Univerzita Palackého v Olomouci
Právnická fakulta

Lukáš Černý

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

Diplomová práce

Olomouc 2019

Prohlašuji, že jsem diplomovou práci na téma *Zpracování osobních údajů ve světle Nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR)* vypracoval samostatně a citoval jsem všechny použité zdroje.

V Liberci dne 25. března 2019

Lukáš Černý

Poděkování:

Touto cestou bych rád vyjádřil poděkování Mgr. Petře Melotíkové, Ph.D. za její cenné rady, vstřícnost a trpělivost při vedení mé diplomové práce. Rovněž bych chtěl poděkovat advokátní kanceláři Havelka & Musil VGD Legal, s.r.o., zejména partnerovi kanceláře, panu Robertu Musilovi, za poznatky z praxe ochrany osobních údajů, materiální pomoc při získání potřebných informací a podkladů, jakož i za morální podporu při psaní diplomové práce. Poděkování patří též mé rodině a blízkým přátelům za pomoc a podporu během studia.

Obsah

Seznam použitých zkratek

ZOOÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
ObčZ	zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
Směrnice 95/46/ES	směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
GDPR	nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Úmluva č. 108	úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat
SFEU	Smlouva o fungování Evropské unie
SEU	Smlouva o Evropské unii
LZPS	usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů
Listina EU	Listina základních práv Evropské unie
ÚOOÚ	Úřad pro ochranu osobních údajů
SDEU	Soudní dvůr Evropské unie
NSS	Nejvyšší správní soud
Sbor	Evropský sbor pro ochranu osobních údajů
WP29	Pracovní skupina 29 zřízená podle čl. 29 Směrnice 95/46/ES
DPIA	Data Protection Impact Assessment, neboli posouzení vlivu na ochranu osobních údajů

DPO	Data Protection Officer, neboli pověřenec pro ochranu osobních údajů
RBA	Risk-based Approach, neboli přístup založený na riziku

Úvod

V dubnu roku 2016 vstoupilo v platnost nové nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[1]. GDPR má za cíl mimo jiné sjednocení úpravy ochrany osobních údajů v členských státech Evropské unie a ve státech Evropského hospodářského prostoru. Jedná se o významný právní předpis na poli zpracování osobních údajů, neboť ruší Směrnici 95/46/ES a do jisté míry nahrazuje dosavadní národní úpravy ochrany osobních údajů v členských státech.

Někdy v prvním čtvrtletí roku 2017 jsem poprvé zaregistroval výraznou reklamní kampaň často zmiňující slovo GDPR spolu se slogany „*Připravte se včas!*“ nebo „*Obrovské pokuty*“ či dokonce „*Revoluce v ochraně osobních údajů*“. Začal jsem se o tuto problematiku (tak trochu povinně) zajímat blíže během praxe v advokátní kanceláři, kde bylo téma GDPR velmi často skloňovaným termínem i v souvislosti se zadáním nových úkolů od klientů, kteří něco jako implementaci Nařízení do sfér jejich podnikatelské činnosti často požadovali. Po přečtení základní odborné literatury a zejména informativních příspěvků ÚOOÚ[2] k tomuto tématu jsem začal být toho názoru, že hysterie kolem nového předpisu je přehnaná a současně jsem cítil potřebu tuto skutečnost nějakým způsobem vyjádřit a dokázat. Ideální se tak jevil podzim roku 2017, kdy jsem jako student 4. ročníku podával žádost o schválení tématu diplomové práce. Nenapadlo mě nic aktuálnějšího než právě tematika zpracování osobních údajů.

Téma jsem si vybral proto, že mám velmi blízko k informačním a zejména komunikačním technologiím, kde je otázka ochrany osobních údajů čím dál tím důležitější. Domnívám se, že interpretační otázky vyvolané GDPR budou ještě dlouho předmětem odborné diskuze, neboť i přes přímý účinek tohoto předpisu zůstávají některá jeho ustanovení neurčitá. Především nové instituty vyvolávají výkladové otázky, a tak významnou roli bude hrát nejen Soudní dvůr Evropské unie se svou výkladovou pravomocí, ale také pokyny a stanoviska dozorových orgánů nebo nově zřízeného Sboru.

Je evidentní, že přijetím obecné regulativy na úrovni Evropské unie se ochrana osobních údajů dostala do popředí aktuálních trendů v oblasti poskytování právních služeb. Odborná veřejnost se s problematikou stále spíše seznamuje a téma samo o sobě není právní vědou vyčerpáno. Zejména dosud nejsou vypořádány některé otázky související s neurčitými právními pojmy GDPR, kterých je v nařízení mnoho a nesvědčí právní jistotě správců a zpracovatelů.

---

[1] Dále také jen „*GDPR*“
[2] Úřad pro ochranu osobních údajů.

Cílem mé diplomové práce je tedy analýza základních koncepčních bodů GDPR a jejich následná komparace s relevantní právní úpravou dosavadního ZOOÚ[3]. Vzhledem k tomu, že GDPR v některých případech zmocňuje členský stát, aby v mezích tohoto zmocnění přijal zvláštní právní úpravu, jako přiléhavé shledávám zmínit i odpovídající specifika návrhu českého adaptačního zákona, který byl ke dni odevzdání diplomové práce postoupen prezidentovi České republiky k podpisu. S ohledem na rozmanitost právní úpravy zpracování osobních údajů je diplomová práce zaměřena pouze na vybrané otázky a nikoli na všechny aspekty zpracování osobních údajů. Za tím účelem je diplomová práce strukturována do čtyř kapitol. V kapitole první se obecně věnuji ochraně osobních údajů ve vztahu k ochraně soukromí a stručně také vývojem právní úpravy ochrany osobních údajů. Ve druhé kapitole pojednávám o ústavních, zákonných, komunitárních a mezinárodních pramenech ochrany osobních údajů. Třetí kapitola je věnována vymezení základních pojmů, se kterými bude v diplomové práci pracováno, jako je osobní údaj, kde pozornost upínám také k otázce jeho objektivního či subjektivního pojetí, dále pojmu správce či zpracovatele osobních údajů a také samotnému pojmu zpracování. Čtvrtá kapitola, která tvoří jádro této diplomové práce, pojednává o samotné komparaci právní úpravy zpracování osobních údajů v České republice. V této kapitole se zaměřuji na analýzu zásad zpracování, právních titulů zpracování, práv a povinností subjektů, postavení ÚOOÚ a sankce. V kontextu čtvrté kapitoly odpovídám na následující výzkumné otázky: *Jak se mění práva náležící subjektům údajů? Jak se změnily povinnosti správce a zpracovatele osobních údajů? Vyhoví malý a střední podnik[4] povinnostem GDPR již při dodržování dosavadních povinností dle ZOOÚ? Jaké pokuty hrozí správcům a zpracovatelům pro případ porušení povinností z GDPR? Jaké je postavení ÚOOÚ po nabytí účinnosti GDPR?* Po zodpovězení shora uvedených otázek budu schopen učinit závěr o oprávněnosti nazývat GDPR revolucí v ochraně osobních údajů. V duchu uvedené teze o revoluci v ochraně osobních údajů se budu snažit potvrdit nebo vyvrátit hypotézu, že malý a střední podnik bude v souladu s novou právní úpravou GDPR již při dodržování povinností dle ZOOÚ.

V této diplomové práci je využívána především metoda komparace, která má za cíl porovnat základní instituty dosavadní právní úpravy ochrany osobních údajů v České republice

---

[3] zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

[4] Pro účely této diplomové práce je využíváno těchto pojmů tak, jak je definuje Doporučení Komise Evropské unie, na které odkazuje i bod 13 odůvodnění GDPR. Podnikem je podle čl. 1 a čl. 2 tohoto doporučení „*každý subjekt vykonávající hospodářskou činnost, bez ohledu na jeho právní formu.*“ Jedná se například o osoby samostatně výdělečně činné, rodinné firmy, obchodní společnosti či jakékoli jiné subjekty, které pravidelně vykonávají hospodářskou činnost. Pro naplnění kritéria malého až středního podniku, musí tyto subjekty mít méně než 250 zaměstnanců a roční obrat do 50 milionů EUR nebo rozvahu do 43 milionů EUR. K podrobnostem srov. Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků. Úř. věst. L 124, 20.5.2003, s. 36 a násl.

s odpovídající úpravou v GDPR. Do předmětu komparace budou zahrnuta i ustanovení návrhu zákona o zpracování osobních údajů, jež v mezích nového nařízení upřesňují některé jeho instituty nebo stanoví výjimky. Ve vztahu k nově vymezeným institutům je užívána především metoda popisná s cílem upozornit na základní otázky, se kterými se subjekty na poli zpracování osobních údajů budou muset vypořádat. Kromě mé vlastní tvůrčí činnosti a mých vlastních názorů v diplomové práci vycházím z názorů právní teorie, a to zejména z komentářové literatury NULÍČEK, Michal a kol. (ed.) *GDPR - obecné nařízení o ochraně osobních údajů (2016/679/EU) - Praktický komentář*. Praha: Wolters Kluwer, 2017, 525 s. či monografie ŽŮREK, Jiří. Praktický průvodce GDPR. 2. vydání. Olomouc: ANAG, 2018, 224 s. a také z odborných časopisů a odborných internetových článků k dané problematice.

Od této práce očekávám, že na základě prostudování příslušné literatury u mě dojde k prohloubení znalostí v oblasti ochrany osobních údajů, které mi mimo jiné rozšíří možnosti uplatnění na trhu práce.

Diplomová práce vychází z právního stavu ke dni 25. 3. 2019.

1 Právo na ochranu soukromí a osobních údajů

Ochrana osobních údajů patří bezesporu k jedné z velmi aktuálních právních otázek, a to nejen kvůli přijetí obecného nařízení o ochraně osobních údajů (GDPR), které je toliko důsledek velkého zájmu o problematiku, ale zejména v souvislosti s rychlým vývojem moderních technologií během předchozí dekády 21. století. Dnes si totiž nejde představit oblast společenského života, ve které by nedošlo ke zpracování osobních údajů v nějaké formě. Ať už jde o nákup prostřednictvím bankovní karty, o běžný telefonický hovor, nákup přes e-shopy nebo o nástup do zaměstnání, všude dochází ve větší či menší míře ke zpracování osobních údajů a k ohrožení soukromí fyzických osob.[5]

1.1 Ochrana soukromí

Právo na ochranu osobních údajů je součástí práva na ochranu soukromí[6], přičemž soukromí fyzických osob je tvořeno mimo jiné jejich osobními údaji.[7] Jak již z předchozí věty vyplývá, soukromí není tvořeno pouze osobními údaji, ale rozličným množstvím různorodých součástí, z nichž jen některé souvisí s ochranou osobních údajů[8]. Soukromí bylo v právních normách zmiňováno již po mnoho staletí, avšak pouze jako přívlastek, tedy jako vyjádření skutečnosti, že něco někomu patří anebo musí být respektováno.[9] Právo na ochranu soukromí, jako samostatná právní kategorie, bylo vůbec poprvé formulováno v článku S.D. Warrena a L.D. Brandeise „*The Right of Privacy*" vydaném v Harvard Law Review v roce 1890[10]. Obsah práva na ochranu soukromí se autoři zmíněného článku snažili vymezit s odkazem na rozhodnutí evropských soudů a evropské legislativy k ochraně osobní cti a dobré pověsti. Poslání tohoto příspěvku později rozvinul sám L.D. Brandeis disentem v případu *Olmstead vs. USA,* jež se týkal přípustnosti důkazu získaného nezákonným odposlechem. K výraznému judikaturnímu posunu chápání práva na ochranu soukromí však došlo až ve věci *Nardone a Weiss,* ze kterého byl zjevný příklon ke konceptu soukromí jako sféře myšlení a jednání, která má být svobodná od zásahů ze strany státu.[11] Soukromí lze proto obecně vymezit jako určité prostředí, ve kterém se určitá osoba pohybuje a kde se předpokládá, že do tohoto prostředí nebude bez souhlasu této osoby ze strany jiné osoby nebo státu zasahováno.[12]

---

[5] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 7.
[6] KUČEROVÁ, Alena. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 1-4 (§ 1).
[7] MATES, Pavel. *Ochrana soukromí ve správním právu*. 2. vydání. Praha: Linde, 2006, s. 184.
[8] NOVÁK, Daniel. In NOVÁK, Daniel (ed). *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2015, s. XVIII.
[9] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 9.
[10] Tamtéž., s. 11.
[11] NOVÁK, Daniel. In NOVÁK, Daniel (ed). *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2015, s. XVII.
[12] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 13.

Právo na ochranu soukromí ve smyslu povinnosti státu nezasahovat do soukromé sféry osob nabylo společenského významu zejména po druhé světové válce[13], kdy se již v legislativě objevují pravidla omezující zásahy do soukromí osob právě s ohledem na zkušenosti s řízenou perzekucí obyvatelstva z náboženských či etnických důvodů[14]. Ochrana soukromí nabývala na důležitosti také ve druhé polovině 20. století, a to právě s rozvojem informačních a komunikačních technologií.[15] Proto již v 70. letech dochází v demokratických zemích Evropy k přijetí vůbec prvních zvláštních zákonů o ochraně osobních údajů[16], přičemž další vlna přijímání této legislativy přišla s pádem totalitních režimů států východního bloku Sovětského svazu v 90. letech 20. století.

Nutno ovšem poznamenat, že žádná mezinárodní smlouva, ústava ani zákony a jiné právní předpisy žádného státu obsah pojmu ochrana soukromí nedefinují a netroufá si tak učinit ani judikatura.[17] To plně koresponduje se skutečností, že v právní teorii neexistuje jednoznačná shoda na obsahu tohoto pojmu. Například Mates ve své analytické definici do práva na ochranu soukromí zahrnuje ochranu obydlí, vstup na pozemky a jiné nemovitosti, nedotknutelnost osoby, zjišťování totožnosti, omezení osobní svobody, jméno a příjmení, ochranu korespondence a komunikace, ochranu soukromí ve správním řízení, ochranu soukromí v reklamě, ochranu osobních údajů, ochranu soukromí v činnosti policie a povinnost mlčenlivosti[18]. Jiní právní teoretici zase právo na ochranu soukromí vnímají ve čtyřech rovinách, tj. v rovině informační, zahrnující ochranu údajů o jednotlivci a jeho korespondenci před neoprávněným zveřejněním, dále v rovině fyzické, jež je tvořena tělesnou integritou jednotlivce, v rovině rozhodovací týkající se práva jednotlivce učinit svobodné rozhodnutí a konečně v rovině vlastnické, která je tvořena majetkovými zájmy jednotlivců.[19] Z této teorie 4 rovin ochrany soukromí je evidentní, že právo na ochranu osobních údajů má nejužší vztah právě k soukromí ve smyslu informačním.[20]

Od původního pojetí soukromí ve smyslu určité vnitřní sféry, do které nesmí nikdo zasahovat se právní doktrína posunula o něco dále zejména díky judikatuře Evropského soudu pro lidská práva. Tak např. ve věci *Niemitz vs. Německo* soud dospěl k závěru, že omezovat pojem soukromí pouze na vnitřní sféru jednotlivce by bylo příliš restriktivní. Pod pojem

---

[13] NOVÁK: *Zákon o ochraně osobních údajů…*, s. XVI-XVII.
[14] Tamtéž.
[15] MATES, Pavel. *Ochrana soukromí ve správním právu*. 2. vydání. Praha: Linde, 2006, s. 187.
[16] MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana. 2. vydání*. Praha: Wolters Kluwer, 2008, s. 1.
[17] Tamtéž, s. 14.
[18] Tamtéž, s. 20.
[19] ALLEN, A. L. In ROTSHTEIN, M. A. (ed). *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*. New Haven: CT: Yale University Press, 1997, s. 31-59.
[20] NOVÁK: *Zákon o ochraně osobních údajů…*, s. XX.

soukromý život se tak má zahrnovat rovněž i právo vytvářet a rozvíjet vztahy k ostatním lidem, zejména příbuzným. V judikatuře Ústavního soudu České republiky se ustálil názor, že právo na ochranu soukromí je třeba chápat ve smyslu pozitivním, zahrnujícím právo člověka na svobodné rozhodnutí, zda a v jakém rozsahu zpřístupní veřejnosti skutečnosti ze svého života a ve smyslu negativním, který indikuje povinnost státu nezasahovat do této vnitřní sféry fyzické osoby a odpovídající právo osoby bránit se proti těmto zásahům.[21]

Lze uzavřít, že právo na ochranu soukromí je velmi široký pojem, na který je v právní nauce nahlíženo rozdílně. Jednoznačná shoda panuje prakticky pouze na tom, že právo na ochranu soukromí není právem absolutním, neboť je do něho možné zasahovat na základě zákona a současně pokud je to v demokratické společnosti nezbytné. [22]

1.2 Ochrana osobních údajů

Jak je zmíněno výše, právo na ochranu osobních údajů úzce souvisí s právem na ochranu soukromí. Jako právní disciplína však nemá na rozdíl od ochrany soukromí příliš dlouhou historii. Značným impulsem pro vznik tohoto právního fenoménu byl kromě událostí během druhé světové války zejména mohutný rozmach informačních technologií ve druhé polovině 20. století. Výpočetní technika zpracovává velké množství dat, provádí selekci či předává osobní údaje dalším osobám zcela automatizovaně, přitom jakmile je osobní údaj poskytnut, už většinou nelze takový úkon vrátit zpět, tedy navrátit stav ve stav předcházející poskytnutí osobních údajů.[23] Zvláštní předpisy o ochraně osobních údajů vznikaly zejména jako reakce na možnosti jednotlivce využívat osobní údaje o sobě samém, přičemž tyto zvláštní předpisy měly zajišťovat, aby tato ochrana byla jednotlivcům poskytnuta, aniž by se jí jednotlivec musel aktivně domáhat.[24] Domnívám se tedy, že bylo nevyhnutelné, aby státy přijmuly zvláštní právní úpravu o ochraně osobních údajů, která by poskytla fyzickým osobám nezbytnou úroveň ochrany jejich soukromí.

Smyslem ochrany osobních údajů samozřejmě není poskytnout absolutní ochranu všem případům používání osobních údajů, ale mimo jiné stanovit jasná pravidla pro legální použití těchto údajů.[25]. Podle Matoušové je ochrana osobních údajů založena na několika obecných zásadách, a to zejména, že subjekt údajů má určitá práva, dále že osoba, která zpracovává osobní údaje jiných osob, má určité povinnosti uložené jí zákonem nebo na základě zákona, že práva a povinnosti, které jsou obsahem ochrany osobních údajů, jsou stanoveny na základě

[21] MATES: *Ochrana soukromí…*, s. 15.
[22] Tamtéž, s. 16.
[23] Tamtéž, s. 184.
[24] MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. vydání. Praha: Wolters Kluwer, 2008, s. 2.
[25] Tamtéž, s. 3.

proporcionality a že na dodržování plnění povinností dle zákona dohlíží nezávislý dozorový orgán.[26] Z výše uvedeného tedy vyplývá, že v právních vztazích vznikajících při ochraně osobních údajů na jedné straně stojí nositelé povinností, kterými jsou stát a právnické a fyzické osoby, a na straně druhé fyzické osoby požívajících určitých práv na poli ochrany osobních údajů.

Právo na ochranu osobních údajů, jakožto kategorie práva na ochranu soukromí, však musí být náležitě právními předpisy definováno, neboť původní pojetí ochrany soukromí jako práva být ponechán sám je v současné moderní společnosti nenaplnitelné.[27] Pramenům ochrany osobních údaj se věnuje následující kapitola.

[26] MATOUŠOVÁ, HEJLÍK: *Osobní údaje…*, s. 3.
[27] Tamtéž, s. 8.

