informace mají být uchovávány telekomunikačními společnostmi a poskytovateli internetového připojení po dobu minimálně šesti a maximálně čtyřiadvaceti měsíců.

[21] INFORMAČNÍ PRÁVO. *Faculty of Informatics, Masaryk University | Faculty of Informatics Masaryk University* [online]. Dostupné z: https://www.fi.muni.cz/~smid/inf_pravo_ochd1.html#_ftn33

[22] Rozhodnutí Komise z 26. července 2000, č. 2000/520/ES o adekvátnosti ochrany poskytované dle principů bezpečného přístavu

Zmiňovaný mezník představuje spíše skutečnost, že v dubnu roku 2014 byla rozhodnutím velkého senátu SDEU prohlášena za neplatnou, a to pro rozsáhlý a mimořádně závažný zásah do základních práv na respektování soukromého života a na ochranu osobních údajů, aniž by tento zásah byl omezen na nezbytné minimum.[23] Podle soudního dvora došlo k zásahu do soukromí tím, že z uchovávaných údajů lze mimo jiné zjistit, jakým způsobem, v jaké době, na jakém místě, s jakou další osobou a kolikrát probíhala komunikace v daném časovém období. Kombinace těchto údajů mohou ve svém celku poskytnout velice přesné informace o soukromí konkrétní osoby, které se uchovávané údaje týkají. Zároveň skutečnost, že k uchovávání a následnému využití těchto údajů docházelo bez informování či poskytnutí souhlasu dané osoby, může vzbuzovat dojem, že je jejich soukromí pod neustálým dohledem. Dle SDEU nebylo stanoveno žádné objektivní kritérium, které by zaručovalo, že přístup příslušných vnitrostátních orgánů k údajům a jejich následné využití, bude možné jen pro účely vyšetřování, odhalování a stíhání trestných činů, které lze vzhledem k povaze zásahu do dotčených práv považovat za dostatečně závažné na to, aby takový zásah odůvodnily.

Dále směrnice nezajišťovala dostatečné záruky účinné ochrany údajů proti riziku jejich zneužití ani proti veškerému neoprávněnému přistupování k údajům a jejich protiprávnímu využívání.[24] Nestanovila ani povinnost nevratné likvidace údajů po skončení doby jejich povinného uchovávání. Jak je zmíněno výše, tyto údaje by ve svém celku a v nepovolaných rukou mohli způsobit velice závažné újmy, a to prakticky každému jednotlivci, kterého se týkají. Po prohlášení směrnice za neplatnou, byla povinnost *"data retention"* zrušena na Slovensku, Rakousku, Rumunsku a Slovinsku. V České republice je povinnost *"data retention"* upravena v zákoně č. 127/2005 Sb., o elektronických komunikacích, v § 97 odst. 3. Na základě zrušení směrnice podala v roce 2017 Pirátská strana návrh na zrušení příslušných ustanovení k Ústavnímu soudu, právě pro nesoulad se základními lidskými právy v podobě plošného sledování občanů.[25]

[23] *Tisková zpráva č. 54/14* [online]. Copyright ©yjP9s [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=9488

[24] *Tisková zpráva č. 54/14* [online]. Copyright ©yjP9s [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=9488

[25] Piráti a IuRe podali návrh na zrušení plošného sledování občanů Ústavnímu soudu ČR.. *Pirátská strana* [online]. Copyright © [cit. 28.03.2019]. Dostupné z: https://www.pirati.cz/tiskove-zpravy/navrzeno-zruseni-smirovani.html

Současná situace je ovšem velice paradoxní, jelikož data jsou stále uchovávána na základě povinnosti plynoucí z platné zákonné úpravy, nikoli tedy na základě zrušené směrnice. Pokud by ale operátoři data uchovávat přestali, jednali by v rozporu se zákonem. Nicméně tím, že takto nadále činí zároveň zasahují do základních lidských práv, jak konstatoval SDEU ve svém rozhodnutí. Dle názoru autora lze také shledat jistý rozpor se základními zásadami Obecného nařízení, které jsou popisovány níže.

2.4.8 Nařízení komise č. 611/2013

V roce 2013 byl prostřednictvím Evropské komise vydán prováděcí předpis ke Směrnici 2002/58/ES a to *Nařízení komise č. 611/2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích.* Jednalo se o prováděcí opatření, které přesně určovalo, jak mají provozovatelé telekomunikačních sítí a poskytovatelé internetových služeb jednat, pokud dojde ke ztrátě, odcizení či jinému ohrožení osobních údajů jejich zákazníků.[26] Zároveň tento předpis zpřesňoval povinnost oznámení takové události příslušnému vnitrostátnímu orgánu a sjednocoval postup při řešení takové události ve všech členských státech aby v případě narušení bezpečnosti osobních údajů jednali se všemi zákazníky stejným způsobem. Toto opatření bylo klíčové zejména pro podniky působící ve více členských státech.

Důležitým aspektem vyplývajícím z tohoto nařízení, bylo stanovení technických ochranných opatření v článku 4 tohoto nařízení, jejichž zavedení osvobozovalo subjekty od oznamovací povinnosti, jelikož tato technická opatření zajišťovala, že osobní údaje nebyly čitelné ani srozumitelné pro nikoho, kdo nebyl k přístupu k nim oprávněn.[27] Jednalo se o různé druhy šifrovací techniky, způsobující nečitelnost a nerozluštitelnost daného osobního údaje.

[26] *Tisková zpráva Evropské komise ze dne 24. června 2013* [online]. Copyright © [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=3061

[27] NAŘÍZENÍ KOMISE (EU) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích, článek 4.

2.4.9 Rozhodnutí C-131/12 Google Spain vs Mario Costeja Gonzáles

Dalším důležitým mezníkem ve vývoji ochrany osobních údajů, je rozhodnutí SDEU z roku 2014 ve věci *C-131/12 Google Spain/Google Inc v. Agencia Española de Protección de Datos*[28] (AEPD), *Mario Costeja Gonzáles*[29], ze kterého bylo dovozeno tzv. *"právo být zapomenut".*

Tento rozsudek se zabýval problematikou upravenou výše zmiňovanou Směrnicí 95/46/ES. Spor se odehrál mezi skupinou Google a P. Gonzálesem, který požadoval vymazání informací z veřejného prostoru o nepříjemné události ve svém životě z roku 1998. Jednalo se o informace o nuceném prodeji jeho nemovitostí z důvodu nesplaceného dluhu na sociálním pojištění (dluh byl následně vyrovnán)[30], zveřejněné prostřednictvím internetových stránek novin *La Vanguardia*. Pan Gonzáles se nejprve obrátil na AEPD, ten nařídil, aby společnost Google Inc. přijala nezbytná opatření k odstranění osobních údajů pana Gonzálese a zabránila přístupu k těmto údajům v budoucnu.[31]
Věc se dostala ke španělskému nejvyššímu soudu (Audencia Nacional), který se obrátil na SDEU se třemi předběžnými otázkami. Předložené prejudiciální otázky se týkali věcné a místní příslušnosti směrnice, a hlavně výkladu práva subjektu *"být zapomenut".* Nicméně nutno podotknout, že zmiňovaná směrnice pojem "právo být zapomenut" zatím neobsahovala.

Předběžnou otázku týkající se výkladu tohoto práva si SDEU vyložil následujícím způsobem *"zda čl. 12 písm. b) a čl. 14 první pododstavec písm. a) směrnice 95/46 musí být vykládány v tom smyslu, že umožňují subjektu údajů požadovat od provozovatele vyhledávače, aby vymazal ze zobrazeného seznamu výsledků vyhledávání provedeného na základě jména tohoto subjektu odkazy na webové*

[28] Španělský úřad pro ochranu osobních údajů
[29] Rozsudek ve věci C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González
[30] Právo být zapomenut a další dopady rozsudku SDEU | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-sdeu-c-13112-google-spain-94498.html
[31] *Tisková zpráva Evropské komise č.70/14* [online]. Copyright © [cit. 28.03.2019]. Dostupné z:https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070cs.pdf

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“.[32] Zjednodušeně řečeno, jedná se o to, zda je subjekt údajů schopen rozhodovat, kdo o něm jaké osobní údaje zpracovává a zda může případně toto zpracování nějakým způsobem omezit.

SDEU vycházel z toho, že subjekt může požadovat opravu nebo výmaz či blokování osobních údajů, které jsou neúplné nebo nepřesné[33], což v tomto případě nebyli. Dle článku 14 této Směrnice, mají subjekty údajů právo uplatnit námitku proti zpracování osobních údajů z legitimních důvodů (nikoli tedy na základě pouhého přání subjektu) a je-li námitka oprávněná, může vést k ukončení zpracování.

Dle SDEU neslučitelnost zpracování osobních údajů s touto směrnicí *„může plynout nejen ze skutečnosti, že uvedené údaje jsou nepřesné, ale konkrétně také ze skutečnosti, že jsou nepřiměřené, nepodstatné a přesahují míru s ohledem na účely, pro které jsou zpracovávány, že nejsou aktualizovány nebo že jsou uchovávány po dobu delší, než je nezbytně nutné, pokud nejsou uchovávány pro historické, statistické nebo vědecké účely“*[34]

Dále dovodil, že osobní údaje mají být uchovávány ve formě umožňující identifikaci jejich subjektů po dobu ne delší, než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány. Nutno podotknout, že význam slova “nezbytné” v tomto kontextu nelze vykládat jakožto “nevyhnutelné” nebo “nezastupitelné”, nýbrž spíše jako zpracování, které není zbytné, tedy je důležité a má svůj konkrétní smysl. Informace o existenci dluhu na sociálním zabezpečení a následný prodej nemovitosti pana Gonzálese, je tedy vykládána jakožto zcela zbytná. Významově tedy menší, s ohledem na dobu uplynulou od inkriminované události.
Lze tedy dovodit, že požadavek subjektu údajů na výmaz jeho osobních údajů může být relevantním jen za situace, pokud subjekt údajů upozorní na skutečnost, že jsou

[32] Rozsudek ve věci C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ods. 89
[33] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, článek 12
[34] Rozsudek ve věci C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ods. 92

jeho osobní údaje zpracovány protiprávně. Protiprávnost může pramenit jak z doby uchovávání údajů, rozsahu zpracování či věcné nesprávnosti daných osobních údajů. Celou situaci shrnul ve svém vyjádření generální advokát Niila Jääskinen - *"směrnice neupravuje všeobecné právo být zapomenut v tom smyslu, že subjekt údajů má nárok na omezení nebo ukončení šíření osobních údajů, které jsou podle jeho názoru škodlivé, nebo odporují jeho zájmům. Kritérii, která mají být uplatněna v případě zpracování údajů bez souhlasu subjektu údajů, jsou účel zpracování a zájmy, kterým zpracování slouží, ve srovnání se zájmy subjektu údajů, a nikoli subjektivní preference uvedené osoby. Samotná subjektivní preference nepředstavuje naléhavý legitimní důvod ve smyslu čl. 14 písm. a) směrnice."*[35]

2.5 Obecné nařízení o ochraně osobních údajů

Veškeré výše uváděné mezníky neboli události podstatným způsobem ovlivňující vývoj základního lidského práva na soukromí, jehož aspektem je právo na informační sebeurčení a z něj vycházející ochranu osobních údajů, byly zásadně ovlivněny okolnostmi a dobou jejich přijetí či vydání. Pokud dřívější předpisy vznikaly jako reakce na rychlý technologický rozvoj, první a druhé desetiletí jednadvacátého století svým rozvojem v oblasti technologií postavilo před zákonodárce nesrovnatelně náročnější cíl. Tímto cílem bylo reagovat na dosud nevídaný nárůst naprosto nových technologií, které svou povahou stavěly ochranu osobních údajů před nové výzvy. Pro upřesnění je třeba vyzdvihnout alespoň ty, které se během velice krátké doby staly globálním standardem a svým charakterem nejvíce zasahují do oblasti ochrany osobních údajů. Obrovský nárůst internetové nabídky a služeb, elektronické bankovnictví, elektronické obchodování a v neposlední řadě gigantický nárůst využití sociálních sítí, to vše sebou nese rozsáhlý sběr a zpracování osobních údajů. Monitorování a profilování fyzických osob na základě osobních údajů, monitorování chování zaměstnanců, klientů a spotřebitelů se během krátké doby stalo využitelným v globálním měřítku. Neméně důležitá potřeba ochrany osobních údajů vyvstala s využíváním nejnovějších typů

[35] Stanovisko generálního advokáta N. Jääskinena přednesené dne 25. června 2013. odst. 108

internetových služeb, jako je VoIP[36], instant messaging[37], či jiné webové služby obsahující data a metadata umožňující identifikaci koncového uživatele.[38] Všechny tyto technologie a služby mění jak ekonomiku, tak i společenský život jednotlivce a v tomto ohledu je nutné budovat důvěryhodné prostředí internetu, jelikož zpracování a sdílení osobních údajů je pro současnou ekonomiku nezbytným předpokladem pro uskutečňování obchodních transakcí nejrůznějšího charakteru.[39]

Výše uvedené skutečnosti zajistily, že ochrana osobních údajů se stala jedním ze stěžejních témat v *Digitální agendě pro Evropu*, která je jedním z pilířů ve strategii EU pojmenované *"Evropa 2020"*. Téma ochrany osobních údajů v této strategii má své základy ve zprávě Evropského parlamentu ze dne 6. července 2011, tím byl podpořen přístup Komise k reformování rámce ochrany osobních údajů. Úmysl Komise byl podpořen i ze strany Rady EU a Evropským hospodářským a sociálním výborem, tedy zajištění jednotnějšího uplatňování pravidel EU pro ochranu osobních údajů ve všech členských státech a přezkum Směrnice 95/46/ES, která byla dosavadním předpisem upravujícím ochranu osobních údajů na komunitární úrovni.

Dostatečné zabezpečení osobních údajů v takto prudce se rozvíjejícím informačním prostředí již nebylo možné řešit jen další novelizací dosavadní směrnice, proto instituce EU zvolily odlišnou formu předpisu pro úpravu ochrany osobních údajů a to nařízení. [40] Nařízení EU má unifikační, tedy sjednocující efekt a je nejúplnějším a nejvíce bezprostředním právním aktem v rámci jejích právních nástrojů. Pro členské státy je bezprostředně závazné a přímo použitelné, takže není nutná jeho implementace do právních řádů členských států.

[36] *Voice over Internet Protocol, technologie umožňující přenos hlasu prostřednictvím počítačové sítě*
[37] *Internetová služba pro okamžité zasílání zpráv (Viber, Whattsup apod.)*
[38] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7., str. 29
[39] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6., str. 125
[40] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7., str. 29

Evropský zákonodárce při tvorbě tedy vycházel z článku 16 SFEU, kde je uvedeno, že *"Každý má právo na ochranu osobních údajů, které se jej týkají."*[41] a také z článku 8 Listiny základních práv EU, kde je právo na ochranu osobních údajů zakotveno jako jedno ze základních práv.

Dne 25. ledna 2012 byl po veřejných konzultacích s občany EU a průzkumu Eurobarometru číslo 359[42] předložen návrh nařízení. Následovalo mnoho projednávání v rámci institucí EU, převážně v Radě EU, která v červnu roku 2015 dosáhla obecného přístupu a mohla tedy zahájit jednání s Evropským Parlamentem.[43] K dohodě mezi Radou, Parlamentem a Komisí bylo v rámci trialogu dosaženo dne 15. prosince 2015, jak požadovala Evropská rada. Na začátku dubna 2016 na základě doporučení Výboru pro občanské svobody, spravedlnost a vnitřní věci, schválil ve druhém čtení Parlament postoj Rady v prvním čtení bez pozměňovacích návrhů.[44] K podpisu právního aktu došlo dne 27. dubna 2016, v Úředním věstníku EU byl zveřejněn dne 4. května 2016 a dne 24. května vstoupilo v platnost *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů),* známé také jako *General Data Protection Regulation,* neboli *GDPR* (Obecné nařízení).

Skutečnost, že evropský zákonodárce novou úpravu ochrany osobních údajů přijal ve formě nařízení jen potvrzuje, jaký význam je v dnešní době osobním údajům a jejich ochraně přikládán, dle autora zaslouženě. Obecné nařízení, účinné od 25. května 2018 představuje nový právní rámec ochrany osobních údajů v EU a má zásadní vliv i na zpracování osobních údajů v nečlenských státech. Univerzálně použitelné je i na Islandu, v Norsku a Lichtenštejnsku.[45]

---

[41] Smlouva o fungování Evropské unie, čl. 16
[42] Special Eurobarometer 359 [online]. ©2010 [cit. 28.03.2019]. Dostupné z: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf
[43] Ochrana údajů: Rada se dohodla na obecném přístupu - Consilium. *Home - Consilium* [online]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2015/06/15/jha-data-protection/
[44] Jak vznikalo nařízení o ochraně osobních údajů (GDPR)? [online]. ©2018 [cit. 28.03.2019]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/
[45] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7., str. 30

V České republice Obecné nařízení do značné míry nahradilo zákon č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů a na základě toho měl být do účinnosti Obecného nařízení schválen nový zákon o zpracování osobních údajů. Bohužel k tomu nedošlo a nestalo se tak ani o téměř rok později. V současné době Senát návrh zákona o zpracování osobních údajů vrátil Poslanecké sněmovně s pozměňovacími návrhy. Tento zákon bude omezen pouze na úpravu některých otázek ve věcech, u kterých to obecné nařízení umožňuje, také se dotkne některých oblastí, které nejsou obecným nařízením upraveny. Obecné nařízení totiž umožňuje v některých věcech odchylnou národní úpravu, respektive ji přímo ukládá vytvořit.

2.5.1 Zhodnocení období legisvakance Obecného nařízení

V souvislosti s přijetím Obecného nařízení, tedy v mezidobí od 27. dubna 2016 a jeho účinnosti 25. května 2018 vyvstalo celospolečensky mnoho otázek týkající se ochrany osobních údajů, které se vlivem mnoha faktorů během krátké doby změnily v doslova vlnu hysterických domněnek a mýtů. V této podkapitole chce autor zhodnotit situaci, která v tomto období ochranu osobních údajů a z ní vyplývající problematiku doprovázela.

Legisvakanční lhůta byla evropským zákonodárcem stanovena na poměrně dlouhou, nicméně k rozsahu a významu tohoto nařízení úměrnou dobu 2 let. V tomto kontextu legisvakanční lhůta sloužila předně členským státům k přijetí adaptačního zákona. Tím, že Česká republika nepřijala adaptační zákon ani téměř rok po účinnosti Obecného nařízení neplní jednak povinnost plynoucí z členství v EU, zároveň ale přichází o možnost aplikace odchylek a vnitrostátních úprav, které Obecné nařízení ukládá vytvořit a tím dává členským státům možnost určité segmenty ochrany osobních údajů upravit odlišným způsobem. Vlastní pravidla a výjimky z Obecného nařízení se týkají převážně veřejnoprávního prostoru, nepřijetím adaptačního zákona tedy stát škodí primárně sám sobě.
Oproti tomu v soukromoprávním prostředí bylo možné legisvakanční lhůtu využít primárně k dosažení souladu s Obecným nařízením. Nutno podotknout, že nepřipravenost vyplývající z nedodržování dosavadní úpravy ochrany osobních údajů soukromoprávními subjekty, přispěla k výše zmiňované hysterii a připravila

půdu pro možnost zneužití této neznalosti a nepřipravenosti, ze strany jiných soukromoprávních subjektů.

Další skutečnost, která nepřispěla k vytvoření racionálního prostředí v období legisvakance je autorem shledávána v obrovské kritice jak politického, tak i mediálně společenského charakteru. Objektivní kritika plynoucí ze znalosti daného tématu a spatřování zjevných nedokonalostí je samozřejmě žádoucí a přínosná. Na druhou stranu, kritika plynoucí z populismu některých politických subjektů ve snaze znehodnotit prakticky cokoli, co pochází z pera evropských zákonodárců se za přínosnou označit nedá, a právě ta se v souvislosti s Obecným nařízením ozývala nejčastěji. Toto je samozřejmě podmíněno existencí cílové skupiny, bez které by tato kritika, nebo spíše kritické nicneříkající výkřiky postrádali smyslu. Největší problém je z pohledu autora spatřován právě v neznalosti a neinformovanosti veřejnosti v oblastech, které jsou často využívány k jejich zastrašování. Jako důkaz lze považovat skutečnost, že institut ochrany osobních údajů je na úrovni Ústavního pořádku v České republice zakotven od devadesátých let a prováděcí předpis v podobě zákona vznikl na přelomu tisíciletí i tak období legisvakance budilo dojem, že se jedná o úplnou novinku přicházející právě z Bruselu. Tím není však myšleno, že každý jeden občan by měl ve volném čase studovat návrhy předpisů EU. Důraz by měl být kladen na objektivní informování občanů ze strany veřejnoprávních médií, politických subjektů a hlavně státu, k čemuž dle názoru autora v období legisvakance příliš nedocházelo.

Autor tímto nehodnotí odvedenou práci dozorového úřadu před účinností Obecného nařízení, nicméně právě na názory úřadu byl tazatel odkazován, pokud položil odborný dotaz někomu, kdo neměl v úmyslu předmětný dotaz využít jako lákavý obchodní artikl. Tím je myšleno, že ne každá advokátní kancelář pojala Obecné nařízení jako příležitost k vytvoření zisku a při nevědomosti raději odkazovala na národní dozorový úřad. O to více ležérněji působí fakt, že ÚOOÚ sice projevil snahu o seznámení široké veřejnosti s novou legislativou prostřednictvím webu, který měl za cíl neprávnicky seznámit čtenáře s jejím obsahem, nicméně pouhých 14 dní před její účinností.

Nelze se nezmínit také o mediálním prostředí v období legisvakance. V souvislosti s Obecným nařízením se v českých mediích psalo soustavně a vzniklá hysterie byla tímto velice posílena. Respektive soustavně se v médiích psalo, ale až po dubnu 2016, tedy uvedení v platnost a na možnost vyvolat společenskou debatu bylo tedy již pozdě. Pokud se totiž v České republice začne problém probírat až ve chvíli, kdy už neexistuje způsob, jak ho účinně řešit, nezbývá většinou nic jiného než si stěžovat. Nehledě na to, že titulky článků, které se věnovaly tématu Obecného nařízení a ochraně osobních údajů obecně, nepůsobily v žádném případě pozitivně. Média většinou převzala rétoriku politiků kritizujících EU a tím také přispěla k vlně negativní kritiky široké veřejnosti. Samozřejmě, hysterie a strach se prodává lépe než například informace o tom, že v Německu se adaptační zákon podařilo přijmout během první poloviny legisvakančního období, nebo ať podnikatelé na adaptační zákon nečekají, jelikož nařízení EU je přímo aplikovatelné a není potřeba implementačního předpisu na národní úrovni. Nebylo třeba Obecné nařízení vychvalovat, nejspíše to nebylo ani možné, nicméně podat čtenáři objektivní pohled na danou problematiku, či ho seznámit s novou úpravou jinak, než negativně kritickou formou by dle autora byla lepší cesta pro většinu médií.
Nutno podotknout, že faktický dopad, respektive změny, které přineslo Obecného nařízení se v praxi týkaly naprosté menšiny společnosti. Situaci ve společnosti v období legisvakance shrnul novinář Petr Honzejk tímto trefným komentářem, ze dne 21. května 2018: *"Vlastně si myslím, že českou společnost lze nyní rozdělit na dvě skupiny. První neví, co to je GDPR a je jí to jedno. Druhá to neví také a existence něčeho takového ji hluboce uráží."*

Všechny výše uvedené okolnosti určitým způsobem přispěly k vytvoření prostředí plného hysterie, nevědomosti a strachu. Tato kombinace byla zdá se ideální příležitostí ke zneužití této ne příliš pozitivní atmosféry okolo Obecného nařízení a nahrávala velkému množství subjektů, jenž se rozhodly rozšířit své pole působnosti a na panující panice vydělat. Tímto nejsou myšleny advokátní kanceláře, které své know-how týkající se ochrany osobních údajů prodávaly za standardní advokátní hodinovou odměnu, spíše konzultační a poradenské firmy, bez předchozí zkušenosti v oblasti ochrany osobních údajů, které pouze využily hysterií uměle vyvolanou poptávku.