2 Právní rámec ochrany osobních údajů

2.1 Ústavní prameny

Mezi základní vnitrostátní pramen ochrany osobních údajů na ústavní úrovni v České republice se řadí především Listina základních práv a svobod.[28] Podle čl. 7 odst. 1 LZPS je zaručena nedotknutelnost osoby a jejího soukromí, přičemž toto ustanovení lze považovat za základní a obecné pravidlo, které určuje podklad pro další ustanovení upravující různé zvláště chráněné projevy soukromí.[29] Mezi tato ustanovení LZPS patří čl. 10 odst. 2, podle kterého má každý právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Přímo osobních údajů se dotýká čl. 10 odst. 3 LZPS, podle kterého má každý právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Ochranu před nezákonným zpracováním osobních údajů na ústavní úrovni poskytuje ještě čl. 13 LZPS, který stanoví, že nikdo nesmí zasahovat do listovního tajemství a záznamů uchovávaných v soukromí nebo zasílaných poštou a dalšími způsoby či tajemství podávaného telefonem, telegrafem nebo jiným podobným zařízením. Tento posledně citovaný článek je v dnešní době velmi důležitý v souvislosti se sledováním elektronické komunikace, jejíž ochrana s ohledem na široké pojetí listovního tajemství podle čl. 13 LZPS tomuto ustanovení rovněž podléhá.[30] Odlišně na systematiku ochrany soukromí nahlíží Wagnerová, která za základ pro ochranu soukromí na ústavní úrovni považuje čl. 10 LZPS, když v odst. 1 je podle autorky obsažena ochrana lidské důstojnosti, v odst. 2 obecné vymezení ochrany soukromí a rodinného života a v odst. 3 explicitně uvedené právo na informační sebeurčení, které však Evropský soud pro lidská práva dovozuje z práva na soukromý život. Na tento článek pak navazují výše zmíněná další ustanovení LZPS vztahující se k ochraně soukromí.[31]

2.2 Zákonné prameny

Vnitrostátní prameny zákonné úrovně lze rozdělit na prameny soukromoprávní a veřejnoprávní povahy.[32] Mezi soukromoprávní prameny jednoduchého práva se řadí zejména ObčZ[33]. Domnívám se, že je to hlavně proto, že především v úvodních ustanoveních zákonodárce vymezil základní zásady soukromého práva včetně obecných imperativů ochrany

[28] KUČEROVÁ, Alena. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 1-4 (§ 1).
[29] NULÍČEK, Michal a kol. In NULÍČEK, Michal a kol. (ed.) *GDPR - obecné nařízení o ochraně osobních údajů (2016/679/EU) - Praktický komentář*. Praha: Wolters Kluwer, 2017, s. 58 (čl. 1).
[30] Tamtéž.
[31] WAGNEROVÁ, Eliška. In WAGNEROVÁ, Eliška a kol. (ed). *Listina základních práv a svobod – Komentář*. Praha: Wolters Kluwer ČR, 2012, s. 280.
[32] KUČEROVÁ: *Zákon o ochraně osobních údajů…*, s. 1-4 (§ 1).
[33] Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

soukromí člověka. Konkrétní projevy ochrany soukromí jsou promítnuty do právní úpravy ochrany osobnosti podle § 81 a násl. ObčZ, jakož i do ust. § 77 a násl. ObčZ, pokud se jedná o ochranu práva ke jménu.

Veřejnoprávních pramenů ochrany osobních údajů na zákonné úrovni je široká škála, přičemž mezi obecnou úpravu řadíme ZOOÚ, který se vztahuje na jakékoliv zpracování osobních údajů, a to bez ohledu na to, zda se tak děje automatizovaně nebo jinými prostředky.[34] Ochraně osobních údajů se však věnuje další řada zvláštních zákonů. Mezi ně patří například zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 127/2005 Sb., o elektronických komunikacích o změně některých souvisejících zákonů, ve znění pozdějších předpisů, zákon č. 480/2004, o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů, nebo zákon č. 46/2000 Sb., právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), ve znění pozdějších předpisů.[35] Podle Kučerové ZOOÚ nepatří mezi pramen čistě veřejnoprávní povahy, ale považuje jej za předpis smíšené povahy, když kombinuje veřejnoprávní a soukromoprávní normy. Tak například ustanovení týkající se dozorové činnosti dozorového orgánu považuje za úpravu veřejnoprávní a ustanovení týkající se ochrany soukromí a osobního života naopak za normy soukromého práva.[36] Vzhledem k tomu, že Česká republika je smluvní stranou mnoha mezinárodních smluv a také k tomu, že se v roce 2004 stala členským státem Evropské unie, nelze prameny ochrany osobních údajů izolovat pouze na tuzemské právní předpisy, ale i na prameny mezinárodního práva nebo komunitárního práva. To ostatně plyne i z ust. § 1 ZOOÚ. O těchto zdrojích práva pojednávají následující podkapitoly.

2.3 Právo Evropské unie

Komunitární prameny ochrany osobních údajů lze rozdělit podle toho, zda mají svůj původ v primárním anebo sekundárním právu EU. V primárním právu EU je ochraně osobních údajů věnováno zejména ust. čl. 16 SFEU, podle kterého má každý právo na ochranu osobních údajů, které se jej týkají. Dalším pramenem primárního práva EU na poli ochrany osobní údajů je Listina EU. Podle čl. 7 tohoto dokumentu má každý právo na respektování svého soukromého a rodinného života, obydlí a komunikace. Speciálně osobních údajů se dotýká ust. čl. 8 odst. 1 až 3 Listiny EU, které stanovuje, že každý má právo na ochranu osobních údajů, které se ho týkají, přičemž tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na

[34] MATES:. *Ochrana soukromí…*, s. 189.
[35] NULÍČEK, Michal a kol. In NULÍČEK, Michal a kol. (ed.) *GDPR - obecné nařízení o ochraně osobních údajů (2016/679/EU) - Praktický komentář*. Praha: Wolters Kluwer, 2017, s. 58 (čl. I.).
[36] KUČEROVÁ: *Zákon o ochraně osobních údajů…*, s. 1-4 (§ 1).

základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. [37]

Mezi základní pramen sekundárního práva EU byla dosud řazena Směrnice 95/46/ES ze dne 24. 10. 1995, která je též nazývána Data Protection Directive.[38] Do nabytí účinnosti nové legislativy se jednalo o hlavní nástroj stanovení minimální úrovně ochrany osobních údajů v členských státech.[39]V České republice byla tato směrnice provedena ZOOÚ. Na směrnici 95/46/ES navazují další speciální směrnice, které materiálně obsahují zvláštní úpravu ochrany osobních údajů.[40] Jako příklad lze uvést směrnici 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), zkráceně též jako DPEC, resp. Directive on Privacy and Electronic Communications nebo též jako e-Privacy směrnice.

Na jaře roku 2016 došlo k přijetí GDPR. Důvodem byla zejména skutečnost, že stávající unijní legislativa v podobě Směrnice 95/45/ES státům při implementaci pravidel do vnitrostátních předpisů umožňovala přijetí celé řady odchylek, což vedlo k tomu, že ochrana osobních údajů byla v Evropské unii v závislosti na národní úpravě roztříštěna. Posláním GDPR bylo a je právní úpravu Evropské unie sjednotit, což ostatně zjevně vyplývá již ze zákonodárcem použité formy právního předpisu – nařízení podle čl. 288 SFEU. Nařízení je totiž, na rozdíl od směrnice, přímo použitelné v členském státě, aniž by tento členský stát musel přijímat zvláštní implementační zákon. Právní předpis ve formě nařízení se značí také tím, že má aplikační přednost před národní úpravou a pro případ, že by právní předpis členského státu byl s nařízením v rozporu, aplikuje se přednostně právě nařízení. Zásadu přímého účinku a aplikační přednosti dovodil výkladem v minulosti jak Soudní dvůr Evropské unie[41], tak později i Ústavní soud České republiky.[42] Aby mohl být účel nařízení v podobě unifikace právní úpravy naplněn, neměl by žádný členský stát přijmout právní úpravu, která by se odchylovala od nařízení, ledaže to nařízení samo dovoluje.[43] Kromě sjednocení právních úprav je cílem GDPR posílit účinnou ochranu osobních údajů fyzických osob, ale také stanovení pravidel týkající se volného pohybu osobních údajů zejména ve vztahu k jejich předávání do

[37] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 28 (§ 1).
[38] Tamtéž, s. 40 (§ 1).
[39] NULÍČEK: *GDPR - Obecné nařízení…*, s. 59 (čl. 1.).
[40] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 41 (§ 1).
[41] Soudní dvůr: Rozsudek ze dne 5. února 1963, *Van Gend en Loos*, věc 26/62; Soudní dvůr: rozsudek ze dne 15. července 1964, *Costa vs. ENEL*, věc 6/64; Soudní dvůr: rozsudek ze dne 9. března 1978, *Simmenthal*, věc 106/77.
[42] nález Ústavního soudu ze dne 8. března 2006, sp. zn. Pl. ÚS 50/2004.
[43] NULÍČEK: *GDPR - Obecné nařízení…*, s. 59 (čl. I.).

třetích zemí. GDPR se však nevztahuje na osobní údaje právnické osoby.[44]Podrobněji bude o GDPR v této diplomové práci pojednáno níže v rámci komparace s dosavadní právní úpravou.

V současné době je v legislativním procesu Evropské unie v přípravě nové nařízení, které má nahradit shora uvedenou e-privacy směrnici. Nařízení e-Privacy, jak je připravovaný právní předpis triviálně označován, bude mít za cíl mimo jiné ochranu soukromí na poli elektronických komunikací, zejména v oblasti internetu, nevyžádané elektronické pošty, takzvaného internetu věcí (IoT) a dalších souvisejících oblastí, tedy pouze určitou výseč ochrany osobních údajů.[45] Nařízení e-Privacy bude k GDPR zvláštním předpisem a GDPR subsidiární právní úpravou. Nové nařízení mělo nabýt účinnosti ve stejný okamžik jako GDPR, avšak z důvodu značného prodloužení legislativních příprav se platnost očekává nejdříve v roce 2020.[46]

2.4 Mezinárodní právo

Nemálo významné jsou pro ochranu osobních údajů i prameny mezinárodního práva. Domnívám se, že vzhledem k provázanosti práva na ochranu osobních údajů a práva na ochranu soukromí lze za pramen ochrany osobních údajů považovat i mnohé dokumenty vztahující se obecně k ochraně přirozených práv člověka. Základním pramenem je tak nepochybně Všeobecná deklarace lidských práv, která ve svém čl. 12 stanoví, že nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Podle navazující části tohoto článku má proti takovým zásahům nebo útokům každý právo na zákonnou ochranu. Shodné pravidlo obsahuje i Mezinárodní pakt o občanských a politických právech.[47]

Prakticky mnohem významnější mezinárodní smlouvy jsou ty, které byly přijaty na poli Rady Evropy.[48] Nelze tak opomenout Úmluvu o ochraně lidských práv a základních svobod a její čl. 8 odst. 1 přiznávající každé fyzické osobě právo na respektování svého soukromého a rodinného života, obydlí a korespondence. Na zmíněný dokument navazuje Úmluva č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních údajů, když podle jejího čl. 3 odst. 1 se smluvní strany zavazují uplatnit Úmluvu č. 108 pro automatizované soubory osobních údajů a jejich automatizovaná zpracování ve veřejném a soukromém sektoru. Úmluva č. 108 byla přijata v roce 1981 a byla vůbec prvním mezinárodním dokumentem týkajícím se specificky ochrany osobních údajů.[49] Česká republika Úmluvu č. 108 ratifikovala v roce

[44] Bod 14 odůvodnění GDPR.
[45] NEŠPŮREK, Robert a kol. Nařízení e-privacy: *Jak se změní nakládání s cookies?* [online]. profipravo.cz, 27. září 2018 [cit. 1. prosince 2018]. Dostupné na <https://www.pravniprostor.cz/clanky/ostatni-pravo/narizeni-e-privacy-jak-se-zmeni-nakladani-s-cookies>.
[46] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. vydání. Olomouc: ANAG, 2018, s. 19.
[47] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 6 (§ 1)
[48] Tamtéž.
[49] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 8 (§ 1)

2001. [50] Praxe však ukázala, že není vhodné v ochraně osobních údajů oddělovat automatizované a neautomatizované zpracovaní osobních údajů, nýbrž je potřeba na způsob zpracování osobních údajů nahlížet jako na rovnocennou volbu odpovědného subjektu.[51] Tento problém nejednotnosti však navazující právní úprava odstranila, když nejen GDPR, ale i dosavadní směrnice (a tedy i ZOOÚ) poskytuje ochranu osobních údajů při zpracování osobních údajů, které probíhá jak automatizovaně, tak neautomatizovaně.[52]

[50] Tamtéž, s. 9 (§ 1)
[51] KUČEROVÁ: *Zákon o ochraně osobních údajů…*, s. 1-4 (§ 1).
1-4 (§ 1).
[52] Srov. čl. 2 odst. 1 GDPR; čl. 3 odst. 1 Směrnice 95/46/ES; ust. § 3 odst. 2 ZOOÚ.

3 Vymezení základních pojmů

3.1 Osobní údaj

Vymezení pojmu osobní údaj je z hlediska problematiky ochrany osobních údajů zásadní, protože jen osobním údajům je v kontextu ZOOÚ a GDPR poskytnuta ochrana. Údaje, které nenaplňují definiční znaky pojmu osobní údaj sice mohou být rovněž chráněny, avšak prostřednictvím jiných právních mechanismů, mezi které se řadí například institut ochrany osobnosti podle občanského zákoníku.[53]

Osobní údaj je podle ZOOÚ „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.*“.[54] Tato definice, byť českým zákonodárcem mírně doplněna, má svůj původ v Úmluvě č. 108 a směrnici 95/46/ES.

Ze směrnice 95/46/ES definici osobního údaje doslovně přebírá GDPR, které původní definici (převzatou také ZOOÚ) doplňuje o několik dalších identifikátorů, kterými lze fyzickou osobu identifikovat, a to jmenovitě o lokační údaje, síťové identifikátory a co se týče prvků lidské identity, i o její genetický aspekt.[55] K rozšíření definice osobního údaje však podle všeho nedochází. Dokladem toho je SDEU, který již v roce 2016 judikoval, že za osobní údaj je nutno považovat i dynamickou IP adresu[56], jakožto druh síťového identifikátoru, který se nyní objevil v demonstrativním výčtu definice dle čl. 4 písm. a) GDPR. ÚOOÚ, jehož postavení po nabytí účinnosti GDPR bude vymezeno dále v této diplomové práci, dokonce konstatoval, že tvrzení o rozšíření definice osobního údaje v GDPR je jedním z omylů laické a leckdy i odborné veřejnosti.[57] Úmyslem unijního a posléze českého zákonodárce bylo vymezením osobního údaje pokrýt co nejširší škálu informací, které se vztahují ke konkrétní fyzické osobě a souladně s tímto širokým pojetím osobního údaje je i SDEU ve své rozhodovací praxi (viz shora uvedený judikát).[58]

S ohledem na shora uvedené se domnívám, že definice osobního údaje se oproti směrnicové a vnitrostátní úpravě téměř nezměnila. Rozhodně nelze přijmout závěr, že došlo k jejímu rozšíření, byť unijní zákonodárce do výčtu identifikátorů přidal síťové identifikátory,

---

[53] NONNEMANN, František. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 50 (§ 4 písm. a))
[54] § 4 písm. a) ZOOÚ.
[55] Čl. 4 odst. 1 GDPR.
[56] Rozsudek ze dne 19. října 2016, *Patrick Breyer proti Spolkové republice Německo*, C-582/14, výrok I.
[57] Úřad pro ochranu osobních údajů. *Desatero omylů* [online]. uoou.cz, [cit. 1. prosince 2018]. Dostupné na <https://www.uoou.cz/desatero%2Domylu/ds-4818/p1=4818>
[58] NULÍČEK: *GDPR - Obecné nařízení…*, s. 77 (čl. 4 písm. a).

lokační údaje a mezi prvky identity fyzické osoby zahrnul i genetický aspekt. Definice osobního údaje nemůže být výčtová a ani výčet identifikátorů v takové definici nemůže být taxativní. Právní úprava by pak totiž zůstala zafixovaná ve stupni vývoje vědy a informačních technologií ke dni přijetí daného předpisu. Množství druhů osobních údajů se mimo jiné s každou novou technologií totiž výrazně zvětšuje. Právě z toho důvodu byla definice osobního údaje od počátku pojata široce.[59] Vzhledem k neměnnosti definice osobního údaje od dob přijetí směrnice 95/46/ES jsem toho názoru, že na pojem osobního údaje lze aplikovat dosavadní doktrinální závěry, výkladová stanoviska příslušných úřadů a judikaturu SDEU či tuzemských soudů.

Možnost identifikace subjektu (identifikatelnost) údajů vyvolává jistou interpretační otázku, a to sice, zda identifikovatelnost fyzické osoby vykládat na základě objektivních, nebo subjektivních kritérií. Jinými slovy jde o to, zda může být tentýž údaj osobním údajem jak pro správce, který je schopen jednoznačně určit konkrétní fyzickou osobu, tak i pro jiného správce, který takové identifikace subjektivně schopen není. Judikatura českých soudů v názoru na pojetí osobního údaje není zcela jednotná.[60] Subjektivní pojetí osobního údaje vyplývá z rozsudku NSS sp. zn. 1 As 98/2008 ze dne 29. 7. 2009. Zcela opačný závěr však NSS přijal v rozsudku sp. zn. 9 As 34/2008, ze dne 12. 2. 2009. V posledně uvedeném rozhodnutí soud konstatoval, že osobním údajem je i číslo mobilního telefonu určité fyzické osoby, byť takové číslo osoba má mnohdy jen dočasně. Určitý posun k objektivnímu pojetí lze zaznamenat v rozsudku NSS sp. zn. 1 As 113/2012, ze dne 25. 2. 2019, kde se soud zabýval otázkou identifikovatelnosti osob při provozu kamerového systému.[61] Názory se přitom liší i v právní doktríně. Pro subjektivní pojetí pojmu osobní údaj je Novák[62] a rovněž Aujezdský.[63] Naopak k objektivnímu výkladu pojmu osobní údaj tenduje Matoušová a Hejlík.[64] Objektivní pojetí osobního údaje pak podporuje jak Nonnemann[65], tak i autoři komentářové literatury ke GDPR. Opačný výklad by podle nich totiž jinak nedůvodně směřoval ke snížení ochrany osobních údajů. Správce či zpracovatel by pak mohl volně, např. za úplatu, nakládat s osobními údaji, aniž by byl vázán veřejnoprávní regulací, a to pouze z důvodu, že sám subjektivně není schopen

---

[59] Úřad pro ochranu osobních údajů. *Desatero omylů* [online]. uoou.cz, [cit. 1. prosince 2018]. Dostupné na <https://www.uoou.cz/desatero%2Domylu/ds-4818/p1=4818>

[60] NONNEMANN, František. Objektivní, či subjektivní pojetí osobních údajů?. *Právní rozhledy*, 2015, č. 12, s. 425-432.

[61] Tamtéž.

[62] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 90 (§ 4 písm.a).

[63] AUJEZDSKÝ, Josef. *Jsou cookies nebo IP adresa vždy osobním údajem?* [online]. Lupa.cz, 13. září 2019 [cit. 4. prosince 2019]. Dostupné na <https://www.lupa.cz/clanky/jsou-cookies-nebo-ip-adresa-vzdy-osobnim-udajem/>.

[64] MATOUŠOVÁ, HEJLÍK: Osobní údaje…, s. 34.

[65] NONNEMANN, František. Objektivní, či subjektivní pojetí osobních údajů?. *Právní rozhledy*, 2015, č. 12, s. 425-432.

identifikovat subjekt údajů, ačkoliv jiný správce tak učinit může.[66] K objektivnímu pojetí se konečně klaní i SDEU, když podle jeho shora citovaného rozsudku je IP adresa osobním údajem, byť identifikovat osobu na základě takového údaje nebude jednoduché.

Podle mého názoru by pojem osobní údaj měl být vykládán objektivně, neboť osoba nakládající s údaji by vždy měla počítat s konsekvencí, že někdo jiný na základě těchto údajů fyzickou osobu určit může, a to i s přihlédnutím k dnešním digitálním platformám, kdy se osobním údajem stává prakticky cokoli, co se váže k určitému subjektu. Domnívám se tedy, že by skutečně došlo ke snížení úrovně ochrany osobních údajů, pokud by údaj měl být osobním údajem jen pro toho, kdo reálně dokáže ukázat na konkrétního člověka. Pokud by se takové údaje dostaly ze sféry původního správce, zcela jistě by jiný správce fyzickou osobu identifikovat dokázal. Proto má objektivní pojetí podle mého názoru dobrý smysl.

Souhlasím s názorem právní teorie, že objektivní pojetí vyplývá i ze samotného čl. 26 odůvodnění GDPR, kde možnost identifikace subjektu údajů má být rozumná, což lze podle mého názoru považovat za jakýsi korektiv objektivního pojetí osobního údaje, který má zamezit absurdním závěrům o tom, jaký údaj již má kvalitu osobního údaje. S ohledem na shora uvedené se tak domnívám, že GDPR je postaveno na objektivním pojetí osobního údaje, a to právě s ohledem na recentní judikaturu SDEU, ale i odůvodnění samotného předpisu.

3.2 Správce

ZOOÚ za správce považuje „*subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele…*“[67] Definice je, stejně jako mnoho dalších pojmů, převzata ze Směrnice 95/46/ES, a to nikoliv doslovně. Hlavním definičním znakem správce je tak skutečnost, že se jedná o subjekt, který určuje účel a prostředky zpracování.[68] Účelem se rozumí smysl a důvod zpracování osobních údajů, tedy cíl, kterého má být zpracováním osobních údajů určitými způsoby dosaženo, přičemž tento účel musí být zákonný.[69] GDPR (na rozdíl od ZOOÚ) definici správce doslovně přejímá ze Směrnice 95/46/ES a namísto ZOOÚ užitého slova „každý“ povinné subjekty vypisuje, avšak tak širokým způsobem, že lze mezi správce řadit v podstatě každého. Stejně jako v českém zákoně i v nařízení platí, že správce určuje účely a prostředky zpracování.[70] Rovněž na rozdíl od ZOOÚ není definičním znakem správce podle

[66] NULÍČEK: *GDPR - Obecné nařízení…*, s. 80 (čl. 4 písm. a). (Shodně též PINKAVOVÁ, Adéla. FOŘT, Ferdinand. In PATTYNOVÁ a kol (ed). *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě*. Praha: Leges, 2018, s. 52 (čl.4 odst. 1)).
[67] Ust. § 4 písm. j ZOOÚ.
[68] NONNEMANN, František. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 78. (§ 4 písm. j)).
[69] Tamtéž.
[70] Čl. 4 odst. 7 GDPR

GDPR skutečnost, že správce sám provádí zpracování a že je za zpracování odpovědný. Jak ostatně vyplývá z druhé věty zákonné definice, tato podmínka mohla být „deaktivována“ tím, že správce pověřil zpracováním zpracovatele.[71] Autorský kolektiv komentáře k GDPR považuje tyto posledně jmenované definiční znaky správce dle ZOOÚ za nadbytečné, matoucí a také zavádějící. Správce totiž vůbec nemusí provádět zpracování. Pro naplnění definice správce totiž postačí, že určí účel a prostředky zpracování. Odpovědnost správce zákon zmiňoval rovněž zcela nadbytečně, když tu bylo možné dovodit již z postavení správce jako nositele práv a povinností, za jejichž porušení bylo možné, stejně jako za účinnosti GDPR, uložit správní sankce.[72] Lze tak uzavřít, že ani z hlediska vymezení správce údajů, GDPR nepřináší významné změny.

3.3 Zpracovatel

Dalším klíčovým subjektem na poli zpracování osobních údajů je tzv. zpracovatel. Podle ZOOÚ je zpracovatelem „*každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje…*.“[73] Obdobně jako u správce GDPR povinné subjekty široce vypisuje, a to tak, že se týká v podstatě každého, kdo zpracovává osobní údaje.[74] I tuto definici ZOOÚ i GDPR definici zjevně přebírají ze Směrnice 95/46/ES. Zpracovatelem je v zásadě osoba s vlastní právní subjektivitou odlišná od osoby správce, která provádí zpracování pro správce. Hlavním definičním znakem je tedy určitá závislost na správci, neboť ten určuje účel a prostředky zpracování.[75] Ke stejnému závěru bylo možné dojít i za dosavadní právní úpravy. [76]Nadále tedy platí, že správce může pověřit třetí subjekt (zpracovatele), aby pro něho provedl zpracování osobních údajů. S ohledem na shora uvedené je tak možné učinit závěr, že přijetím GDPR nedošlo ke změně v institutu zpracovatele, protože GDPR okruh povinných osob nijak nerozšiřuje ani nestanovuje další pojmové znaky.

3.4 Pojem zpracování osobních údajů

Podstatné pro účely komparace je vymezení pojmu zpracování osobních údajů. Podle ZOOÚ se zpracováním osobních údajů rozumí *„jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání*

[71] NONNEMANN: *Zákon o ochraně osobních…*, s. 78. (§ 4 písm. j)).
[72] NULÍČEK: *GDPR - Obecné nařízení…*, s. 89 (čl. 4 písm. 7).
[73] Ust. § 4 písm. k ZOOÚ.
[74] Srov. čl. 4 odst. 8 GDPR.
[75] PINKAVOVÁ, Adéla. FOŘT, Ferdinand. In PATTYNOVÁ a kol (ed). *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě*. Praha: Leges, 2018, s. 52 (čl.4 odst. 8).
[76] NONNEMANN: *Zákon o ochraně osobních…*,s. 82. (§ 4 písm. k)).

na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.“[77] ZOOÚ definici převzal ze Směrnice 95/46/ES a Úmluvy č. 108, přičemž zákonodárce nejprve obecně vymezuje zpracování a posléze příkladmo uvádí nejběžnější způsoby zpracování osobních údajů.[78] Z hlediska zákonné definice však není a nebylo rozhodné, zda se jedná o jedinou operaci s osobními údaji nebo zda pro naplnění definice bude potřeba provést úkonů několik. Zpravidla totiž správce nebo zpracovatel zpracovává osobní údaje vícero způsoby.[79]

GDPR definici obsahuje v čl. 4 odst. 2. Na první pohled definice zpracování nedostála žádných výrazných změn, neboť není zjevné, že by se rozšiřovala, nebo naopak zužovala na užší spektrum forem zpracování. Oproti GDPR však definice dle ZOOÚ obsahuje jednu odchylku, a sice, že zpracování osobních údajů nemusí vykazovat systematičnost operací. Vzhledem k tomu, že definice zpracování byla do českého zákona přebrána ze Směrnice 95/46/ES, jedná se o právní úpravu nad rámec směrnice a příklad nesprávné a matoucí implementace provedené českým zákonodárcem. Podle anglického znění Směrnice 95/46/ES totiž postačí jednorázovost zpracování, což je vlastně pravý opak prvku systematičnosti podle českého zákona.[80] Rovněž ÚOOÚ považuje podmínku systematického zpracování za okrajovou a nadbytečnou.[81] ZOOÚ má tedy širší dosah než směrnice 95/46/ES, což mělo být v případě výkladových problémů řešeno institutem tzv. nepřímého účinku směrnice.[82] Podle mého názoru bylo možné rozpor odstranit také tzv. eurokonformním výkladem zákona. Samotné GDPR definici zpracování přejímá ze směrnice 95/46/ES, a to doslovně. Lze se tedy domnívat, že prvek systematičnosti není (a podle stanoviska ÚOOÚ zřejmě ani nebyl) podmínkou zpracování osobních údajů dle platné úpravy na území České republiky a pochopitelně ani v jiných členských státech. Do jisté míry tak lze uzavřít, že definice zpracování nedoznala, i přes absenci podmínky systematičnosti, žádných změn. I nadále bude možné aplikovat názory právní doktríny, výkladová stanoviska Úřadu i stávající judikaturu soudů ke zpracování osobních údajů.

---

[77] Ust. § 4 písm. e) ZOOÚ.
[78] POSPÍŠIL, Daniel. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 68. (§ 4 písm. e)).
[79] Tamtéž, s. 69.
[80] Tamtéž, s. 68.
[81] Stanovisko Úřadu pro ochranu osobních údajů, č. 4/2013.
[82] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 110 (§ 4 písm.e).

4 Komparace vybraných otázek právní úpravy zpracování osobních údajů podle GDPR a dosavadní právní úpravy

Jak bylo popsáno výše, GDPR mělo za cíl sjednotit právní úpravu v členských státech EU. Nová právní úprava je často nazývána „*revolucí v ochraně osobních údajů*“, přičemž některé obavy z dopadů GDPR na činnost správců a zpracovatelů mnohdy hraničí s panikou. Obavy pramení zejména z potenciálního nárůstu administrace a provozních nákladů a pochopitelně i ze sankcí za porušení některých povinností. Následující kapitoly této diplomové práce tak mají za cíl porovnat dosavadní právní úpravu zpracování osobních údajů v České republice spolu s GDPR, a zejména zjistit, zda nová úprava je hodna označení „*revoluce*“, nebo zda malý až střední podnik vyhoví novým pravidlům již při dodržování ZOOÚ. Smyslem této diplomové práce však není podrobit GDPR a ZOOÚ komplexní analýze. Účelem je analyzovat vybrané základní instituty a vybrané změny, které budou mít vliv na činnost správců a zpracovatelů, jakož i na postavení subjektů údajů.

4.1 Zásady zpracování

Zásady zpracování osobních údajů tvoří jakýsi základ právní úpravy ochrany osobních údajů.[83] Právní zásady se vyznačují především vyšším stupněm obecnosti než právní pravidla a rovněž určitou mírou závažnosti.[84] Pro právní zásady je typická jejich způsobilost zaplnit mezery v právních pravidlech, což je velmi přínosné právě pro právní úpravu ochrany osobních údajů jakožto oboru, který je stižen velmi častými změnami právních vztahů kvůli dynamickému rozvoji informačních technologií.[85] Zásady zpracování osobních údajů mají svůj pramen zejména v mezinárodních smlouvách, především v Úmluvě č. 108 a v jejím Dodatkovém protokolu. Je třeba zmínit, že tyto zásady prozařují do všech národních zákonů o ochraně osobních údajů, jakož i do právních předpisů Evropské unie, tedy jak do dosavadní obecné Směrnice 95/46/ES, tak pochopitelně i do GDPR, přičemž pro každou zásadu se ustálil jistý název, který se v praxi běžně užívá.[86]

ZOOÚ nemá explicitní výčet zásad zpracování osobních údajů. Zákon tyto zásady promítl do obdobně znějících povinností v ust § 5 odst. 1 ZOOÚ. Směrnice 95/46/ES šla naopak cestou výčtu zásad a není tomu jinak ani v GDPR. Mezi zásady zpracování osobních údajů tak lze řadit především zásadu korektního (férového), transparentního a zákonného zpracování, zásadu účelového omezení, zásadu minimalizace údajů, zásadu přesnosti, zásadu omezení uložení

[83] NOVÁKOVÁ, Ludmila. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 102. (§ 5 odst. 1)
[84] TRIDIMAS, Takis. *The General Principles of EU Law*. 2. vydání. Oxford: Oxford University Press, 2006, s. 1.
[85] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 139 (§ 5).
[86] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012. s. 9.

(časového omezení), zásadu integrity a důvěrnosti (zabezpečení), zásadu odpovědnosti a další, jako je např. zásada přístupu k údajům, opravě, či výmazu údajů.

Zásada zákonnosti patří mezi nejdůležitější zásady na poli ochrany osobních údajů i mimo něj.[87] Jedná se o princip, který prozařuje celým právním řádem z Ústavy, Listiny, ale i mezinárodních pramenů. Obecně totiž znamená, že osobní údaje mají být zpracovávány v souladu s právními předpisy. Je však s podivem, že ZOOÚ tuto povinnost výslovně nestanovuje. Je tomu zřejmě proto, že požadavek zákonnosti je něco tak samozřejmého, že zákonodárce neměl potřebu tuto povinnost explicitně vyjadřovat. Tuto zásadu lze ostatně dovodit ústavněkonformním, ale i eurokonformním výkladem.[88] GDPR zásadu zákonnosti výslovně upravuje v čl. 5 odst. 1 písm. a) a významově neznamená nic jiného, než že zpracování musí proběhnout alespoň na základě jednoho z právních titulů ve smyslu čl. 6 GDPR.[89] Zásada zákonnosti se tedy přijetím GDPR zjevně neposouvá. I nadále tak lze použít závěr právní teorie, že zpracování nesmí být protiprávní, tedy v rozporu s právním řádem obecně, tedy např. s právem duševního vlastnictví, s právem na ochranu osobnosti apod.[90]

Další důležitou zásadou je zásada korektnosti a transparentnosti zpracování. Tato zásada vyjadřuje, že správce a zpracovatel mají být vůči subjektům údajů otevření, čestní a poctiví, a to zejména ve vztahu k tomu, jak je nebo bude nakládáno s jejich osobními údaji.[91] Podle britského dozorového úřadu má být korektnost splněna vůči každému subjektu údajů. Nepostačuje, pokud je správce korektní jen ve vztahu k většině subjektů.[92] ZOOÚ zásadu korektnosti rovněž výslovně neupravuje, její obsah však lze dovodit z ust. § 5 odst. 1 písm. g) o povinnosti shromažďovat údaje otevřeně, jakož i z dalších ustanovení dle tohoto zákona[93]. GDPR zásadu korektnosti a transparentnosti upravuje v čl. 5 odst. 1 písm. a). Blíže se této zásadě věnuje bod 39 odůvodnění GDPR, které akcentuje na to, aby subjekt byl vhodně, jasně a srozumitelně informován o zpracování osobních údajů podle čl. 13 a 14 GDPR a také informován o svých právech. Tomu odpovídá mj. informační povinnost dle ust. § 5 odst. 4 ZOOÚ. Lze do jisté míry uzavřít, že GDPR velmi detailně upřesňuje již známou zásadu korektnosti tím, že ji doplňuje o prvek transparentnosti. Transparentnost však má obdobný obsah jako korektnost, resp. férovost. Doplnění právní úpravy o zásadu transparentnosti tak má

---

[87] Tamtéž.
[88] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 139 (§ 5).
[89] NULÍČEK: *GDPR - Obecné nařízení…*, s. 106 (čl. 5 odst. 1 písm. a)).
[90] NOVÁK: *Zákon o ochraně osobních údajů…*, s. 139 (§ 5), (k tomu srov. stanovisko WP29 ze dne 11. února 2004, č. 4/2004)
[91] Bod 39 odůvodnění GDPR.
[92] Information Commissioner's Office. *Principle (a): Lawfulness, fairness and transparency* [online]. ico.org.uk, [cit. 16. února 2019]. Dostupné na <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>.
[93] Například informační povinnost dle ust. § 11 či povinnost oznámit zpracování dle ust. § 16 ZOOÚ.

spíše deklaratorní účel.[94] Podle mého názoru se jedná o určité zdůraznění důležitosti této zásady, a to i s ohledem na to, že zásada korektnosti a transparentnosti je výslovně uvedena jako první ve výčtu zásad spolu se zásadou zákonnosti. Transparentnost se v GDPR dále promítá zejména do zcela nové úpravy obecných postupů správce vůči subjektu údajů při výkonu jeho práv dle GDPR, o kterých bude pojednáno níže.

Stěžejní je zásada účelového omezení. ZOOÚ v ust. § 5 odst. 1 písm. a) určuje povinnost správce stanovit účel zpracování. Ačkoliv zákon stanovoval toliko povinnost stanovit účel, bylo nutné dovozovat další požadavky stanovené Směrnicí 95/46/ES a Úmluvou č. 108, a sice, že účel má být vyjádřen výslovně a že má být legitimní.[95] GDPR evidentně doslovně přebírá dikci Směrnice 95/46/ES a oproti ZOOÚ zásadu účelového omezení upřesňuje atributy tzv. dalšího zpracování, když slučitelná s původním účelem je skutečnost, že posléze dojde ke zpracování pro účely vědecké nebo historické anebo pro statistické účely. Oproti Směrnici 95/46/ES však GDPR upravuje navíc možnost dalšího zpracování za účelem archivace ve veřejném zájmu.[96] GDPR v konečném důsledku tedy nepřináší žádnou výraznou změnu, kromě drobného upřesnění již známé zásady.

Prakticky nezměněna zůstala zásada minimalizace údajů, která dle GDPR stanoví, že osobní údaje musí být „*přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány*“[97] ZOOÚ ekvivalentní povinnost stanovuje v ust. § 5 odst. 1 písm. d). Před přijetím GDPR byla tato zásada označována jako zásada potřebnosti a proporcionality. Ve zkratce minimalizace údajů znamená, že údaje mají být zpracovávány pouze v omezeném rozsahu ve vztahu ke stanovenému účelu. Nadbytečné osobní údaje nemají být předmětem zpracování.[98] ZOOÚ však tuto povinnost vztahuje pouze k jedné složce zpracování, a to ke shromažďování. Na jiné nakládání s osobními údaji než shromažďování se pravidlo § 5 odst. 1 písm. d) nevztahovalo, avšak takové případy byly spíše výjimkou, a proto není relevatní se touto odchylkou blíže zabývat.[99] Zásada minimalizace údajů se promítá například do institutu záměrné a standardní ochrany osobních údajů, který je zakotven v čl. 25 a o němž bude pojednáno níže v této diplomové práci.

Prakticky nezměněna zůstala rovněž zásada přesnosti údajů dle ust. § 5 odst. 1 písm. c) ZOOÚ a čl. 5 odst. 1 písm. d) GDPR. I nadále tak má správce, resp. zpracovatel povinnost

---

[94] NOVÁKOVÁ, Ludmila. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 102. (§ 5 odst. 1)
[95] Tamtéž, s. 104. (§ 5 odst. 1 písm. a)).
[96] PATTYNOVÁ, Jana. In PATTYNOVÁ a kol (ed). *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě. Praha*: Leges, 2018, s. 62 (čl. 5 odst. 1 písm. b)).
[97] Čl. 5 odst. 1 písm. c) GDPR.
[98] NULÍČEK: *GDPR - Obecné nařízení…*, s. 110 (čl. 5 odst. 1 písm. c)).
[99] POSPÍŠIL, Daniel. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 116. (§ 5 odst. 1 písm. d)).

aktualizovat nepřesné údaje, a to v případě nutnosti sám, nebo na žádost subjektu údajů. Žádných změn nedoznala ani tzv. zásada časového omezení, resp. omezení uložení dle ust. § 5 odst. 1 písm. e) ZOOÚ a čl. 5 odst. 1 písm. e). Osobní údaje mají být uchovávány pouze po dobu nezbytně nutnou pro naplnění účelu.[100] I podle GDPR lze tuto dobu překročit výhradně pro účely archivace, vědy či statistiky.[101] Do ust. § 13 ZOOÚ je promítnuta i tzv. zásada bezpečnosti. GDPR však na rozdíl od Směrnice 95/46/ES a ZOOÚ bezpečnost řadí mezi základní zásady zpracování, čímž zdůrazňuje zabezpečení osobních údajů jako klíčovou povinnost v celém zpracování osobních údajů.[102]

4.1.1 Princip odpovědnosti a přístup založený na riziku

Považuji za přiléhavé se více pozastavit u principu odpovědnosti správce dle čl. 5 odst. 2 GDPR. Ustanovení sice přebírá již dříve známý princip odpovědnosti správce za dodržování povinností při zpracování osobních údajů. Nově však GDPR výslovně uvádí, že správce je povinen dodržování povinností dle GDPR doložit.[103] Ve správních řízeních vedených se správci princip odpovědnosti bude především znamenat plné obrácení důkazního břemene ohledně dodržování GDPR.[104]

Účelem principu odpovědnosti je především povinnost správce přijmout taková opatření, která povedou k efektivnímu uplatňování základních zásad zpracování osobních údajů.[105] GDPR ale konkrétně neuvádí, která opatření má správce přijmout. Určité vodítko však přináší čl. 24 odst. 1 GDPR, podle kterého správce zavede vhodná technická a organizační opatření „*s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob…*“ Správce tedy musí provést analýzu konkrétních okolností zpracování a zvážit rizika zpracování pro základní práva a svobody subjektů údajů. Na podkladě této analýzy rizik následně zvolí přiměřená technická a organizační opatření,[106] a to rovněž s „*přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování…“*[107] Tento přístup založený na riziku[108] zpracování nebyl vyloučen ani doposud, a to právě na podkladě ust. § 13 ZOOÚ.

---

[100] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012. s. 13.
[101] Srov. Čl. 5 odst. 1 písm e) GDPR
[102] NULÍČEK: *GDPR - Obecné nařízení…*, s. 118 (čl. 5 odst. 1 písm. f)).
[103] Čl. 5 odst. 2 GDPR
[104] PATTYNOVÁ: *Obecné nařízení…*, s. 72 (čl. 5 odst. 2).
[105] Stanovisko WP29 ze dne 13.7.2010, č. 3/2010, s. 8.
[106] ZEMANOVÁ ŠIMONOVÁ, Hana. Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů. *Bulletin advokacie*. 2017, č. 9, s. 25.
[107] Čl. 32 odst. 1 GDPR
[108] Tzv. Risk-based Approach (RBA), což znamená, že čím větší riziko pro základní práva a svobody subjektů údajů, tím vyšší jsou požadavky na zákonné zpracování osobních údajů.

Analýza rizik se však vztahovala pouze k určení rozsahu opatření k zabezpečení údajů.[109] GDPR přístup založený na riziku nově zavádí plošně ve vztahu ke všem aspektům zpracování. S ohledem na některé nové instituty se tak domnívám, že riziko pro práva a svobody subjektů údajů působí jako kritérium pro konkrétní rozsah povinností správce dle GDPR. Závisí na něm totiž míra uplatnění celé řady institutů včetně druhu a výše sankce za porušení GDPR. Hodí se také dodat, že kritérium míry rizika nemusí být u dané povinnosti dle GDPR výslovně uvedeno, neboť posuzování rizik má být zohledněno již při naplňování samotných zásad zpracování.[110]

Lze tak uzavřít, že GDPR šlo cestou výčtu zásad obdobně, jako činila Směrnice 95/46/ES, přičemž většina zásad je převzata právě z tohoto předpisu anebo Úmluvy č. 108. GDPR tak zásady pouze upřesňuje a některé z nich výslovně zakotvuje, přestože jejich aplikace nebyla vyloučena ani za účinnosti dosavadní právní úpravy. Výraznou změnou je povinnost správce dodržování svých povinností doložit. To současně s plošným zavedením přístupu založeném na riziku výrazně mění postavení správce, který nově musí analyzovat rizika zpracování na práva a svobody fyzických osob a přijmout odpovídající opatření. Nelze ani vyloučit povinnost správce příslušné analýzy a opatření dokumentovat.