Autor čerpá z vlastní zkušenosti, když hovoří o poradenských a konzultačních společnostech, které v období legisvakance nabízely služby spojené s ochranou osobních údajů a zavedením souladu s Obecným nařízením. Minulý čas je uveden záměrně, jelikož s odstupem času od účinnosti Obecného nařízení se na trhu vyprofilovaly pouze ty společnosti, které svoji práci dělají zodpovědně a nečinily tak pouze s vidinou obřích zisků, alespoň v to doufá. Výstup jedné z těchto společností měl možnost při své praxi v advokátní kanceláři prostudovat a zhodnotit. Výsledek byl přinejmenším znepokojující, jelikož dle informací od klienta, bylo za tento výstup zaplaceno několik desítek tisíc korun, za které klient obdržel nicneříkající zprávu o několika desítkách stran, která byla pravděpodobně vytvořena nekvalitním překladem v té době v České republice nedostupné metodiky a částí samotného Obecného nařízení. Mimo to tato zpráva neodpovídala oboru podnikání zmíněného klienta, lze tak předpokládat, že byl tento produkt prodáván univerzálně, nehledě na velikost, potřeby či odvětví cílového klienta. Běžnou praxí té doby se také staly metodiky a návody, které možná odpovídaly co do odbornosti, nicméně nikoli co do rozsahu potřebného pro danou společnost. Jít totiž nad rámec toho, co Obecné nařízení požadovalo, mohlo být velice výhodné. Větší rozsah znamená možnost vykázat vetší množství času nutného k vypracování a zároveň požadovat větší odměnu. V praxi docházelo i k případům, kdy součástí výstupu bylo doporučení pro zavedení nových IT systémů, opět nad rámec potřeb dané společnosti, s odkazem na partnerskou společnost zabývající se řešením IT rozhraní pro ochranu dat. Zdánlivá win-win[46] situace, bohužel nikoli pro cílového klienta. Tuto praxi shrnula i eurokomisařka Věra Jourová ve svém komentáři pro Euroaktiv: *"U nás v ČR jsme zase papežtější než papež a bruselštější než Brusel"*.

Atmosféra doprovázející legisvakanční lhůtu Obecného nařízení byla totiž v České republice poměrně ojedinělá, samozřejmě obavy z nových pravidel ochrany osobních údajů panovaly v celé EU, nicméně nesměřovaly k hysterii, panice a komentářům připomínající blížící se konec světa. Jak moc je totiž pravděpodobné, že evropský zákonodárce má za cíl svými předpisy zničit život více než půl miliardě

[46] *Proces řešení konfliktu, který si klade za cíl vyjít vstříc všem jeho účastníkům*

svých obyvatel? A i kdyby to tak bylo, jak moc je pravděpodobné, že tento záměr odhalili pouze Češi?[47]

Závěrem této podkapitoly by autor rád podotkl, že obava z Obecného nařízení byla určitým způsobem opodstatněná. Být totiž v roli jednatele společnosti, pro kterou nová evropská legislativa představuje vynaložení nemalých finančních prostředků, a hlavně energie a času, musí být velmi stresující. Na druhou stranu *"právo patří bdělým"* a právě zachování bdělosti může v těchto situacích vést k nejpříznivějším výsledkům.

3 Ochrana osobních údajů dle Obecného nařízení

První část této diplomové práce, tedy vývoj ochrany osobních údajů byla završena posledním významným milníkem, a to přijetím Obecného nařízení. Jelikož se jedná o jednotnou právní úpravu pro oblast ochrany osobních údajů na úrovni EU, bude v následující části rozebrána samotná ochrana osobních údajů v jejím světle.

3.1 Vymezení základních pojmů

3.1.1 Osobní údaj

Z podstaty věci se jedná o pojem zcela klíčový, neboť jak aktuální právní úprava ochrany osobních údajů, tak úprava předešlá se vztahuje pouze na informace, které lze za osobní údaje označit. Samotná definice ve vnitrostátním zákoně byla velice široká a Obecné nařízení demonstrativní výčet jednotlivých osobních údajů uvedený v definici ještě rozšiřuje: "*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více*

[47] České specifikum: Z GDPR se stal byznys se strachem | Právo21 – Časopis nové generace pro studenty, právníky i veřejnost. *Právo21 – Časopis nové generace pro studenty, právníky i veřejnost* [online]. Copyright © Masarykova univerzita [cit. 28.03.2019]. Dostupné z: https://pravo21.online/pravo/ceske-specifikum-z-gdpr-se-stal-byznys-se-strachem

zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby".[48]

Osobním údajem se rozumí jakákoliv informace, která se týká určené nebo přímo či nepřímo určitelné fyzické osoby.[49] Přímou identifikací je možné zjistit identitu osoby jednoznačně na základě přesného identifikátoru, kterým může být například jméno, příjmení, adresa, datum narození či rodné číslo, popřípadě jejich kombinace. Oproti tomu nepřímou identifikací se myslí identifikace na základě jakékoli jiné kombinace údajů, která umožňuje od sebe jednotlivé osoby odlišit.[50]
Význam pojmu určitelnost, který je pro tuto definici klíčový, lze chápat jako stav, kdy je možné na základě dostupných informací fyzickou osobu odlišit od jiných fyzických osob. Pokud posuzujeme, zda je subjekt na základě dostupných údajů určitelný, je nutné přihlédnout ke všem prostředkům, které by pro provedení identifikace museli být použity[51], lze ale předpokládat, že k identifikaci nebude užito nadměrného úsilí ani vynaloženo nadměrných nákladů.

Jedná se tedy o veškeré informace, které se určeného nebo určitelného člověka nějakým způsobem týkají, byť jej sami o sobě ani v kombinaci nemusí nutně identifikovat. Není relevantní, zda je osobní údaj zcela pravdivý a objektivně měřitelný nebo zda se jedná o pouhý odhad charakteristiky člověka. Ani formát zachycené informace není rozhodný, tzn. jakým způsobem je informace zachycena, tedy písemně či ve formě audio nebo videozáznamu. Klíčový je také fakt, že abychom mohli danou informaci označit za osobní údaj, musí se nutně týkat fyzické osoby, a to fyzické osoby žijící, jelikož ochrany osobnostních práv zemřelé osoby je třeba se domáhat prostředky soukromého práva. Stejně tak osobní údaje nelze přiřazovat k právnické osobě.

[48] Obecné nařízení o ochraně osobních údajů, čl. 4 odst. 1
[49] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. str. 77
[50] Stanovisko č. 3/2012 – K pojmu osobní údaj: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/stanovisko-c-3-2012-k-pojmu-osobni-udaj/d-1535
[51] Obecné nařízení o ochraně osobních údajů, recitál č. 26

Pro posouzení, zda se informace týká určité či určitelné osoby, lze použít kritéria vycházející ze stanoviska WP29 k pojmu osobní údaje. V tomto stanovisku osobní údaj definovali jako *"široký pojem, jenž má zahrnout veškeré informace, které mohou s fyzickou osobou souviset a to jak informace objektivní, tak informace subjektivní, kterými jsou názory a hodnocení."*[52] a tím dle názoru autora poskytli do té doby nejpřesnější vymezení tohoto pojmu.

Opakem osobních údajů jsou údaje anonymní. Jedná se o informace, které se netýkají určené nebo určitelné fyzické osoby a které nikdy nebyly a ani v současnosti nejsou osobními údaji. Oproti tomu osobní údaje anonymizované jsou informace, které v minulosti byly přiřaditelné ke konkrétní fyzické osobě, nicméně prošly určitou úpravou, tedy anonymizací, což způsobilo jejich neurčitelnost a nepřiřaditelnost.

3.1.1.1 Pseudonymizace

V souvislosti s výše uvedenými anonymizovanými údaji, které jakožto původní osobní údaje prošli procesem anonymizace a jejich nerozluštitelnost je nevratná, je potřeba vyzdvihnout novou kategorii osobních údajů, jež Obecné nařízení zavádí ve svém článku 4 odst. 5. Jedná se o proces tzv. pseudonymizace, kterou Obecné nařízení definuje jako *"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 fyzické osobě".*[53]

Pseudonymizaci lze v praxi provést například tak, že jménu a příjmení subjektu v databázi se přidělí kód tvořený náhodnými znaky s tím, že se zároveň odděleně uchová informace o tom, že právě tento kód odpovídá konkrétnímu jménu a příjmení. V databázi se bude tedy nacházet na první pohled nečitelný kód, který ale bude možné na základě určitého klíče přidělit konkrétnímu subjektu.

[52] Stanovisko WP29 č. 4/2007 k pojmu osobní údaje
[53] Obecné nařízení o ochraně osobních údajů, článek 4 odst. 5

Pseudonymizované osobní údaje prošli tedy také určitým procesem, který se svou podstatou podobá šifrování. Nicméně i po tomto procesu se nadále jedná o osobní údaje, jelikož oproti anonymizaci, tyto osobní údaje lze v kombinaci s dalšími informacemi udělat znovu čitelnými a určitelnými.
Dle recitálu č. 26 a č. 28 Obecného nařízení má zavedení pojmu pseudonymizace za cíl zvýšit ochranu subjektů osobních údajů a také výrazně přispět k plnění povinností týkajících se ochrany osobních údajů a jejich zabezpečování.

3.1.1.2 Zvláštní kategorie osobních údajů

Jak vyplývá přímo z termínu, který je Obecným nařízením pro označení této skupiny osobních údajů používán, jedná se o tzv. *"zvláštní kategorii osobních údajů"*. Jejich zvláštnost vyplývá hlavně ze skutečnosti, že jejich zpracování představuje podstatně vyšší zásah do soukromí daného subjektu a z tohoto důvodu také požívají větší úrovně ochrany. Pro doplnění v národní úpravě byl zvolen odlišný termín a to *"citlivé údaje"*. Dle Obecného nařízení se jedná osobní údaje, které *"vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby."*[54]

Z článku 9 Obecného nařízení vyplývá, že zpracování zvláštní kategorie osobních údajů se zakazuje, nicméně dále stanovuje případy, ve kterých k takovému zpracování docházet může. Jedná se například o udělení výslovného souhlasu subjektu s takovým zpracováním nebo pokud subjekt není fyzicky nebo právně způsobilý takový souhlas udělit, ale zpracování je nutné pro ochranu životně důležitých zájmů subjektů nebo jiné fyzické osoby.[55]

[54] Obecné nařízení o ochraně osobních údajů, článek 9 odst. 1
[55] Obecné nařízení o ochraně osobních údajů, článek 9 odst. 1 a 2

3.1.1.2.1 Genetické údaje a biometrické údaje

Obecné nařízení pod skupinu zvláštních osobních údajů nově řadí genetické a biometrické údaje. Jak vyplývá z recitálu číslo 34 Obecného nařízení, jsou genetické údaje definovány jako osobní údaje týkající se zděděných či získaných genetických znaků určité fyzické osoby a jako takové vyplývají z analýzy biologického vzorku dotčené osoby.[56] Zejména pak chromozomů, kyseliny deoxyribonukleové, tedy DNA či kyseliny ribonukleové, tedy RNA. Dále se jedná o krevní skupinu, Rh faktor krve apod.

Co se týče biometrických údajů, jedná se o takové informace vypovídající o jedinečných biologických aspektech stavby nebo fungování či chování biologického organismu fyzické osoby a na jejich základě je tak možné je od sebe přímo či nepřímo odlišovat[57]. V praxi se může jednat o snímky obličeje, otisky prstů, snímky zadní části oční duhovky či sítnice, ale také barva hlasu. Mezi biometrické údaje se řadí také dynamický biometrický podpis.[58]

Zařazení Obecným nařízením genetických a biometrických údajů pod zvláštní kategorii osobních údajů, pro českého adresáta neznamená žádnou změnu, jelikož tento druh údajů byl pod skupinu citlivých údajů řazen již v zákoně o ochraně osobních údajů. Obecné nařízení pro zpracování zvláštní kategorie osobních údajů stanoví určitá specifika ve svém článku 9 odst. 2, nicméně v odst. 4 dává členským státům možnost rozšířit či omezit tato specifika, týkající se převážně právních titulů pro zpracování genetických, biometrických a údajů o zdravotním stavu ve své národní úpravě. Česká republika nemá jako jedna z posledních členských států zákon upravující tyto odchylky stále přijatý, takže zůstává otázkou, jaký postoj zaujmou zákonodárci k tomuto tématu.

[56] Obecné nařízení o ochraně osobních údajů, recitál číslo 34
[57] J. Matejka, A. Krausová, V. Güttler: Biometrické údaje a jejich právní režim, *Časopisy Masarykovy univerzity* [online]. Copyright © [cit. 28.03.2019]. Dostupné z: https://journals.muni.cz/revue/article/viewFile/8801/pdf
[58] Stanovisko ÚOOÚ č. 2/2014, Dynamický a biometrický podpis z pohledu zákona o ochraně osobních údajů

3.1.1.3 Síťové identifikátory

Síťové identifikátory jsou Obecným nařízením nově upraveným druhem osobních údajů, jak plyne ze samotné definice osobního údaje[59] a také z recitálu číslo 30, který říká *"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."*[60] K zařazení adresy internetového protokolu (IP adresy) do definice, již před účinností Obecného nařízení výrazně přispěl SDEU ve svém poměrně zásadním rozhodnutí[61], ve kterém konstatoval nutnost považovat IP adresy za osobní údaj.

Je třeba připomenout, že IP adresa (nebo jiné síťové identifikátory) nemusejí vést k přímé identifikaci konkrétní osoby, nicméně postačí, že tuto identifikaci umožňují nepřímo. K identifikaci konkrétní fyzické osoby prostřednictvím IP adresy tedy v praxi nestačí znalost tohoto osobního údaje, ale je potřeba provedení dalších zjištění, použití dalších prostředků a zkombinování IP adresy s dalším osobním údajem. Podobně k této problematice přistoupil i SDEU ve výše zmiňovaném rozsudku, kde ve zkratce konstatoval, že lze předpokládat možnost užití prostředků ze strany orgánů veřejné moci Spolkové republiky Německo, k identifikaci subjektu na základě uchovávaných IP adres. Totožný názor vyslovila i WP29 ve svém stanovisku, kde mj. konstatovala, že zejména v případech, kdy je zpracování osobních údajů prováděno za účelem identifikace uživatele počítače, lze předpokládat existenci prostředků potřebných k této identifikaci např. prostřednictvím soudů, na které se správce obrátí a tyto informace by se proto za osobní údaje považovat měly.

[59] Obecné nařízení o ochraně osobních údajů, článek 4 odst. 1
[60] Obecné nařízení o ochraně osobních údajů, recitál č. 30
[61] Rozsudek Soudního dvora EU ze dne 19. října 2016 Patrick Breyer proti Spolkové republice Německo, věc C-213/15

3.1.1.4 Lokační údaje

Dalším po novu upraveným druhem osobních údajů, jsou údaje lokační, kterým je nutno rozumět jako informacím týkajícím se místa pohybu nebo pobytu dané fyzické osoby.[62] V tuzemské právní úpravě lze vycházet z § 91 zákona č. 127/2005 Sb., o elektronických komunikacích, kde je použit obdobný pojem a to lokalizační údaj. Lokalizačním údajem se podle tohoto zákona myslí údaje vytvořené na základě telekomunikačních zařízení, tedy údaje umožňující sledovat či zjišťovat pohyb pomocí těchto zařízení. Tvoří tedy jakousi podmnožinu údajů lokačních, jelikož tyto údaje umožňují sledovat a zjišťovat pohyb fyzické osoby pomocí jakéhokoli zařízení, které to umožňuje, typicky se jedná o GPS.

V souhrnu tento typ údajů o zeměpisné poloze, může v závislosti na své kvalitě, přesnosti detailu a kvantitě, tedy jednorázové označení polohy nebo naopak sledování polohy za delší časové období, vést k identifikaci konkrétní fyzické osoby. V souvislosti s mírou využití těchto údajů prostřednictvím moderních technologií, považuje autor tento krok evropského zákonodárce za logický, zároveň velice zdařilý.

3.1.2 Zpracování osobních údajů

Dalším z klíčových pojmů z oblasti ochrany osobních údajů je jejich zpracování, které je Obecným nařízením definováno jako "*jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů"*[63] s tím, že je definice doplněna demonstrativním výčtem operací, které lze za zpracování osobních údajů považovat. Nutno podotknout, že pojem zpracování nebyl Obecným nařízením oproti minulým úpravám nijak pozměněn.

Za zpracování osobních údajů se tedy považuje taková operace nebo soustava operací, která je prováděna systematicky, za určitým cílem či účelem, a to bez

[62] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. str. 82
[63] Obecné nařízení o ochraně osobních údajů, článek 4 odst. 2

ohledu na prostředky, kterými byla tato operace realizována. Není tedy rozhodující, zda ke zpracování dochází manuálně, elektronicky, kombinací těchto dvou způsobů nebo za využití určitého softwarového nástroje či IT řešení.[64] V praxi se nejčastěji jedná o operace spočívající ve shromažďování, úpravě, uchovávání, blokování či likvidaci osobních údajů.

Zároveň daná operace, kterou lze považovat za zpracování, musí být prováděna systematicky a za účelem dosažení určitého cíle nebo při realizaci činnosti, kterou ukládá zvláštní zákon. Pokud někdo pouze shromažďuje osobní údaje bez jakéhokoli cíle, případně pouze pro osobní potřebu, o zpracování osobních údajů se nejedná. Ve chvíli, kdy takto nahodile sebraná data někdo systematicky uspořádá, se však o zpracování ve smyslu Obecného nařízení jednat bude.
Co se týče stanovení cíle zpracování, jedná se o individuální záležitost, která náleží tomu, kdo zpracování provádí. Cílem zpracování může být oslovování nové klientely, plnění smluvních závazků se stávajícími klienty, ochrana majetku apod. Pokud se jedná o plnění povinností vyplývajících ze zvláštního zákona, může se jednat o uchování dat, přístupu k nim, jejich hodnocení, analýzy, spojování či převod do jiného formátu.

3.1.2.1 Profilování

Zvláštním a také nově upraveným způsobem zpracování osobních údajů, je tzv. profilování. Dle Obecného nařízení se jím rozumí *"jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu"*[65] Také ho lze definovat jako techniku zpracování, s cílem získání prediktivních informací na základě vytvořeného profilu složeného z vlastností, charakteristik či preferencí. Cílem profilování je předpovídat s významnou mírou pravděpodobnosti chování konkrétního člověka.[66] V praxi je

[64] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. str. 84
[65] Obecné nařízení o ochraně osobních údajů, článek 4 odst. 4
[66] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. str. 87

rozsah využití profilování velice široký, může se jednat o informační základ o návštěvnících webových stránek za účelem cílené reklamy vytvořené dle konkrétních kritérií pro konkrétního člověka či o vyhodnocení ekonomické situace a splátkové příslušnosti klientů finančních institucí, za účelem vyhodnocení vhodnosti při poskytování hypotečních či jiných úvěrů.

3.1.3 Subjekt údajů

Pokud hovoříme o subjektu údajů, jedná se o osobu, která stojí v samotném středobodu ochrany osobních údajů a jež byla poprvé přesně definována ve výše zmíněné Úmluvě 108. Definice se v průběhu let žádným závratným způsobem nezměnila a subjektem údajů se rozumí fyzická osoba, k níž se osobní údaje vztahují a kterou lze na základě osobních údajů identifikovat. To vyplývá i z definice osobních údajů v Obecném nařízení.

Často diskutovaná otázka, zda se osobní údaje vztahují i na osoby zemřelé byla řešena ÚOOÚ v jeho stanovisku ze kterého vyplynulo, že po úmrtí subjektu údajů pozbývají platnosti ustanovení zákona o ochraně osobních údajů, kde subjekt zároveň vystupuje jako účastník občanskoprávních vztahů, tedy ustanovení o jeho právech a povinnostech správce ve vztahu k němu.[67] V platnosti naopak zůstanou ustanovení, v nichž jako účastník občanskoprávních vztahů subjekt údajů nevystupoval, což jsou povinnosti správce nikoli ve vztahu k samotnému subjektu. Obecné nařízení ve svém recitálu 27 přímo stanovuje, že se nevztahuje na osobní údaje zesnulých osob, nicméně dává členským státům možnost tuto otázku upravit. Dle návrhu zákona o zpracování osobních údajů této možnosti český zákonodárce nevyužil.

3.1.4 Správce

Další osobou hrající klíčovou roli na poli ochrany osobních údajů je tzv. správce. Dle definice Obecného nařízení, je správcem *"fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a*

[67] Stanovisko ÚOOÚ č. 4/2012, Zpracování osobních údajů zemřelých osob

prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení".[68]

Pojmové znaky správce lze s ohledem k výše uvedené definici rozdělit podle okolností do dvou samostatných skupin. V prvním případě se jedná o situace, ve kterých určitá osoba vykonává určitou činnost, jež nezbytně doprovází zpracování osobních údajů ve smyslu Obecného nařízení a také to, že se k vykonávání takové činnosti sama rozhodla. Tato osoba si také sama určuje prostředky zpracování, jeho účel a cíl. Účelem jest cíl určité činnosti neboli konkrétní smysl zpracování, může se jednat o provozování webové stránky, ochranu majetku prostřednictvím kamerového systému, nabízení služeb různorodého charakteru potencionálním klientům a jejich marketingové oslovování. Prostředky zvolené k realizaci účelu a cíle, jsou nástroje či zvolené postupy pro konkrétní zpracování.[69] Zda se tedy v konkrétním případě jedná o správce osobních údajů, nelze určit pouze skutečností, že se na zpracování podílí nebo zda ho dokonce sám provádí. Není rozhodující ani fakt, že má předmětné osobní údaje v držení nebo jestli dané informace vytvořil a vlastní je. Rozhodující je skutečnost, zda sám stanovil účel zpracování a prostředky pro jeho realizaci a pokud ano, jedná se o správce osobních údajů.

Druhý případ je podmíněn tím, že zpracování osobních údajů za určitým účelem bylo určitému subjektu uloženo přímo zákonem. Zpracování osobních údajů neboli povinnost zajistit určitou činnost, pro kterou je zpracování osobních údajů nezbytné, může být například uložena každému zaměstnavateli, například povinnost vedení evidence odpracované doby nebo evidence pracovních úrazů.[70] Tuto povinnost mají zákonem uloženou také obce při výkonu samostatné či přenesené působnosti, jedná se o celou řadu agend. Dále poskytovatelé zdravotnických služeb mají povinnost vést zdravotnickou dokumentaci.[71]
Za správce osobních údajů, může být určitý subjekt také výslovně označen ve zvláštním zákoně. Tento případ je typický pro oblast veřejného práva. Například zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů,

[68] Obecné nařízení o ochraně osobních údajů, článek 4 odst. 7
[69] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. str. 89
[70] Zákon č.262/2006 Sb., zákoník práce, § 105 odst. 7
[71] Vyhláška č. 98/2012 Sb. o zdravotnické dokumentaci

výslovně stanoví každému ze základních registrů správce osobních údajů. Kupříkladu pro Registr územní identifikace, adres a nemovitostí je správcem osobních údajů Český úřad zeměměřický a katastrální.[72]

3.1.5 Zpracovatel

Další osobou v klíčovém postavení v oblasti ochrany osobních údajů je tzv. zpracovatel osobních údajů. Dle definice Obecného nařízení se v pozici zpracovatele osobních údajů nachází *"fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce".*[73] V praktické rovině se může jednat o dvě následující situace. Zpracovatel může pro správce zpracovávat osobní údaje buďto na základě pověření nebo na základě zákonného zmocnění. V obou případech ale zpracovatel zpracovává osobní údaje pro správce, tedy místo něj ale stále dle pokynů správce, tedy stanoveného účelu a prostředků.

Pokud se jedná o zpracování na základě pověření, pak je zpracování uskutečňováno na základě platné písemné zpracovatelské smlouvy mezi správcem a zpracovatelem. Nezbytné náležitosti smlouvy o zpracování osobních údajů upravuje článek 28 Obecného nařízení, který mimo jiné klade na osobu zpracovatele celou řadu požadavků. V praxi k tomuto případu dochází velice často, když správce využívá služby nějakého externího dodavatele. Může se jednat o externí mzdové účetnictví či poskytovatele IT řešení, kdy jsou tyto činnosti vždy doprovázeny i zpracováním osobních údajů. Vždy však platí, že se musí jednat o osobu odlišnou od správce, s vlastní právní identitou[74], kdyby totiž ve společnosti mzdové účetnictví vedlo HR oddělení, nejednalo by se o zpracovatele osobních údajů, nýbrž jen o organizační složku daného podniku.