Podle mého názoru přístup založený na riziku výrazně tlumí panické obavy o byrokratických opatřeních a s nimi spojené náklady na implementaci nových pravidel dle GDPR. Míra rizika totiž výrazně zužuje rozsah povinností správců a zpracovatelů. Rozsah technických a organizačních opatření se tak bude lišit u kadeřnictví s on-line rezervačním systémem, které učiní svým povinnostem zadost, když jako správce stanoví účel, najde vhodný právní titul zpracování a řádně poučí o zpracování v souladu se zásadou transparentnosti, neboť rizika pro práva osob jsou zde minimální. Jinak tomu bude pro praxi lékaře nebo nemocnice, a ještě jinak u nadnárodní společnosti provozující sociální síť, kde z důvodu zpracování citlivých dat je riziko vysoké.

4.2 Důvody zpracování

Právním důvodem zpracování osobních údajů se rozumí určité oprávnění správce osobní údaje zpracovávat, aby takové zpracování prováděné správcem bylo považováno za zákonné. Obecně není rozhodné, že správce dodržuje všechny ostatní povinnosti plynoucí z právní

[109] BARTÍK, Václav. JANEČKOVÁ, Věra. Bezpečnost osobních údajů podle zákona o ochraně osobních údajů. *Právní rozhledy*, 2010, č. 23, s. 839-844.
[110] MATOUŠOVÁ, Miroslava. *Sdělení ÚOOÚ k přístupu založenému na riziku* [online]. uoou.cz, 31. srpna 2017 [cit. 8. března 2019]. Dostupné na < https://www.uoou.cz/sdeleni-uoou-k-pristupu-zalozenemu-na-riziku-i-s-prilohou-narizeni-evropskeho-parlamentu-a-rady-eu-2016-679-ze-dne-27-dubna-2016-o-ochrane-fyzickych-osob-v-souvislosti-se-zpracovanim-osobnich-udaju-a-o-volnem-pohybu-tec/d-26811>.

úpravy. Nemá-li totiž správce platný právní titul ke zpracování údajů, jedná se o zpracování nezákonné a správce musí tyto osobní údaje zlikvidovat.[111]

ZOOÚ v ust. § 5 odst. 2 upravoval následující právní tituly ke zpracování osobních údajů: a) souhlas subjektu údajů; b) zpracování nezbytné pro dodržení právní povinnosti; c) zpracování nezbytné pro plnění smlouvy; d) zpracování nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů; e) zpracování již oprávněně zveřejněných osobních údajů; f) nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; g) zpracování osobních údajů o veřejně činné osobě; h) zpracování výlučně pro účely archivnictví podle zvláštního zákona.

Také na tomto místě je patrné, že provedení Směrnice 95/46/ES ze strany českého právního řádu neproběhlo úplně šťastně. Dokladem toho je legislativní vyjádření návětí[112] ust. § 5 odst. 2, jehož jazykové znění vedlo k tomu, že za hlavní titul byl chápán souhlas a ostatní právní tituly podle písm. a) až f) jako výjimky z tohoto pravidla.[113] Podle mého názoru však závěr o souhlasu jako základním titulu ze Směrnice 95/46/ES nevyplývá, neboť unijní zákonodárce souhlas zahrnuje do všeobecného výčtu právních titulů a z formulace čl. 7 směrnice je naopak evidentní, že tyto právní tituly jsou postaveny sobě naroveň.

GDPR evidentně přebírá úpravu právních titulů ze Směrnice 95/46/ES, přičemž oproti ZOOÚ výslovně neupravuje samostatný právní titul pro zpracování oprávněně zveřejněných osobních údajů podle ust. § 5 odst. 2 písm. e) a titul pro poskytování osobních údajů o veřejně činných osobách podle ust. § 5 odst. 2 písm. f) zákona. GDPR naopak nově upravuje právní titul zpracování nezbytného pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci ve smyslu čl. 6 odst. 1 písm. e) GDPR.[114]

Za podstatnou změnu v právní úpravě považuji především nové chápání institutu souhlasu se zpracováním osobních údajů. GDPR totiž (obdobně jako Směrnice 95/46/ES) souhlas staví naroveň ostatním právním titulům. Nová úprava podmínek jeho udělování navíc nutí správce, aby ho jako právní titul zamýšleného zpracování používali jen tehdy, pokud jim k tomuto zpracování nepostačuje jiný právní titul. Přednostně tak má být zpracování provedeno na podkladě jiného důvodu, pokud tento k naplnění stanoveného účelu zpracování postačuje.[115] ZOOÚ podmínky jeho udělování blíže nestanovoval, přičemž autoři komentářové literatury

---

[111] Úřad pro ochranu osobních údajů. *Zásady a právní důvody zpracování* [online]. uoou.cz, [cit. 14. ledna 2019]. Dostupné na <https://www.uoou.cz/4-zasady-a-nbsp-pravni-duvody-zpracovani/d-27271/p1=3938>

[112] „*Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat…*“

[113] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. vydání. Olomouc: ANAG, 2018, s. 68.

[114] NULÍČEK: *GDPR - Obecné nařízení…*, s. 124 (čl. 6).

[115] NEŠPŮREK a kol. Souhlas ve světle GDPR. *EU Právní novinky*. 2018, č. 2, s. 3; k tomu srov. Bod 43 in fine odůvodnění GDPR.

některé podmínky jeho udělování dovozovali z obecné úpravy občanského zákoníku, který byl ve vztahu k ZOOÚ v postavení lex generalis.[116] Podmínky udělování souhlasu jsou tedy nyní výslovně upraveny v čl. 7 a násl. GDPR. Nový předpis tak vyžaduje, aby souhlas byl svobodný, konkrétní, informovaný a jednoznačný a aby byl učiněn písemným prohlášením nebo jiným zjevným potvrzením.[117] Velký důraz je přitom kladen právě na podmínku svobody udělení souhlasu. O svobodném souhlasu lze pochybovat, pokud je udělen za následujících situací: a) správce je v nadřazeném postavení[118]; b) nemožnost vyjádřit souhlas s jednotlivými operacemi zpracování[119]; c) plnění smlouvy nebo poskytnutí služby je závislé na souhlasu, i když to není pro toto plnění nezbytné. Posledně uvedený příklad je podle mého názoru jasný důkaz toho, že GDPR zcela obrací pojetí souhlasu jako základního titulu pro zpracování podle ZOOÚ. GDPR tak souhlas spíše upozaďuje na úkor ostatních právních titulů. [120]

Revoluční ve vztahu k poměrům nastolených ZOOÚ je pravidlo tzv. oddělitelnosti souhlasu podle čl. 7 odst. 2 GDPR. Pokud je totiž souhlas poskytován formou písemného prohlášení, měl by souhlas být od ostatních ujednání jasně odlišitelný. V souladu s GDPR tak nebude dosavadní praxe některých správců, kteří žádost o poskytnutí souhlasu učinili součástí obchodních podmínek, neboť takový způsob vyjádření žádosti správce o souhlas je jednoduše v rozporu s dikcí čl. 7 odst. 2.[121] Podle mého názoru však není nutné, aby žádost o souhlas byla subjektům údajů předložena na samostatném formuláři, neboť GDPR požaduje toliko odlišitelnost souhlasu od jiných skutečností. O odlišitelný souhlas se podle mě bude jednat, pokud součástí jedné listiny bude jednak text smlouvy a dále (např. tučným nadpisem či jinak) dostatečně oddělena žádost o udělení souhlasu se samostatným podpisovým políčkem.

GDPR také výslovně upravuje podmínky souhlasu dítěte v souvislosti s nabídkou služeb tzv. informační společnosti[122], když o zákonné zpracování se bude jednat jen tehdy, poskytuje-li souhlas dítě starší 16 let, ledaže byl tento souhlas vyjádřen zákonným zástupcem.[123] GDPR současně zmocňuje členské státy, aby předpisem tuto hranici snížily na maximálně 13 let. Český zákonodárce tak činí v ust. § 7 návrhu zákona o zpracování osobních údajů, když

---

[116] KUČEROVÁ: *Zákon o ochraně…*, s. 133. (§ 5 odst. 2).
[117] Čl. 4 odst. 11 GDPR
[118] Například orgán veřejné moci, ale i zaměstnavatel. Orgánům veřejné moci se nedoporučuje zpracovávat osobní údaje na základě souhlasu. Takový souhlas subjektu totiž bude v zásadě považován za nesvobodný a tudíž neplatný, čímž se příslušný orgán vystaví riziku porušení zásady zákonnosti (k tomu srov. Bod 43 odůvodnění GDPR).
[119] Jedná se o problematiku tzv. granular consentu, tedy možnosti dát souhlas jen k některým operacím zpracování, o které má subjekt skutečně zájem. Lze se s ním setkat zejména v digitálních platformách.
[120] ŠVÉDA, Martin. *Nenechme se strašit souhlasy*. [online]. epravo.cz, 27. listopadu 2017 [cit. 15. ledna 2019]. Dostupné na <https://www.epravo.cz/top/clanky/nenechme-se-strasit-souhlasy-106690.html>
[121] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. vydání. Olomouc: ANAG, 2018, s. 74.
[122] V GDPR tento pojem není definován, zřejmě se však bude jednat o provozovatele sociálních sítí.
[123] Čl. 7 odst. 1 GDPR

způsobilé k udělení souhlasu bude dítě dovršením 15. roku věku. Protože souhlasem subjekt údajů vyjadřuje svolení k tomu, aby správce zpracovával jeho osobní údaje, lze projevení souhlasu považovat za právní jednání a v tomto ohledu se na jeho náležitosti tedy, stejně jako ve vztahu k ZOOÚ, subsidiárně použije ObčZ. Zejména se použije právní úprava zastoupení subjektu údajů při udělování souhlasu, která v rámci GDPR výslovně upravena není.[124] V kontextu způsobilosti k udělení souhlasu Nulíček správně připomíná, že hranice věku pro udělení souhlasu stanovená GDPR může být v konkrétním případě odlišná v závislosti na způsobilosti daného jedince a náročnosti zpracování.[125]

V čl. 6 odst. 1 písm. d) GDPR je vymezen právní titul zpracování nezbytné pro plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci. Ačkoliv tento právní titul figuroval již ve Směrnici 95/46/ES, ve výčtu dle ust. § 6 ZOOÚ se takový právní důvod zpracování neobjevuje. Nejblíže má však k právnímu titulu zpracování nezbytné pro splnění právní povinnosti, které je upraveno rovněž v ZOOÚ. Od tohoto titulu se však liší především právním základem, který dává zmocnění ke zpracování. U právního důvodu splnění právní povinnosti je totiž nutné, aby zvláštní právní předpis stanovil konkrétní povinnost nakládat s osobními údaji za nějakým účelem. Někteří správci však mohou plnit úkoly ve veřejném zájmu, aniž by plnili nějakou právní povinnost, přičemž takové zpracování bude v souladu s GDPR.[126] Plnit úkol ve veřejném zájmu či při výkonu veřejné moci může i fyzická nebo právnická osoba[127], které byl výkon veřejné správy propůjčen. Tak například tento právní titul budou využívat jak obce a kraje, tak i profesní komory pro účely vedení disciplinárního řízení s jeho členy, avšak neměl by být považován za titul univerzální, neboť vždy musí být naplněna podmínka plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci.[128] Podle mého názoru se jedná o flexibilní právní důvod, který pro orgány veřejné správy může být velkým přínosem v cestě za nalezením vhodného právního titulu pro zpracování osobních údajů, s nimiž během své činnosti správce přichází do styku. Využitelný však může být i pro osoby soukromého práva, které poskytují součinnost orgánům činném v trestním řízení nebo v případě podávání trestního oznámení. Tento titul však nebude možné použít jako důvod pro preventivní sběr dat z průmyslových kamer za účelem případného podání trestního oznámení.[129] K tomuto účelu bude zpravidla sloužit právní titul oprávněného zájmu správce.

---

[124] NULÍČEK: *GDPR - Obecné nařízení…*, s. 125 (čl. 6).
[125] Tamtéž, s. 159 (k tomu srov. ust. § 31 ObčZ)
[126] ŽŮREK: *Praktický průvodce…*, s. 83
[127] K tomu srov. Bod 46 odůvodnění GDPR
[128] NULÍČEK: *GDPR - Obecné nařízení…*, s. 131 (čl. 6).
[129] PATTYNOVÁ: *Obecné nařízení…*, s. 90 (čl. 6 odst. e).

Návrh zákona o zpracování osobních údajů u zpracování prováděného na podkladě posledně uvedených právních důvodů stanoví, že splnění informační povinnosti bude možné způsobem umožňujícím dálkový přístup, tedy zveřejněním „*poučení*“ na webových stránkách nebo úřední desce správce.[130]

Jak bylo uvedeno shora, GDPR neupravuje přímý právní titul pro zpracování údajů veřejně přístupných osobních údajů na rozdíl od ust. § 5 odst. 2 písm. d) a odst. 5 ZOOÚ. Znamená to tedy, že po nabytí účinnosti GDPR je možnost zpracovávat veřejně dostupné osobní údaje výrazně omezena, nebo snad dokonce vyloučena? Podle Nonnemanna jako nejvhodnější právní titul by bylo možné použít čl. 6 odst. 1 písm. f) GDPR, tedy oprávněný zájem správce. Zpracování na podkladě tohoto titulu předpokládá určitý oprávněný zájem správce (nebo třetí strany), avšak pod podmínkou, že nad tímto zájmem nepřevažují zájmy nebo základní práva a svobody subjektu údajů vyžadujících ochranu osobních údajů.[131] ZOOÚ znal obdobný právní titul, avšak zpracovávat údaje bylo možné, bylo-li to nezbytné „*za účelem ochrany práv či právem chráněných zájmů správce…“*[132] ZOOÚ tak neumožňoval, na rozdíl od GDPR, zpracovávat osobní údaje za subjektivním nebo vlastním oprávněným zájmem správce, ale pouze a jen za účelem ochrany právem chráněných zájmů, jako např. ochrana vlastnictví nebo práva na život.[133] Právem chráněný zájem je totiž pojmem užším než oprávněný zájem správce, který je chápán spíše subjektivně. GDPR, které dosavadní unijní úpravu přebírá, tak podle mého názoru možnosti využití titulu oproti ZOOÚ značně rozšiřuje. GDPR podmiňuje zpracování z titulu oprávněného zájmu[134] správce provedením tzv. balančního testu[135], na podkladě kterého by měl správce dojít k závěru, zda nad jeho oprávněným zájmem převažují práva a svobody fyzických osob či nikoliv. Test proporcionality, jak se také jinak označuje, je správce povinen provést vždy, jestliže hodlá zpracovávat údaje na základě právního titulu oprávněného zájmu.[136] Právní doktrína tento titul považuje za zbytkový důvod, pod který lze podřadit celou řadu zpracování prováděných správcem.[137] Oprávněný zájem se jako právní důvod zpracování bude využívat především pro provoz kamerových systémů nebo sběr dat za účelem vymáhání právních nároků.[138]

---

[130] ust. § 8 návrhu zákona o zpracování osobních údajů.
[131] Čl. 6 odst. 1 písm. f) GDPR
[132] Ust. § 5 odst. 2 písm. e) ZOOÚ.
[133] NULÍČEK: *GDPR - Obecné nařízení…*, s 132.
[134] K podrobnostem k posouzení oprávněného zájmu správce srov. NULÍČEK: *GDPR - Obecné nařízení…*, s. 133 a násl., jakož i PATTYNOVÁ: *Obecné nařízení…*, s. 90 (čl. 6 odst. e).
[135] K podrobnostem viz bod 47 odůvodnění GDPR.
[136] Úřad pro ochranu osobních údajů. *Právní důvody zpracování* [online]. uoou.cz, [cit. 18. ledna 2019]. Dostupné na < https://www.uoou.cz/pravni-duvody-zpracovani/d-27318/p1=3938>
[137] ŽŮREK: *Praktický průvodce…*, s. 83.
[138] NULÍČEK: *GDPR - Obecné nařízení…*, s. 133.

Vrátím-li se k otázce zpracování veřejně dostupných údajů na podkladě oprávněného zájmu správce, vhodnost tohoto důvodu bude tedy nutno posuzovat v každém individuálním případě, a to s přihlédnutím k účelu zpracování, způsobu zpracování, rozsahu zpracovávaných údajů, kategorii osobních údajů (kontaktní, citlivé aj.) a kategorii zdroje (veřejný seznam, soukromé databáze…). K tomu všemu bude muset zamýšlené zpracování projít balančním testem. [139] Žůrek, stejně jako Neumann a další připouští možnost zpracování veřejně dostupných údajů na základě oprávněného zájmu správce nebo třetí strany, avšak tuto možnost často shledávají jako teoretickou a problematickou, právě s ohledem na nutný komplex posouzení v rámci testu proporcionality.[140] S ohledem na shora uvedené tak lze uzavřít, že jasno v otázce zpracování zveřejněných osobních údajů zcela není a bude tak nutné počkat na vývoj judikatury a stanovisek dozorových úřadů. Zřejmé však je, že zpracování těchto údajů na podkladě souhlasu bude spíše prakticky nevyužitelné s ohledem na vyšší počet subjektů údajů. Ostatně ÚOOÚ se k této věci již na podzim 2018 sdělením vyjádřil tak, že oprávněný zájem bude nejčastějším titulem pro zpracování zveřejněných údajů z veřejných rejstříků a seznamů. Po nabytí účinnosti GDPR totiž prudce narostl počet stížností na provozovatele neoficiálních rejstříků. V návaznosti na stížnosti ÚOOÚ zdůraznil především povinnost správců provést test proporcionality, na základě kterého mají správci prokazovat jejich převažující zájem nad zájmy subjektů údajů.[141]

Obdobně bude podle mého názoru možné postupovat ve vztahu ke zpracování údajů o veřejně činné osobě, které podle dosavadního ZOOÚ mělo základ v samostatném právním titulu. Směrnice ani GDPR však obdobný titul neznají. Domnívám se, že nově bude ke zpracování těchto údajů možné využít titulu oprávněného zájmu správce, anebo plnění úkolu ve veřejném zájmu.

4.3 Práva subjektů údajů

Práva fyzických osob při zpracování osobních údajů tvoří základní pilíř právní úpravy ochrany osobních údajů. Dosavadní právní úprava v České republice subjektům údajů poskytovala zejména právo na informace dle ust. § 11, právo na přístup k informacím dle ust. § 12, právo na vysvětlení podle ust. § 21 odst. 1 písm. a), či právo na blokování, opravu, doplnění nebo likvidaci osobních údajů ve smyslu ust. § 21 odst. 1 písm. b) ZOOÚ. Vzhledem

---

[139] NONNEMANN, František. Zpracování veřejně dostupných osobních údajů a GDPR. *Právní rozhledy*, 2018, č. 5, s. 167.
[140] ŽŮREK: *Praktický průvodce…*, s. 70.
[141] Úřad pro ochranu osobních údajů. *Nesouhlasím se způsobem, jakým jsou zpracovávány mé osobní údaje získané z veřejného rejstříku v soukromých databázích na internetu. Jak se mohu bránit?* [online]. uoou.cz, [cit. 16. února 2019]. Dostupné na <https://www.uoou.cz/nesouhlasim-se-zpusobem-jakym-jsou-zpracovavany-me-osobni-udaje-ziskane-z-verejneho-rejstriku-v-soukromych-databazich-na-internetu-jak-se-mohu-branit/ds-5314/archiv=0&p1=3942>.

k hlavnímu poslání GDPR posílit ochranu osobních údajů, je oproti Směrnici 95/46/ES a ZOOÚ na první pohled zjevná podrobnější úprava práv subjektů údajů (a tomu odpovídajících povinností správců a zpracovatelů). Vedle aktualizace dosavadní právní úpravy GDPR nově vymezuje některá nová práva subjektů údajů, která budou objasněna dále v této diplomové práci.

GDPR obsahuje právní úpravu práv subjektů údajů především v kapitole III nařízení. V oddíle 1 této kapitoly nově podrobně vymezuje obecné postupy správce pro výkon práv fyzických osob. Vedle požadavku na stručnost, srozumitelnost a vhodnost sdělení, GDPR nově stanoví lhůty pro poskytování informací o přijatých opatřeních. Správce má totiž poskytovat sdělení bez zbytečného odkladu, v každém případě však do jednoho měsíce od obdržení žádosti subjektu údajů. Tuto lhůtu bude možné v souladu s článkem 12 odst. 3 GDPR prodloužit o další dva měsíce (tj. celkem 3 měsíce), a to v závislosti na složitosti případu a počet žádostí.[142] Ve vztahu ke sdělením správce nově platí, že mají být poskytnuty bezplatně, potažmo za přiměřenou úhradu v případě, že žádost subjektu údajů je zjevně nedůvodná nebo nepřiměřená. Směrnice 95/46/ES ani ZOOÚ bezplatnost ani lhůty pro poskytování informací a odpovědí na žádosti subjektů údajů neupravovali, naopak, ZOOÚ dle ust. § 12 odst. 3 dokonce výslovně stanovil právo správce požadovat po subjektu údajů přiměřenou úhradu nepřevyšující náklady spojené s výkonem práva na přístup k informacím.