Stejně tak je možné zpracovávat osobní údaje pro správce na základě zákonného zmocnění. Právním titulem tedy nebude platná písemná smlouva o zpracování,

[72] Co (ne)jsou ZR?, Správa základních registrů. *Správa základních registrů* [online]. Copyright ©2010 [cit. 28.03.2019]. Dostupné z: http://www.szrcr.cz/co-jsou-to-zakladni-registry
[73] Obecné nařízení o ochraně osobních údajů, článek 4 odst. 8
[74] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 91

nýbrž existence zvláštního právního předpisu. I v tomto případě musí jít o subjekt odlišný od správce, nicméně daný správce musí fakticky existovat. Situace, kdy by docházelo ke zpracování osobních údajů bez existence správce je nepřijatelná, nebylo by totiž osoby odpovědné za samotné zpracování. K tomuto zpracování dochází opět v oblasti veřejného práva, výše zmiňovaný Český úřad zeměměřický a katastrální je správcem osobních údajů a dle § 54 odst. 2 Katastrálního zákona jsou zpracovateli osobních údajů jednotlivé katastrální úřady.[75]

3.2 Principy zpracování osobních údajů dle Obecného nařízení

Základní principy neboli zásady zpracování osobních údajů nejsou v evropském právním rámci ochrany osobních ničím novým, neboť základní zásady a mechanismy ochrany osobních údajů obsahovali již výše zmíněné Pokyny o ochraně soukromí přeshraničních toků osobních údajů OECD z roku 1980. Obdobné principy obsahovala i Úmluva č. 108 a Směrnice 95/46/ES ve svém článku 6. Oproti tomu národní úprava České republiky výčet těchto zásad neobsahuje, nicméně prakticky totožné zásady jsou v zákoně upraveny formou obecných povinností správce osobních údajů v § 5.

Obecné nařízení, stejně jako předchozí komunitární úprava věnuje základním zásadám zpracování samostatný článek a to článek 5. Oproti staré úpravě Obecné nařízení tyto zásady materiálně zpřesňuje a upravuje. Základní zásady zpracování osobních údajů jsou samy o sobě nejvýznamnějšími povinnostmi, které určují, jak může správce osobní údaje zpracovávat.[76] Celý zbytek Obecného nařízení se těmito zásadami musí řídit a veškerá jeho ustanovení musí být vykládána v souladu s nimi. Jedná se o jakési obecné klausule, pod které lze podřadit většinu konkrétních povinností ukládaných správci v Obecném nařízení.

[75] zákon č. 256/2013 Sb., o katastru nemovitostí, § 54 odst. 2
[76] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 105

3.2.1 Zásada zákonnosti, korektnosti a transparentnosti

Zásadu zákonnosti lze považovat za stěžejní a pravděpodobně nejdůležitější princip ochrany osobních údajů. Obecným nařízením je upravena v článku 6 a stanoví, že zpracování osobních údajů musí probíhat v souladu s právem, respektive s právními předpisy.[77] To znamená, že musí být prováděno na základě alespoň jednoho z právních titulů, které článek 6 vyjmenovává. Zákonnost též stanoví, že zpracování nesmí být prováděno za nelegálním či nelegitimním účelem. Protiprávnost zpracování ale neznamená pouze rozpor s Obecným nařízením, znamená rozpor s právním řádem obecně. Ve chvíli, kdy by zpracování bylo prováděno v souladu s Obecným nařízením, ale bylo by v rozporu v občanským zákoníkem či trestním řádem, bude zásada zákonnosti porušena. Nedodržení zásady zákonnosti může představovat i získání či jiné zpracování osobních údajů, které bude v rozporu se základním lidským právem na ochranu soukromí[78], či právem na informační sebeurčení. V praxi bude docházet k porušení této zásady nejspíše zpracováním osobních údajů bez platného právního titulu dle článku 6 nebo nenaplněním podmínek při zpracování zvláštní kategorie osobních údajů dle článku 9.

Zásada korektnosti, v anglickém znění Obecného nařízení "*principle of fairness*", tedy "princip férovosti", zavazuje správce postupovat lidově řečeno fér, neboli poctivě a ohleduplně, čímž se zpřesňuje zásada přiměřenosti.[79] Správce by dle této zásady měl zohledňovat zájmy subjektu údajů a zároveň jim umožnit a ulehčit výkon jejich zaručených práv. Zásada transparentnosti v praktické rovině zaručuje subjektům aplikaci jejich práva na informační sebeurčení, tedy rozhodnout o tom, které osobní údaje o sobě poskytnou v rámci zákonem stanovených hranic.
Zároveň tyto zásady zaručují povinnost správce informovat subjekt údajů o zpracování jeho osobních údajů a jeho rozsahu, jak vyplývá z článku 13 a 14 Obecného nařízení. Transparentnost se také promítá v právu subjektu údajů na

[77] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7., str. 39
[78] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 106
[79] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7., str. 40

přístup k osobním údajům dle článku 15, jehož odepřením dojde k závažnému porušení této zásady. Předpokládá se tedy, že veškeré informace a sdělení ohledně zpracování osobních údajů budou dle zásady transparentnosti jednoduše přístupné, srozumitelné, a vyhotovené v jasné a jednoduché formě.[80]

V zákoně o ochraně osobních údajů jsou tyto zásady zakotveny v § 5 odst. 1 písm. g) v povinnosti zpracovávat osobní údaje otevřeně, v informační povinnosti dle § 11 a v oznamovací povinnosti zamýšleného zpracování ÚOOÚ dle § 16, kterou nahradila povinnost vedení záznamů o činnostech zpracování osobních údajů.

3.2.2 Zásada účelového omezení

Zásada účelového omezení funguje jako nejvýznamnější určovatel toho, jakým způsobem bude správce s osobními údaji nakládat a jak je bude zpracovávat. Správce vymezením účelu určí důvod zpracování a následně musí tento účel dodržovat a až na výjimky může zpracovávat osobní údaje pouze za tímto účelem. Od tohoto určení se odvíjejí níže popsané zásady minimalizace a omezení uložení údajů. Určení účelu zpracování je nutností v případě, že správce provádí zpracování na základě vlastního rozhodnutí nebo pokud provádí zpracování na základě povinnosti stanovené zvláštním zákonem. Pokud ale provádí zpracování na základě povinnosti ze zvláštního zákona, bývá účel zpravidla určen tímto zákonem.

Provádí-li správce zpracování osobních údajů na základě vlastního rozhodnutí, je určujícím momentem pro další zpracování již samotné shromažďování osobních údajů, jelikož ke stanovení účelu musí dojít nejpozději s touto činností.[81]
Účel musí být určitý, výslovně vyjádřený a legitimní.[82] Jak vyplývá ze stanoviska WP29, hlavním požadavkem na účel je jeho dostatečná určitost. Pokud bude účel určitý, bude zároveň zcela jisté, jaká zpracování budou na jeho základě probíhat a lze tak provést posouzení souladu s Obecným nařízením. WP29 ve svém stanovisku dále doporučuje nevymezovat účel zpracování příliš úzce, jelikož by správce mohl

[80] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, str. 40
[81] Obecné nařízení o ochraně osobních údajů, recitál č. 39
[82] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 108

sám sebe omezit v rozsahu možných operací zpracování a zároveň by prováděním těchto operací mohlo dojít ke zpracování v rozporu s touto zásadou. Při stanovení účelu je také třeba dbát na to, aby nebyl vymezen příliš obecně. [83]

Stanovil-li správce osobních údajů účel zpracování, je třeba aby došlo k jeho výslovnému vyjádření, tedy aby byl účel zpracování výslovně sdělen subjektům údajů. V souvislosti s určitostí účelu je třeba, aby ho všechny osoby zúčastněné na zpracování chápaly ve stejném kontextu, proto by vyjádření účelu mělo být co nejjasnější.

Aby byl účel legitimní, musí být vždy v souladu s právními předpisy zákonné i podzákonné formy. Pokud bude účel právním předpisům odporovat, nebude legitimní a zpracovávat osobní údaje pro jeho naplnění bude nelegální.[84]

3.2.2.1 Další zpracování a podmínky jeho provedení

Z výše popsané zásady účelového omezení existuje jistá výjimka, upravena v článku 5 odst. 1 písm. b) a článku 6 odst. 4 Obecného nařízení. Pokud totiž dochází ke zpracování za jiným než stanoveným účelem, označujeme tuto situaci za tzv. další zpracování, které je ovšem možné jen ve čtyřech případech.
Prvním z nich je situace, kdy udělí subjekt údajů s tímto dalším zpracováním výslovný souhlas. Problematika souhlasu bude popisována níže.
Pokud se jedná o zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo statistické účely a probíhá-li toto zpracování v souladu s článkem 89, je další zpracování taktéž přípustné. Dále za předpokladu, je-li zpracování založeno na právu členského státu nebo EU, které představuje nutné a přiměřené opatření v demokratické společnosti. Jedná se například o národní bezpečnost, obranu státu, ochranu nezávislosti soudnictví a soudních řízení či vymáhání občanskoprávních nároků.[85]

[83] Stanovisko WP29 č.3/2013 k účelovému omezení, strana 16
[84] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 109
[85] Obecné nařízení o ochraně osobních údajů, článek 23, odst 1.

Poslední možnost dalšího zpracování přichází v úvahu, pokud správce posoudil slučitelnost zpracování dle článku 6 odst. 4 Obecného nařízení a závěrem provedení posouzení je slučitelnost původního a nového účelu zpracování. Při provádění tzv. posouzení slučitelnosti musí správce zohlednit pět zásadních faktorů a v souvislosti se zásadou odpovědnosti o tomto interním posouzení vypracovat záznam. Prvním z těchto faktorů je existence jakékoli spojitost mezi stanoveným účelem, pro který byly osobní údaje shromážděny a účelem zamýšleného dalšího zpracování. Příkladem je získání osobních údajů při prodeji za účelem provedení smlouvy a následné uchovávání osobních údajů za účelem ochrany svých práv v případě potencionálních soudních sporů. Dále je třeba zohlednit okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem. Zde musí správce vhodně posoudit, zda v budoucnu může subjekt údajů předpokládat provedení dalšího zpracování osobních údajů.
Správce musí také posoudit povahu osobních údajů, zejména pokud se zpracování týká zvláštní kategorie osobních údajů. Zde platí, že čím citlivější povahy osobní údaje budou, tím větší nároky budou kladeny na slučitelnost dalšího zpracování.
Správce by měl také předpokládat a odhadnout možné důsledky dalšího zpracování pro subjekty údajů a zda tento dopad bude pozitivního či negativního charakteru.
Vzhledem k povaze provedení posouzení slučitelnosti účelů zpracování lze předpokládat, že u některých z výše uvedených faktoru přetrvají jisté nedostatky, a naopak bezchybné výsledky v posouzení jiného faktoru tuto nedokonalost vyváží. I z tohoto důvodu je správce povinen posoudit, zda je schopen zajistit existenci vhodných záruk, zvýšeného zabezpečení například v podobě šifrování či pseudonymizace.

Po provedení komplexní analýzy všech výše uvedených faktorů musí správce posoudit, zda jsou výstupy pozitivní a účely zpracování jsou navzájem slučitelné. I za předpokladu, že slučitelné jsou, je stále nutné mít pro zpracování právní titul a nelze vždy zpracovávat na základě právního titulu původního.[86]

[86] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 144

3.2.3 Zásada minimalizace údajů

V souvislosti s výše popisovanou zásadou účelového omezení zpracování osobních údajů, je třeba vyzdvihnout zásadu minimalizace údajů, jelikož je od výše uvedené zásady odvozována. V souladu se zásadou účelového omezení je správce povinen stanovit určitý, výslovně vyjádřený a legitimní účel zpracování osobních údajů. Zásada minimalizace údajů tuto skutečnost doplňuje, jelikož stanoví správci povinnost shromažďovat a zpracovávat pouze ten typ osobních údajů, který je vzhledem ke stanovenému účelu relevantní, a to pouze v tom rozsahu, který je pro účel zpracování nezbytný. Z této povinnosti vyplývá, že správce musí při každé jednotlivé operaci s osobními údaji zvažovat, zda je tato operace nutná k naplnění účelu a zda k těmto operacím využívá jen relevantní a přiměřený druh osobních údajů. Tato zásada je uplatňována hlavně z důvodu minimalizace zásahu do soukromí subjektu údajů, jedná se tedy zároveň o projev zásady proporcionality.[87]

Příkladem v praktické rovině může být zpracování osobních údajů za účelem plnění smlouvy organizátorem vědeckého semináře, který po účastnících požaduje krom jména a příjmení, e-mailové adresy také rodné číslo, které používá jako originální identifikátor každého účastníka. Právě zpracování rodného čísla nelze považovat v tomto případě za relevantní ani nezbytné, vzhledem ke stanovenému účelu zpracování, jelikož identifikátor lze vygenerovat náhodně. V tomto případě je tedy zpracování rodného čísla nadbytečné a v rozporu se zásadou minimalizace údajů.

Zásada minimalizace údajů se promítne i v nastavování úrovně zabezpečení správcem, v souladu s principem záměrné a standardní ochrany osobních údajů upravené v článku 25 Obecného nařízení. Záměrná ochrana osobních údajů představuje povinnost správce zvolit vhodné prostředky ke zpracování, respektive prostředky, prostřednictvím kterých je zpracování prováděno v souladu se všemi principy Obecného nařízení. Pokud správce ke zpracování používá určitý software neboli počítačový program, je třeba zajistit, aby tento program při automatickém

[87] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1. str. 243

sběru osobních údajů shromažďoval pouze relevantní osobní údaje a osobní údaje, které jsou vzhledem k účelu nadbytečné automaticky likvidoval.[88]
Zajištění standardní ochrany osobních údajů prakticky odpovídá souladu se zásadou minimalizace údajů, jelikož ukládá správci povinnost přijmout vhodná organizační a bezpečnostní opatření, za účelem zajištění zpracování pouze relevantních a nezbytných osobních údajů.

3.2.4 Další zásady zpracování osobních údajů

Obecné nařízení ve svém článku 5 jmenuje i další, neméně důležité zásady zpracování osobních údajů. První z nich je zásada přesnosti, ze které vyplývá povinnost správce zajistit přesnost, skutečnost a aktuálnost osobních údajů a pokud tomu tak není, musí přijmout všechna rozumná opatření k opravě nepřesných údajů, popřípadě tyto údaje odstranit.

Jak bylo uvedeno výše v kapitole Osobní údaj, pravdivost osobních údajů není totožný pojem s jejich přesností. Může totiž docházet k situacím, kdy subjekt údajů poskytne nepravdivé údaje, což ale nezapříčiní odpovědnost správce za jejich nepřesnost. Stejně tak je hodnocena přesnost údajů ve vztahu ke stanovenému účelu zpracování, bude-li pro tento účel dostačující pouze přibližný osobní údaj, nebude zpracování za tímto účelem považováno za nedodržení zásady přesnosti. Údaje mohou být nepřesné z hlediska formálnosti, tedy důvodem může být existence gramatických či technických chyb. Nicméně i formálně přesné údaje, které v souvislosti se subjektem nevypovídají o pravdivém stavu mohou být nepřesné. Záleží na tom, zda se původně pravdivé údaje změnili vlivem okolností na nepravdivé, například původní dlužník, který již dluh splatil, je stále správcem evidován jako dlužník nebo pokud subjekt o sobě nahlásil nepravdivý údaj. Správce či zpracovatel musí přesnost osobních údajů sledovat a zajišťovat nejen při jejich shromažďování ale i v průběhu zpracování a jakmile dojde k závěru, že jsou údaje nepřesné, je povinen bez zbytečného odkladu tyto údaje upravit nebo vymazat. Povinnost aktualizace osobních údajů není ale žádným způsobem upravena, respektive není upraveno, jakým způsobem jí má správce či zpracovatel dosáhnout.

[88] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 110

Ze stanoviska ÚOOÚ[89] vyplývá, že správce či zpracovatel musí s přihlédnutím k rozsahu a okolnostem zpracování přijmout systém určitých opatření, které budou v budoucnu zajišťovat, že nebude docházet ke zpracování nepřesných či chybných osobních údajů.

Další zásadou, která je odvíjena od zásady účelového omezení je zásada omezení uložení a ta jako taková představuje povinnost správce či zpracovatele uchovávat osobní údaje pouze po dobu, jež je nezbytně nutná pro stanovený účel. V souladu se zásadou transparentnosti musí správce či zpracovatel splnit informační povinnost vůči subjektu údajů tím, že jasně vymezí dobu, po kterou budou jeho osobní údaje zpracovávané. Doba zpracování však nesmí být stanovena jako doba zcela neurčitá[90], nicméně může být stanovena relativně, to znamená ve vztahu k určité události, o které prozatím přesně nevíme, kdy nastane.
Po uplynutí stanovené doby pro zpracování musí být osobní údaje vymazány, nicméně nikoli za předpokladu, budou-li nadále uchovávány za účelem vědeckého či historického výzkumu nebo pro statistické účely, což vytváří jedinou výjimku z této zásady.

Obecné nařízení mezi zásady nově zařazuje zásadu integrity a důvěrnosti, ta stanoví povinnost zpracování osobních údajů způsobem zajišťujícím jejich náležité zabezpečení prostřednictvím vhodných technických či organizačních opatření před náhodnou ztrátou, zničením či poškozením a zároveň vyloučí neoprávněné či protiprávní zpracování. Tato povinnost vyplývá z článku 32 Obecného nařízení, kde jsou také stanovena konkrétní kritéria pro zabezpečení. Povinnost vyplývající z této zásady byla obsažena již v předchozí unijní úpravě ochrany osobních údajů, stejně tak v národní úpravě v českém právním řádu, nicméně až Obecné nařízení integritu a důvěrnost řadí do základních zásad a tím potvrzuje, že zabezpečení osobních údajů je jednou z klíčových povinností při jejich zpracování.

[89] K problematice aktualizace zpracovávaných osobních údajů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/k-problematice-aktualizace-zpracovanych-osobnich-udaju/d-1595
[90] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 114

Klíčovou zásadou je také zásada odpovědnosti, kterou Obecné nařízení upravuje. Z této zásady vyplývají dvě základní povinnosti. Především stanoví, že je správce odpovědný za soulad se všemi výše uvedenými zásadami a ukládá mu povinnost řídit se všemi povinnostmi z nich vyplývajících. Zároveň je správce nově povinen soulad se zásadami a dodržování povinností doložit.[91] Tento princip je zásadní v tom, že přesouvá iniciativu na správce, jenž sám musí zavádět nové systémy ochrany a mít vše řádně zdokumentováno. Postoj správce v souvislosti s ochranou osobních údajů bude tedy muset být proaktivní, nikoli reaktivní.[92]

Nutno podotknout, že Obecné nařízení zmocňuje členské státy k omezení práv a povinností vyplývajících z výše uvedených zásad ale pouze za účelem dosažení určitých cílů uvedených v článku 23 Obecného nařízení a za předpokladu, že tato omezení nepředstavují zásadní zásah do základních práv a svobod a nepopírají základní zásady demokratické společnosti.

3.3 Právní tituly ke zpracování osobních údajů

Jak bylo uvedeno výše, být v souladu se zásadou zákonnosti znamená povinnost správce provádět zpracování na základě jednoho z vyjmenovaných právních titulů v článku 6 odst. 1. Právním titulem je podmínka, bez které není zpracování osobních údajů v žádném případě možné, respektive je od samotného počátku nelegální.[93] Zároveň se jedná o zákonem uznaný důvod pro přiměřený zásah do práva na soukromí. Spolu se stanovením účelu je také existence právního titulu ke zpracování klíčovým prvkem pro zamýšlené zpracování osobních údajů ze strany správce a jedním z prvních kroků, které musí učinit.

Obecné nařízení zcela mění pojetí a způsob využívání právních titulů ke zpracování. Oproti starým úpravám, které chápaly jako hlavní právní titul ke zpracování souhlas a ostatní právní tituly byly pouze alternativou, kdyby souhlas nebylo možné získat, staví Obecné nařízení právní tituly do rovnocenné pozice. Zároveň byl změněn i samotný výčet právních titulů, jelikož v Obecném nařízení

[91] Obecné nařízení o ochraně osobních údajů, článek 5 odst. 2
[92] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 119
[93] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 122

zcela chybí právní titul dle § 5 odst. 2 písm. d) zákona o ochraně osobních údajů, a to právní titul zpracování oprávněně zveřejněných osobních údajů. Stejně tak právní titul, který zákon upravoval v § 5 odst. 2 písm. f), právní titul poskytování osobních údajů o veřejně činných osobách. Neznamená to, že nebude možné tyto osobní údaje zpracovávat, bude ale nutné k takovému zpracování najít jiný právní titul, v praxi nejspíše oprávněný zájem. Nicméně v Obecném nařízení jsou také nově upraveny dva typy právního titulu, a to právní titul zpracování nezbytného pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci dle článku 6 odst. 1 písm. e).

3.3.1 Souhlas se zpracováním osobních údajů

Prvním právním titulem ke zpracování osobních údajů jmenovaným v Obecném nařízení je souhlas subjektu údajů. Jeho povaha se Obecným nařízením podstatně mění, jelikož v předchozích úpravách měl souhlas v podstatě dominantní postavení a nově by měl být používán spíše doplňkově a za předpokladu, nebude-li správce schopen využít jiného právního titulu.

Samotný souhlas lze charakterizovat jako právní jednání, vyjadřující svolení subjektu údajů ke zpracování jeho osobních údajů správcem. Mimo podmínek, které stanoví Obecné nařízení podléhá souhlas také podmínkám platnosti právního jednání vyplývajícím z občanského zákoníku a dopadá na něj také obecná úprava smluvního i zákonného zastoupení. Je tedy možné, aby souhlas za dítě udělil jeho zákonný zástupce.[94]

Podmínky pro udělení souhlasu se zpracováním osobních údajů jsou částečně vyjmenovány již v samotné definici souhlasu, kde se rozumí *"souhlasem subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů"*[95] a podmínky pro vyjádření souhlasu jsou podrobně rozebírány v článku 7 Obecného nařízení. Aby mohl být souhlas považován na svobodný, musí mít subjekt údajů reálnou možnost volby, zda

[94] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 125
[95] Obecné nařízení o ochraně osobních údajů, článek 4 odst. 11

souhlas udělí či neudělí. Zároveň nesmí být plodem zastrašování, nátlaku či předstírání nepravdivých skutečností a v případě neudělení souhlasu nesmí existovat riziko podstatných negativních důsledků pro subjekt údajů.

Mimo definici a popis podmínek pro vyjádření souhlasu samotné nařízení poskytuje několik praktických příkladů jmenovaných v recitálu číslo 43 Obecného nařízení, které demonstrují okolnosti, za kterých nebude souhlas možné považovat za svobodný. Prvním z těchto příkladů je udělení souhlasu v situaci, kdy mezi subjektem a správcem existuje jasná nerovnováha. Toto zejména platí, pokud je správcem orgán veřejné moci, kde je nerovnováha naprosto evidentní, a proto se až na výjimky nedoporučuje, aby orgány veřejné moci zpracovávaly osobní údaje právě na základě souhlasu subjektu údajů. Stejná situace může reálně vzniknout v situaci mezi zaměstnancem a zaměstnavatelem, kde nerovnováha z podstaty věci existuje také, a proto pokud zaměstnavatel zpracovává osobní údaje na základě souhlasu, musí se vyvarovat negativním důsledkům neposkytnutí souhlasu zaměstnancem.[96] Druhým příkladem rovněž popisovaným v recitálu 43, je situace kdy subjekt údajů nemá možnost vyjádřit souhlas pouze s některými dílčími operacemi zpracování, přestože je to v daném případě vhodné a možné. Třetím příkladem, který je popisován v článku 7 odst. 4 Obecného nařízení je situace, kdy je plnění smlouvy a poskytování služby z ní plynoucí závislé na poskytnutí souhlasu ze strany subjektu, byť to není pro účel plnění smlouvy nezbytné. Jedná se o tzv. podmíněný souhlas postavený na principu "take it or leave it", který byl v minulosti běžnou praxí a Obecné nařízení se tímto snaží tuto praktiku omezit. Typickým příkladem je uzavíraní smlouvy s bankovní institucí, která podmíní poskytnutí úvěru souhlasem se zpracováním osobních údajů za účelem marketingu. Tento udělený souhlas bude nesvobodný a v souladu s článkem 7 odst. 4 bude neplatný.

Forma udělení souhlasu není Obecným nařízením výslovně stanovena, nicméně povinnost doložit, že subjekt souhlas udělil v souladu s výše uvedenými požadavky stanovena je. V rámci ověřitelnosti lze s jistotou konstatovat, že pro správce bude ve většině případů nemožné získávat souhlasy se zpracováním ústní formou a správce bude nucen přistoupit k písemné formě souhlasu. Písemná forma neznamená nezbytně formu listinnou, souhlas lze zaznamenávat i v elektronické

[96] WP29, Opinion 15/2011 on the definition of consent

formě. Vždy je ale nutné být schopen doložit udělení souhlasu prostřednictvím záznamu, ze kterého musí vyplývat kdo souhlas udělil, tedy jméno či jiný identifikátor subjektu, kdy souhlas udělil, potvrzení o splnění informační povinnosti, tedy o čem všem byl subjekt před udělením souhlasu informován, také jakým způsobem byl souhlas udělen a případně údaj o tom, zda byl souhlas odvolán.[97]

Souhlas může být udělen písemným prohlášením subjektu údajů, pokud se ale týká i jiných skutečností, musí být subjektu zřejmé, že uděluje souhlas a v jakém rozsahu. Prohlášení o souhlasu by mělo být poskytnuto správcem ve srozumitelném a snadno přístupném znění za použití jednoduchého a jasného jazyka. Nemělo by také obsahovat nepřiměřené podmínky.[98] Žádost o vyjádření souhlasu předkládá subjektu údajů zpravidla správce a měl by zajistit, aby byla odlišitelná od zmíněných jiných skutečností. V praktické rovině to znamená, že by se měl vyvarovat umístění žádosti o souhlas například do obchodních podmínek, které bývají často nepřehledné a psané právnickým jazykem. Také ale jejich potvrzení vylučuje neudělení souhlasu a v tom případě by souhlas nebyl nepodmíněný a svobodný. Stejně tak by žádost o souhlas neměla být umístěna v adhézní smlouvě. Žádost o vyjádření souhlasu by tedy měla být srozumitelná a jasná i pro širokou veřejnost a měla by být umístěna v samostatném dokumentu.

Jak bylo uvedeno výše, souhlas již v Obecném nařízení není preferovaným právním titulem ke zpracování. Je to také z důvodu jeho nestability, jelikož právem subjektu údajů je kdykoli poskytnutý souhlas se zpracováním odvolat a tím správce ztrácí právní základ pro zpracování. Zároveň tím subjekt může uplatnit svoje další právo, a to právo na výmaz, což je realizace práva být zapomenut v Obecném nařízení. Nutno podotknout, že realizace práva být zapomenut není v úpravě osobních údajů ničím novým, v jeho souvislosti bylo výše popisováno revoluční rozhodnutí SDEU a samotné právo být zapomenut má v České republice ústavněprávní ochranu v článku 2 odst. 3 LZPS. V souladu s ním nesmí být předpisem na ochranu osobních údajů ukládána povinnost strpět zpracování osobních údajů za situace, kdy subjekt

[97] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 149
[98] Obecné nařízení o ochraně osobních údajů, recitál č. 42

se zpracováním nesouhlasí.[99] Odvolání souhlasu se zpracováním osobních údajů se dotýká také soukromoprávní úpravy § 87 odst. 1 občanského zákoníku, dle tohoto ustanovení, ten kdo svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkající se jeho osoby nebo projevů jeho osobní povahy, může toto svolení odvolat, třeba že je udělil na určitou dobu.[100]

Pokud dojde k odvolání souhlasu ze strany subjektu údajů je správce povinen vyhledat a odstranit veškeré osobní údaje zpracovávané na základě tohoto souhlasu, a to nejen v databázích a archivech, ale také například v komunikacích, kterou se subjektem vedl a všude jinde, kde se inkriminované osobní údaje mohou vyskytovat.[101] Jak vyplývá z článku 7 odst. 3 Obecného nařízení, odvolání souhlasu nesmí představovat náročnější proces a musí být stejně snadné jako jeho poskytnutí prostřednictvím stejných prostředků. Pokud je tedy souhlas udělen na webové stránce, jeho odvolání by mělo být umožněno stejným způsobem.

3.3.2 Plnění smlouvy

Co se týče plnění smlouvy, v současné době se jedná o pravděpodobně nejvyužívanější právní titul pro zpracování osobních údajů. Správci zpracovávají osobní údaje na základě právního titulu plnění smlouvy, pokud je samotné zpracování nezbytné pro plnění smluvního závazku nebo k jeho uzavření.[102] V těchto případech nemusí získávat další právní titul a zpracování je od počátku zákonné a legitimní. Správce je ale povinen stanovit účel dané smlouvy a osobní údaje zpracovávat pouze k jeho dosažení a nikoli tento účel svévolně překročit. Aby byl tento právní titul využíván správně, je tedy třeba vymezit elementární cíl konkrétního smluvního závazku a osobní údaje zpracovávat k jeho dosažení. Nelze

[99] K problematice odvolatelnosti souhlasu se zpracováním osobních údajů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/k-problematice-odvolatelnosti-souhlasu-se-zpracovanim-osobnich-udaju/d-10891
[100] Zákon č. 89/2012 Sb., občanský zákoník, § 87 odst.1
[101] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. str. 152
[102] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 126

tedy stanovit vedlejší účely a zpracování provádět na základě tohoto právního titulu jenom proto, že je takto vymezeno ve smlouvě.[103]

3.3.3 Plnění právní povinnosti

Ke zpracování osobních údajů může docházet také na základě plnění právní povinnosti, která správci vzniká přímo ze zákona nebo na jeho základě, v důsledku právní skutečnosti nebo rozhodnutím orgánu veřejné moci. Může nastat situace, že právní předpis členského státu či EU po správci požaduje, aby prováděl určitou činnost, pro kterou je zpracování osobních údajů nezbytné. Musí se tedy jednat o povinnost a nikoli pouhé oprávnění a musí vyplývat ze zákona s tím, že upřesněna může být i ve formou podzákonného předpisu. Z odst. 3 článku 6 Obecného nařízení vyplývá, že pokud je správci uložena povinnost na základě právního předpisu nebo rozhodnutím orgánu veřejné moci či při plnění úkolu prováděného ve veřejném zájmu, musí být tento základ stanoven právem EU nebo právem členského státu, které se vztahuje na konkrétního správce.[104] Nemůže se tedy jednat o povinnost vyplývající z právního předpisu třetí země. V právním předpisu musí být povinnost vymezena jasně a určitě, aby bylo možné identifikovat způsoby zpracování, které na jejím základě budou prováděna a správce by měl mít jasně vymezeno, jakým způsobem povinnost splní, aby nemohl účel vyplývající z dané povinnosti překročit. Zároveň musí být stanoven druh osobních údajů, které budou zpracovány, určení subjektů údajů a subjektů, kterým budou osobní údaje případně poskytnuty apod.

Typickým příkladem zpracování osobních údajů na základě plnění právní povinnosti jsou v praxi povinnosti zaměstnavatele, stanovené zákoníkem práce, například evidence pracovní doby, pracovních úrazů nebo povinnost předávat osobní údaje zaměstnanců zdravotním pojišťovnám.

[103]WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC
[104] Obecné nařízení o ochraně osobních údajů, článek 6 odst. 3

Specifické povinnosti stanoví například zákon č. 90/2012 Sb., zákon o obchodních korporacích. Dle § 139 tohoto zákona, je společnost s ručením omezeným povinna vést seznam společníků, kam se zapisuje jméno, bydliště nebo sídlo společníka, případně jiná společníkem určená adresa pro doručování.[105]
Dále společníkův podíl a jeho označení, odpovídající výše vkladu a počet hlasů, které tomuto podílu náleží a další povinné údaje. Stejně tak povinnost pro akciové společnosti, vyplývající z ustanovení § 264 tohoto zákona, ukládá vést seznam akcionářů.

3.3.4 Životně důležitý zájem

Za zákonné lze také považovat zpracování osobních údajů, které je nezbytné pro ochranu životně důležitého zájmu jak samotného subjektu údajů, tak i jiné fyzické osoby. Proto se jedná o další právní titul pro zpracování osobních údajů, nicméně pouze za předpokladu, že není možné využít jiného právního titulu. Samotný pojem není v Obecném nařízení nijak definován, nicméně recitál číslo 46 uvádí, že se jedná o situace, ve kterých je nezbytné zpracovávat osobní údaje v souvislosti s reálným ohrožením subjektu údajů nebo jiné fyzické osoby, které by mohlo mít dopad na život, zdraví či jiný zájem vnímaný jako životně důležitý. Nejčastěji se může jednat o zpracování osobních údajů nezbytné pro humanitární účely, monitorování epidemií a jejich šíření a v případech přírodních či člověkem způsobených katastrof.[106]

Obecné nařízení rozšiřuje možnost využití tohoto právního titulu, jelikož stanoví, že životně důležitý zájem není omezen jen na samotný subjekt údajů, jehož osobní údaje jsou zpracovány a lze ho tak využít i v situacích ohrožení jiné fyzické osoby.[107] Oproti staré úpravě odpadá povinnost dodatečného získání souhlasu subjektu údajů. Dříve totiž správce musel bezodkladně získat od subjektu údajů

[105] Právní titul a rozsah zpracování osobních údajů | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/pravni-titul-a-rozsah-zpracovani-osobnich-udaju-v-kapitalovych-spolecnostech-dle-zakona-o-obchodnich-korporacich-ve-svetle-gdpr-107512.html
[106] Obecné nařízení o ochraně osobních údajů, recitál č. 46
[107] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 129

dodatečný souhlas, jinak zpracování ukončit a osobní údaje vymazat, což mohlo být v těchto situacích problematické.

3.3.5 Oprávněný zájem správce a třetích osob

Pokud je zpracování osobních údajů nezbytné pro účely oprávněných zájmů správce nebo třetích osob a zároveň tímto zpracováním nedochází k zásahu do zájmů subjektu údajů, zejména do jeho práv a základních svobod, pak je správce kompetentní takové zpracování provádět. Je tedy nezbytné, aby správce již před zahájením zpracování osobních údajů na základě tohoto právního titulu důkladně posoudil, zda je jeho zájem opravdu oprávněný a zároveň zda nepřevažuje zájmy nebo práva a svobody subjektu údajů, jejichž osobní údaje mají být zpracovávány.

Předchozí právní úprava omezovala využívání tohoto právního titulu, jelikož umožňovala na jeho základě zpracování pouze v případě, pokud to bylo nezbytné za účelem ochrany práv či právem chráněných zájmů správce či třetí osoby. Muselo se jednat o ochranu konkrétního práva či právem chráněného zájmu, například vlastnictví. Obecné nařízení umožňuje, aby si správce vytvořil vlastní, subjektivní oprávněný zájem a na jeho základě osobní údaje zpracovával.[108]
Nicméně původní omezení stále trvá pro orgány veřejné moci při plnění svých veřejnoprávních úkolů a nově v tomto případě celkově zakazuje zpracování osobních údajů na základě oprávněného zájmu. Pokud tedy orgány veřejné moci při plnění svých úkolů zpracovávali osobní údaje na základě oprávněného zájmu, musí pro toto zpracování najít jiný právní titul, kterým je ve většině případů plnění právní povinnosti nebo zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci. Toto omezení neplatí v situacích, kdy orgán veřejné moci vystupuje v soukromoprávní rovině[109], například při ochraně vlastnictví využívá kamerového systému, v tomto případě bude zpracování osobních údajů na základě oprávněného zájmu legální.

[108] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 132
[109] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. str. 132

Dle stanoviska WP29, lze zpracování osobních údajů na základě oprávněného zájmu provádět jen za předpokladu, provedl-li správce souhrnné posouzení několika hledisek. [110] Správce musí posoudit, zda je jeho zájem opravdu oprávněný a zda splňuje požadované kvality, dále zda je vzhledem k účelu zpracování osobních údajů na základě tohoto právního titulu skutečně nezbytné a také zda nad jeho oprávněný zájem nepřevažují zájmy a základní práva a svobody subjektů údajů. Zároveň musí přesně definovat svůj oprávněný zájem. Na rozdíl od účelu, kterým se myslí spíše konkrétní důvod zpracování, zájmem je širší angažovanost správce nebo výhoda, která vznikne správci na základě tohoto zpracování.[111]

Obecně lze oprávněné zájmy dělit podle kritéria jejich váhy do tří základních skupin, přičemž toto dělení má i praktický význam pro samotné správce. Do první skupiny oprávněných zájmů, lze zařadit ty, které mají sloužit ochraně výkonu základních práv a svobod správce. Jedná se například o svobodu projevu, svobodu podnikání a práva na informace. Z podstaty věci mají největší právní váhu, byť i na jejich základě nelze osobní údaje zpracovávat neomezeně. Druhou skupinu oprávněných zájmů tvoří zájmy širšího okruhu adresátů než jen ty správce a zájmy veřejné. Může se například jednat o různé druhy dobročinné činnosti. Zároveň mezi ně lze zařadit činnost podnikajících osob za účelem předcházení zneužívání služeb. Co se týče subjektivních oprávněných zájmů správce, které tvoří třetí skupinu, jedná se o ty ostatní oprávněné zájmy správce, které nepatří do předchozích dvou skupin. Z recitálu číslo 47 Obecného nařízení konkrétně vyplývá, že se v praxi může jednat zejména o potřeby přímého marketingu či snahu zamezení podvodům. Za další praktické příklady lze uvést ochranu majetkových zájmů zaměstnavatele při monitorování zaměstnanců či fyzická, IT a síťová bezpečnost.[112]

3.3.6 Úkol ve veřejném zájmu nebo výkon veřejné moci

Zpracování osobních údajů, které je nezbytné pro splnění úkolů ve veřejném zájmu nebo pro výkon veřejné moci je v Obecném nařízení upraveno oproti starým úpravám nově, a to v článku 6 odst. 1 písm. e). Směrnice 95/46/ES sice tento právní

[110] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC
[111] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str.133
[112] Obecné nařízení o ochraně osobních údajů, recitál číslo 49

titul obsahovala, nicméně zákon o ochraně osobních údajů nikoli, orgány veřejné moci prováděli tento typ zpracování na základě plnění právní povinnosti. Z podstaty věci slouží tento typ právního titulu ke zpracování osobních údajů převážně orgánům veřejné moci, nicméně jej mohou využívat i soukromoprávní subjekty za předpokladu, že jsou pověřeni výkonem určitého veřejnoprávního úkolu, například Stanice technické kontroly, kterým je veřejná moc delegována.

Ve zpracování osobních údajů orgány veřejné moci na základě plnění právní povinnosti a zpracováním nezbytným pro splnění úkolu ve veřejném zájmu je podstatný rozdíl, který spočívá ve specifikaci vyplývající ze zvláštního předpisu, který je ke zpracování osobních údajů zmocňuje. Pokud zpracování probíhá na základě plnění právní povinnosti, musí z ní plynout plnění konkrétní povinnosti a správce nesmí mít na výběr, zda povinnost splní či ne. Oproti tomu, pokud správce zpracovává osobní údaje při plnění úkolu ve veřejném zájmu nebo pro výkon veřejné moci, je mu udělen určitý úkol ve veřejném zájmu a je předmětem stanovené diskrece zvolit, jakým způsobem bude úkol splněn. Pokud při tomto způsobu vyplyne potřeba zpracovávat osobní údaje, lze tak provést na základě tohoto právního titulu. Zároveň platí, že správci, orgány veřejné moci nebo subjekty výkonem veřejné moci pověřené, nemohou tohoto právního titulu využívat v libovolném rozsahu. Mohou tento právní titul využívat pouze za takovými účely, které přímo směřují k plnění jejich úkolů veřejné správy.[113]

3.4 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů (pověřenec) je na poli ochrany osobních údajů specifickým institutem, který Obecné nařízení nově upravuje a ukládá některým správcům a zpracovatelům povinnost jeho jmenování. Jedná se o osobu s odbornými znalostmi v oblasti právních předpisů a postupů týkající se ochrany osobních údajů, která by měla dohlížet na dodržování souladu s Obecným nařízením a být správci či zpracovateli nápomocná při plnění jeho povinností souvisejících se zpracováním.[114]

[113] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 131
[114] Obecné nařízení o ochraně osobních údajů, recitál č. 97

Funkce pověřence je pro většinu členských států EU novinkou, nicméně koncept této funkce nebyl zaveden až samotným Obecným nařízením, jelikož se v různých formách objevovala v národních úpravách některých členských států. Konkrétně byl upravován národní úpravou v Německu, Francii, Polsku, Slovinsku a částečně na Slovensku, kde sice správci povinnost jmenovat pověřence neměli, nicméně pokud tak učinili, poskytovalo jim to určité výhody.[115]

3.4.1 Povinnost jmenovat pověřence pro ochranu osobních údajů

Povinnost jmenovat pověřence, nemají zdaleka všichni správci a zpracovatelé, jak bylo v období legisvakance často mylně předesíláno. Tato povinnost vyplývá z článku 37 odst. 1 pro ty správce a zpracovatele, kteří naplní alespoň jednu z podmínek zde vyjmenovaných. Jedná se o soubor podmínek, které vymezují situace představující zvýšené riziko plynoucí ze zpracování osobních údajů, a proto je dle Obecného nařízení nutné, aby na takové zpracování dohlížela nezávislá osoba.

V prvním případě se jedná o *"zpracování, které provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci své pravomoci"*.[116] Byť není Obecným nařízením, ani jiným unijním předpisem jasně definován pojem *"orgán veřejné moci",* z praxe a nálezů Ústavního soudu[117] lze dovodit, že se bude jednat o právnické osoby, zřízeny k trvalému a opakujícímu výkonu činnosti, který spočívá v autoritativním rozhodování o právech a povinnostech jiných subjektů.[118] V praxi se jedná o ministerstva a jiné ústřední správní úřady, obce a kraje při výkonu přenesené působnosti. Veřejné subjekty lze chápat jako veřejnoprávní korporace, veřejné ústavy a podniky. WP29 však ve svém stanovisku stanoví pouze doporučení, nikoli povinnost pověřence jmenovat.[119] Výjimka pro soudy vyplývající z tohoto článku se týká ovšem pouze zpracování, které soudy provádí v

[115] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 332
[116] Obecné nařízení o ochraně osobních údajů, článek 37 odst. 1 písm. a)
[117] Nález Ústavního soudu ze dne 10. 11. 1998, sp. zn. I. ÚS 229/98.
[118] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 333
[119] WP29 Guidelines on Data Protection Officers ('DPOs'), str. 6

rámci jejich soudních pravomocí, pokud budou provádět jiný typ zpracování osobních údajů z pozice orgánu veřejné moci budou povinni pověřence jmenovat.

Správci a zpracovatelé jsou povinni jmenovat pověřence také v situaci, kdy jejich *"hlavní činnost spočívá v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů."*[120] Zde je třeba správné a přesné vymezení pojmu hlavní činnost, a právě toto ustanovení činilo v období legisvakance výkladové problémy, nebylo tedy často jasné, zda správci budou povinni pověřence jmenovat či nikoli. Z recitálu číslo 97 Obecného nařízení vyplývá, že hlavní činností se rozumí taková činnost v soukromém sektoru, která souvisí s jeho primární činností a nevztahuje se na zpracování osobních údajů jakožto činnost pomocnou. Je to tedy primární aktivita správce či zpracovatele, pro kterou byl zřízen a tvoří hlavní předmět jeho podnikatelské činnosti, tedy jeho hlavní cíl. Pokud by správce či zpracovatel takovou činnost zpracování neprováděl, nebyl by schopen naplňovat svou primární podnikatelskou činnost. Jedná se například o činnost bezpečnostních agentur, které prostřednictvím kamerových systémů vykonávají dohled na veřejně přístupnými prostory. Dle stanoviska WP29, lze do hlavní činnosti zařadit také aktivity, které od ní nelze oddělit. Spolu s hlavní činností je podmínkou pro jmenování pověřence také provádění rozsáhlého a systematického zpracování, což je další pojem, který Obecné nařízení nevymezuje zcela přesně. Určité vodítko lze nalézt v recitálu číslo 91 Obecného nařízení, které se ovšem věnuje posouzení vlivu na ochranu osobních údajů (DPIA), nicméně s tímto pojmem úzce souvisí a dle kterého se jedná o: "*rozsáhlé operace zpracování, jež mají sloužit ke zpracování značného množství osobních údajů na regionální, celostátní nebo nadnárodní úrovni, jež by mohly mít dopad na velký počet subjektů údajů a u nichž je pravděpodobné, že budou představovat vysoké riziko"*[121] a zároveň stanoví, že zpracování osobních údajů osobních pacientů nebo klientů, jednotlivými lékaři, zdravotníky či právníky, by nemělo být považováno za zpracování velkého rozsahu. Nejednoznačnost tohoto pojmu potvrzuje i WP29 ve svém stanovisku k pověřencům kde uvádí, že není možné vymezit přesná čísla co se týče množství zpracovávaných osobních údajů nebo jejich subjektů, aby byl použitelný ve všech

[120] Obecné nařízení o ochraně osobních údajů, článek 37 odst. 1 písm. b)
[121] Obecné nařízení o ochraně osobních údajů, recitál číslo 91

situacích. Uvádí pouze doporučující kritéria, při určování, zda je zpracování rozsáhlé či není. Správce by měl brát ohled na počet dotčených subjektů, tedy buďto konkrétní nebo procentuální v souvislosti s určitou populací, dále objem celkových dat, dobu trvání zpracování a jeho územní rozsah. [122]

Dalším Obecným nařízením nedefinovaným pojmem je pravidelné a systematické monitorování subjektů údajů, což je také další podmínka pro jmenování pověřence správcem. Obecně lze za monitorování považovat jakoukoli aktivitu spočívající ve sledování subjektů údajů či jejich chování, a to bez ohledu na to, jestli k němu dochází fyzicky nebo v prostředí internetu.[123] Může se jednat například o provozování telekomunikační sítě, behaviorálního marketingu, monitorování určitého prostoru pomocí kamerového systému nebo sledování polohy na základě lokalizačních údajů. K pojmům pravidelné a systematické dává opět vodítko stanovisko WP29 k pověřenci. Pravidelným se myslí, pokud monitorování probíhá v určitých intervalech po určitou dobu, opakovaně v daný čas. Pokud probíhá systematicky, jedná se o monitorování, které je uspořádané, organizované nebo metodické nebo pokud je prováděno jako součást určité strategie.[124]

Třetí kategorie správců či zpracovatelů povinných jmenovat pověřence jsou ti, kteří provozují *"hlavní činnost spočívající 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."*[125] V tomto ustanovení může být zavádějící, který typ osobních údajů musí správce zpracovávat, aby měl povinnost pověřence jmenovat, jelikož jsou oba typy odděleny spojkou "a". Dle stanoviska WP29 povinnost platí pro správce, kteří zpracují buďto zvláštní kategorii osobních údajů nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů, neplatí tedy, že by musel zpracovávat oba tyto druhy osobních údajů zároveň.

V situacích, kdy si správce či zpracovatel nebude zcela jistý, zda do některé z uvedených kategorií patří a zda na něj povinnost jmenování pověřence dopadá, může zvolit cestu dobrovolného jmenování. I v tomto případě bude jmenovaný

[122] WP29 Guidelines on Data Protection Officers ('DPOs') str. 7
[123] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 335
[124] WP29 Guidelines on Data Protection Officers ('DPOs') str. 8
[125] Obecné nařízení o ochraně osobních údajů, článek 37 odst. 1 písm. c)

pověřenec muset plnit všechny požadavky a povinnosti vyplývající z Obecného nařízení, včetně jeho nezávislosti, neexistence konfliktu zájmů, dostatečného proškolení apod.[126] Dobrovolné jmenování ale může být pro správce výhodou, jelikož zajistí přítomnost osoby, která bude neustále posuzovat soulad s Obecným nařízením, mimo to tím dá jasně najevo, že nebere ochranu osobních údajů na lehkou váhu.

3.4.2 Kvalifikace pověřence

Na pověřence jsou v článku 37 odst. 5 kladeny určité nároky, kvalifikační předpoklady, spočívající zejména ve znalostech práva a praxe z oblasti ochrany osobních údajů, což k povaze této funkce není ničím překvapivým. Prvním z těchto předpokladů, je dostatečná úroveň znalostí v oblasti práva ochrany osobních údajů, konkrétně tedy národních a evropských předpisů, zejména Obecného nařízení. Úroveň odborných znalostí pověřence, by měla odpovídat náročnosti a povaze prováděného zpracování. Také ale citlivosti a množství osobních údajů, které správce nebo zpracovatel zpracovává. Žádoucí je také dostatečná znalost všech jednotlivých procesů zpracování, která správce provádí, stejně tak informace o jejich zabezpečení, zároveň znalost oboru podnikání správce či zpracovatele je pro pověřence nezbytná. Znalosti a profesní kvality pověřence musí být na té úrovni, aby byl schopen plnit úkoly stanovené Obecným nařízením, k tomu také musí v organizaci správce disponovat dostatečnými pravomocemi, nezbytnými pro plnění těchto úkolů.[127]

Co se týče úrovně dosaženého vzdělání, není Obecným nařízením výslovně stanovena, není tedy nutné, aby měl pověřenec vysokoškolské vzdělání nebo být absolventem nějaké profesní zkoušky. Není stanovena ani jiná specifická forma prokázání profesních kvalit pověřence, například ve formě certifikátu o absolvování nějakého kurzu. Nicméně dle stanoviska WP29 se doporučuje pořádání pravidelných vzdělávacích seminářů a náležité proškolování v oblasti ochrany osobních údajů, hlavně ze strany dozorových orgánů, byť nejsou povinni takto činit.