Novinkou je též institut odmítnutí žádosti subjektů údajů podle čl. 12 odst. 5 písm. b) GDPR z důvodu zjevné nedůvodnosti nebo nepřiměřenosti. Možnost odmítnout žádost subjektu údajů dosud česká, ani evropská právní úprava správcům výslovně neposkytovala, avšak odmítat některé šikanózní nebo zjevně nedůvodné žádosti bylo výkladem připouštěno s odkazem na zákaz zneužití práva dle ObčZ.[143] Jakkoli GDPR možnost odmítnutí váže na neurčité právní pojmy „*zjevná nedůvodnost*“ nebo „*nepřiměřenost*“, tyto pojmy blíže nedefinuje. Podle Nonnemanna a Matysové bude zjevně nedůvodná především taková žádost, u které GDPR stanoví určité náležitosti. Bude tomu v případě, že neuvede důvody žádosti o omezení zpracování podle čl. 18 GDPR nebo námitky proti zpracování prováděného na základě oprávněného zájmu správce dle čl. 21 odst. 1 GDPR. Zjevně nedůvodná bude podle těchto autorů ale i žádost nesrozumitelná, nebo dožadující se práva, které subjektu v daném případě nepřísluší nebo na jeho situaci ani nedopadá.[144] Přiměřenost žádosti, resp. její nepřiměřenost bude muset být vykládána s přihlédnutím ke konkrétním okolnostem případu

[142] Čl. 12 odst. 3 GDPR
[143] NONNEMANN, František, MATYSOVÁ, Monika. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, č. 12, s. 424.
[144] Tamtéž.

a potenciálnímu dopadu těchto žádostí do práv správce, se zvláštním náhledem zejména na náročnost a náklady na vyřízení podnětu. Jako zjevně nedůvodné nebo nepřiměřené tak budou podle právní teorie zpravidla odmítány opakované žádosti, žádosti, kterými se obchází zákon nebo kterými se zneužívá práva, či žádosti zjevně nepřiměřené.[145] Podle GDPR je nezbytnou součástí sdělení správce o odmítnutí žádosti vedle důvodů odmítnutí i poučení o možnosti podat stížnost k dozorového úřadu či možnosti žádat o soudní ochranu.[146] Podat stížnost k dozorovému úřadu nebo právo na soudní ochranu však bylo možné již podle dosavadní právní úpravy. Jednotlivá práva subjektů údajů jsou pak v stanovena v GDPR v oddíle 2 kapitoly III v článcích 15 až 22. Při bližší analýze těchto práv subjektů údajů je zřejmé, že GDPR převážně přebírá dosavadní úpravu Směrnice 95/46/ES, ze které vychází i ZOOÚ.

Podle čl. 15 GDPR má subjekt údajů právo na přístup k osobním údajům, které je ekvivalentem práva na přístup k informacím o zpracování dle ust. § 12 ZOOÚ. Podstata tohoto práva zůstala nezměněna. I nadále tak má správce povinnost poskytnout „*potvrzení*" o zpracování. GDPR rozsah informací uvedených v potvrzení pouze rozšiřuje zejména o poučení o právu na opravu, výmaz či vznesení námitky proti zpracování.[147]

Podle zásady přesnosti má správce zpracovávat pouze přesné údaje a nepřesné údaje aktualizovat, a to sám, nebo na žádost subjektu údajů. Tato zásada je dále rozvedena v právu subjektů údajů na opravu nebo doplnění dle čl. 16 GDPR, jehož obdobnou úpravu lze nalézt v ust. § 21 odst. 1 písm. b) ZOOÚ. Ve stejném ustanovení je upraveno i právo na blokaci údajů, jež je ekvivalentem nynějšího práva na omezení zpracování dle čl. 18 GDPR. GDPR však oproti ZOOÚ rozšiřuje okruh situací, kdy lze blokaci použít.[148] Vedle rozporu zpracování se zákonem (resp. protiprávností) bude nyní správce muset zpracování omezit, jestliže subjekt popírá přesnost údajů, správce již nepotřebuje údaje ve vztahu k účelu zpracování, potřebuje je však subjekt pro výkon a obhajobu svých právních nároků anebo pokud subjekt vznesl námitku proti zpracování. Po dobu omezení může správce dotčené osobní údaje zpracovávat pouze ve výjimečných případech. Demonstrativní návod postupu správce při omezení nově poskytuje bod 67 odůvodnění GDPR, podle kterého správce například přesune údaje do jiného systému zpracování, znepřístupní údaje uživatelům nebo dočasně odstraní zveřejněné údaje z internetových stránek. ZOOÚ právo na blokaci umožňoval pouze v případě zásahu zpracování do soukromého a osobního života, nebo pokud bylo v rozporu se zákonem.[149]

---

[145] Tamtéž.
[146] Čl. 12 odst. 4 GDPR
[147] Úřad pro ochranu osobních údajů. 6. *Práva subjektu údajů* [online]. uoou.cz, [cit. 3. února 2019]. Dostupné na < https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744>
[148] NULÍČEK: *GDPR - Obecné nařízení*..., s. 216.
[149] Ust. § 21 odst. 1 písm. b) ZOOÚ.

GDPR tak podle mého názoru uplatnitelnost práva na blokaci, resp. omezení zpracování oproti ZOOÚ fakticky rozšiřuje, a to o shora vyjmenované situace.

4.3.1 Právo být zapomenut

Považuji za důležité se pozastavit blíže u práva na výmaz, resp. práva být zapomenut ve smyslu čl. 17 GDPR. Právo na výmaz je v unijní legislativě zakotveno vůbec poprvé. Zdánlivě se však jedná o nový institut, neboť právo na výmaz bylo na jaře roku 2014 dovozeno judikaturou SDEU, a to na základě výkladu práva na opravu, výmaz nebo blokování údajů podle čl. 12 Směrnice 95/46/ES.[150] Závěry uplatňované SDEU tak byly nově výslovně shrnuty do práva na výmaz dle čl. 17 GDPR. Nutno podotknout, že ZOOÚ již v ust. 21 odst. 1 písm. b) právo na likvidaci za tam uvedených podmínek upravoval (viz kapitola 4.3.3.). Byť uplatnění práva na likvidaci bylo užší než v GDPR, eurokonformním výkladem však podle mého názoru bylo možno dojít ke stejnému obsahu tohoto práva dle shora citovaného judikátu SDEU, byť uznávám, že tento výklad by mohl být až příliš extenzivní. Nakonec jsem toho názoru, že právo na výmaz v českém právním prostředí není novinkou.

Právo na výmaz také není právem absolutním. Likvidaci, resp. výmaz údajů lze vyžadovat pouze ve vymezených případech.[151] Je přitom evidentní, že několik podmínek výmazu stanovených GDPR vyplývá již z právní úpravy základních zásad. Tak například má správce povinnost vymazat osobní údaje bez zbytečného odkladu, jestliže pomine účel zpracování těchto údajů, subjekt odvolá souhlas se zpracováním a současně neexistuje jiný právní titul nebo byly osobní údaje zpracovány protiprávně. To však zcela jasně vyplývá ze samotných zásad účelového omezení nebo zásady zákonnosti. GDPR dále stanoví povinnost vymazat osobní údaje, jestliže subjekt údajů vznese námitku proti zpracování dle čl. 21 odst. 1 GDPR a tato je správcem shledána jako důvodná, nebo námitku podle čl. 21 odst. 2 týkající se zpracování pro účely přímého marketingu, kde dojde k výmazu bez dalšího.[152] Osobní údaje budou na žádost subjektu údajů rovněž vymazány, jestliže tak stanoví právo EU nebo členského státu, nebo jestliže byly údaje shromážděny v souvislosti s nabídkou služeb informační společnosti dítěti.[153] Poslední uvedená podmínka se podle právní teorie vztahuje i na takové situace, kde dítě po udělení souhlasu nabyde zletilosti.[154]

Právo na výmaz je však v GDPR výrazně limitováno, a to například výkonem práva na svobodu projevu a informace, plněním právní povinnosti, plněním úkolu ve veřejném zájmu či

---

[150] Rozsudek ze dne 13. května 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12.
[151] ŽŮREK: *Praktický průvodce…*, s. 139.
[152] Zejména proto, že nedochází u tohoto zpracování nedochází k balančnímu testu.
[153] Čl. 17 odst. 3 GDPR
[154] NULÍČEK: *GDPR - Obecné nařízení…*, s. 211 (čl. 17).

výkonu veřejné moci.[155] Výjimky jsou stanoveny velmi široce a v právní teorii se objevují jisté pochybnosti o míře uplatnění a skutečného vymáhání tohoto institutu.[156] Podle mého názoru je výmaz údajů zejména z prostředí internetu velmi složitý, a to z důvodu, že mnohdy tytéž osobní údaje zpracovávají i jiné subjekty než správce, kterému byla žádost o výmaz původně adresována. Bude tomu tak zejména v případě internetových vyhledávačů, které stahují obsah zdrojových stránek a vytváří vlastní databáze. Je možné a velmi pravděpodobné, že stejné osobní údaje se mohou nacházet i ve výsledcích vyhledávání jiného internetového vyhledávače. Podle čl. 19 GDPR mají být sice všichni tito další příjemci údajů o výmazu informováni, ale jak správně vystihuje právní doktrína, jiní správci mohou mít k dispozici vlastní právní titul (a to zpravidla oprávněný zájem) ke zpracování těchto dotčených údajů. K jejich výmazu tak fakticky nemusí dojít, ač o něj subjekt údajů sám žádal.[157] Ve vztahu k výmazu osobních údajů z internetových vyhledávačů tak bude vhodnější, když subjekt upne své snahy k tomu, aby byl vyhledávač „*odstřižen od zdroje*“. To znamená, že subjekt údajů by měl svou žádost o výmaz směřovat na provozovatele zdrojové stránky.[158]

4.3.2 Právo na přenositelnost údajů

GDPR zavádí v čl. 20 právo na přenositelnost údajů neboli právo na portabilitu. Právo na portabilitu je v unijním právním prostředí zakotveno vůbec poprvé a ani v ZOOÚ nemá obdobu. Právo na přenositelnost umožňuje subjektu údajů bezplatně přenášet, kopírovat z prostředí správce do platformy správce jiného, aniž by k tomu původní správce bránil.[159] Právo na portabilitu není použitelné v každém případě, nýbrž jen tehdy, je-li zpracování založeno na souhlasu subjektu, nebo na plnění smlouvy a současně takové zpracování probíhá automatizovaně.[160] Správce je povinen na žádost subjektu údajů údaje poskytnout ve strukturovaném, běžně používaném a strojově čitelném formátu.[161] Je-li to technicky proveditelné, správce by měl na žádost subjektu údaje přímo převést jinému správci.[162] Podle odůvodnění GDPR by se toto právo nemělo vztahovat na případy zpracování při výkonu veřejné moci nebo plnění úkolu ve veřejném zájmu ani při plnění právní povinnosti.[163]

---

[155] Čl. 17 odst. 3 GDPR.
[156] Tak například POMAIZLOVÁ, Karin, FÜRSTOVÁ, Monika. GDPR – revoluce, nebo rozvedení stávajícího? *Bulletin advokacie*, 2017, č. 9, s. 15.
[157] NULÍČEK: *GDPR - Obecné nařízení…,* s. 214 (čl. 17).
[158] NONNEMANN, František. Základní analýza rozhodnutí Soudního dvora EU ve věci internetového vyhledávače Google. *Právní rozhledy*, 2014, č. 13-14, s. 479-486.
[159] Čl. 20 odst. 1 GDPR
[160] Tamtéž.
[161] Tamtéž (blíže k formátům poskytovaných údajů viz Pokyny WP29 ze dne 13. prosince 2016, ve znění revize ze dne 5. dubna 2017, týkající se práva na přenositelnost údajů, č. WP242, rev. 01 dostupné v českém překladu na adrese https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31882).
[162] Čl. 20 odst. 2 GDPR
[163] Bod 68 odůvodnění GDPR.

Portabilita má za cíl mimo jiné posílit konkurenci na trhu poskytování internetových služeb, a to zejména tím, že pro subjekt údajů bude jednodušší přenést data z jedné aplikace do aplikace konkurenčního vývojáře, aniž by tento musel vytvářet obsah v nové aplikaci jejím dlouhodobějším používáním. Tím má dojít k posílení pozice subjektu jako spotřebitele, který nebude nucen setrvávat u jednoho poskytovatele služby.[164] V praxi si tak lze představit přenositelnost údajů mezi běžeckými aplikacemi, hudebními aplikacemi, sdílenými kalendáři, klienty elektronické pošty, aplikacemi shromažďujícími informace o zdravotním stavu apod.[165] V zásadě se však nemusí jednat o data, která aktivně poskytl subjekt údajů, ale i o takové osobní údaje, které vznikly automaticky v souvislosti s užíváním dané platformy subjektem údajů, jako například historie vyhledávání nebo historie příchozích a odchozích hovorů.[166] Podle mého názoru je toto právo velkým přínosem pro spotřebitele, protože dosud byl přenos umožněn fakticky pouze z kulance provozovatele digitální platformy. Musím dát za pravdu autorům právní doktríny, že tato situace v podstatě odrazovala od používání jiných, možná lepších aplikací, neboť jednoduše upravit si novou platformu dle libosti zabere mnoho času, přičemž nejednou jsem si při používání takových aplikací přál možnost „*exportovat*“ své údaje do jiné aplikace. Je však otázka, jak se k tomuto právu budou stavět provozovatelé, pro něž toto právo může být výraznou administrativní zátěží.

4.3.3 Právo vznést námitku proti zpracování

Vedle práva na přenositelnost údajů GDPR zavádí i právo subjektu údajů vznést námitku proti zpracování. Ačkoliv tento institut upravoval již čl. 14 Směrnice 95/46/ES, tuzemská právní úprava obsahovala pouze obecné právo požadovat vysvětlení správce dle ust. § 21 odst. 1 písm. a) bez možnosti, aby žádost byla konkrétně posouzena ve vztahu ke zpracování na podkladě opravného zájmu správce nebo plnění úkolu veřejné moci[167] I v tomto případě se podle mého názoru jedná o příklad nesprávné implementace dosavadní směrnice do tuzemského právního řádu. Právo na vysvětlení totiž bylo navázáno na skutečnost, že správce zpracovával údaje nezákonně nebo pokud mělo vliv na ochranu soukromého a osobního života subjektu údajů. Subjekt údajů měl namísto práva na vysvětlení možnost žádat i blokaci, likvidaci, doplnění nebo opravu údajů. Z komentářové literatury dále vyplývá, že správce žádostí nebyl vázán, přičemž mohl libovolně namísto subjektem zvoleného práva na vysvětlení

[164] POMAIZLOVÁ, Karin, FÜRSTOVÁ, Monika: GDPR – revoluce, nebo…, s. 15.
[165] Tamtéž.
[166] Tamtéž.
[167] NULÍČEK: *GDPR - Obecné nařízení…*, s. 228.

osobní údaje vymazat a naopak.[168] Domnívám se, že dle nové úpravy je správce námitkou vázán, přičemž je povinen se jí zabývat v lhůtách dle čl. 12 odst. 3 GDPR.

GDPR přebírá právní úpravu námitky ze Směrnice 95/46/ES. Námitka dle čl. 21 odst. 1 GDPR směřuje proti zpracování prováděného na podkladě oprávněného zájmu správce nebo plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci. Správce je povinen po podané námitce zpracování přerušit do doby, než prokáže oprávněné důvody pro zpracování, které převažují nad zájmy a právy subjektu údajů, který vznesl námitku. V druhém odstavci čl. 21 GDPR upravuje také námitku proti zpracování osobních údajů za účelem přímého marketingu. V případě takové námitky je správce povinen zastavit zpracování bez dalšího, a to bez podrobnějšího přezkumu důvodnosti námitky. Jedná se o tzv. opt-out režim, který byl možný již dle ust. § 5 odst. 5 ZOOÚ.[169] Zřejmě tak není správný názor právní doktríny[170], že dle ZOOÚ bylo možné dosáhnout stejného výsledku odvoláním souhlasu. Subjekt totiž souhlas ke zpracování údajů za účelem přímému marketingu zpravidla vůbec nemusel dávat. ZOOÚ tak podle mě dával možnost vyslovit nesouhlas a nikoli odvolat souhlas, tedy obsahoval podobnou konstrukci jako nynější čl. 21 odst. 2 GDPR.

O právu na námitku musí správce subjekt údajů při první komunikaci poučit.[171] Tato poučovací povinnost je podle mě upravena nešťastně, neboť je skryta mezi jednotlivými odstavci čl. 21 a je tak s podivem, že se nenachází v obecném výčtu o poskytovaných informacích dle čl. 13 a 14 GDPR, když za nesplnění této poučovací povinnosti správci patrně bude hrozit sankce za porušení ustanovení o právech subjektů údajů dle čl. 83 odst. 5 písm. b) GDPR.

4.4 Povinnosti správců a zpracovatelů

Aby ochrana osobních údajů byla účinná, právní úprava stanoví několik povinností správců a zpracovatelů. Jak bylo uvedeno shora, ZOOÚ základní povinnosti vymezoval v ust. § 5. Směrnice 95/46/ES i GDPR však základní povinnosti ochrany osobních údajů vymezují formou výčtu základních zásad, z nichž lze tyto obecné povinnosti jednoduše dovodit. Jak také bylo uvedeno shora, valná většina těchto zásad a povinností se obsahově nijak nemění, GDPR pouze některé upřesňuje nebo výslovně zakotvuje některé zásady, které se dříve dovozovaly výkladem. Tak například je zpřísněna informační povinnost správce, když tento je nyní povinen reagovat na žádost subjektů údajů ve lhůtách a bezplatně.[172] K podrobnému výkladu ohledně

[168] FOLDOVÁ, Vanda. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 280. (§ 21 odst. 1 písm. a)).
[169] NULÍČEK: *GDPR - Obecné nařízení…*, s. 228.
[170] POMAIZLOVÁ, Karin, FÜRSTOVÁ, Monika: GDPR – revoluce, nebo…, s. 15.
[171] Čl. 21 odst. 4 GDPR
[172] Viz úvod kapitoly 4.3 této diplomové práce.

základních povinností správců a zpracovatelů odkazuji na kapitolu 4.1 a 4.2 této diplomové práce.

GDPR opouští od povinnosti oznámení zamýšleného zpracování dozorovému úřadu, která byla zavedena Směrnicí 95/46/ES a v českém právním řádu v ust. § 16 a násl. ZOOÚ. Důvodem diskontinuity je především fakt, že tato povinnost byla spíše byrokratickou zátěží, než aby přispěla ke zlepšení ochrany osobních údajů. Dle odůvodnění GDPR je notifikace nahrazena účinnějšími postupy a mechanismy, které se uplatní především u zpracování, jež mohou představovat vysoké riziko pro práva a svobody fyzických osob.[173]

Vzhledem k tomu, že GDPR nyní klade důraz na vlastní odpovědnost správce a zavádí povinnost správce dodržování GDPR doložit, mají notifikační povinnost nahradit především záznamy o činnostech zpracování, provedení posouzení vlivu na ochranu osobních údajů, či předběžné konzultace u ÚOOÚ. [174] Vybrané mechanismy budou obecně vymezeny v následujících podkapitolách této diplomové práce s poukazem na některé výkladové problémy.

4.4.1 Záznamy o činnostech

Jak bylo uvedeno shora, velkou změnou v činnosti správců a zpracovatelů je zánik oznamovací povinnosti. Vzhledem k povinnosti správce prokázat soulad s GDPR, je vedení písemných či elektronických záznamů o činnostech dle čl. 30 GDPR jedním z nástrojů, kterými bude správce soulad dokládat. Záznamy o činnostech nahrazují zrušenou oznamovací povinnost správců, o čemž svědčí především náležitosti těchto obecných záznamů dle čl. 30 odst. 1 a 2 GDPR, které se z větší části překrývají s náležitostmi oznámení dle ust. § 16 ZOOÚ.[175] Na rozdíl od notifikační povinnosti dle dosavadních předpisů se navíc povinnost vedení záznamů o činnostech zpracování vztahuje jak na správce, tak i na zpracovatele samotné.[176]

GDPR zavádí výjimku z povinnosti vést záznamy pro podniky a organizace zaměstnávající méně než 250 osob, ledaže takové zpracování pravděpodobně představuje riziko pro práva a svobody subjektů údajů. Výjimka se neuplatní také tehdy, jsou-li zpracovávány na zvláštní kategorie údajů nebo údajů týkajících se rozsudků v trestních věcech a trestných činů.[177]Povinnost vedení záznamů se vztahuje také na subjekty provádějící zpracování, které

---

[173] Bod 89 odůvodnění GDPR
[174]Úřad pro ochranu osobních údajů. *S účinností GDPR končí oznamovací povinnost správců* [online]. uoou.cz, [cit. 3. února 2019]. Dostupné na <https://www.uoou.cz/s-ucinnosti-gdpr-konci-oznamovaci-povinnost-spravcu/d-28855>
[175] KRÁĽ, Štefan. In PATTYNOVÁ a kol (ed). *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě*. Praha: Leges, 2018, s. 246 (čl. 30)
[176] Čl. 30 odst. 2 GDPR
[177] Čl. 30 odst. 5 GDPR

není příležitostné.[178] GDPR však „*příležitostné zpracování"* dále nedefinuje, což vzhledem k neurčitosti tohoto pojmu v praxi představuje interpretační problémy. Podle sdělení WP29 z dubna 2018 nemůže být příležitostné zpracování takové zpracování, které je prováděno pravidelně, např. zpracování osobních údajů zaměstnanců zaměstnavatelem. [179] Britský dozorový úřad za příležitostné sdělení dále nepovažuje jednorázové nebo „*vzácné*" zpracování. Příležitostné zpracování však bude například sběr dat prostřednictvím interních zaměstnaneckých dotazníků za účelem poskytnutí zpětné vazby, pro které záznamy nemusejí být vedeny. [180] Ukazuje se tak, že názor recentní komentářové literatury k GDPR, podle které je příležitostné zpracování takové, které se objevuje v každé společnosti a slouží k podpoře hlavní činnosti, je neudržitelný a podle mého názoru již neobstojí[181] Domnívám se tedy, že povinnost vést záznamy o činnostech se prakticky vztahuje na všechny správce a zpracovatele, kteří pravidelně zpracovávají osobní údaje, a to bez ohledu na riziko pro práva fyzických osob.