[126] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 336
[127] WP29 Guidelines on Data Protection Officers (‘DPOs’) str. 11

Český dozorový orgán ÚOOÚ pořádá dílčí semináře ochrany osobních údajů věnované obvykle konkrétnímu resortu, ale placené kurzy a certifikace jsou v tuzemsku pořádány hlavně ze strany soukromoprávních subjektů, jež tuto formu vzdělávání přijaly jako velice výnosnou formu podnikatelské činnosti, zvláště v období legisvakance před účinností Obecného nařízení.

Ze stanoviska WP29 také vyplývá, že není možné stanovit přesné profesní nároky a univerzální kritéria pro určení nejvhodnějšího kandidáta na tuto funkci. Je vždy nutné zohlednit specifické vlastnosti daného správce, množství osobních údajů a rozsah a složitost daného zpracování, které provádí. Zároveň by měl pověřenec zastávat určitý standard morálních hodnot a etiky, jenž mu umožní v rámci dané organizace vybudovat potřebnou kulturu ochrany osobních údajů.[128]

3.4.3 Postavení pověřence

Obecné nařízení ve svém článku 38 upravuje postavení pověřence jak v rámci dané organizace správce či zpracovatele, tak jeho fungování navenek. Dle odst. 1 tohoto článku, je nezbytné zapojení pověřence do veškerých záležitostí související s ochranou osobních údajů správce, zejména do veškerých procesů zpracování.

WP29 doporučuje za účelem efektivního zapojení správce nastavení určitých postupů. Pověřenec by měl být účasten schůzí středního a vyššího managementu, zejména těch, kde jsou přijímána rozhodnutí mající na ochranu osobních údajů dopad. Měl by být řádně a včas informován o veškerém i zamýšleném zpracování. Pověřencova stanoviska ke zpracování by měla být dodržována, pokud se správce rozhodne od nich odchýlit, pak tento krok náležitě odůvodnit. Pokud dojde k porušení ochrany osobních údajů ze strany správce či zpracovatele, musí o tom být pověřenec bezodkladně informován. Veškeré postupy, které mají být konzultovány s pověřencem, by měli být stanoveny v interní směrnici o ochraně osobních údajů.[129]

[128] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 340
[129] WP29 Guidelines on Data Protection Officers (‘DPOs’) str. 12

Odst. 2 článku 38 dává správci či zpracovateli povinnost podporovat pověřence při plnění jeho úkolů a poskytovat mu k tomu náležité zdroje. Zároveň musí poskytnout zdroje k přístupu k osobním údajům a operacím jejich zpracování a také k udržování jeho odborných znalostí. Správce či zpracovatel by měl tuto povinnost plnit zejména aktivní podporou ze strany vyššího managementu, který by měl pověřenci poskytovat dostatečnou časovou kapacitu ale také dostatečnou finanční a personální podporu.[130]

Nezávislost funkce pověřence vyplývá z odst. 3 tohoto článku, jelikož dle něj pověřenec nesmí přijímat žádné pokyny týkající se plnění jeho úkolů ze strany správce. Nesmí být instruován ohledně vykonávání jeho funkce a nesmí mu být podsouván odlišný právní názor, obvykle výhodnější pro správce.
Zároveň nesmí dojít k situaci, ve které by se pověřenec dostal do střetu zájmů. Pokud se správce rozhodne jmenovat pověřence z řad vlastních zaměstnanců, nesmí být pověřenec v pozici, ve které zároveň schvaluje či určuje operace a prostředky zpracování, jelikož by ze své funkce pověřence kontroloval i svou vlastní činnost.

Pověřenec také slouží jako kontaktní osoba pro subjekty údajů.[131] Subjekty údajů se na pověřence mohou obracet ve všech záležitostech a otázkách týkající se zpracování osobních údajů, zároveň u něj mohou uplatňovat svá práva dle Obecného nařízení. Pověřenec je také dle odst. 5 vázán mlčenlivostí v souladu s právem EU nebo členského státu. Obecně lze předpokládat, že je pověřenci zakázáno takové jednání, prostřednictvím kterého by se mohla neoprávněná osoba seznámit s informacemi, jež pověřenec získal v souvislosti s plněním svých úkolů.[132] Zároveň se mlčenlivost vztahuje na samotné osobní údaje, také na prostředky jejich zabezpečení a jiné důvěrné informace správce či zpracovatele.

[130] WP29 Guidelines on Data Protection Officers (‘DPOs’) str. 12
[131] Obecné nařízení o ochraně osobních údajů, článek 38 odst. 4 GDPR
[132] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 347

3.4.4 Úkoly pověřence

Obecné nařízení ve svém článku 39 dost. 1 písm a) až e) jmenuje úkoly, které je pověřenec ze své funkce povinen vykonávat. Vyjmenovaný výčet je spíše demonstrativní, jelikož se jedná o minimum činností, které lze po pověřenci vyžadovat a správce či zpracovatel je oprávněn přidělit pověřenci i další úkoly, související s ochranou osobních údajů a jejich zpracováním. Vždy musí ale zvážit, zda spolu s nimi bude pověřenec schopen vykonávat úkoly stanovené Obecným nařízením a že v souvislosti s nimi nepřijde do střetu zájmů.

Pověřenec musí poskytovat informace a poradenství správcům či zpracovatelům, včetně jejich zaměstnanců. Vzhledem k výše uvedeným profesním kvalitám, by měl pověřenec schopen své znalosti zprostředkovat i ostatním a umět Obecné nařízení vyložit všem zaměstnancům správce či zpracovatele. V případě nejistého výkladu by měl být schopen radit ohledně povinností vyplývajících z Obecného nařízení, také je vyložit, vysvětlit a pomoci aplikovat v praxi. Zároveň by měl sám aktivně zaměstnance poučit, informovat a proškolovat v oblasti ochrany osobních údajů, převážně prostřednictvím organizace nejrůznějších školení. V ideálním případě vypracovat interní směrnici pro ochranu osobních údajů, nebo jiný dokument obsahující návody, mechanismy a postupy při zpracování osobních údajů, a to vždy na míru dle potřeb konkrétního správce či zpracovatele.

Dalším úkolem stanoveným v písm. b) je monitorování souladu s Obecným nařízením. Pověřenec by měl sbírat informace o zpracování a identifikovat jeho jednotlivé procesy, na jejichž základě posoudit, zda je takové zpracování v souladu s Obecným nařízením. V souvislosti s monitorováním by měl správci poskytovat odborné rady a doporučení vedoucí k zajištění souladu.

Pokud správce zvažuje provedení posouzení vlivu na ochranu osobních údajů dle článku 35 Obecného nařízení, je povinen vyžádat si od správce jeho odborné stanovisko. Dle WP29 by ze stanoviska pověřence mělo vyplývat, zda je nebo není nutné posouzení vlivu provést a pokud ano, jakou metodiku pro provedení posouzení vlivu zvolit. Dále zda je správce schopen posouzení vlivu provést sám nebo zda pověřenec doporučuje jeho vypracováním pověřit externistu. Také jaká ochranná, technická a organizační opatření pověřenec doporučuje uplatnit pro

zmírnění rizik vůči právům a zájmům subjektů údajů. Pokud bylo posouzení vlivu provedeno, měl by pověřenec zhodnotit jeho správnost a soulad s Obecným nařízením.[133]

Další pověřencova povinnost vyplývající z písm. d) a e) je spolupráce s dozorovým orgánem a povinnost fungovat jako kontaktní osoba pro dozorový úřad. S tím souvisí poskytnutí potřebné součinnosti při provádění kontrolní, nápravné či povolovací pravomoci úřadu. Pověřenec může dozorový úřad žádat o rady a konzultovat s ním jakoukoli problematiku související s ochranou osobních údajů či jejich zpracováním.

3.4.5 Interní a externí pověřenec

Právní postavení pověřence pro ochranu osobních údajů může být stanoveno dvojím způsobem. Z článku 37 odst. 6 Obecného nařízení vyplývá, může být pracovníkem správce či zpracovatele nebo může funkci pověřence vykonávat na základě smlouvy o poskytování služeb externí osoba. Volba, kterou z uvedených možností správce či zpracovatel využije je čistě na něm, jelikož Obecné nařízení nestanoví konkrétní situace, ve kterých je nutné jmenovat buď interního či externího pověřence. Sám může tedy uvážit, která z těchto možností je pro něj vhodnější, vždy s přihlédnutím k okolnostem a povaze jím prováděného zpracování.

Interního pověřence, buďto z řad svých zaměstnanců nebo nově přijatého, jmenují v praxi nejspíše větší správci a zpracovatelé, jež disponují velkými prostředky a provádějí složitější zpracování velkého rozsahu. Výhodou bude bezesporu znalost procesů, informačních systémů a chodu samotné organizace. V případě velkých správců či zpracovatelů bude pověřenec obvykle vytížen plněním svých úkolů a nebude moci vykonávat žádné doprovodné činnosti. Správce by měl zajistit, aby pověřenci nebyli přidělovány jiné úkoly nesouvisející s ochranou osobních údajů, tím také zajistí, že nenastane situace, ve které by se pověřenec dostal do střetu zájmů. Interní pověřenec vykonává svou funkci na základě pracovní smlouvy a

[133] WP29 Guidelines on Data Protection Officers (‘DPOs’) str. 16

právní režim tohoto vztahu se bude řídit zákoníkem práce, bude ovšem nutné zajistit zvláštní ochranu proti ukončení pracovního poměru.[134]

Druhou alternativou je jmenování externího pověřence pro ochranu osobních údajů, kterou pravděpodobně využívají spíše menší a střední organizace, pro které by zřízení funkce interního pověřence mohlo být příliš finančně náročné, zároveň neprovádí zpracování na takové úrovni, aby mohli interního pověřence plně vytížit. Pokud správce jmenuje pověřence externího, přímo tím předejde potencionálnímu střetu zájmů. Nevýhodou může ale být skutečnost, že externí pověřenec nebude mít tak rozsáhlou znalost interních procesů a chodu organizace správce či zpracovatele. Vztah externího pověřence a správce či zpracovatele se řídí smlouvou o poskytování služeb, což je soukromoprávní smlouva obsahující označení osoby, která funkci pověřence vykonává. Může se jednat i o osobu právnickou. Také jasné vymezení úkolů pověřence, dále ujednání záruky nezávislosti výkonu funkce pověřence, zahrnující povinnost oznámit případný střet zájmů a také závazek o zachování mlčenlivosti.[135]

Nutno podotknout, že osoba pověřence nesmí být dle článku 38 odst. 3 v souvislosti s plněním svých úkolů propuštěn ani sankciován. Toto je další ustanovení, které zajišťuje nezávislost funkce pověřence. Pověřenec tedy nesmí být žádným způsobem postihován za výkon své funkce, nicméně za porušení povinností dle zákoníku práce, například za porušení pracovněprávních předpisů ano. Zároveň není vyloučen nárok na náhradu škody způsobenou pověřencem, jelikož náhrada škody je prostředek kompenzační, nikoli sankční.[136]

Obecné nařízení také dává možnost jmenovat skupině podniků jediného a společného pověřence, vždy s přihlédnutím k jejich velikosti a struktuře. Článek 37 odst. 3 tuto možnost dává i orgánům veřejné moci a veřejným subjektům.

---

[134] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 341

[135] Pověřenec pro ochranu osobních údajů - Ochrana osobních údajů. Úvodní strana - Ministerstvo vnitra České republiky [online]. Copyright © 2019 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/poverenec-pro-ochranu-osobnich-udaju-poverenec-pro-ochranu-osobnich-udaju.aspx

[136] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 345

Obecné nařízení nestanoví konkrétní počet správců či zpracovatelů, kteří mohou mít jednoho společného pověřence, nicméně dle doporučení Ministerstva vnitra[137], by jeden pověřenec neměl být jmenován pro více jak 10 správců, v tomto případě obcí. Dle stanoviska WP29 by také společný pověřenec neměl sídlit mimo EU, byť správce či zpracovatel sídlo mimo EU mají.

Dle studie IAPP by bylo pro dosažení globálního souladu s Obecným nařízením na území EU, v souvislosti s povinností jmenovat pověřence osobních údajů nutné přijmout 28 000 nových pověřenců.[138] Autor je proto názoru, že využívání externích, a hlavně sdílených pověřenců bude častou praxí, jelikož jen na území České republiky funguje nespočet soukromoprávních subjektů, kteří zastávají funkci pověřence jakožto externí služby. Tuto službu poskytují převážně advokátní kanceláře, nicméně i konzultační společnosti nově se specializující na ochranu a zabezpečení dat a osobních údajů.

3.5 Porušení zabezpečení osobních údajů

Obecné nařízení ve svém článku 33 odst. 1 zavádí nově povinnost pro všechny správce osobních údajů, jedná se o povinnost ohlašovat porušení zabezpečení osobních údajů dozorovému úřadu. Porušením zabezpečení osobních údajů se rozumí situace, která vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.[139] Povinnost ohlašování porušení zabezpečení se již v Českém právním řádu vyskytuje v zákoně č. 127/2005 Sb., o elektronických komunikacích a platí pouze pro povinné subjekty, stejně tak v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti.

[137] Pověřenec pro ochranu osobních údajů - Ochrana osobních údajů. Úvodní strana - Ministerstvo vnitra České republiky [online]. Copyright © 2019 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/poverenec-pro-ochranu-osobnich-udaju-poverenec-pro-ochranu-osobnich-udaju.aspx
[138] IAPP. *Study: At least 28,000 DPOs needed to meet GDPR requirements* [online]. IAPP © 2019 [cit. 28.03.2019]. Dostupné z: https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/
[139] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 296

Správce je povinen ohlásit porušení zabezpečení bez zbytečného odkladu, pokud možno do 72 hodin od incidentu nebo od okamžiku, kdy se o něm správce dozvěděl. Výjimkou je situace, kdy není pravděpodobné, že by porušení zabezpečení mohlo mít za následek riziko pro práva a svobody fyzických osob, pak není správce povinen incident hlásit, nicméně i tak je povinen porušení zabezpečení řádně zdokumentovat. Například porušení zabezpečení osobních údajů, které jsou již veřejně dostupné a dohledatelné.[140]

Dle stanoviska WP29 v praxi pravděpodobně dochází ke třem základním druhům porušení zabezpečení. Pokud porušení vede k neoprávněnému zveřejnění či zpřístupnění osobních údajů, jedná se o porušení důvěrnosti - "*confidentiality breach."* Také může dojít k porušení dostupnosti osobních údajů - "*availability breach"* ve chvíli, kdy dojde ke ztrátě přístupu k osobním údajům, případně k jejich zničení či ztrátě osobních údajů samotných. Poslední případ je porušení integrity - *"integrity breach"* v případě, že dojde k neoprávněnému pozměnění osobních údajů. [141]

Porušení zabezpečení osobních údajů může pro jejich subjekty představovat újmu různého charakteru. V recitálu číslo 85 Obecného nařízení jsou uvedeny příklady možných následků, které mohou být fyzickým osobám způsobeny: *"fyzická, hmotná či nehmotná újma, jako je ztráta kontroly nad jejich osobními údaji nebo omezení jejich práv, diskriminace, krádež nebo zneužití identity, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti, ztráta důvěrnosti osobních údajů chráněných služebním tajemstvím nebo jakékoliv jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob."*[142]

Zmiňovaná povinnost ohlašovat případy porušení zabezpečení se však vztahuje pouze na správce osobních údajů, nicméně zpracovatel osobních údajů je dle článku 33 odst. 2 povinen bez zbytečného odkladu ohlásit porušení zabezpečení správci. Dle článku 34 Obecného nařízení, je správce v některých případech také povinen oznámit porušení zabezpečení osobních údajů samotným subjektům údajů, pokud je pravděpodobné, že porušení zabezpečení bude mít za následek vysoké riziko pro

[140] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679
[141] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679
[142] Obecné nařízení o ochraně osobních údajů, recitál číslo 85

práva a povinnosti fyzických osob. Správce je povinen analyzovat dopad porušení zabezpečení a posoudit újmu hrozící subjektům údajů. Může dojít k situacím, že dozorový úřad nařídí, aby správce incident oznámil subjektu údajů, i když ten hrozící rizika neshledal, jelikož správce má povinnost porušení zabezpečení úřadu nahlásit. Dle článku 34 odst. 4 dozorový úřad může na základě vlastního vyhodnocení posouzení rizik dospět k závěru, že správce musí oznámit porušení zabezpečení. Zároveň může dozorový úřad shledat, že byla naplněna jedna z níže uvedených podmínek a oznámení porušení zabezpečení subjektům údajů není nutné.

Odst. 3 tohoto článku stanoví podmínky, za kterých není správce povinen incident hlásit subjektu údajů, jedná se tedy o možné výjimky z této povinnosti. Dle písm. a) se oznámení subjektům údajů nevyžaduje, zavedl-li správce náležitá technická a organizační ochranná opatření, které následně použil u osobních údajů dotčených porušením zabezpečení. Zejména se jedná o situace, kdy tato ochranná opatření zajišťují nesrozumitelnost osobních údajů, v praktické rovině toto zajistí použití pseudonymizace a šifrování osobních údajů. Může jednat o případ, kdy došlo k odcizení přenosného pevného disku, který obsahoval velké množství osobních údajů. Ten byl však zašifrován a klíč nezbytný k jeho dešifrování má k dispozici pouze majitel pevného disku a jeho nadřízený a nehrozí tedy zpřístupnění osobních údajů nepovolaným osobám. V tomto případě bude podmínka dle článku 34 odst. 3 písm. a) naplněna a není nutné porušení zabezpečení oznamovat subjektům údajů. Nicméně správce má i tak povinnost o tomto porušení evidovat záznam.

Druhá podmínka vyplývající z písm. b) odst. 3 článku 34 Obecného nařízení stanoví, že pokud již k porušení zabezpečení určitým způsobem došlo, nicméně správce přijal následná opatření zajišťující eliminaci rizik pro subjekty údajů, které se díky tomuto opatření pravděpodobně neprojeví, není povinen incident oznámit subjektům údajů. Příkladem může být situace, kdy byl u správce osobních údajů zaznamenán hackerský útok, způsobující únik přihlašovacích jmen a hesel k jeho online službě. Správce bezprostředně po útoku provedl reset těchto přihlašovacích údajů a zkontroloval protokoly o přístupech do online služby. Pokud nebyl v mezidobí evidován žádný přístup, může správce vyhodnotit, že k újmě subjektů údajů nedošlo a porušení zabezpečení není povinen subjektům oznamovat.

Třetí případ, kdy nemusí správce oznamovat porušení zabezpečení subjektům údajů, lze aplikovat, pokud by pro správce osobních údajů znamenalo nepřiměřené úsilí toto oznámení provést. Například za předpokladu, nemá-li správce osobních údajů možnost dotčené subjekty údajů přímo kontaktovat. Je-li ale pro správce možné s přiměřeným úsilím kontaktní údaje subjektů získat například od jiného správce, není tato výjimka aplikovatelná.[143] I za předpokladu, že není správce schopen oznámení porušení zabezpečení provést přímo kontaktováním subjektů, je povinen subjekty údajů informovat například prostřednictvím veřejného oznámení na svých webových stránkách a tím splnit informační povinnost.

3.5.1 Zásada nemo tenetur ipsum accusare

V souvislosti s výše uvedenou povinností ohlášení porušení zabezpečení, si autor pokládá otázku, zda tento postup není v rozporu s jednou ze základních zásad právního státu a to zásadou *"nemo tenetur ipsum accusare"*, neboli *"nikdo není povinen sám sebe obviňovat"*. Tato zásada je zakotvena v LZPS v článku 37 odst. 1, který stanoví, že *"Každý má právo odepřít výpověď, jestliže by jí způsobil nebezpečí trestního stíhání sobě nebo osobě blízké".* Zároveň také v článku 40 odst. 4 LZPS, ze kterého vyplývá právo obviněného odepřít výpověď a také, že jej nesmí být žádným způsobem zbaven. Tato zásada tvoří základ obhajoby obviněného v trestním řízení, nicméně platí i v řízení o přestupku nebo jiném správním deliktu, a to jak pro fyzické osoby, tak pro osoby právnické.[144]

Totiž skutečnost, že povinnost ohlášení porušení zabezpečení není provedeno řádně a včas, může zároveň poukázat na nesoulad dané organizace s povinnostmi Obecného nařízení a v tomto případě by správce byl odpovědný, jak za nesplnění povinnosti ohlásit zabezpečení, tak za nesoulad s Obecným nařízením.

[143] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3., str. 308
[144] *Právní prostor. Několik krátkých úvah k problematice aplikace zásady nemo tenetur na právnické osoby*, [online]. Právní prostor© 2019 [cit. 28.03.2019] Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/nekolik-kratkych-uvah-k-problematice-aplikace-zasady-nemo-tenetur-na-pravnicke-osoby

Ústavní soud se povahou této zásady zabýval ve svém nálezu, ze kterého mimo jiné vyplývá zákaz vydávání věcí a důkazů proti sobě samému a zákaz ukládání donucovacích pokut k vynucování předložení takových důkazů.[145] Obviněný tedy nesmí být nucen k předložení důkazů proti sobě samému, nicméně je povinen pasivně strpět úkony orgánů činných v trestním řízení, v tomto případě orgánu veřejné moci. Samotné ohlášení porušení zabezpečení ale nelze považovat za pasivní strpění, nýbrž za aktivní jednání.

Pokud správce ohlásí porušení zabezpečení osobních údajů, může tím sám sebe vystavit riziku odhalení nesouladu s některými povinnostmi Obecného nařízení, zejména nedostatečným zabezpečením zpracování. V tomto případě by správci hrozila správní pokuta za nedodržení takové povinnosti a ohlášení porušení zabezpečení lze dle názoru autora považovat za předložení důkazu proti sobě samému.

Odpověď na otázku, zda je povinnost ohlašování porušení zabezpečení v rozporu se zásadou nemo tenetur ipsum accusare, zodpoví nejspíše až praxe ÚOOÚ a soudů České republiky.

3.6 Následky porušení práva na ochranu osobních údajů

Za účelem dodržování souladu s právními předpisy na poli ochrany osobních údajů existují právní mechanismy, kterými lze postihnout správce či zpracovatele za porušování povinností vyplývajících z těchto předpisů. Podle právní povahy lze tyto mechanismy dělit na veřejnoprávní, kdy se povinný subjekt vystavuje nedodržováním stanovených povinností hrozbě postihu za přestupek či trestný čin, a soukromoprávní mechanismy představující povinnost k náhradě újmy způsobené nedodržováním povinností vyplývajících z práva na ochranu osobních údajů.

Obecná úprava náhrady újmy je v České republice zakotvena v § 2894 občanského zákoníku, ten stanoví, že povinnost k náhradě nemajetkové újmy zahrnuje vždy i povinnost nahradit majetkovou škodu. Zároveň stanoví, že povinnost k náhradě

[145] Nález Ústavního soudu České republiky ze dne 8. 11. 2005, sp. zn. US I. 402/05, bod IV

újmy postihuje škůdce pouze pokud byla výslovně ujednána nebo pokud tak stanoví zvláštní zákon. V obecném nařízení je náhrada újmy upravena v článku 82 odst. 1, kde stanoví, že kdo v důsledku porušení povinností plynoucích z Obecného nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce či zpracovatele náhradu utrpěné újmy.[146]

Odpovědnost správce je ale v tomto případě širší než odpovědnost zpracovatele. U správce se totiž jedná o objektivní odpovědnost, jelikož je odpovědný za jakékoli porušení povinností vyplývajících z Obecného nařízení, bez ohledu na jeho zavinění. Zpracovatel je dle článku 82 odst. 2 odpovědný pouze v případě, poruší-li povinnost, která je ukládána Obecným nařízením konkrétně zpracovateli nebo pokud jedná nad rámec zákonných pokynů správce nebo v rozporu s nimi, například pokud do zpracováni osobních údajů zapojí dalšího zpracovatele bez souhlasu správce. Pokud existuje více odpovědných osob, tedy správců a zpracovatelů a některý z nich nahradí újmu vzniklou při zpracování, je oprávněn uplatnit tzv. regres vůči ostatním odpovědným osobám. Může tedy požadovat po zbylých odpovědných osobách nahradit poměrnou část vynaložené částky na náhradu újmy, vždy podle jejich podílu odpovědnosti za danou újmu.

Nutno podotknout, že správce či zpracovatel mohou být odpovědnosti za porušení Obecného nařízení zproštěni v případě, že prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla. [147] Nicméně se musí jednat o zcela ojedinělou událost a správce či zpracovatel má povinnost její existenci náležitě prokázat.

Druhým prostředkem postihnu nedodržování povinností z Obecného nařízení plynoucích je veřejnoprávní mechanismus, tedy udělování správních pokut, upravený v článku 83 Obecného nařízení. Správní trest je možné dozorovým úřadem uložit za pouhé porušení povinností nezávisle na vzniku újmy, nicméně pokud újma vznikla, nemá uhrazení správní pokuty vliv na povinnost tuto újmu nahradit. V článku 83 odst. 1 jsou stanoveny principy ukládání správních pokut, dle kterého by pokuta měla být účinná a odrazující od dalšího porušování, a to i pro

[146] Obecné nařízení o ochraně osobních údajů, článek 82 ods.1
[147] Obecné nařízení o ochraně osobních údajů, článek 82 odst. 3

další správce a zpracovatele. Má tedy preventivní funkci, za účelem zefektivnění a zkvalitnění ochrany osobních údajů jako takové. Zároveň by měla být přiměřená, co do okolností případu porušení povinností, s přihlédnutím k ekonomické situaci dané osoby a obecné úrovni příjmů daného členského státu. Kritéria pro určení výše sankce jsou uvedena v odst. 2 tohoto článku. Při ukládání sankce by mělo být zohledněno, zda byla povinnost porušena úmyslně či z nedbalosti, zda porušitel podnikl kroky ke zmírnění škody, jaké kategorie osobních údajů se porušení týká a také zda toto porušení oznámil dozorovému úřadu apod.

Obecné nařízení stanoví dle závažnosti dvě úrovně maximální výše správní pokuty, kterou lze udělit za porušení povinností z Obecného nařízení plynoucích. Článek 83 odst. 4 stanoví nižší limit možné pokuty a obsahuje výčet povinností, za jejichž porušení lze uložit pokutu až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.[148] V odst. 5 je limit pro udělení správní pokuty zvýšen na dvojnásobek, maximální výše pokuty může tedy dosahovat 20 000 000 EUR nebo 4 % celkového ročního obratu, jedná-li se o podnik.

Právě hrozba astronomických pokut byla v období legisvakance pravděpodobně největším strašákem a zároveň častým argumentem soukromých subjektů, nabízejících komplexní implementaci Obecného zařízení jako součásti jejich obchodního artiklu. Nutno podotknout, že dřívější úprava umožňovala dozorovému úřadu uložit pokutu ve výši 5 000 000 Kč fyzické osobě, pokud se jednalo o osobu právnickou byla maximální výše pokuty stanovena na 10 000 000 Kč, nicméně český dozorový úřad ÚOOÚ nejčastěji uděloval pokuty v řádech desetitisíců až statisíců. Historicky nejvyšší pokutu udělil ÚOOÚ v roce 2016 společnosti T-mobile Czech Republic a. s. v celkové výši 3 600 000 Kč, za nedostatečné zabezpečení ochrany osobních údajů, které způsobilo odcizení osobních údajů více jak 1 200 000 klientů.[149] Dalším případem milionové správní pokuty, také v

[148] Obecné nařízení o ochraně osobních údajů, článek 83 odst. 4
[149] Tisková zpráva: Správní řízení se společností T-Mobile Czech Republic a.s.: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=20991&n=tiskova-zprava-spravni-rizeni-se-spolecnosti-t-mobile-czech-republic-a-s

souvislosti s nedostatečným zabezpečením osobních údajů a jejich následnou krádeží, byla společnost Mall, a. s., jež byla pokutována částkou 1 500 000 Kč. V tomto případě se jednalo o únik osobních údajů v mezidobí let 2014-2017, a to nejméně 735 000 zákazníků.[150]

V článku 83 odst. 7 dává Obecné nařízení možnost členským státům modifikovat výši správní pokuty a stanovit specifické postupy při postihování orgánů veřejné moci a veřejných subjektů. Návrh zákona o zpracování osobních údajů upravuje maximální výši této sankce na 10 000 000 Kč ve svém § 62 odst. 5.[151] Maximální výše pokuty, kterou bude možné dle tohoto zákona uložit je tedy značně snížená, oproti soukromoprávním subjektům. Toto rozhodnutí českého zákonodárce se zdá poměrně nespravedlivé, jelikož tím dochází ke značnému znevýhodnění soukromoprávních subjektů v situacích, kdy hrozí uložení správní pokuty. Například v situaci, kdy zpracování provádí fakultní nemocnice či jednotlivá ministerstva, kteří často zpracovávají zvláštní kategorii našich osobních údajů, by za předpokladu porušení Obecného nařízení byli postihovány nepoměrně nižší sankcí než například nemocnice soukromé, které většinou zpracovávají totožný druh osobních údajů. Na druhou stranu je zřejmé, že při sankciování orgánů veřejné moci, by docházelo k pouhému přesunu finančních prostředků mezi organizačními složkami státu, jelikož často bývají financovány z veřejných zdrojů, a právě tímto zákonodárce argumentuje v důvodové zprávě k návrhu zákona.

[150] Úřad udělil společnosti Internet Mall, a.s. pokutu 1,5 milionu korun: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/urad-udelil-spolecnosti-internet-mall-a-s-pokutu-1-5-milionu-korun/d-31959

[151] https://drive.google.com/file/d/1DSF-HPQyLAPD65Ke5pZ_rpwPpNDEBSmZ/view navrh zakona o zpracovani osobnich udaju

4 Vybrané aspekty digitálně informačního rozmachu

Žijeme v tzv. digitálním nebo také informačním věku, tedy době, ve které jsme ze všech stran obklopeni obrovským množstvím dat a informací. Tento fakt nám mnohdy dodává pocit, že se naše společnost nachází na pomyslném technologickém vrcholu, což může být z určitého úhlu pohledu pravdou. Nikdy v naší historii nebyla dostupnost dat a informací na takové úrovni, ve které se nacházíme dnes. Ještě před několika desítkami let se každodenní realita současnosti zdála být spíše námětem pro film se science fiction tématikou. Ona totiž samotná představa absolutního propojení celého "moderního" světa, ve kterém se čerstvé zprávy a informace šíří v rámci několika sekund a komunikace prostřednictvím zpráv a chatů je dostupná každému prakticky kdekoli na zeměkouli, byla přinejmenším utopická. Dnes se v takové době nacházíme, a to díky internetu, který navždy změnil celou naši společnost. Pro upřesnění, co se týče dostupnosti internetu v rozmezí let 2000 až 2018 došlo k nárůstu celosvětového počtu uživatelů internetu o celých 1066 %.[152]

V tomto směru, co se týče dostupnosti a bezprostřednosti užívání moderních technologií, jsme opravdu v bodě, který lze považovat za technologický vrchol. V ideálním světě by taková byla i realita, nicméně do ideálního světa má naše společnost velice daleko, a tak je nutné zohlednit i bod, v jakém se nacházíme v souvislosti se zkušenostmi, vzděláním a samotnou schopností správně zpracovávat data a informace. Z tohoto úhlu pohledu se naopak nacházíme v jakési digitální džungli. Bezesporu to souvisí se zmiňovanou dostupností nejrůznějších technologií a služeb informačního světa, ale také s tím, že za poměrně krátkou dobu se rapidně změnili postupy při práci s nimi, a to napříč spektrem všech oborů a zejména starší členové společnosti neměli dostatek času a prostředků k adaptování se na nový systém práce s daty a informacemi.

[152] World Internet Users Statistics and 2019 World Population Stats. Internet World Stats - Usage and Population Statistics [online]. Copyright © 2019, Miniwatts Marketing Group. All rights reserved worldwide. [cit. 28.03.2019]. Dostupné z: https://www.internetworldstats.com/stats.htm

4.1 Internet a jeho právní regulace

Definovat informační prostředí internetu v právním kontextu je prakticky nemožné. Jedná se bezesporu o fenomén sui generis a jako takový nestojí sám o sobě, ale je regulován zejména prostřednictvím regulace jeho uživatelů, tedy spíše jejich chování. Prostřednictvím nedokonalých normativních konstrukcí je právo jedním z jeho možných regulativů a v informačním prostředí internetu platí více než kde jinde, že mezi tím, co je v tomto prostředí skutečně realizováno a tím, co by z vůle regulátora být realizováno mělo, nebývá obvykle shoda. Realita internetu a jeho normativní regulace jsou tedy dvě relativně samostatné kategorie.[153]

Samotné právo je často konfrontováno s technologickým rozvojem a pokrokem, nicméně zásadním faktorem by mělo být dosažení rovnováhy mezi podporou technologického rozvoje s ochranou jeho pozitivních stránek a regulací souvisejících negativních důsledků tohoto rozvoje prostřednictvím vytváření efektivních překážek. Cílem právní regulace internetu není čelit technologickým proměnám, které s ním přichází, ale spíše jejich pochopení a zařazení do existujících podmínek právních regulací, popřípadě jejich adaptace na nově vzniklý stav. Jen a pouze vydání se tímto směrem může vést k poznání právních problému a nových jevů, které v souvislosti s existujícími technologiemi vznikají. Při právním uvažování tak není předmětem samotná technologie, ale spíše její aplikace v prostředí dosavadních právních standardů a postulátů.

Nabízí se myšlenka, že některé z nynějších technologických a společenských změn mohou vzhledem ke své globální povaze ovlivnit dosavadní právní vztahy natolik, že dojde k určitému narušení fungování některých právních standardů. Tyto změny mohou svou povahou generovat normativně obtížně řešitelné právní problémy, které by mohli vyústit v přeformulování podstaty právních institutů, jež se historicky formovali a jsou po staletí uznávány.

Dle názoru autora je nutné za právní standardy považovat zejména základní lidská práva a svobody, jejich ochranu a zároveň ochranu oprávněných, případně

[153] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6. str. 25

legitimních očekávání subjektů práv na jejich ochranu. Povaha informačních společností může do aplikace těchto práv vnášet nové otázky týkající se realizace těchto práv.

4.1.1 Právní problémy globální povahy internetu

Internet již v okamžiku svého zrodu představoval zcela ojedinělý komunikační model, který svou vnitřní strukturou a koncepcí způsoboval nekontrolovatelnost ze strany států či jejich orgánů. Naopak byl na nedůvěře k centralizované kontrole postaven. Toto pojetí ve svém důsledku zapříčinilo vznik centrálně nekontrolovatelné sítě, která zároveň postrádá úctu k teritoriální působnosti práva. V tomto kontextu lze hovořit o bezhraničnosti internetu. Internet byl původně budován jako vojenská technologie a nebyl tvořen k masovému použití, proto také u jeho zrodu nebyly řešeny právní souvislosti jeho civilního využití, jako působnost a pravomoc státních orgánů, včetně možnosti ukládat nové povinnosti a vynucovat jejich dodržování.[154] Veřejná moc jako jeden ze základních znaků státu je uplatňována v rámci územní výsosti daného státu, jak tedy regulovat něco, co má bezhraničnost a globálnost jako klíčové charakteristiky.

Pokud chce stát provést efektivní regulaci, musí mu být dána pravomoc uplatnit svou veřejnou moc na daném území, případně tímto pověřit jiný stát. Reálná možnost státu vynutit svou moc k regulaci internetu by představovala formu globální regulace rozšířenou na celosvětový internetový prostor. Momentálně žádná taková globální jurisdikce neexistuje a je otázkou, zda by globální vynutitelnost práva byla tím správným postupem, jelikož pokud jeden stát zastává a chrání jiné hodnoty než jiný stát, byla by globální spolupráce jen těžko proveditelná. Například v kontextu ochrany soukromí, EU staví do popředí ochranu osobních údajů prostřednictvím právních předpisů a Spojené státy americké spíše formu seberegulace. Jiným příkladem může být Čínská lidová republika, jež zvolila za efektivním zajištěním vlastních hodnot poměrně radikální přístup, když vytvořila

[154] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6. str. 160

tzv. *Golden shield*, také známý jako *Great Chinese Firewall*[155], což je vlastně separovaná část internetu. Čína má tímto možnost jejich internetové prostředí regulovat o poznání efektivněji než jiné státy, nicméně pro státy, které mají základní lidská práva a svobody jako jeden ze základních principů je toto řešení nemyslitelné.

Existují ale i svým způsobem progresivnější názory na regulaci internetového prostředí. Například Lawrence Lessig ve své knize *Code version 2.0*[156] uvádí, že internet jako takový je nezbytné určitým způsobem regulovat, nicméně je třeba vycházet z tzv. *kódu*, který přirovnává v prostředí internetu k zákonu neboli vnitřní stavbě internetu, která již svou podstatou chování na internetu určitým způsobem přirozeně reguluje. Dle Lessiga by bylo vhodné tímto kódem řídit i působnost práva, což by z něj dělalo do určité míry kodex v právním smyslu a řešení regulace internetu by tedy muselo vycházet z jeho vnitřní stavby. Tento názor je dle autora velice zajímavý a dost možná přináší jisté řešení do zatím příliš neřešené problematiky.

4.1.2 Svobodný internet

Svoboda internetu byla od jeho počátku jeho stěžejním atributem, nicméně lze tuto svobodu považovat za absolutní osvobození od státu a práva? Dle názoru autora nikoli, nicméně internetový aktivista John Perry Barlow, vytvořil Deklaraci nezávislosti internetu[157], kde tuto tezi přímo potvrdil. "*Vy unavení obři z masa a oceli. Já, přicházející z Kyberprostoru, nového sídla Mysli, Vás v zájmu budoucnosti vyzývám: Nechte nás být! Nejste mezi námi vítáni. Nemáte žádnou moc nad místy, kde přebýváme. Nemáme vládu ani po žádné netoužíme. Mluvím k Vám tedy z pozice autority ne větší, než jakou má sama Svoboda. Vyhlašuji, že globální společenství, jež budujeme, nezávisí na tyranii a zákazech, kterými jste nás svázali.*

[155] *The Great Firewall of China: Background Torfox*. Stanford Computer Science [online]. [cit. 28.03.2019] Dostupné z: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html
[156] *Codev2*: Lawrence Lessig [online]. Copyright © [cit. 28.03.2019]. Dostupné z: http://codev2.cc/download+remix/Lessig-Codev2.pdf
[157] *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation | Defending your rights in the digital world [online]. [cit. 28.03.2019] Dostupné z: https://www.eff.org/cyberspace-independence

Nemáte morální právo nás řídit a nemáte ani nástroje, kterých bychom se museli bát. Moc vlád je odvozena ze souhlasu těch, kterým vládnou. Náš souhlas jste však nežádali a nikdy jej neobdržíte. Nechceme Vás. Neznáte nás, jako neznáte náš svět."[158] Na tuto myšlenku nepřímo navazují i někteří právní filozofové, často označovaní za *"kyber-libertariány".*

Byť je z výše uvedené citace cítit jistá míra aktivismu, s některými názory nelze nesouhlasit. Kyberprostor internetu lze totiž rozdělit do několika vrstev, ve kterých se jako uživatel můžete pohybovat. První z nich je *Surface Web*, často označován za *Visible Web*, jedná se o tu část internetu, která je dostupná široké veřejnosti a lze se v ní pohybovat prostřednictvím všem dostupných prostředků. Existují ale také tzv. *Darknets*, jež se skládají z *Deep Webu* a *Dark Webu*. První část, tedy Deep Web je ta část internetového kyberprostoru, jejíž obsah nelze vyhledávat prostřednictvím klasických webových vyhledávačů (Google, Seznam apod.) ať už proto že tohoto vyhledávání nejsou schopny, nebo proto, že obsah Deep Webu do svého vyhledávání zahrnout nechtějí. Deep Web tvoří jak soukromé weby, chráněné obsahy tak i stránky s nelegálním obsahem, například prodejem zbraní. Oproti tomu Dark Web je specifická část Deep Webu, kterou nelze zobrazit ani prostřednictvím běžně používaných webových prohlížečů (Google Chrome, Safari, Mozilla apod.). Samotná existence Dark Webu je zcela legální, nicméně stránky s obsahem, který lze díky absolutní anonymitě na Dark Webu navštívit legální rozhodně nejsou. Jedná se o stránky, které umožňují například prodej drog, falešných identit ale i pro nás důležitých osobních údajů.

Dle dostupných studií právě Darknets tvoří absolutní většinu internetového kyberprostoru, dosahující až 96 %. Ta zbylá 4 % připadají na všem dostupný Surface Web.[159]

[158] POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012. Téma (Auditorium). ISBN 978-80-87284-22-3. (převzatý překlad)

[159] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. str. 48

4.1.3 Ohrožení svobody internetu aneb Směrnice DSM

Dle názoru autora je jedním z nejpozitivnějších přínosů internetu právě možnost vyhledávání a sdílení informací a obsahu nejrůznějšího typu. Právě toto je jedna z oblastí, kterou se evropští zákonodárci rozhodli regulovat prostřednictvím *Směrnice DSM* neboli *Směrnice Evropského parlamentu a Rady o autorském právu na jednotném digitálním trhu.*[160] Toto téma je v době psaní této diplomové práce velice aktuální, jelikož hlasování o jejím přijetí v Evropském parlamentu by mělo proběhnout během několika málo dnů. Zda se EU vydala správným směrem na cestě revize autorského práva se autor pokusí zhodnotit v následujícím textu. Titulek této podkapitoly je samozřejmě záměrně nadnesený, a to hlavně z důvodu, jakým způsobem na tuto problematiku reaguje veřejnost a její kritici. Dle předsedy spolku Wikimedia ČR Vojtěcha Dostála by přijetí Směrnice DSM v jejím aktuálním znění poškodila svobodný internet a zamezila by svobodnému sdílení informací na internetu v podobě, v jaké ho známe nyní.[161] Nejproblematičtěji působí znění článků 11 a 13 a jejich dopad bude také dále rozebírán.

Článek 11 této směrnice bývá označován jako *"link tax"* neboli *"daň z odkazů"*[162], jelikož na jeho základě mají být vydavatelům tiskových publikací poskytnuta autorská práva k obsahu online médií. Tedy právo online médií požadovat licenční poplatky za zveřejňování částí svých textů například prostřednictvím služeb internetových gigantů jako je Google nebo Facebook. Služba Google News totiž nabízí svým uživatelům výběry ze zpráv novinových periodik ve formě odkazů či krátkých shrnutí bez nutnosti mít od vydavatele tohoto obsahu licenci k jeho šíření a zároveň tím může být způsobeno, že uživatel není motivován navštívit webovou stránku samotného vydavatele. Celý příjem z reklamy tak získávají poskytovatelé

[160] Návrh Směrnice Evropského parlamentu a Rady o autorském právu na jednotném digitálním trhu

[161] Česká Wikipedie se na protest odmlčela. Svobodný internet je v ohrožení, říká Dostál - Aktuálně.cz. Video - Aktuálně.cz [online]. Copyright © Economia, a.s. [cit. 28.03.2019]. Dostupné z: https://video.aktualne.cz/dvtv/ceska-wikipedie-se-na-protest-odmlcela-svobodny-internet-je/r~1e39ea904bbf11e98aa4ac1f6b220ee8/ 1:00

[162] *Směrnice o autorském právu na jednotném digitálním trhu – máme se i nadále bát?* | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/smernice-o-autorskem-pravu-na-jednotnem-digitalnim-trhu-mame-se-i-nadale-bat-107952.html

těchto služeb. Autorským právem k obsahu momentálně disponují pouze jeho autoři, aby se tedy vydavatel proti výše uvedenému zveřejňování mohl bránit, musí být majetková autorská práva k obsahu převedena autorem na něj, což se Evropské komisi jeví jako nedostatečné a neefektivní.[163] Článek 11 stanoví výjimky vztahující se k prostému odkazování na daný obsah a také na soukromé či nekomerční využití obsahu jednotlivcem. Výjimka se také týká "jednotlivých slov nebo velmi krátkých úryvků"[164] Co se pod tímto pojmem skrývá je zatím nejasné, nicméně jelikož se jedná o směrnici, definování tohoto pojmu bude nejspíše na jednotlivých členských státech ve svých implementačních předpisech. Nutno podotknout, že článek 11 prošel od svého prvního zveřejnění určitým vývojem, například v prvotním návrhu by měla být práva vydavatelů poskytována na dobu 20 let od zveřejnění obsahu, znamenalo by to právo požadovat zmíněnou "*daň z odkazů*" po takto nesmyslně dlouhou dobu. Následně byla doba snížena na 5 let a v současné podobě je opět snížena a to na 2 roky.

V určitém kontextu lze v článku 11 spatřovat posílení pozice vydavatelů samotného obsahu, jelikož by se tím příjmy z reklamy určitým způsobem rozdělili mezi vydavatele a poskytovatele služeb, které jejich obsah šíří. Na druhou stranu, sdílení obsahu například Facebookem, přináší vydavatelům nesrovnatelně větší návštěvnost jejich webů a tímto krokem by vlastně došlo ke zpoplatnění něčeho, co jim samotným dělá určitým způsobem reklamu. Nicméně pro koncového uživatele, tedy konzumenta obsahu se tímto situace nemění a změna podstaty internetu v tomto není autorem žádným způsobem spatřována.

Ještě větší míra kontroverze je spatřována v článku 13 této směrnice, který sklidil o poznání více kritiky a ve kterém je právě spatřován nebezpečný prostředek pro cenzuru internetu. Dle evropského zákonodárce se ale jedná o účinný nástroj proti tzv. *warezu,* tedy pirátskému obsahu, který je sdílen a publikován v rozporu s autorskými právy. Z tohoto článku totiž vyplývá povinnost pro poskytovatele

[163] *Směrnice o autorském právu na jednotném digitálním trhu – máme se i nadále bát?* | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/smernice-o-autorskem-pravu-na-jednotnem-digitalnim-trhu-mame-se-i-nadale-bat-107952.html

[164] Návrh Směrnice Evropského parlamentu a Rady o autorském právu na jednotném digitálním trhu, článek 11

služeb informační společnosti, kteří ukládají velké množství obsahu, přijmout vhodná a přiměřená opatření, prostřednictvím kterých bude možné v nahrávaném obsahu rozpoznat předměty autorskoprávní ochrany a jejichž následné užití bude nadále možné jen v souladu s příslušnou licencí, umožňující tímto obsahem nadále komunikovat s veřejností. V praxi se bude jednat o servery YouTube, Facebook, 9GAG a v českém prostředí například Uložto, tedy *"online content sharing service provider"*[165] servery, jejichž hlavním účelem je ukládat a poskytovat veřejný přístup k velkému množství autorsky chráněných děl a jejich následné uspořádání a zviditelňování za účelem zisku.

Není pochyb, že v činnosti těchto poskytovatelů lze spatřit významné nedostatky v souladu se současnou autorskoprávní ochranou a zavedení určitého opatření je tedy logickým důsledkem, způsob jeho provedení se ale nezdá být krokem správným směrem. Dle odstavce 7 tohoto článku, nemá vést jeho aplikace k povinnosti poskytovatele obecně monitorovat veškerý obsah, nicméně jiným než preventivním skenováním a filtrováním obsahu se vyplývajícím požadavkům nejspíše vyhovět nedá. Praxe tedy nejspíš povede k zavádění filtrů, které budou veškerý nahrávaný obsah kontrolovat a automaticky byť jen podezřelý obsah mazat a také zabraňovat tomu, aby byl takový obsah na web nahráván. Zároveň vývoj a provoz systému schopného identifikovat chráněná díla v rámci gigantického množství dat, může v praxi znamenat vynaložení značných finančních nákladů, což by mohlo způsobit vytvoření překážky vstupu na trh pro malé a střední poskytovatele, kteří by si tato technická opatření nemohli dovolit. Výjimku z tohoto článku tvoří dle směrnice nekomerční online encyklopedie, nezisková výuková nebo vědecká úložiště, úložiště pro sdílení open source softwaru, komunikační služby nebo cloudové služby, které umožňují uživatelům nahrávat obsah pro jejich vlastní využití.[166] Další výjimku tvoří začínající společnosti, které existují dobu ne delší než tři roky, jejich roční obrat je nižší než 10 000 000 EUR a nejsou navštěvovány více jak 5 000 000 uživateli měsíčně ale pouze za předpokladu, že splňují všechna uvedená kritéria. Zároveň i tito poskytovatelé budou muset prokázat, že podniknou veškerou

[165] Návrh Směrnice Evropského parlamentu a Rady o autorském právu na jednotném digitálním trhu, článek 2

[166] *Otázky a odpovědi: Jak může reforma copyrightu s články 11 a 13 změnit internet?* - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 28.03.2019]. Dostupné z: https://www.lupa.cz/clanky/otazky-a-odpovedi-jak-muze-reforma-copyrightu-s-clanky-11-a-13-zmenit-internet/

snahu o získání příslušných licencí od nositelů práv. Pod působnost směrnice také nemají spadat díla, která jsou zveřejňována za účelem citace, kritiky nebo recenze. Také díla upravovaná za účelem karikatury, parodie či napodobeniny. V tom ale může být veliký problém, jelikož současné filtrační systémy postavené na principu vyžadující směrnice, jsou poměrně nespolehlivé a vykazují vysokou míru chybovosti. V praxi by tedy mohlo docházet k situacím, vedoucím k mazání a cenzurování všech děl, u nichž bude automaticky vygenerováno, že jsou podezřelé. Svým způsobem by nahrávací filtry mohli způsobit ohrožení základních lidských práv, zejména právo na svobodu projevu.