Právní úprava záznamů o činnostech je dokladem toho, že zavedení GDPR do sfér činností správců a zpracovatelů není jednorázová záležitost, ale dlouhodobá činnost, která se má stát běžnou součástí činnosti správců, kteří po celou dobu účinnosti nařízení budou muset dodržování GDPR dokumentovat a tyto dokumenty aktualizovat, aby byli schopní soulad dokázat.[182]

4.4.2 Princip záměrné a standardní ochrany

Novým přístupem je tzv. záměrná a standardní ochrana osobních údajů dle čl. 25 GDPR. Tento princip je postaven na zásadě záměrné ochrany (privacy by design) a zásadě standardní ochrany osobních údajů (privacy by default). ZOOÚ ani Směrnice 95/46/ES toto právo neznali, avšak jisté náznaky měla Směrnice ve svém odůvodnění bodu 46, tj. zejména apel na správce při přípravě zpracování zavést jistá opatření.[183]

Záměrná ochrana má být klíčovou součástí všech IT systémů, které zpracovávají osobní údaje a které jsou poskytovány dalším správcům a zpracovatelům anebo koncovým spotřebitelům. Mnohé osoby totiž nemají tolik znalostí v oblasti počítačových systémů, aby samy zavedly příslušná opatření za účelem ochrany jejich nebo cizích osobních údajů. [184]

---

[178] Čl. 30 odst. 5 GDPR
[179] WP29. *Position Paper related to article 30(5)* [online]. ec.europa.eu, 19. dubna 2018 [cit. 17. února 2019]. Dostupné na <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422>.
[180] Information Commissioner's Office. *Who needs to document their processing activities?* [online]. ico.org.uk [cit. 17 února 2019]. Dostupné na <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/who-needs-to-document-their-processing-activities/>.
[181] Blíže k tomuto názoru viz KRÁĽ, Štefan. In PATTYNOVÁ a kol (ed). *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě*. Praha: Leges, 2018, s. 250 (čl. 30).
[182] PERRY, Rob. GDPR – project or permanent reality? *Computer Fraud & Security*. 2019, č. 1, s. 9-11.
[183] KRÁĽ: *Obecné nařízení…*,s. 228 (čl. 25).
[184] SCHAAR, Peter. Privacy by Design. *Identity in the Information Society*, 2010, č. 3, s. 267-274.

Zásada záměrné ochrany tedy tkví v tom, že správce má již ve fázi vývoje prostředků zpracování zavést technická a organizační opatření tak, aby již od začátku byly respektovány zásady ochrany soukromí a ochrany osobních údajů dle čl. 5 GDPR, tedy zejména minimalizace údajů a transparentnost. Příkladem prostředků, které budou v souladu se záměrnou ochranou je využívání pseudonymizace[185] a šifrování.[186] Zásada privacy by default rozvádí zásadu záměrné ochrany tak, že všechna opatření provedená v souladu se zásadou privacy by design mají být zavedena již ve výchozí verzi, resp. výchozím nastavení aplikace, produktu nebo služby, tedy má být standardní, aby údaje především nebyly zpřístupněny neomezenému počtu fyzických osob. Jako příklad lze uvést platformu sociální sítě, která by uživatelské profily měla mít „*defaultně*" nastavené možná nejvstřícněji k ochraně soukromí například tím, že od začátku omezí přístupnost uživatelského profilu pro neomezený počet osob.[187]

Míra uplatnění těchto zásad a s ní spojených opatření však záleží zejména na míře rizika zpracování pro práva a svobody osob. Domnívám se, že u velké části správců bude povinnost zavést některá z těchto opatření prakticky vyloučena, a to právě s odkazem na nízké riziko jejich zpracování pro práva a svobody osob.

4.4.3 Pověřenec pro ochranu osobních údajů

Novinkou je institut tzv. pověřence pro ochranu osobních údajů v čl. 37 a násl. GDPR. Pověřenec vykonává zejména poradenství a poskytování informací správcům a zpracovatelům a jejich zaměstnancům, monitorování souladu s GDPR a dalšími předpisy, školení pracovníků, zvyšování povědomí, spolupráci s dozorovým úřadem a také subjekty údajů.[188] K řádnému výkonu těchto úkolů mu správce a zpracovatel poskytují zdroje a umožní mu přístup k osobním údajům subjektů údajů.[189] Pověřenec může být jak zaměstnancem správce či zpracovatele, tak externím subjektem[190]. Jmenování externího pověřence bude podle literatury vhodné především pro malé a střední společnosti, které nemají dostatek personálních kapacit pro obsazení této pozice.[191]

---

[185] Takové zpracování osobních údajů, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací (k tomu viz čl. 4 odst. 5 GDPR). Příkladem může být nahrazení jména a příjmení číselným kódem, aniž by však příslušný správce ztratil schopnost tyto osoby zpětně identifikovat. Jedná se rovněž o jedno z vhodných technických opatření k zajištění zabezpečení zpracování (srov. čl. 32 odst. 1 písm. a) GDPR)
[186] Evropská komise. *Co to znamená „záměrná" a „standardní" ochrana osobních údajů?* [online]. ec.europa.eu, [cit. 5. února 2019]. Dostupné na <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_cs>.
[187] Tamtéž.
[188] Čl. 39 odst. 1 GDPR
[189] Čl. 38 odst. 2 GDPR
[190] Čl. 37 odst. 6 GDPR
[191] SUCHÁNKOVÁ, Lenka. In PATTYNOVÁ a kol (ed). *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě*. Praha: Leges, 2018, s. 294 (čl. 37 odst. 6).

Předpokladem jmenování pověřence však je, aby tato osoba měla dostatečné profesní kvality, zejména odborné znalosti práva a praxe v oblasti ochrany osobních údajů pro řádné plnění úkolů pověřence.[192] Tato podmínka však neznamená, že by pověřenec měl být vždy kvalifikovaným právníkem. Mělo by jít o osobu, která je srozuměna s vnitřními procesy daného podniku, ale konkrétní požadavky budou záviset na komplexnosti daného zpracování.[193] Tato osoba by však měla mít obecnou znalost práva a adekvátní míru odbornosti v oblasti informačních systémů a bezpečnosti. Adekvátním řešením tak může být určení týmu odborníků nebo jmenování právnické osoby. Vždy však bude muset být určena konkrétní fyzická osoba, která bude za výkon této funkce odpovědná a která bude kontaktní osobou, na kterou se správce, zpracovatel nebo subjekty údajů budou moci obracet.[194]

Z pohledu vzdělání pověřenců bylo na podkladě mé analýzy zjištěno, že u 13 zkoumaných krajských měst, z nichž tři údaj o dosaženém titulu nezveřejnila, má pověřenec právnické vzdělání pouze ve Statutárním městě Olomouc. Z mé analýzy tedy vyplývá, že pověřenci ve veřejné správě budou zpravidla osoby neprávnického vzdělání. Kvalifikovaným právníkem ostatně není ani pověřenec pro ochranu osobních údajů při Univerzitě Palackého v Olomouci.[195]

Ne každý správce či zpracovatel musí v každém případě pověřence jmenovat. Tuto povinnost má pouze ten správce a zpracovatel za splnění alespoň jedné ze tří podmínek v čl. 37 odst. 1 GDPR, a sice: zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů; hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů. Pokud se žádná tato podmínka na správce nevztahuje, není povinen jmenovat pověřence. To však nevylučuje, aby tak správce či zpracovatel učinil dobrovolně. I v případě dobrovolného jmenování se na postavení a úkoly pověřence budou vztahovat příslušná ustanovení GDPR.[196] Dále pokud správce nebo zpracovatel neshledá důvod pro jmenování pověřence, doporučuje WP29, aby tito provedli interní analýzu s cílem posoudit, proč by pověřenec měl, nebo neměl být jmenován,

---

[192] Čl. 37 odst. 5 GDPR
[193] POMAIZLOVÁ, Karin, FÜRSTOVÁ, Monika: GDPR – revoluce, nebo…, s. 15.
[194] SUCHÁNKOVÁ, Lenka. In PATTYNOVÁ a kol (ed). *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě*. Praha: Leges, 2018, s. 292 (čl. 37 odst. 5).
[195] Pověřencem pro ochranu osobních údajů byl jmenován kancléř Univerzity Palackého v Olomouci, pan PhDr. Rostislav Hladký, MBA.
[196] KALÍŠEK, Jindřich, VĚŽNÍKOVÁ, Petra. *Pověřenec pro ochranu osobních údajů dle nařízení GDPR – Nové pokyny WP29 k výkonu funkce* [online]. epravo.cz, 24. ledna 2017 [cit. 13. února 2019]. Dostupné na <https://www.epravo.cz/top/clanky/poverenec-pro-ochranu-osobnich-udaju-dle-narizeni-gdpr-nove-pokyny-wp29-k-vykonu-funkce-104829.html>.

aby v souladu s principem odpovědnosti mohli prokázat, že posoudili případná rizika a faktory. Není totiž vyloučeno, že dozorové úřady tyto dokumenty budou při kontrolách vyžadovat.[197] Z mého pohledu bych u hraničních případů zpracování doporučil správcům a zpracovatelům pověřence na dobrovolné bázi jmenovat, aby tím z opatrnosti předešli porušení ustanovení GDPR a zároveň posílili svou pozici v dokazování souladu s GDPR.

Ačkoliv GDPR stanoví povinnost jmenovat DPO pro správce, jenž provádí „*rozsáhlé zpracování*", GDPR tento pojem nedefinuje. Určité vodítko se nachází v bodu 91 odůvodnění GDPR, dle něhož se jedná o 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.*" Podle pokynů W29 zpracování ve velkém rozsahu zahrnují především zpracování údajů pacientů v nemocnici, údajů cestujících v MHD v rámci jejich sledování prostřednictvím cestovních karet, údajů zákazníků v rámci pravidelné činnosti banky nebo pojišťovny, údajů o obsahu, provozu a umístění zákazníků poskytovatele telefonních nebo internetových služeb. Zpracování ve velkém rozsahu však nezahrnuje zpracování prováděné jedním lékařem nebo samostatným advokátem.[198]

Pověřence rovněž musí jmenovat téměř všechny veřejné instituce, a to včetně obcí a krajů. Podle recentního sdělení ÚOOÚ však tato povinnost nepostihuje organizace zřizované těmito celky, jako jsou např. domy dětí a mládeže, školní jídelny, muzea, galerie, informační centra či dobrovolní hasiči.[199] Návrh adaptačního zákona v souladu s GDPR rozšiřuje okruh orgánů povinných jmenovat pověřence i na orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu.[200].

Institut pověřence patří k nejdiskutovanějším otázkám GDPR. Proto bude tento institut ještě mnohokrát předmětem výkladových stanovisek dozorových úřadů nebo Sboru. Ostatně jak uvedeno shora, WP29 poskytla několik vodítek k neurčitým pojmům některých ustanovení o tomto institutu. Zajímavou otázkou je odpovědnost pověřence pro ochranu osobních údajů. Podle čl. 38 odst. 3 GDPR není pověřenec sankcionován ani propuštěn v souvislosti s plněním svých úkolů. To by do jisté míry mohlo znamenat, že pověřenec není ze své funkce prakticky odpovědný, což odpovídá principu odpovědnosti vyjadřující odpovědnost pouze správce

---

[197] Pokyny pracovní skupiny 29 ze dne 13. prosince 2016, ve znění revize ze dne 5. dubna 2017, týkající se pověřenců pro ochranu osobních údajů, s. 6, č. WP243 rev. 01 (dostupné v českém překladu na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31880).
[198] Tamtéž, s. 10.
[199] Úřad pro ochranu osobních údajů. *K povinnosti jmenovat pověřence vybranými městskými a krajskými organizacemi* [online]. uoou.cz, [cit. 5. února 2019]. Dostupné na <https://www.uoou.cz/k-nbsp-povinnosti-jmenovat-poverence-vybranymi-mestskymi-a-nbsp-krajskymi-organizacemi/d-31980>.
[200] Ust. § 14 návrhu zákona o zpracování osobních údajů.

samotného. Podle mého názoru by však odpovědnost pověřence mohla nastat v režimu soukromého práva, konkrétně by mohl být odpovědný za náhradu škody dle ust. § 2950 ObčZ, a to v případě nesprávné rady nebo informace.

4.4.4 Posouzení vlivu na ochranu osobních údajů (DPIA)

Zdánlivě novým institutem je institut posuzování vlivu na ochranu zpracování osobních údajů, resp. DPIA. Významem tohoto institutu je popis zpracování údajů, posouzení nezbytnosti a přiměřenosti a řízení rizik a vyhodnocení zejména původu, povahy, zvláštnosti a závažnosti těchto rizik pro práva a svobody fyzických osob. Jedná se o jeden z nástrojů k zajištění odpovědnosti správce, kterým bude správce mimo jiné dokládat, že přijal příslušná opatření.[201] Podle mého názoru se jedná o mechanismus, jenž má za cíl „*podchytit*" všechny hrozby zamýšleného zpracování, které představuje vysoké riziko pro práva subjektů údajů.

Povinnost provést DPIA je velmi podobná povinnosti posuzování rizik dle ust. § 13 odst. 3 ZOOÚ. Shodný je i cíl této úpravy, jímž je zejména snížení rizika neoprávněného zpracování, odhalení mezer a snížení potenciální újmy zejména subjektu údajů.[202] Oproti ZOOÚ však GDPR přináší jisté odchylky, a sice, že DPIA musí mít písemnou formu, což plyne zejména z minimálních náležitostí DPIA dle čl. 37 odst. 7 GDPR jakož i z odůvodnění tohoto předpisu.[203]

DPIA je však vázána na pravděpodobnost, že zamýšlené zpracování představuje vysoké riziko pro práva a svobody osob, aniž by však „*vysoké riziko*" bylo v GDPR definováno. Vodítka přitom obecně vymezuje čl. 35 odst. 3 GDPR, podle kterého je provedení DPIA nutné například při rozsáhlém systematickém monitorování veřejných prostorů, rozsáhlém zpracování zvláštních kategorií osobních údajů apod. Podle WP29 vysoké riziko bude pravděpodobné rovněž u zpracování údajů pacientů v nemocnici, používání kamerových systémů na pozemních komunikací za účelem monitoringu chování řidičů či systematické monitorování chování zaměstnanců (včetně jejich činnosti na internetu).[204]

Výjimku z povinnosti posouzení DPIA může představovat přijatý seznam dozorového úřadu dle čl. 35 odst. 4 a 5 GDPR, sestavující seznam druhů operací, které budou či nebudou podléhat DPIA. Podle návrhu seznamu ÚOOÚ tak například nebudou podléhat DPIA zpracování prováděná v rámci vedení účetnictví, personální a mzdové agendy, spočívající

---

[201] Pokyny pracovní skupiny 29 ze dne 4. dubna 2017, ve znění revize ze dne 4. října 2017, týkající se posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679, s. 4, č. WP248 rev. 01 (dostupné v českém překladu na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31892),

[202] NEŠPŮREK a kol. GDPR: Kdy a jak posuzovat vliv zpracování na ochranu osobních údajů a kdy konzultovat dozorový orgán? *EU Právní novinky*, 2017, č. 2, s. 7.

[203] Tamtéž.

[204] Pokyny pracovní skupiny 29 ze dne 4. dubna 2017…, s. 13.

v přímém marketingu, zpracování prováděná advokáty a notáři či snímání veřejné komunikace kamerou umístěnou na vozidle.[205] Návrh adaptačního zákona současně v ust. § 10 vylučuje povinnost provést DPIA v případech, ve kterých je povinnost zpracovávat údaje uložena právním předpisem.

Na institut DPIA je navázána povinnost předběžné konzultace s dozorovým úřadem dle článku 36 odst. 1 GDPR. V případě, že se v DPIA správci nepodaří odstranit nebo snížit rizika i po zavedení (v DPIA navržených) opatření, anebo správce taková opatření ke snížení rizik nemá k dispozici a tzv. zbytková rizika zůstanou stále vysoká, vznikne povinnost správce konzultovat zpracování s dozorovým úřadem.[206]

4.4.5 Oznámení, resp. ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a subjektům údajů

Staronovou[207] povinností správce je ohlašování porušení zabezpečení osobních údajů. Podle čl. 33 odst. 1 GDPR správce ohlásí bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, jakékoli porušení zabezpečení osobních údajů příslušnému dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. GDPR následně v čl. 33 odst. 2 stanoví podrobné náležitosti takového ohlášení, přičemž pokud tyto informace není schopen poskytnout správce současně, musí být poskytnuty alespoň bez dalšího zbytečného odkladu.[208]

Správce má konečně povinnost veškeré případy porušení zabezpečení a další související skutečnosti včetně přijatých nápravných opatření dokumentovat.[209] Podle mého názoru se povinnost dokumentace porušení zabezpečení bude vztahovat na všechny případy porušení bez ohledu na riziko pro práva a svobody osob. V souladu s principem odpovědnosti by tak měl správce věnovat pozornost této dokumentaci, aby v případě kontroly ze strany ÚOOÚ byl schopen doložit soulad s GDPR.

Správce má povinnost bez zbytečného odkladu oznamovat porušení zabezpečení také subjektům údajů, a to v případě, že by porušení zabezpečení představovalo vysoké riziko pro práva a svobody těchto osob.[210]Oznámení adresovaného subjektu údajů by mělo být jasné s použitím jednoduchých jazykových prostředků a s náležitostmi dle čl. 33 odst. 2 GDPR.

---

[205]Úřad pro ochranu osobních údajů. *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)* [online]. uoou.cz, [cit. 5. února 2019]. Dostupné na <https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385>.
[206] Pokyny pracovní skupiny 29 ze dne 4. dubna 2017…, s. 22.
[207] Tato povinnost dosud existovala pouze pro poskytovatele elektronických komunikací dle zákona č. 127/2005, o elektronických komunikacích, ve znění pozdějších předpisů. Nyní však postihuje všechny správce.
[208] Čl. 33 odst. 4 GDPR
[209] Čl. 33 odst. 5 GDPR
[210] Čl. 34 odst. 1 GDPR

Správce by tak měl ohlásit subjektům údajů porušení zabezpečení pouze v případě vysokého rizika porušení zabezpečení pro práva a svobody osob. Podle mého názoru lze k určení těchto případů použít vodítka v článku 35 odst. 3 GDPR, který stanoví povinnost u tam popsaných zpracování provést DPIA. K příkladům zpracování, které pravděpodobně budou představovat vysoké riziko odkazuji na podkapitolu 4.4.4 této diplomové práce.

U obou případu oznámení se pracuje s rizikem pro práva a svobody fyzických osob. Podle mého názoru tak opět bude záviset na povaze zpracování a míře rizika, které, stejně jako u ostatních povinností obsahujících tento korektiv, bude působit na rozsah povinností správce dle GDPR, tedy i na povinnost ohlásit nebo oznámit porušení zabezpečení.

4.5 Postavení ÚOOÚ jako dozorového úřadu

Klíčovou součástí ochrany osobních údajů je existence specializovaného úřadu, který bude mít za cíl ochranu základních práv a svobod osob v souvislosti se zpracováním jejich osobních údajů. Požadavek na zřízení takové instituce plyne již z čl. 28 odst. 1 Směrnice 95/46/ES. GDPR zjevně přebírá právní úpravu obsaženou ve Směrnici 95/46/ES, přičemž některé úkoly a pravomoci dozorového úřadu upřesňuje či rozšiřuje. V České republice vykonává působnost dozorového úřadu ÚOOÚ, jakožto nezávislý orgán, který byl zřízen ust. § 2 odst. 1 ZOOÚ. Jeho postavení a působnost byla doposud poměrně nesystematicky zakotvena až v ust. § 28 a násl. tohoto zákona.