Byť se autor domnívá, že úmysl regulovat autorské právo na území EU, pro zlepšení postavení samotných autorů je zcela logickým a vlastně i správným krokem, nástroje k jeho provedení s přihlédnutím k jejich dosavadní technické úrovni nepovedou dle autora ke spolehlivým výsledkům. Nelze totiž očekávat, že automatický filtrační počítačový systém bude schopen rozpoznat legální užívání autorských děl, například jejich citaci, karikaturu či parodii rozlišit od jejich neoprávněného užití a ve výsledku by se tak mohlo opravdu jednat o nástroj pro cenzuru obsahu na internetu. Kupříkladu výše zmiňovaná společnost YouTube, zaznamená denní nahrání přibližně 600 000 hodin videoobsahu[167] a u takového množství nelze předpokládat, že by byly požadavky směrnice splněny jiným prostředkem než automatizovaným filtračním počítačovým systémem. Zároveň je pravděpodobné, že dopad, který bude směrnice v praxi mít výrazně ohrozí konkurenční prostředí, jelikož menší společnosti, které si systémy na filtrování obsahu nebudou moci dovolit pravděpodobně buď zaniknou, nebo přestanou nabízet své služby občanům EU.

4.1.4 Netiquette

Jak bylo uvedeno výše, internet by měl být regulován převážně prostřednictvím regulování chování jeho samotných uživatelů, a právě na chování na internetu v jeho pravém slova smyslu, by se autor rád zaměřil v této podkapitole. Tímto chováním je myšlen soubor vnějších projevů člověka, v reakci na vnější i

[167] *160 YouTube Statistics and Facts (2019) By the Numbers* [online]. [cit. 28.03.2019] Dostupné z: https://expandedramblings.com/index.php/youtube-statistics/

vnitřní podněty.[168] V prostředí internetu byl za čas jeho užívání vytvořen soubor pravidel a doporučení, jimiž by se jeho uživatelé měli řídit. Internet je totiž dle autora živým prostředím, byť se jedná o počítačovou síť, s ohledem na jeho globální využívání je třeba brát internet jako nedílnou součást společnosti. Nejuznávanější uspořádání těchto pravidel je spatřován v článku *Netiquette* od Sally Hambridge[169]. Nutno podotknout, že se jedná o soubor pravidel pouze doporučujícího charakteru, které nejsou nijak právně závazné, nicméně nedodržování dílčích segmentů internetové etiky, může v některých situacích vést až k naplnění skutkové podstaty trestného činu. Domnělá anonymita internetu v jeho uživatelích často probouzí jejich nejhorší stránku a motivuje je chovat se hůře než v reálném životě. Dle Aleše Rozehnala dochází v prostředí internetu stále k většímu počtu verbálních trestných činů, nejčastěji se jedná o podněcování k trestnému činu dle § 364 a schvalování trestného činu dle § 365 trestního zákoníku. V souvislosti s touto trestnou činností jsou v České republice aktuální zejména reakce na teroristický útok na Novém Zélandu ze dne 15. března 2019, které v současné době prověřují orgány činné v trestním řízení. Na našem území došlo i k pravomocnému odsouzení v souvislosti s trestným činem podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle § 356 trestního zákoníku, ke kterému došlo na sociální síti Facebook pod fotografií romských žáků prvního ročníku základní školy. Autorka nenávistného komentáře byla potrestána pokutou ve výši 20 000 Kč a podmíněným odsouzením na rok a půl.

Dle názoru autora je v kontextu s verbálními trestnými činy v prostředí internetu a jejich následného trestního postihu velmi náročné rozlišit, zda se jedná o jen o emotivní výkřik nebo o snahu proměnit slova v činy. Zároveň internet považuje za sociální prostředí jako každé jiné a měla by být dodržována teze, že co by si člověk nedovolil říci nahlas mezi lidmi, neměl by ani zveřejňovat v internetovém prostředí. Některé projevy na sociálních sítích jsou totiž natolik extrémní a extrémistické, že trestněprávní represe a její exemplární použití je v některých případech pro

[168] HARTL, Pavel a Helena HARTLOVÁ. *Velký psychologický slovník*. Ilustroval Karel NEPRAŠ. Praha: Portál, 2010. ISBN 978-80-7367-686-5.
[169] *Netiquette Guidelines*, Sally Hambridge, Albury's Local Internet Service Provider, Personalised service, professional support. [online]. [cit. 28.03.2019] Dostupné z: http://www.albury.net.au/new-users/rfc1855.txt

společnost jediným ochranným prostředkem pro zamezení či předcházení takovému chování.

4.2 Právo na soukromí v prostředí internetu

Pokud hovoříme o realizaci ochrany práva na soukromí v prostředí internetu, vyvstávají nám nová specifika a limity, jež výkon tohoto práva obsahuje. Nelze tedy nesouhlasit s výrokem soudce Nejvyššího soudu Spojených států amerických Antonina Scalii, který prohlásil, že *"by bylo bláznovstvím tvrdit, že míra soukromí zůstala technickým pokrokem zcela nedotčena"*[170]. Samotný technologický pokrok totiž vytvořil prostor pro další problémy zpochybňující soudržnost aplikace práva na soukromí a ohrožující jeho aplikaci v informačním prostředí internetu. Dle Jána Matejky s nástupem digitálních technologií vyvstávají některé zásadní problémy.[171]

4.2.1 Legitimní očekávání ochrany soukromí

Prvním z nich je stále rostoucí propast mezi mírou ochrany soukromí, očekávanou ze strany jednotlivce v informačním prostředí internetu a ochotou společnosti uznat toto očekávání za přiměřené. Neboli to, co jednotlivec subjektivně považuje za soukromé a očekává tak, že bude chráněno často nemusí odpovídat tomu, co je soud za soukromé ochoten uznat. Samotné fungování v internetovém prostředí totiž pro jednotlivce znamená, že za sebou zanechává stále větší digitální stopu (problematika digitálních stop bude popsána v samostatné podkapitole), než naprostá většina společnosti vůbec tuší a přístup k těmto digitálním stopám má stále větší množství subjektů, než jednotlivec předpokládá. Tato skutečnost může být důsledkem stále většího nárůstu využívání on-line služeb v podobě chatů, messengerů a hlasových služeb, což způsobuje shromažďování stále většího množství informací o jejich uživatelích. Například uživatelé chytrých telefonů, respektive jejich funkcí a aplikací nejspíše neočekávají, že jejich pohyb a základní atributy komunikace jsou neustále sledovány. Děje se tak kdykoli, když

[170] Kyllo proti Spojeným státům americkým, 533 U.S. 27, 33–34 (2001).
[171] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6. str. 39

telefon získá informace o své přesné poloze za účelem geografické personalizace dané služby[172] (viz výše uvedené lokační osobní údaje). Uživatelé těchto technologií mají často subjektivní očekávání ochrany soukromí ve vztahu k informacím a datům sdíleným v digitálním prostředí, to ale neznamená, že jsou soudy a správní orgány ochotné jejich očekávání uznávat za přiměřené.

Rozdílná situace je u těch, co vkládají své materiály, data, osobní údaje na veřejně přístupné blogy. Zde je třeba akceptovat, že sdílením těchto typů informací přichází o své právo na ochranu soukromí a obvykle tuto skutečnost i očekávají, jelikož své soukromí otvírají před veřejností.

Nutno dodat, že zásada legitimního očekávání vyplývá jak z mezinárodních a lidskoprávních smluv, tak ochranu legitimního očekávání konstatoval i Ústavní soud v celé řadě svých nálezů: *"Ústavní soud již ve své judikatuře konstatoval, že ke znakům právního státu a mezi jeho základní hodnoty patří neoddělitelně princip právní jistoty (čl. 1 odst. 1 Ústavy), jehož neopominutelným komponentem je nejen předvídatelnost práva, nýbrž i legitimní předvídatelnost postupu orgánu veřejné moci v souladu s právem a zákonem stanovenými požadavky."*[173]

4.2.2 EULA a právo na soukromí

Jedním z dalších úskalí plynoucích z fungování v informačním prostředí je nedostatečné respektování základních principů práva na soukromí ze strany ISP, tedy *Information Service Provider* neboli *"poskytovatel informačních služeb"*[174], v Obecném nařízení definovaný jako *"poskytovatel služeb informační společnosti"*[175] (ISP), prostřednictvím jejich smluvních podmínek a samotnou povahou jejich služeb.

Právo na soukromí, jakožto jedno ze základních lidských práv v České republice chráněno ústavním pořádkem je nezadatelné, nezcizitelné, nepromlčitelné a

[172] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6., str. 40
[173] Nález Ústavního soudu ze dne 11. 5. 2005, sp. zn. II. ÚS 487/03
[174] Směrnice Evropského parlamentu a rady 2000/31/ES, článek 2, písm. a) a b)
[175] Obecné nařízení o ochraně osobních údajů, článek 4 odst. 25

nezrušitelné.[176] Z jeho nezadatelnosti vyplývá, že by nemělo docházet k situacím, kdy subjekt uzavře smlouvu, ve které se vzdává svého práva na ochranu soukromí. Realita je ovšem rozdílná a k těmto situacím v souvislosti s fungováním v informačním prostředí dochází stále častěji. Děje se tak prostřednictvím smluv s mobilními operátory, smluv o užívání kreditních karet, v některých případech i pracovních smluv ale hlavně ve smlouvách s poskytovateli služeb informační společnosti.[177] Podepsáním těchto smluv, uděluje jednotlivec druhé straně právo přístupu ke svým osobním údajům a ke svému soukromí, nicméně zdaleka ne v míře nezbytně nutné k plnění předmětu smlouvy od druhé strany. Čímž se může jednoduše dostat do rozporu s výše uvedenou zásadou účelového omezení.

Je potřeba podotknout, že samotné užívání těchto služeb, je podmíněno odsouhlasením jejich smluvních podmínek tzv. *EULA, End Users Licence Agreement*. V praxi nazývány jako *"podmínky užívání služby", "licenční smlouvy s koncovým uživatelem", "lhůty a podmínky"* nebo jen *"podmínky"*.
Tyto smluvní podmínky, jejichž akceptace umožňuje užívání předmětné služby informační společnosti nejsou vlastně ničím jiným, než zpravidla jednostranně vymezeným definováním práv a povinností ze strany poskytovatele služby. Jednostranným proto, že je nelze ze strany uživatele nikterak měnit ani do nich zasahovat. Jedná se tedy o adhézní typ smlouvy založený na principu *"take it or leave it."*

Z výše uvedeného vyvstává otázka, zda si jednotlivý uživatelé uvědomují, jaké smluvní podmínky vlastně odsouhlasili, kdy se pro ně stávají závaznými a jaký možný legální zásah do jejich základních lidských práv a svobod takto vyslovený souhlas může představovat. Výše uvedené smluvní podmínky se totiž koncovému uživateli obvykle zobrazí prostřednictvím tzv. *"clickwrap"* smluv, v praxi se jedná o smlouvy, které uživatel uzavře s poskytovatelem služby prostřednictvím kliknutí políčko "souhlasím". Dalším typem smluv uzavíraných v digitálním prostředí jsou tzv. *"browsewrap"* smlouvy, kdy k uzavření smlouvy dochází pouhým prohlížením obsahu dané webové stránky. U obou těchto způsobů odsouhlasení podmínek je

[176] Usnesení předsednictva České národní rady č. 2/1993 Sb. o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, článek 1
[177] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6., str. 41

velice problematická skutečnost, a to že není nutné, aby se uživatel seznámil s jejich obsahem, a tudíž s právním závazkem z nich plynoucím. Vzhledem k častému výskytu těchto smluv, může být z pohledu uživatele velice nepohodlné podrobné seznámení se s tímto obsahem, z čehož plyne, že naprostá většina koncových uživatelů takto nečiní.

Obsah smluv uzavíraných výše uvedenými způsoby se tedy zdá poměrně nevyvážený, nerovný až nemravný, jelikož vytváří zřejmý prostor pro budoucí zásah do soukromí jednotlivců.

4.2.3 Cloudové služby a digitální odpad

Další problém, a to spíše dle názoru autora, který vyplývá z globálního užívání technologií a internetu, je nedostatečná obezřetnost při práci s daty ze strany samotných uživatelů. Jedná se o celková data, nikoli jen o osobní údaje, byť ty představují největší hrozbu v nepovolaných rukou. Není to tak dávno, co byla společnost zvyklá k přenosu dat používat plastikové diskety s kapacitou kilobytů, maximálně megabytů. V dnešní době je naprosto běžné vlastnit úložný prostor o velikosti gigabytů, terabytů a možnosti týkající se úložného prostoru se stále rozvíjejí. Pro upřesnění, ke dnešnímu dni proběhne internetem během jedné vteřiny přenos více jak 60 tisíc gigabytů, denně se jedná o miliardy gigabytů dat.[178] V praxi tedy dochází k produkování obrovského množství dat, které ve svém výsledku tvoří nezměrné množství tzv. digitálního odpadu s tím, že co jedna strana vyprodukuje, další potencionálně shromáždí.

Častým způsobem pro uchovávání i zálohování dat je využívání cloudových úložišť, které spadají pod tzv. *cloud computing.* Jedná se o poskytování služeb a možnosti užívání softwaru, který je uložen na serverech na internetu. Výhoda těchto služeb tkví v tom, že uživatelé k nim mohou přistupovat například pomocí webového prohlížeče vzdáleně a prakticky odkudkoli. Uživatelská výhoda určitě ano, nicméně tento fakt představuje obrovská bezpečnostní rizika. Historicky se

[178] *1 Second - Internet Live Stats*. Internet Live Stats - Internet Usage & Social Media Statistics [online]. Copyright © Copyright internetlivestats.com [cit. 28.03.2019]. Dostupné z: http://www.internetlivestats.com/one-second/#traffic-band

jedná o nespočet případů úniku či zneužití dat nacházejících se v cloudovém úložišti. Uživatel totiž přichází o kontrolu nad samotnými daty, i nad úrovní zabezpečení v podobě technického řešení a ochrany dat. Pro uživatele existují reálná rizika v podobě nedostupnosti dat, znehodnocení, poškození i ztráta dat, ale i potencionální únik a zneužití.[179]

Užívání cloudových úložišť je podmíněno uzavřením smlouvy mezi poskytovatelem této služby a uživatelem dle soukromoprávní úpravy, která ale nemá konkrétně vymezenou podobu a náležitosti mezi smluvními typy. Jedná se o inominátní, nepojmenovanou smlouvu dle § 1746 zákona č. 89/2012 Sb., občanského zákoníku. Vztah mezi poskytovatelem a uživatelem se v praxi vyskytuje ve třech základních formách. Buďto je uživatelem fyzická osoba nepodnikatel, podnikatel nebo podnikatel, který třetím osobám nabízí poskytování cloudových služeb. Vztah poskytovatele s uživatelem je často uzavírán v podobě adhézní smlouvy. Uzavírání adhézní smlouvy on-line s uživatelem je standardním postupem, který na jednu stranu umožňuje rychlé a pohodlné řešení pro obě smluvní strany, ale zároveň poskytovateli umožňuje zásadně smluvně omezit odpovědnost za škodu nebo jinou újmu, vzniklou uživateli v souvislosti s poskytováním služby.[180]

Uživatel nemá vzhledem k povaze smluv možnost navrhnout jakoukoli úpravu či změnu. Výsledkem byla v minulosti existence takových smluv, které vylučovali odpovědnost poskytovatele za jakékoli přerušení, pozastavení a omezení přístupu k jeho vlastním datům. V extrémním případě smlouvou vylučovali i odpovědnost za ztrátu, poškození nebo únik dat či jakoukoli škodu, která v této souvislosti vznikla nebo mohla vzniknout.[181] Spornost těchto ustanovení je samostatným tématem a namítána by mohla být bezesporu ochrana dobrých mravů či osobnostních práv dle soukromoprávního režimu občanského zákoníku.[182] Nehledě na to, že většina

[179] *Cloudová úložiště* | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/cloudova-uloziste-105755.html
[180] *Cloudová úložiště* | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/cloudova-uloziste-105755.html
[181] *Rizika smluv o cloudových službách* | Právní prostor. Právní prostor [online]. [cit. 28.03.2019]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/rizika-smluv-o-cloudovych-sluzbach
[182] Zákon č. 89/2012 Sb., občanský zákoník § 1 odst. 2

těchto smluv bývá uživateli předložena prostřednictvím výše uvedeného clickwrapu.

Částečné řešení této problematiky přišlo s účinností Obecného nařízení, který rozšiřuje pojem osobní údaj a nyní zahrnuje například e-mailové adresy, IP adresy a soubory cookies. Zároveň klade na poskytovatele cloudových služeb větší nároky týkajících se povinností z jeho strany jakožto zpracovatele osobních údajů, které sice nejsou v plném rozsahu ničím zcela novým, nicméně vzhledem k rapidnímu zvýšení možné výše sankce za jejich nedodržení lze předpokládat, že i menší poskytovatelé cloudových služeb budou tyto povinnosti dodržovat a budou s Obecným nařízením v souladu.

4.3 Digitální stopa

Pokud v dnešní době dochází k nekontrolovanému a zdá se i nekontrolovatelnému shromažďování a získávání dat nejrůznějšího typu, musíme si také uvědomit, jaká data naopak sami produkujeme a poskytujeme. Tedy co po nás, jakožto uživatelích, v souvislosti s užíváním nových technologií a internetu zůstane. Obecně totiž platí, že vše, co jeden subjekt poskytne či vytvoří, druhý subjekt shromáždí, zaznamená či zpracovává. Tuto problematiku lze zahrnout pod pojem "digitální stopa". V širší rovině se jedná o data, která vznikají při interakci uživatele s digitálním prostředím, tzn. počítačem, chytrým telefonem nebo televizí.

Tyto digitální stopy jsou vytvářeny téměř při každém pohybu uživatele na internetu a v určitém kontextu představují zásadní riziko pro ochranu soukromí samotných uživatelů, kteří o tom ve většině případů nemají téměř žádné povědomí. Naopak v užším slova smyslu, tato data tvoří digitální stopu jednotlivých fyzických osob a jsou zároveň jejich osobními údaji. Právě tímto faktem se dostáváme do souvislosti s tématem této diplomové práce a v tomto kontextu budou digitální stopy dále popisovány.

Abychom mohli spolehlivě vymezit, jak digitální stopy vznikají a jak jsou využívány, je nutné se seznámit s dnešní vývojovou fází samotného internetu. Tato fáze vývoje internetu bývá často označována jako tzv. Web 2.0, tedy web druhé

generace. V této fázi se uživatel internetu přetransformoval z pouhého konzumenta na konzumenta tvůrce, jelikož obsah na internetu sám vytváří a nikoli jen konzumuje a čerpá. V dnešní době je naprosto běžné, že uživatel internetu vlastní svou originální webovou stránku, blog a v neposlední řadě využívá některou z široké palety sociálních sítí, byť přitom obvykle ovládá jen elementární základy práce s počítačem nebo samotným internetem. Ross Mayfield, zakladatel Socialtextu tento trend shrnul ve své známé větě - "Web 1.0 was commerce, Web 2.0 is people".[183]

4.3.1 Aktivní digitální stopa

Samotné digitální stopy lze rozdělit do dvou základních skupin. První z nich jsou vědomé, ovlivnitelné, jinak také aktivní digitální stopy. Jedná se o soubor veškerých informací, které o sobě uživatelé internetu publikují zcela dobrovolně a vědomě při vytváření určitého obsahu, většinou prostřednictvím nějaké služby. De facto dochází k předání nějaké informace. Tuto digitální stopu tedy uživatel vytváří a zveřejňuje s vědomím, že tento typ obsahu bude dostupný určité skupině dalších uživatelů, nicméně nemusí si plně uvědomovat šíři a počet těchto uživatelů. V praxi se nejčastěji jedná o komentáře, příspěvky na diskuzních fórech nebo sdílení jakýchkoli médií, ať už se jedná o fotografie, videozáznam či audiozáznam. Aktivní digitální stopa může být vytvořena také prostřednictvím označování určitých položek, například označování zájmu na sociálních sítích, typickým příkladem je interakce tlačítka "To se mi líbí", nebo jiné funkce, která dokáže vyjádřit uživatelovu pozitivní emoci nad obsahem. Může se také jednat o samotné profily vytvořené na sociálních sítích, e-shopech nebo jiných webových službách.

Základní vlastností digitálních stop aktivních je jejich relativní kontrolovatelnost ze strany uživatele a fakt, že je pouze na jeho vůli, které informace o sobě hodlá zpřístupnit jiným uživatelům. Zde ovšem platí jedno nepsané pravidlo, které je třeba brát v potaz a to, že jakákoli data či informace, sdílené či vložené do kyberprostoru

[183] Are You Ready for Web 2.0? | WIRED. *WIRED* [online]. Copyright © 2018 Condé Nast. All rights reserved. [cit. 28.03.2019]. Dostupné z: https://www.wired.com/2005/10/are-you-ready-for-web-2-0/

již v kyberprostoru zůstanou navždy, a to bez ohledu na vůli uživatele, který tak učinil.[184]

Pro ověření výše uvedeného tvrzení autor uvádí dva následující příklady všem dostupných nástrojů, které uživateli umožní určitým způsobem zkontrolovat svou digitální stopu zanechanou v kyberprostoru.

Prvním z nich je webová stránka www.archive.org a služba "Wayback Machine"[185], na které naleznete velice jednoduchý vyhledávač umožňující doslova cestovat časem. Tedy v kyberprostoru na internetu, samozřejmě. Pokud do tohoto vyhledávače zadáte internetovou adresu, jako výsledek se zobrazí kalendář, prostřednictvím kterého můžete zjistit, jak ona stránka vypadala v příslušný rok a den. Tato stránka funguje jako internetový archiv, který pravidelně ukládá všechna volně přístupná data na internetu a ke dnešnímu dni umožňuje vyhledat historii 370 milionů webů s více než 349 miliardami jednotlivých archivovaných stránek. Samotný projekt funguje jako jakési digitální muzeum, jelikož kromě webových stránek archivuje také textové články, knihy, audio a videozáznamy a obrázky. Zároveň se ale může jednat o pomyslné smetiště digitálního odpadu, které by v očích autora mohlo posloužit k potencionální těžbě "ropy internetu"[186], tedy osobních údajů.

Druhým nástrojem je webová stránka www.pipl.com, tato webová služba slouží k vyhledávání fyzických osob, agreguje totiž informace, které po sobě v kyberprostoru zanecháváme a vytváří tak ucelený obrázek o každém, kdo se historicky registroval pod svým skutečným jménem, e-mailem nebo telefonním číslem. To jen potvrzuje myšlenku, že opatrnost v souvislosti se zveřejňováním svých osobních údajů v informačním prostředí internetu není na škodu, naopak.

[184] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. str. 145
[185] Internet Archive: Digital Library of Free & Borrowable Books, Movies, Music & Wayback Machine. [online]. Dostupné z: https://archive.org/index.php
[186] Personal data is the new oil of the Internet and the new currency of the digital world - Meglena Kuneva, European Consumer Commissioner. WORLD ECONOMIC FORUM. Personal Data: The Emergence of a New Asset Class. 2011. [online]. [cit. 28.03.2019]. Dostupné z: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

Samotná kontrola nebo kontrolovatelnost aktivních digitálních stop je opravdu jen relativní. Existuje totiž jistá podskupina digitálních stop, které stojí jaksi na pomezí a kterou lze označit za hypoteticky ovlivnitelné digitální stopy.[187] Tyto digitální stopy obsahují informace a skutečnosti, na které nebo na jejich vytváření má samotný uživatel faktický vliv a může je tedy ovlivnit, ale běžně to nedělá, jelikož by si sám sobě omezil možnosti svého fungování v digitálním prostředí. Tyto digitální stopy používají poskytovatelé těch největších internetových služeb na světě (Apple, Microsoft, Facebook, Google), a samotné používání jimi nabízené služby je podmíněno odsouhlasením jejich smluvních podmínek, které umožňují poskytovatelům těchto služeb získávat a shromažďovat obrovské množství informací.

4.3.2 Pasivní digitální stopa

Druhou skupinou digitálních stop jsou nevědomé, neovlivnitelné digitální stopy, také označovány za pasivní. Tento druh digitální stopy odpovídá informaci či souboru informací, které vznikají bez uživatelova přímého záměru při interakci v prostředí internetu a jsou utvářeny jako vedlejší produkt tvorby aktivní digitální stopy. Tyto nevědomé digitální stopy v praxi obsahují například informace jako je fyzická adresa uživatele, IP adresa, vyhledávané výrazy na internetu, GPS poloha daného uživatele, údaj o času stráveném na určité webové stránce nebo oblast jeho zájmu. Tyto údaje jsou sami o sobě, nebo v kombinaci s jiným údajem právě osobními údaji a ve většině případů se zaznamenávají prostřednictvím tzv. cookies. Jedná se o krátké textové soubory, které jsou generované webovým serverem a ukládané do počítače prostřednictvím webového prohlížeče. Pokud stejnou webovou stránku navštívíte opakovaně, prohlížeč pošle tento textový soubor zpět na server a ten pak získá veškeré informace, které si o daném uživateli vytvořil a uložil.[188] K upřesnění jejich využití v praxi, cookies slouží například jako pomocník při volbě jazyka dané webové stránky nebo na jejich základě fungují různé statistiky a jiné měřící systémy fungující na internetu. Na tomto principu funguje i tzv.

[187] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. str. 145

[188] GDPR | Obecné nařízení o ochraně osobních údajů - prakticky [online]. [cit. 28.03.2019]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/cookies

behaviorální reklama, která spočívá v zobrazování reklamy na internetových stránkách či v aplikacích v závislosti na chování daného uživatele.[189] Pokud například daný uživatel často navštěvuje webové stránky věnované sportovnímu zpravodajství, prostřednictvím behaviorální reklamy jsou mu na dalších webových stránkách nabízeny odkazy na obchody se sportovním zbožím či online sázkové kanceláře.

[189] Behaviorální reklama | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů - prakticky [online], [cit. 28.03.2019]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/behavioralni-reklama/

5 Závěr

Autor svou diplomovou práci na téma *Ochrana osobních údajů v České republice a EU* rozdělil do třech relativně samostatných částí.
První z nich byla věnována vývoji ochrany osobních údajů, a to ve světle pro ni stěžejních institutů což byl také jeden z cílů stanovených v úvodu práce. Zároveň z historického kontextu rozpoznat okolnosti vzniku a mimoprávní skutečnosti, které postupně vedli k vytvoření právních pramenů v jejich formálním pojetí. Autor se snažil analyzovat tento vývoj pomocí nejzásadnějších milníků, které postupně vedly k poskytování ochrany osobním údajům v její dnešní podobě.

Za nejzásadnější institut pro ochranu osobních údajů klíčový lze považovat jedno ze základních lidských práv, a to právo na soukromí a jeho ochranu, které jako takové má svůj původ a bylo poprvé definováno ve Spojených státech amerických. Pro autora byla poměrně překvapující skutečnost, že k vymezení práva na soukromí vedl ve Spojených státech právě technický a mediální pokrok té doby, byť k jeho definování došlo již před téměř 130 lety. Autor také vymezil jeho zakotvení v lidskoprávních smlouvách a provedl stručnou analýzu jeho vývoje na území České republiky. Právo na soukromí bylo totiž v České republice zakotveno vlivem dlouho trvajícího totalitního režimu až poměrně nedávno s přijetím Listiny základních lidských práv a svobod. Dalším institutem, který se již přímo dotýká ochrany osobních údajů je právo na informační sebeurčení a v jejich souvislosti bylo také poprvé definováno v rozhodnutí Německého Spolkového ústavního soudu. K podobnému scénáři došlo i na území České republiky, kdy jeho existenci dovodil Ústavní soud ve svém nálezu z roku 2011.
Vývoj samotné ochrany osobních údajů započal na přelomu sedmdesátých a osmdesátých let minulého století. Za zajímavé autor považuje, že prvním předpisem věnujícím se ochraně osobních údajů, byly právně nezávazné pokyny vydané Organizací pro hospodářskou spolupráci a rozvoj, OECD v roce 1980. Byť měly pouze doporučující charakter, položily základ pro následnou úpravu co do terminologie, tak i základních zásad ochrany osobních údajů. Na těchto zásadách vznikl i první právně závazný nástroj ochrany osobních údajů a to Úmluva 108, kterou v roce 1981 přijala Rada Evropy. Tato úmluva se věnovala předně automatizovanému zpracování osobních údajů, lze tedy dovodit, že reagovala na

nástroje pro zpracování vytvořené v souvislosti s technologickým pokrokem. Autor také následně uvádí případ ze Spojeného království, kdy došlo k pravděpodobně prvnímu zneužití osobních údajů dnešního typu.
Dalším důležitým mezníkem, který autor uvádí bylo přijetí Směrnice 95/46/ES, která představovala první právní akt EU upravující ochranu osobních údajů. Tato směrnice reagovala na vzniklé tržní prostředí, kdy vlivem volného pohybu zboží a služeb bylo třeba regulovat i práci s osobními údaji pro vnitřní trh nezbytnou. Zároveň bylo nutné reflektovat i technologický posun v oblasti telekomunikací. Samotná směrnice představovala právní rámec ochrany osobních údajů, ze které vycházela i platná právní úprava na území České republiky a byla nahrazena až Obecným nařízením v roce 2018. Následně vydávané právní akty EU upravovaly ochranu osobních údajů spíše zpřesňujícím způsobem, vždy ale reagovaly na technologický posun v dané oblasti, obvykle v oblasti telekomunikací a jejího zabezpečení. V závěru této části je shrnuto přijetí Obecného nařízení o ochraně osobních údajů, které svou formou unifikovalo ochranu osobních údajů na území celé EU, včetně důvodů, které evropského zákonodárce k tomuto kroku vedly. Poslední podkapitola je doplněna o autorův názor na období legisvakance před účinností Obecného nařízení. Je pozoruhodné, že negativní atmosféra v souvislosti s ochranou osobních údajů byla v České republice poměrně ojedinělá, autor došel k závěru, že příčinou této hysterie se jeví jak populistické výroky některých politiků, tak nedostatečná informovanost veřejnosti ze strany médií ale i státu.

Stěžejním tématem pro tuto diplomovou práci byla také analýza vybraných institutů ochrany osobních údajů dle platné právní úpravy, tedy Obecného nařízení. Autor se zaměřil na oblasti, které prošly s přijetím Obecného nařízení určitou změnou a na instituty, jejichž výklad se od počátku jeví jako problematický. Byť je aktuální úprava ochrany osobních údajů provedena formou nařízení, evropský zákonodárce v tomto předpisu užívá poměrně neurčitých pojmů i pro velice důležité instituty. Následkem této skutečnosti by v budoucnu mohla být rozdílná rozhodovací praxe jednotlivých dozorových úřadů. Zároveň absence adaptačního zákona v České republice této situaci nijak nepřispívá.

Za pozitivní přínos Obecného nařízení autor hodnotí zpřesnění základních zásad zpracování a z nich vyplývajících povinností, jelikož se jedná o jakési obecné

klausule v jejichž světle mají být povinnosti Obecným nařízením zřízené vykládány.

Zvýšená pozornost je věnována právním titulům k samotnému zpracování osobních údajů, jelikož Obecné nařízení jejích pojetí a uplatňování zcela změnilo. Dříve preferovaný souhlas se zpracováním osobních údajů byl naopak postaven do pozice, kdy na jeho základě lze osobní údaje zpracovávat až v situaci, kdy nelze použít jiný právní titul, ačkoli před účinností Obecného nařízení bylo mylně předesíláno, že zpracování osobních údajů bude možné provádět jen s výslovným souhlasem subjektu údajů.

Další problematickou oblastí se jeví zavedení povinnosti jmenování pověřence pro ochranu osobních údajů, který by měl plnit nezávislou poradní funkci při zpracování osobních údajů a svými znalostmi a zkušenostmi přispět ke zkvalitnění jejich ochrany. Byť úmysl evropského zákonodárce prostřednictvím pověřence pozdvihnout úroveň ochrany osobních údajů lze považovat za zdařilý, dle názoru autora jsou na funkci pověřence kladeny až příliš vysoké nároky. Pověřenec musí splňovat kvalifikační předpoklady v podobě znalosti práva ochrany osobních údajů, často i znalostí v oblasti IT a také mu nesmí chybět rozsáhlá znalost oboru činnosti daného správce či zpracovatele. Kombinace těchto předpokladů může způsobit, že je v praxi velice obtížné tuto funkci obsadit. Zároveň kritéria na určení, zda je daný správce pověřence povinen jmenovat, jsou díky jejich neurčitosti poměrně nejasná. Jak vlivem této povinnosti, tak i celkovým přijetím Obecného nařízení vznikají správcům nemalé finanční náklady, vyvstává tedy otázka, zda tento zásah do soukromoprávní sféry lze považovat za legitimní.

V celkovém souhrnu se ochrana osobních údajů přijetím Obecného nařízení změnila pouze částečně. Nedodržování předchozí úpravy bylo nejspíše napraveno a soulad s Obecným nařízením, byl díky zvýšenému zájmu a povědomí o ochraně osobních údajů, v mnohých případech zajištěn. Zda přijetí Obecného nařízení přinese pozitivní výsledky v oblasti ochrany osobních údajů nejspíše ukáže až čas, jelikož dnes, téměř rok po jeho účinnosti je na podobné úvahy dle názoru autora příliš brzo. Zároveň nutno podotknout, že od 25. května 2018 pozdvižení okolo ochrany osobních údajů utichlo a celkový zájem o tuto oblast rapidně poklesl.

Doufejme tedy, že náhlý rozmach v období legisvakance nebyl jen pouhou bublinou, a že přijetí nové unijní úpravy celkově zlepší situaci okolo ochrany osobních údajů a soukromí obecně.

Historie a vývoj ochrany osobních údajů dokazuje, že materiálním pramenem pro ni stěžejním, je právě technologický posun naší společnosti v posledních několika desetiletích. Dnešní dobu lze přirovnat k digitálnímu či informačnímu věku, a to autor považuje za důsledek globálního rozšíření užívání internetu, který je zároveň největším úskalím pro ochranu osobních údajů. Autor je také názoru, že adaptace právních standardů v prostředí internetu je nezbytným úkolem budoucích let.

Třetí část této diplomové práce je tedy věnována vybraným aspektům digitálně informačního rozmachu. Autor se zaměřil na otázky související s právní regulací internetu a na fenomény posledních let. Pozornost je věnována také právu na soukromí, jelikož právě k zásahům do tohoto základního lidského práva s příchodem internetového prostředí často dochází. Byť je logické, že technologickým pokrokem byla míra soukromí značným způsobem dotčena, a to zejména chováním samotných uživatelů internetu, je potřeba na ochranu práva na soukromí nerezignovat. Je tedy potřeba budovat a zlepšovat právní povědomí samotných uživatelů internetu, ale také věnovat pozornost novým právním oblastem, které s příchodem informačního věku vstupují do popředí.

Resumé

Diplomová práce autora se skládá z třech samostatných částí, úvodu a závěru. V úvodu samotné diplomové práce se autor věnuje uvedení do problematiky ochrany osobních údajů a jejímu významu pro společnost. Zároveň jsou v něm stanoveny základní cíle práce.

První část této diplomové práce je věnována vývoji ochrany osobních údajů a institutů, které jsou pro ni stěžejní s přihlédnutím k mimoprávním skutečnostem a okolnostem jejich vzniku. Jedná se o právo na soukromí, právo na informační sebeurčení, právo na svobodný přístup k informacím a samotné právo na ochranu osobních údajů. Jako taková je zakončena shrnutím přijetí Obecného nařízení o ochraně osobních údajů a autorovým zhodnocením situace v období legisvakance.

Ve druhé části se autor věnuje ochraně osobních údajů dle platné právní úpravy, tedy Obecného nařízení o ochraně osobních údajů. Důraz je kladen na problematické oblasti, vymezení základních pojmů a nové instituty, které byly Obecným nařízením zavedeny. Závěr této kapitoly je věnován porušení povinností dle obecného nařízení a z něho vyplývajícím následkům, zároveň se autor zaměřuje na otázku možné kolize se zásadou nemo tenetur ipsum accusare.

V části třetí se autor věnuje vybraným aspektům digitálního rozmachu a internetu, jelikož jej považuje za nedílný aspekt ochrany osobních údajů. Z první části autor odvodil, že materiálním pramenem úpravy ochrany osobních údajů je právě technologický a informační rozvoj, a proto se jej rozhodl v poslední části této diplomové práce rozebrat.

Cizojazyčné resumé

The author's thesis consists of three separate parts, introduction and conclusion. At the beginning of the thesis, the author deals with the introduction to the issue of personal data protection and its importance for society. At the same time, it sets out the basic goals of the work.

The first part of this thesis is devoted to the development protection of personal data and facilities, which are crucial for it with regard to the non-legal facts and circumstances of their origin. These include the right to privacy, the right to information self-determination, the right to free access to information and the right to personal data protection itself. It concludes with a summary of the acceptance of the General Data Protection Regulation and the author's evaluation of the situation during the legislative period.

In the second part, the author deals with the protection of personal data under the valid legal adjustment, i.e the General Data Protection Regulation. The focus is on problematic areas, a definition of the basic concepts and new institutes which have been introduced by the General Data Protection Regulation. The end of this chapter is devoted to the violation of obligations according to general regulation and it's consequences while the author focuses on the issue of a possible collision with the principle of nemo tenetur accusare.

In the third part, the author deals with the selected aspects of the digital boom and internet, because it's considered as an integral aspect of personal data protection. From the first part, the author concluded, that the material source of personal data protection adjustment is the technological and information development and therefore decided to analyze it in the last part of this thesis.

Seznam použité literatury a dalších zdrojů

Knižní publikace, odborné časopisy

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

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

MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6.

MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1.

KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012. Téma (Auditorium). ISBN 978-80-87284-22-3.

HARTL, Pavel a Helena HARTLOVÁ. *Velký psychologický slovník*. Ilustroval Karel NEPRAŠ. Praha: Portál, 2010. ISBN 978-80-7367-686-5.

DONÁT, Josef a Jan TOMÍŠEK. *Právo v síti: průvodce právem na internetu*. V Praze: C.H. Beck, 2016. ISBN 978-80-7400-610-4.

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

Listina základních práv a svobod: komentář. Praha: Wolters Kluwer Česká republika, 2012. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7357-750-6.

MATES, Pavel a Karel NEUWIRT. *Právní úprava ochrany osobních údajů v ČR: znění zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů: vybrané předpisy EU poznámkové vydání se zapracovanou důvodovou zprávou*. Praha: IFEC, 2000. AZ-IUS. ISBN 80-86412-02-4.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. *Harvard Law Review*, 1890

LESSIG, Lawrence. *Code*. Version 2.0. New York: Basic Books, 2006. ISBN 9780465039142.

Právní předpisy České republiky

Zákon č. 121/1920 Sb., kterým se uvozuje ústavní listina Československé republiky

Ústavní zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního

Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky

Ústavní zákon č. 1/1993 Sb., Ústava České republiky

Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, ve znění pozdějších předpisů

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Zákon č. 480/2004 Sb., o některých službách informační společnosti

Zákon č. 127/2005 Sb., o elektronických komunikacích

Zákon č. 262/2006 Sb., zákoník práce

Zákon č. 111/2009 Sb., o základních registrech

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 90/2012 Sb., o obchodních korporacích

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 256/2013 Sb., o katastru nemovitostí

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Vyhláška č. 211/2018 Sb., o technických kontrolách vozidel

Návrh zákona o zpracování osobních údajů

Právní prameny Evropské unie a mezinárodní dokumenty

Evropská úmluva o ochraně lidských práv a základních svobod

Všeobecná deklarace lidských práv

The Freedom of Information Act

Data Protection Act 1984

Rozhodnutí Komise z 26. července 2000, č. 2000/520/ES o adekvátnosti ochrany poskytované dle principů bezpečného přístavu

Smlouva o fungování Evropské unie

Listina základních práv Evropské unie

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

Směrnice Evropského parlamentu a Rady 97/66/ES ze dne 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v odvětví telekomunikací

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 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejný

Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislost se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

Nařízení Komise (EU) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích

Judikatura

Nález Ústavního soudu ze dne 10. 11. 1998, sp. zn. I. ÚS 229/98.

Nález Ústavního soudu České republiky ze dne 8. 11. 2005, sp. zn. US I. 402/05

Nález Ústavního soudu ze dne 11. 5. 2005, sp. zn. II. ÚS 487/03

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

Rozsudek Spolkového ústavního soudu SRN ze dne 15. prosince 1983, sp. zn. BVerfGE 65, 1

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

Rozsudek Soudního dvora EU ve věci C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González

Kyllo proti Spojeným státům americkým, 533 U.S. 27, 33–34 (2001).

Další prameny, vč. cizojazyčných

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Stanovisko generálního advokáta N. Jääskinena přednesené dne 25. června 2013

Ministerstvo vnitra České republiky, Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí, podle právního stavu k 10. srpnu 2017

Důvodová zpráva k návrhu zákona o zpracování osobních údajů

Stanovisko ÚOOÚ č. 3/2012 k pojmu osobní údaj

Stanovisko ÚOOÚ č. 2/2014, Dynamický a biometrický podpis z pohledu zákona o ochraně osobních údajů

Stanovisko ÚOOÚ č. 4/2012, zpracování osobních údajů zemřelých osob

Stanovisko ÚOOÚ k problematice aktualizace zpracovávaných osobních údajů

Stanovisko ÚOOÚ k problematice odvolatelnosti souhlasu se zpracováním osobních údajů

Stanovisko WP29 č. 4/2007 k pojmu osobní údaje

Stanovisko WP29 č. 3/2013 k účelovému omezení

WP29 Opinion 15/2011 on the definition of consent

WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

WP29 Guidelines on Data Protection Officers (‘DPOs’)

WP29 Guidelines on Personal Data Breach Notification under Regulation 2016/679

Internetové zdroje

Modernizace Úmluvy 108, základního nástroje Rady | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html

Právo být zapomenut a další dopady rozsudku SDEU | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-sdeu-c-13112-google-spain-94498.html

Právní titul a rozsah zpracování osobních údajů | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/pravni-titul-a-rozsah-zpracovani-osobnich-udaju-v-kapitalovych-spolecnostech-dle-zakona-o-obchodnich-korporacich-ve-svetle-gdpr-107512.html

Směrnice o autorském právu na jednotném digitálním trhu – máme se i nadále bát? | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/smernice-o-autorskem-pravu-na-jednotnem-digitalnim-trhu-mame-se-i-nadale-bat-107952.html

Cloudová úložiště | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 28.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/cloudova-uloziste-105755.html

A brief history of data protection: How did it all start? | Cloud Privacy Check (CPC). *Homepage | Cloud Privacy Check (CPC)* [online]. Dostupné z: https://cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

Volkszählungsurteil in englischer Sprache: Census Act [online]. Dostupné z: https://freiheitsfoo.de/census-act/

INFORMAČNÍ PRÁVO. *Faculty of Informatics, Masaryk University | Faculty of Informatics Masaryk University* [online]. Dostupné z: https://www.fi.muni.cz/~smid/inf_pravo_ochd1.html#_ftn33

Piráti a IuRe podali návrh na zrušení plošného sledování občanů Ústavnímu soudu ČR.. *Pirátská strana* [online]. Copyright © [cit. 28.03.2019]. Dostupné z: https://www.pirati.cz/tiskove-zpravy/navrzeno-zruseni-smirovani.html

Special Eurobarometer 359 [online]. ©2010 [cit. 28.03.2019]. Dostupné z: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf

Jak vznikalo nařízení o ochraně osobních údajů (GDPR)? [online]. ©2018 [cit. 28.03.2019]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/

Ochrana údajů: Rada se dohodla na obecném přístupu - Consilium. *Home - Consilium* [online]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2015/06/15/jha-data-protection/

České specifikum: Z GDPR se stal byznys se strachem | Právo21 – Časopis nové generace pro studenty, právníky i veřejnost. *Právo21 – Časopis nové generace pro studenty, právníky i veřejnost* [online]. Copyright © Masarykova univerzita [cit. 28.03.2019]. Dostupné z: https://pravo21.online/pravo/ceske-specifikum-z-gdpr-se-stal-byznys-se-strachem

J. Matejka, A. Krausová, V. Güttler: Biometrické údaje a jejich právní režim, *Časopisy Masarykovy univerzity* [online]. Copyright © [cit. 28.03.2019]. Dostupné z: https://journals.muni.cz/revue/article/viewFile/8801/pdf

Co (ne)jsou ZR?, Správa základních registrů. *Správa základních registrů* [online]. Copyright ©2010 [cit. 28.03.2019]. Dostupné z: http://www.szrcr.cz/co-jsou-to-zakladni-registry

IAPP. *Study: At least 28,000 DPOs needed to meet GDPR requirements* [online]. IAPP © 2019 [cit. 28.03.2019]. Dostupné z: https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/

Právní prostor. Několik krátkých úvah k problematice aplikace zásady nemo tenetur na právnické osoby, [online]. Právní prostor© 2019 [cit. 28.03.2019] Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/nekolik-kratkych-uvah-k-problematice-aplikace-zasady-nemo-tenetur-na-pravnicke-osoby

Tisková zpráva: Správní řízení se společností T-Mobile Czech Republic a.s.: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=20991&n=tiskova-zprava-spravni-rizeni-se-spolecnosti-t-mobile-czech-republic-a-s

Úřad udělil společnosti Internet Mall, a.s. pokutu 1,5 milionu korun: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 28.03.2019]. Dostupné z: https://www.uoou.cz/urad-udelil-spolecnosti-internet-mall-a-s-pokutu-1-5-milionu-korun/d-31959

World Internet Users Statistics and 2019 World Population Stats. Internet World Stats - Usage and Population Statistics [online]. Copyright © 2019, Miniwatts Marketing Group. All rights reserved worldwide. [cit. 28.03.2019]. Dostupné z: https://www.internetworldstats.com/stats.htm

The Great Firewall of China: Background Torfox. Stanford Computer Science [online]. [cit. 28.03.2019] Dostupné z: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html

A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation | Defending your rights in the digital world [online]. [cit. 28.03.2019] Dostupné z: https://www.eff.org/cyberspace-independence

Česká Wikipedie se na protest odmlčela. Svobodný internet je v ohrožení, říká Dostál - Aktuálně.cz. Video - Aktuálně.cz [online]. Copyright © Economia, a.s. [cit. 28.03.2019]. Dostupné z: https://video.aktualne.cz/dvtv/ceska-wikipedie-se-na-protest-odmlcela-svobodny-internet-je/r~1e39ea904bbf11e98aa4ac1f6b220ee8/

Otázky a odpovědi: Jak může reforma copyrightu s články 11 a 13 změnit internet? - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 28.03.2019]. Dostupné z: https://www.lupa.cz/clanky/otazky-a-odpovedi-jak-muze-reforma-copyrightu-s-clanky-11-a-13-zmenit-internet/

160 YouTube Statistics and Facts (2019) By the Numbers [online]. [cit. 28.03.2019] Dostupné z: https://expandedramblings.com/index.php/youtube-statistics/

Netiquette Guidelines, Sally Hambridge, Albury's Local Internet Service Provider, Personalised service, professional support. [online]. [cit. 28.03.2019] Dostupné z: http://www.albury.net.au/new-users/rfc1855.txt

1 Second - Internet Live Stats. Internet Live Stats - Internet Usage & Social Media Statistics [online]. Copyright © Copyright internetlivestats.com [cit. 28.03.2019]. Dostupné z: http://www.internetlivestats.com/one-second/#traffic-band

Are You Ready for Web 2.0? | WIRED. *WIRED* [online]. Copyright © 2018 Condé Nast. All rights reserved. [cit. 28.03.2019]. Dostupné z: https://www.wired.com/2005/10/are-you-ready-for-web-2-0/

GDPR | Obecné nařízení o ochraně osobních údajů - prakticky [online]. [cit. 28.03.2019]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/cookies

Behaviorální reklama | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů - prakticky [online], [cit. 28.03.2019]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/behavioralni-reklama/