Podle § 29 odst. 1 ZOOÚ Úřad prováděl dozorovou činnost nad dodržováním zákona, ukládal sankce nebo jiná nápravná opatření, poskytoval konzultace (poradenství), vydával výroční zprávy, přijímal podněty a stížnosti, spolupracoval s obdobnými úřady jiných států a vykonával další úkoly na základě zvláštních zákonů.[211] GDPR působnost dozorového úřadu vymezuje obdobně – byť velmi obsáhle – zejména v čl. 57. Nulíček a kolektiv úkoly ÚOOÚ podle GDPR přehledně shrnují do následujících skupin: a) monitorování uplatňování GDPR v praxi; b) osvětová a poradenská činnost; c) dozor v užším smyslu (především kontrola a ukládání nápravných a sankčních opatření); d) mezinárodní spolupráce; e) úkoly týkající se konkrétních institutů či procesů a f) ostatní úkoly (zbytková klauzule).[212] Při porovnání shora uvedené věcné působnosti Úřadu podle GDPR a ZOOÚ je evidentní, že její rozsah se nabytím účinnosti GDPR zvlášť nemění. K naplňování věcné působnosti čl. 58 GDPR dozorovému úřadu výslovně poskytuje tam specifikované pravomoci. Valnou většinu těchto pravomocí však mohl ÚOOÚ vůči správcům a zpracovatelům uplatňovat již před nabytím účinnosti GDPR, a to

[211] Ust. § 29 odst. 1 ZOOÚ.
[212] NULÍČEK: *GDPR - Obecné nařízení…*, s. 426 (čl. 58).

především na podkladě zákona č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.[213]

GDPR má například nově pravomoc provádět vyšetřování formou auditu ve smyslu čl. 58 odst. 1 písm. b) GDPR. S ohledem na bod 126 odůvodnění a názor právní doktríny se však bude jednat o běžnou kontrolu s cílem zjistit skutečný stav věci, fakticky se tedy o novou pravomoc nejedná.[214] Novou kompetencí je možnost ohlásit správci nebo zpracovateli údajné porušení nařízení podle čl. 58 odst. 1 písm. d), což lze ve zkratce charakterizovat jako postup ÚOOÚ při řešení bagatelních porušení GDPR, aniž by však muselo být využito formálního postupu v podobě kontroly, nápravného opatření nebo sankce.[215] Podle literatury však takto ÚOOÚ postupuje již dnes ve věcech stížností na nežádoucí obchodní sdělení, aniž by však tato možnost byla zákonem upravena. [216] ÚOOÚ tento postup pravděpodobně využil v závěru roku 2018, z důvodu podezření, že určitý zpracovatel porušuje GDPR.[217] Úřadu dále přibude několik kompetencí navazující na nově zakotvené instituty, a to např. poradenství navazující na institut konzultací, schvalování kodexů chování, akreditace subjektů vydávající osvědčení o ochraně osobních údajů, vydávání osvědčení a další kompetence související s předáváním osobních údajů do třetích zemí.[218] Nabytím účinnosti GDPR naopak přišel ÚOOÚ o jeden z úkolů, a to o vedení tzv. registru zpracování na základě zápisu oznámení o zpracování podle § 16 ZOOÚ, a to z důvodu zrušení této notifikační povinnosti. Podle připravovaného adaptačního zákona má být registr a údaje v něm evidované ponechán zpřístupněný veřejnosti ještě 18 měsíců po nabytí účinnosti tohoto adaptačního zákona.[219]

GDPR v čl. 52 podrobně stanoví požadavek nezávislosti dozorového úřadu, a to jak po stránce funkční (odst. 1), finanční (odst. 6), tak i personální (odst. 2,3 a 5). Vzhledem k tomu, že český zákonodárce dosud nepřijal zvláštní úpravu adaptující český právní řád na GDPR, použije se na organizaci Úřadu stále ZOOÚ.[220] Ten stanovuje toliko, že ÚOOÚ je nezávislý a jeho činnost je hrazena ze samostatné rozpočtové kapitoly.[221] Taková právní úprava je podle všeho v souladu s GDPR, neboť nezávislost úřadu dle ZOOÚ podle dosavadních názorů právní teorie platí co do jeho stránky institucionální, tak i personální ve vztahu k jeho

---

[213] Tak například ÚOOÚ mohl vyžadovat od osob podklady, mohl vstupovat do prostor apod.
[214] NULÍČEK: *GDPR - Obecné nařízení*..., s. 426 (čl. 58).
[215] ŽŮREK: *Praktický průvodce*..., s. 176.
[216] NULÍČEK: *GDPR - Obecné nařízení*..., s. 426 (čl. 58).
[217] Úřad pro ochranu osobních údajů. *Úřad k případu webu white-media.info* [online]. uoou.cz, [cit. 27. ledna 2019]. Dostupné na <https://www.uoou.cz/urad%2Dk%2Dnbsp%2Dpripadu%2Dwebu%2Dwhite%2Dmedia%2Dinfo/d-32952>.
[218] Čl. 58 odst. 3 GDPR
[219] Ust. § 66 odst. 4 návrhu zákona o zpracování osobních údajů.
[220] ŽŮREK: *Praktický průvodce*..., s. 173.
[221] Ust. § 28 ZOOÚ.

zaměstnancům,[222] kterými jsou předseda, inspektoři a další zaměstnanci.[223] Nezávislost ÚOOÚ podle dosavadních předpisů je s největší pravděpodobností narušována ve vztahu k ostatním pracovníkům (vyjma posledně uvedených) ve služebnímu poměru. V řízeních ve věcech služebního poměru totiž v prvním stupni rozhoduje předseda ÚOOÚ, jako odvolací orgán však rozhoduje náměstek ministra vnitra pro státní službu, což v konečném důsledku vede k závěru, že někteří pracovníci ÚOOÚ nejsou nezávislí, neboť fakticky podléhají služebnímu dozoru Ministerstva vnitra, což je jednak v rozporu s GDPR a směrnicí 95/46/ES, ale i závěry judikatury SDEU.[224] Český zákonodárce si tohoto nedostatku při přípravě adaptačního zákona všiml, a proto v ust. § 51 odst. 3 návrhu tohoto zákona výslovně stanoví, že „*Náměstek ministra vnitra pro státní službu není nadřízeným služebním orgánem vůči předsedovi Úřadu. Proti rozhodnutí předsedy Úřadu ve věci státní služby a proti rozhodnutí kárné komise prvního stupně zřízené v Úřadu není odvolání přípustné.*“ Adaptační zákon však dosud nebyl schválen, a tak je postavení ÚOOÚ evidentně stále v rozporu s požadavky nové unijní úpravy.

Dosavadní zákon stanovoval, že kontrolní činnost ÚOOÚ vykonávají inspektoři a jeho pověření zaměstnanci. Český zákonodárce však institut inspektora v návrhu adaptačního zákona se tento institut dále nepřebírá. V organizaci ÚOOÚ se však nově bude počítat se dvěma místopředsedy, kteří se v souladu s článkem 53 budou považovat za členy dozorového úřadu a plnohodnotné zástupce v případě nepřítomnosti předsedy. Tím má být dle důvodové zprávy k adaptačnímu zákonu „*zajištěna plná funkčnost úřadu za všech předvídatelných okolností.*“[225] GDPR v čl. 53 odst. 2 GDPR na členy dozorového úřadu stanoví přísnější kvalifikační požadavky než ZOOÚ na předsedu a inspektory. Nyní totiž bude muset člen dozorového úřadu mít „*kvalifikaci, zkušenosti a dovednosti, zejména v oblasti ochrany osobních údajů.*“ Podle autorů komentářové literatury měl v roce 2017 tyto předpoklady pouze jeden z tehdejších 7 inspektorů ÚOOÚ.[226]Zákonodárce v návrhu adaptačního zákona na kvalifikační požadavky GDPR reaguje tak, že kromě svéprávnosti a bezúhonnosti členové dozorového úřadu (tj. předseda a místopředsedové ÚOOÚ) budou muset splňovat podmínku věkové hranice 40 let a podmínku ukončení vysokoškolského studia se zaměřením na právo nebo informatiku. K tomu navíc bude muset uchazeč o člena dozorového úřadu mít potřebnou úroveň znalostí anglického, německého nebo francouzského jazyka a nejméně 5 let praxe v oblasti ochrany

[222] NOVÁKOVÁ, Ludmila. In KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, s. 304-305.
[223]Ust. § 30 ZOOÚ.
[224] NULÍČEK: *GDPR - Obecné nařízení…*, s. 409 (čl. 52). (k tomu viz Soudní dvůr: Rozsudek ze dne 9. března 2010, *Evropská komise proti Spolkové republice Německo*, C-518/07, Sb. Rozh. S. I-01885 a dále Soudní dvůr: Rozsudek ze dne 16. října 2012, *Evropská komise proti Rakousku*, C-614/10.).
[225] Důvodová zpráva k ust. § 53 návrhu zákona o zpracování osobních údajů.
[226] NULÍČEK: *GDPR - Obecné nařízení…*, s. 410.

osobních údajů či práva na informace nebo lidských práv a základních svobod. V případě jiného zaměření studijního programu než shora uvedeného bude podmínka vzdělání splněna, má-li osoba praxi delší než 10 let. [227] Nová podmínka jazykového vybavení podle mě souvisí s posílením spolupráce mezi dozorovými úřady v rámci Evropské unie, která bude nastíněna níže. Je proto nutností, aby příslušní členové ÚOOÚ byli schopni této komunikace a spolupráce alespoň v jednom z uvedených jazyků.

GDPR velmi výrazně posiluje spolupráci dozorových úřadů v rámci Evropské unie. S jistou unijní kooperací počítala Směrnice 95/46/ES ve svém čl. 8 odst. 6, jakož i ZOOÚ, který směrnici implementoval, a to v ust. § 29 odst. 1 písm. i), ale komentářová literatura k ZOOÚ již v době příprav GDPR konstatovala, že tato spolupráce v podstatě není efektivní, a to zejména kvůli odlišnému rozsahu kompetencí jednotlivých dozorových úřadů. Proto se nově klade důraz na prvek mezinárodní spolupráce, jakožto významné součásti činností dozorových úřadů.[228] Je tomu například u přeshraničního zpracování osobních údajů, kde GDPR stanovuje příslušnost tzv. vedoucího dozorového úřadu, který spolupracuje s ostatními dotčenými úřady a sdílí s nimi relevantní informace, a to v rámci tzv. mechanismu jednotnosti, především za účelem jednotné aplikace GDPR. [229] Tato příslušnost je dána sídlem jediné nebo hlavní provozovny správce či zpracovatele. Vůči tzv. vedoucímu dozorovému úřadu pak správce či zpracovatel plní všechny příslušné povinnosti, jako např. povinnost konzultace dle čl. 36 odst. 1 GDPR.

Domnívám se, že skutečně došlo k výraznému posunu spolupráce, neboť dosud bylo z důvodu roztříštěnosti právních úprav a s tím spojené odlišnosti v rozsahu kompetencí jednotlivých dozorových úřadů fakticky nemožné, aby úřady postupovaly vůči správcům jednotně. Je evidentní, že Evropská unie má zájem o rozvinutí tzv. volného pohybu osobních údajů, podmínkou však je řádné a jednotné fungování soustavy dozorových úřadů, které budou mít obdobné pravomoci a úkoly. A právě to je jedna ze změn, jež je podle mého názoru hodna označení revoluce v ochraně osobních údajů.

4.6 Sankce za porušení povinností správce nebo zpracovatele

K jedné z nejdiskutovanějších otázek především mezi laickou veřejností patří výše pokut za nezákonné zpracování. Narovinu je třeba přiznat, že v porovnání s dosavadní právní úpravou GDPR horní hranice pokut za nezákonné zpracování posunuje výrazně směrem nahoru. ZOOÚ upravoval dvě skupiny přestupků, a to a) přestupky fyzických osob, za které bylo možno uložit

[227] Ust. § 52 odst. 3 návrhu zákona o zpracování osobních údajů.
[228] KUČEROVÁ: *Zákon o ochraně…*, s. 317 (29 odst. 1 písm. i).
[229] MAŠTALKA, Jiří. Nové nařízení EU o ochraně osobních údajů a některé záležitosti spojené s jeho aplikací v ČR. *Právní rozhledy*, 2016, č. 21, s. 737.

pokutu až ve výši 5 mil. Kč a dále b) přestupky právnických osob a podnikajících fyzických osob, za jejichž spáchání mohl ÚOOÚ uložit pokutu ve výši až 10 mil. Kč.[230]

GDPR stanoví obecné podmínky ukládání správních pokut v čl. 83, přičemž rozlišuje dva druhy porušení právních povinností, které jsou setříděny v závislosti na možný dopad porušení těchto povinností na práva a svobody subjektu údajů. Od důležitosti porušené normy se pak odvíjí, zda subjektu hrozí udělení pokuty ve výši až 10 mil. EUR (nebo 4 % z celosvětového obratu, jedná-li se o podnik[231]) nebo ve výši 20 mil. EUR (nebo 4 % z celosvětového obratu, jde-li o podnik). Pokutu s vyšší sazbou bude ÚOOÚ udělovat nejčastěji za porušení nejdůležitějších právních povinností, jako dodržování základních zásad zpracování, podmínek vyjádření souhlasu, práv subjektů údajů, nebo nesplnění příkazu dozorového úřadu apod.[232] V rámci nižší sazby bude postihováno např. porušení povinnosti ohledně záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů.

Český zákonodárce v adaptačním zákoně využil možnost danou článkem 83 odst. 7 GDPR ohledně výše udělovaných pokut orgánům veřejné moci a veřejným subjektům a snížil maximální výši pokuty pro tyto subjekty na 10 mil. Kč. Současně snižuje horní hranici sazby pokuty obcím nevykonávajícím přenesenou působnost v rozsahu obce s rozšířenou působností, dobrovolným svazkům těchto obcí, jejich příspěvkovým organizacím, případně jimi zřizovaným právnickým osobám vykonávající činnost školy nebo školského zařízení, a to na částku 5 tis. Kč.[233] Podle důvodové zprávy k tomuto připravovanému předpisu je důvodem snaha smířit odrazující a sankční povahu pokuty s faktem, že finanční prostředky těchto pokutovaných institucí zpravidla plynou z veřejných rozpočtů. Právní teorie rovněž konstatuje, že ukládání pokut těmto subjektům ve výši dle GDPR by bylo neúčelné.[234]

Neznamená to však, že každému správci či zpracovateli hrozí vysoká pokuta. Ukládání správních pokut musí být v prvé řadě účinné, přiměřené, ale také odrazující. Platí obecná premisa správního trestání, že správní pokuty se ukládají podle okolností každého jednotlivého případu. GDPR navíc stanoví povinnost zohlednit další okolnosti stanovené v čl. 83 odst. 2 GDPR, které doplňují obecnou úpravu ukládání správních trestů.[235] Dále bude podle mě záležet na celkovém riziku zpracování pro práva osob, které v souladu s přístupem založeným na riziku musí před zpracováním posoudit. V návaznosti na závažnost porušení GDPR může být správce

---

[230] K jednotlivým skutkovým podstatám viz ust. § 44 a násl. ZOOÚ.
[231] Podle článku 4 odst. 18 GDPR „*jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost.*“
[232] ŽŮREK: *Praktický průvodce…*, s. 191.
[233] Ust. § 62 návrhu zákona o zpracování osobních údajů.
[234] ŽŮREK: *Praktický průvodce…*, s. 189. (k tomu srov. i důvodová zpráva k návrhu zákona o zpracování osobních údajů.)
[235] Ust. § 37 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízeních o nich, ve znění pozdějších předpisů.

například nejprve upozorněn, že zamýšlené operace zpracování pravděpodobně porušují GDPR, nebo může být správci uděleno napomenutí nebo mu může být nařízeno, aby vyhověl žádosti subjektu údajů nebo též nařízeno uvést zpracování do souladu s GDPR.[236]

Jakkoliv se může zdát, že pokuty ukládané podle GDPR mohou být vysoké, je třeba se na zvýšení pokut dívat optikou racionálního zákonodárce. Pro nadnárodní společnosti s miliardovými obraty jako je Google, Facebook nebo Twitter přestala fixní horní hranice pokut plnit odstrašující a preventivní funkci. Proto je trendem právních úprav stanovit pokutu procentuálně ve vztahu k obratu podniků. Musím konstatovat, že cesta Evropské unie je v tomto ohledu správná, neboť s ohledem na to, že na sociálních sítích někteří lidé sdílí prakticky celý svůj soukromý život a že úniky těchto dat ze sociálních sítí nejsou ojedinělou událostí, je spravedlivé požadovat, aby provozovatelé dbali na ochranu osobních údajů. Určitá motivace by pro ně tak mohla být mimo jiné hrozba vysokých pokut. Ostatně francouzský dozorový úřad udělil na počátku ledna 2019 rekordní pokutu ve výši 50 mil. EUR společnosti Google právě za porušování pravidel GDPR.[237] Běžnému malému až střednímu podniku v žádném případě ÚOOÚ pokuty v jednotkách miliónů EUR udělovat nebude. Ostatně předsedkyně ÚOOÚ Ivana Jourová veřejnost uklidňovala tím, že pokuty nebudou likvidační.[238] Podle mého se pokuty budou pohybovat nejčastěji v řádech tisíců nebo desetitisíců korun českých pro fyzické osoby, a to v závislosti na jejich majetkových poměrech a individuálních okolnostech případů.

---

[236] Úřad pro ochranu osobních údajů. *11. Sankce, pokuty* [online]. uoou.cz, [cit. 27. ledna 2019]. Dostupné na < https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=27287&n=11%2Dsankce%2Dpokuty&p1=3938>

[237] SLÍŽEK, David. *Google porušuje GDPR a zaplatí pokutu 50 milionů eur, rozhodl francouzský úřad* [online]. Lupa.cz, [cit. 27. ledna 2019]. Dostupné na <https://www.lupa.cz/aktuality/google-porusuje-gdpr-a-zaplati-pokutu-50-milionu-eur-rozhodl-francouzsky-urad/>

[238] Úřad pro ochranu osobních údajů. *Pokyny WP29 ke správnímu pokutování* [online]. uoou.cz, [cit. 27. ledna 2019]. Dostupné na < https://www.uoou.cz/pokyny-wp29-ke-spravnimu-pokutovani/d-27625>.

Závěr

Téma v žádném případě nemělo za cíl podrobně rozebrat každý aspekt nového unijního předpisu. Naopak, cílem bylo zaměřit se na základní instituty dosavadní právní úpravy zpracování osobních údajů v České republice a ty posléze komparovat s odpovídající úpravou GDPR a nastínit stěžejní přístupy nového nařízení. Do předmětu komparace byla zahrnuta i odpovídající ustanovení návrhu zákona o zpracování osobních údajů, jež má český právní řád adaptovat ve vztahu k novému nařízení. Konkrétně jsem zjišťoval, jak se v kontextu nové právní úpravy GDPR mění práva subjektů údajů, jak se mění povinnosti správců a zpracovatelů nebo jak se mění postavení ÚOOÚ po nabytí účinnosti GDPR, a to zejména v souvislosti s označením GDPR jako revoluce v ochraně osobních údajů. Při hledání odpovědí na stanovené výzkumné otázky jsem dospěl k následujícím závěrům.

GDPR převážně vychází z dosavadní právní úpravy zrušené Směrnice 95/46/ES, kterou do českého právního řádu implementoval ZOOÚ. Smyslem nové, stejně jako dosavadní právní úpravy, je účinně chránit osobní údaje. Po zjištění, že se definice pojmu osobní údaj nemění, byl z hlediska právní ochrany subjektů údajů důležitý závěr, že GDPR staví na objektivním pojetí pojmu osobní údaj, ačkoli dosavadní judikatura tuzemských soudů, jakož i právní teorie, se k této otázce dosud stavěly nejednotně.

Z hlediska posílení práv subjektů údajů byla také důležitá analýza konkrétních práv subjektů údajů. GDPR katalog práv subjektů přebírá ze Směrnice 95/46/ES a ZOOÚ. Mnohé z oprávnění však upřesňuje a některá práva zakotvuje zcela nově. Výslovně upraveno je právo na výmaz, které bylo ovšem již dříve judikováno SDEU, nové je právo na portabilitu, jakož i právo nebýt předmětem žádného rozhodnutí založeného na automatizovaném zpracování. Oproti ZOOÚ je nová i právní úprava námitky proti zpracování. Na všechny žádosti subjektů údajů o výkon práv musí nově správce reagovat ve stanovených lhůtách a bezplatně. Takto podrobná úprava postupů vůči subjektům údajů dosud neměla obdoby a společně s nově zakotvenými právy ji nelze posoudit jinak než jako posílení postavení subjektů údajů.

Výrazně se mění i postavení správců. GDPR sice opouští oznamovací povinnost zamýšleného zpracování dozorovému úřadu, avšak více klade důraz na vlastní odpovědnost správce, který musí soulad s GDPR aktivně dokládat. K tomu mají sloužit v GDPR stanovené prostředky, jejichž rozsah užití závisí na riziku zpracování pro práva a svobody fyzických osob v duchu nového konceptu přístupu založeného na riziku, na kterém je GDPR postaveno. V návaznosti na rizika zpracování pak bude záležet, zda je správce povinen k některým novým povinnostem, kterými jsou jmenování pověřence pro ochranu osobních údajů, vedení záznamů o činnostech zpracování, posuzování vlivu na ochranu osobních údajů a navazující předběžná konzultace s dozorovým úřadem, nebo ohlašování porušení zabezpečení osobních údajů všem

dotčeným subjektům údajů a dozorovému úřadu. Jinými slovy, rozsah povinností správce není možno stanovit paušálně, nýbrž pouze s ohledem na individuální okolnosti daného zpracování a zejména jeho rizicích pro práva a svobody osob. Ve vztahu k ZOOÚ se mění chápání souhlasu, který je dnes sice postaven naroveň ostatním právním titulům, avšak jeho použití by mělo připadat v úvahu až tehdy, nelze-li použít jiný právní titul. Pro orgány veřejné moci je souhlas v zásadě dokonce zapovězeným právním titulem.

Také s ohledem na riziko zpracování, jakož i na individuální okolnosti daného porušení, se mají pohybovat i skutečné výše udělovaných pokut. Pravděpodobně nikdy žádnému správci na území České republiky nebude udělena pokuta ve výši 10, nebo dokonce 20 mil. EUR. Spíše tak lze očekávat, že jejich výše se v konkrétních případech nebude lišit od výše pokut udělovaných na podkladě dosavadního ZOOÚ. Návrh českého adaptačního zákona dále využívá zmocnění GDPR a snižuje maximální výši pokuty pro orgány veřejné moci a obce.

Konečně předmětem výzkumu bylo rovněž postavení ÚOOÚ po nabytí účinnosti GDPR. ÚOOÚ má stále postavení jediného dozorového úřadu na českém území. Nařízení podrobně stanoví jeho úkoly a k jejich naplnění stanoví mnoho kompetencí. V zásadě se však většina oprávnění ÚOOÚ nemění, neboť dosud bylo možno postupovat obdobně podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů, který se uplatní i nadále. GDPR nově zavádí některé zcela nové pravomoci, jako je např. ohlášení porušení nařízení správci nebo zpracovateli, jakož i některé další pravomoci související s nově zakotvenými instituty, které však na postavení ÚOOÚ nemají zásadní vliv.

Podle připravovaného českého adaptačního zákona se však změní model personálního složení ÚOOÚ. Adaptační zákon totiž evidentně opouští model inspektorů a zavádí vedle předsedy úřadu funkce dvou místopředsedů. Zároveň oproti ZOOÚ stanoví vyšší kvalifikační požadavky a také nutnou dobu praxe. Činnost ÚOOÚ se výrazně změní ve vztahu k mezinárodní spolupráci. Nově může mít ÚOOÚ příslušnost tzv. vedoucího dozorového úřadu pro přeshraniční zpracování. Výrazně je také posílena mezinárodní spolupráce v rámci mechanismu jednotnosti, který má zajistit jednotný výklad nařízení a postup vůči správcům napříč celou Evropskou unií.

Striktně vzato tak byla vyvrácena v úvodu stanovená hypotéza, že pro malé až střední podniky, které nezpracovávají zvláštní kategorie osobních údajů nebo mezi jejichž hlavní činnosti nepatří rozsáhlé zpracování, se s nabytím účinnosti GDPR ničeho nemění za předpokladu, že tito správci důsledně dodržovali povinnosti dle ZOOÚ. Správci by totiž minimálně měli zhodnotit, zda paušálně udělované souhlasy se zpracováním z hlediska GDPR obstojí a pokud ne, zvolit jiný adekvátní právní titul zpracování. Dále by správci měli aktualizovat dokumenty vztahující se k informačním povinnostem a připravit se na žádosti

subjektů údajů, na které musejí reagovat. Správci sice ekvivalentní povinnosti měli již podle ZOOÚ, avšak vzhledem k aktualizaci některých povinností nelze přijmout závěr, že by následování právní úpravy zpracování podle ZOOÚ bylo nyní v souladu s GDPR. Dokladem toho je i povinnost vést záznamy o činnostech zpracování dle čl. 30 GDPR, jež správce a zpracovatel, kteří zpracovávají osobní údaje nikoli jednorázově, musí bezpodmínečně vést, a to bez ohledu na riziko pro práva a svobody osob. Ačkoliv se v konečném důsledku povinnosti správců výrazně nemění, povinnost vedení záznamů o činnostech bude zatěžovat v podstatě všechny správce a zpracovatele pravidelně zpracovávající osobní údaje. Velkou administrativní zátěž a finanční výdaje však může přinést GDPR také např. pro zaměstnavatele, nemocnice nebo instituce, které zpracovávají zvláštní kategorie osobních údajů nebo provádějí rozsáhlé zpracování, a to v důsledku vyššího rizika pro práva a svobody fyzických osob. U těchto správců je důraz na ochranu osobních údajů logicky vyšší, čemuž odpovídá i širší rozsah jejich povinností.

Spíše než revolucí je tak GDPR evolucí, která, podle mého názoru, hlavně díky médiím, rozšířila povědomí o ochraně osobních údajů i mezi laickou veřejnost. Revoluční je ovšem forma právního předpisu, která v oblasti ochrany osobních údajů a dosti možná ani v jiné právní oblasti pro tak široký okruh právních vztahů dosud použita nebyla. GDPR je tedy třeba vnímat jako příležitost do budoucna, jako jakýsi další stupeň společenského vývoje, standard, který možná v některých požadavcích předbíhá svou dobu, nicméně v blízké budoucnosti bude mít své pevné místo. Ochrana osobních údajů bude čím dál víc zásadní, zejména s ohledem na mohutný vzestup e-commerce a IT technologií. Do budoucna však bude potřeba ještě vyřešit některé otázky plynoucí z neurčitých právních pojmů, což osobně vnímám jako největší slabinu tohoto předpisu. Z důvodu nejistoty a opatrnosti tak např. správci plní některé povinnosti, ačkoli k tomu ve skutečnosti vůbec nemusí být povinní.

Seznam použité literatury

Monografie a komentáře

1. MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012, 206 s.
2. KUČEROVÁ, Alena a kol. (ed). *Zákon o ochraně osobních údajů*. Praha: Nakladatelství C. H. Beck, 2012, 516 s.
3. MATES, Pavel. *Ochrana soukromí ve správním právu*. 2. vydání. Praha: Linde, 2006, 313 s.
4. NOVÁK, Daniel (ed). *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2015, 504 s.
5. MELOTÍKOVÁ: *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, 152 s.
6. ROTSHTEIN, M. A. a kol. (ed). *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*. New Haven: CT: Yale University Press, 1997, 511 s.
7. MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. vydání. Praha: Wolters Kluwer, 2008, 456 s.
8. NULÍČEK, Michal a kol. (ed.) *GDPR - obecné nařízení o ochraně osobních údajů (2016/679/EU) - Praktický komentář*. Praha: Wolters Kluwer, 2017, 544 s.
9. WAGNEROVÁ, Eliška a kol. (ed). *Listina základních práv a svobod – Komentář*. Praha: Wolters Kluwer ČR, 2012, 906 s.
10. ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. vydání. Olomouc: ANAG, 2018, 344 s.
11. TRIDIMAS, Takis. *The General Principles of EU Law*. 2. vydání. Oxford: Oxford University Press, 2006, 800 s.
12. PATTYNOVÁ a kol (ed). *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě*. Praha: Leges, 2018, 488 s.

Odborné články

1. NONNEMANN, František. Objektivní, či subjektivní pojetí osobních údajů? *Právní rozhledy*, 2015, č. 12, s. 425-432.
2. ZEMANOVÁ ŠIMONOVÁ, Hana. Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů. *Bulletin advokacie*, 2017, č. 9, s. 25-33.
3. BARTÍK, Václav. JANEČKOVÁ, Věra. Bezpečnost osobních údajů podle zákona o ochraně osobních údajů. *Právní rozhledy*, 2010, č. 23, s. 839-844.
4. NEŠPŮREK a kol. Souhlas ve světle GDPR. *EU Právní novinky*, 2018, č. 2, s. 12-14.

5. NONNEMANN, František. Zpracování veřejně dostupných osobních údajů a GDPR. *Právní rozhledy*, 2018, č. 5, s. 167-173.
6. NULÍČEK, Michal a kol. GDPR v otázkách a odpovědích. Bulletin advokacie, 2017, č. 9, s. 33-39.
7. NONNEMANN, František, MATYSOVÁ, Monika. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, č. 12, s. 424-433.
8. POMAIZLOVÁ, Karin, FÜRSTOVÁ, Monika. GDPR – revoluce, nebo rozvedení stávajícího? *Bulletin advokacie*, 2017, č. 9, s. 15-25.
9. PERRY, Rob. GDPR – project or permanent reality? *Computer Fraud & Security*, 2019, č. 1, s. 9-11.
10. SCHAAR, Peter. Privacy by Design. *Identity in the Information Society*, 2010, č. 3, s. 267-274.
11. NEŠPŮREK a kol. GDPR: Kdy a jak posuzovat vliv zpracování na ochranu osobních údajů a kdy konzultovat dozorový orgán? *EU Právní novinky*, 2017, č. 2, s. 7-10.
12. MAŠTALKA, Jiří. Nové nařízení EU o ochraně osobních údajů a některé záležitosti spojené s jeho aplikací v ČR. *Právní rozhledy*, 2016, č. 21, s. 737-742.
13. NONNEMANN, František. Základní analýza rozhodnutí Soudního dvora EU ve věci internetového vyhledávače Google. *Právní rozhledy*, 2014, č. 13-14, s. 479-486.

Internetové zdroje

1. NEŠPŮREK, Robert a kol. *Nařízení e-privacy: Jak se změní nakládání s cookies?* [online]. profipravo.cz, 27. září 2018 [cit. 1. prosince 2018]. Dostupné na <https://www.pravniprostor.cz/clanky/ostatni-pravo/narizeni-e-privacy-jak-se-zmeni-nakladani-s-cookies>.
2. Úřad pro ochranu osobních údajů. *Desatero omylů* [online]. uoou.cz, [cit. 1. prosince 2018]. Dostupné na <https://www.uoou.cz/desatero%2Domylu/ds-4818/p1=4818>
3. AUJEZDSKÝ, Josef. *Jsou cookies nebo IP adresa vždy osobním údajem?* [online]. Lupa.cz, 13. září 2019 [cit. 4. prosince 2019]. Dostupné na <https://www.lupa.cz/clanky/jsou-cookies-nebo-ip-adresa-vzdy-osobnim-udajem/>.
4. Úřad pro ochranu osobních údajů. *Zásady a právní důvody zpracování* [online]. uoou.cz, [cit. 14. ledna 2019]. Dostupné na <https://www.uoou.cz/4-zasady-a-nbsp-pravni-duvody-zpracovani/d-27271/p1=3938>.
5. ŠVÉDA, Martin. *Nenechme se strašit souhlasy* [online]. epravo.cz, 27. listopadu 2017 [cit. 15. ledna 2019]. Dostupné na <https://www.epravo.cz/top/clanky/nenechme-se-strasit-souhlasy-106690.html>.

6. Úřad pro ochranu osobních údajů. *Právní důvody zpracování* [online]. uoou.cz, [cit. 18. ledna 2019]. Dostupné na < https://www.uoou.cz/pravni-duvody-zpracovani/d-27318/p1=3938>.
7. Úřad pro ochranu osobních údajů. *6. Práva subjektu údajů* [online]. uoou.cz, [cit. 3. února 2019]. Dostupné na < https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744>.
8. Úřad pro ochranu osobních údajů. *S účinností GDPR končí oznamovací povinnost správců* [online]. uoou.cz, [cit. 3. února 2019]. Dostupné na <https://www.uoou.cz/s-ucinnosti-gdpr-konci-oznamovaci-povinnost-spravcu/d-28855>
9. Evropská komise. *Co to znamená „záměrná" a „standardní" ochrana osobních údajů?* [online]. ec.europa.eu, [cit. 5. února 2019]. Dostupné na <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_cs>.
10. KALÍŠEK, Jindřich, VĚŽNÍKOVÁ, Petra. *Pověřenec pro ochranu osobních údajů dle nařízení GDPR – Nové pokyny WP29 k výkonu funkce* [online]. epravo.cz, 24. ledna 2017 [cit. 13. února 2019]. Dostupné na <https://www.epravo.cz/top/clanky/poverenec-pro-ochranu-osobnich-udaju-dle-narizeni-gdpr-nove-pokyny-wp29-k-vykonu-funkce-104829.html>.
11. Úřad pro ochranu osobních údajů. *K povinnosti jmenovat pověřence vybranými městskými a krajskými organizacemi* [online]. uoou.cz, [cit. 5. února 2019]. Dostupné na <https://www.uoou.cz/k-nbsp-povinnosti-jmenovat-poverence-vybranymi-mestskymi-a-nbsp-krajskymi-organizacemi/d-31980>.
12. Úřad pro ochranu osobních údajů. *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)* [online]. uoou.cz, [cit. 5. února 2019]. Dostupné na <https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385>.
13. Úřad pro ochranu osobních údajů. *Úřad k případu webu white-media.info* [online]. uoou.cz, [cit. 27. ledna 2019]. Dostupné na <https://www.uoou.cz/urad%2Dk%2Dnbsp%2Dpripadu%2Dwebu%2Dwhite%2Dmedia%2Dinfo/d-32952>.
14. Úřad pro ochranu osobních údajů. *11. Sankce, pokuty* [online]. uoou.cz, [cit. 27. ledna 2019]. Dostupné na < https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=27287&n=11%2Dsankce%2Dpokuty&p1=3938>.
15. SLÍŽEK, David. *Google porušuje GDPR a zaplatí pokutu 50 milionů eur, rozhodl francouzský úřad* [online]. Lupa.cz, [cit. 27. ledna 2019]. Dostupné na

<https://www.lupa.cz/aktuality/google-porusuje-gdpr-a-zaplati-pokutu-50-milionu-eur-rozhodl-francouzsky-urad/>.

16. Úřad pro ochranu osobních údajů. *Pokyny WP29 ke správnímu pokutování* [online]. uoou.cz, [cit. 27. ledna 2019]. Dostupné na < https://www.uoou.cz/pokyny-wp29-ke-spravnimu-pokutovani/d-27625>.
17. Information Commissioner's Office. *Principle (a): Lawfulness, fairness and transparency* [online]. ico.org.uk, [cit. 16. února 2019]. Dostupné na <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>.
18. WP29. *Position Paper related to article 30 (5)* [online]. ec.europa.eu, 19. dubna 2018 [cit. 17. února 2019]. Dostupné na <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422>.
19. Information Commissioner's Office. *Who needs to document their processing activities?* [online]. ico.org.uk [cit. 17 února 2019]. Dostupné na <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/who-needs-to-document-their-processing-activities/>.
20. MATOUŠOVÁ, Miroslava. *Sdělení ÚOOÚ k přístupu založenému na riziku* [online]. uoou.cz, 31. srpna 2017 [cit. 8. března 2019]. Dostupné na < https://www.uoou.cz/sdeleni-uoou-k-pristupu-zalozenemu-na-riziku-i-s-prilohou-narizeni-evropskeho-parlamentu-a-rady-eu-2016-679-ze-dne-27-dubna-2016-o-ochrane-fyzickych-osob-v-souvislosti-se-zpracovanim-osobnich-udaju-a-o-volnem-pohybu-tec/d-26811>.

Právní předpisy

1. Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.
2. Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
3. Zákon č. 127/2005 Sb., o elektronických komunikacích o změně některých souvisejících Zákonů, ve znění pozdějších předpisů.
4. Zákon č. 480/2004, o některých službách informační společnosti a o změně některých Zákonů, ve znění pozdějších předpisů.
5. Zákon č. tiskový zákon č. 46/2000 Sb., právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), ve znění pozdějších předpisů.
6. Zákon č. 127/2005, o elektronických komunikacích, ve znění pozdějších předpisů.

7. 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.
8. Zákon č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.
9. 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).
10. 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).
11. Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat.
12. Smlouva o fungování Evropské unie.
13. Smlouva o Evropské unii.
14. Usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů.
15. Listina základních práv Evropské unie.

Soudní rozhodnutí

1. Soudní dvůr: Rozsudek ze dne 5. února 1963, *Van Gend en Loos*, věc 26/62.
2. Soudní dvůr: rozsudek ze dne 15. července 1964, *Costa vs. ENEL*, věc 6/64.
3. Soudní dvůr: rozsudek ze dne 9. března 1978, *Simmenthal*, věc 106/77.
4. Soudní dvůr: Rozsudek ze dne 19. října 2016, *Patrick Breyer proti Spolkové republice Německo*, C-582/14.
5. Soudní dvůr: Rozsudek ze dne 13. května 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12.
6. Soudní dvůr: Rozsudek ze dne 9. března 2010, *Evropská komise proti Spolkové republice Německo*, C-518/07, Sb. Rozh. s. I-01885.
7. Soudní dvůr: Rozsudek ze dne 16. října 2012, *Evropská komise proti Rakousku*, C-614/10.
8. nález Ústavního soudu ze dne 8. března 2006, sp. zn. Pl. ÚS 50/2004.

Ostatní zdroje

1. Návrh zákona o zpracování osobních údajů.
2. Důvodová zpráva k návrhu zákona o zpracování osobních údajů.
3. Odůvodnění GDPR.

4. Stanovisko Úřadu pro ochranu osobních údajů, č. 4/2013.
5. Stanovisko WP29 ze dne 11. února 2004, č. 4/2004.
6. Stanovisko WP29 ze dne 13. července 2010, č. 3/2010.
7. Pokyny WP29 ze dne 13. prosince 2016, ve znění revize ze dne 5. dubna 2017, týkající se práva na přenositelnost údajů, č. WP242 rev.01 (dostupné v českém překladu na adrese https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31882).
8. Pokyny pracovní skupiny 29 ze dne 13. prosince 2016, ve znění revize ze dne 5. dubna 2017, týkající se pověřenců pro ochranu osobních údajů, č. WP243 rev.01 (dostupné v českém překladu na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31880).
9. Pokyny pracovní skupiny 29 ze dne 4. dubna 2017, ve znění revize ze dne 4. října 2017, týkající se posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, č. WP248, rev. 01 (dostupné v českém překladu na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31892).
10. Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků. Úř. věst. L 124, 20.5.2003, s. 36 a násl.

Shrnutí

Diplomová práce nazvaná "Zpracování osobních údajů ve světle Nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR)" se věnuje fenoménu GDPR. Téma v žádném případě nemá ambice podrobně rozebrat každý aspekt nového unijního předpisu. Naopak, cílem je zaměřit se na základní instituty dosavadní právní úpravy zpracování osobních údajů v České republice a ty současně komparovat s odpovídající úpravou GDPR. Součástí diplomové práce je i vymezení stěžejních přístupů nového nařízení. Úkolem je také zkoumat, jak se mění práva subjektů údajů a povinnosti správců a zpracovatelů při zpracování osobních údajů, jakož i sankce za jejich porušení. Zkoumáno je též postavení ÚOOÚ po nabytí účinnosti GDPR. Diplomová práce čerpá z řady odborných českých a zahraničních monografií, časopiseckých článků, internetových zdrojů, ze soudních rozhodnutí a dalších zdrojů. Mezi relevantní zdroje jsou zahrnuty i nejaktuálnější výkladová sdělení ÚOOÚ nebo WP29, jakož i aktuální názorové proudy právní doktríny.

Práce je vedle úvodu a závěru členěna do čtyř kapitol. Ponejprv se věnuje ochraně osobních údajů ve vztahu k ochraně soukromí a stručně také vývojem právní úpravy ochrany osobních údajů. Posléze pojednává o pramenech ochrany osobních údajů. Následuje vymezení základních pojmů, jako například „*osobní údaj*“, kde se výklad dotýká také jeho objektivního či subjektivního pojetí. Jádro diplomové práce tvoří samotná analýza vybraných otázek právní úpravy zpracování osobních údajů v České republice a následná komparace s GDPR. V této kapitole se zaměřuji na analýzu zásad zpracování, právních titulů zpracování, na práva a povinnosti subjektů údajů, správců a zpracovatelů, postavení ÚOOÚ a sankce dle GDPR a ZOOÚ. Celá diplomová práce je vedena v duchu skutečného dopadu nové právní úpravy na malé až střední podniky. V diplomové práci jsou zahrnuty též některá specifika návrhu zákona o zpracování osobních údajů, který má adaptovat český právní řád ve vztahu k GDPR.

Diplomová práce vychází z právní úpravy aktuální k 25. 3. 2019.

Abstract

The diploma thesis titled "*Personal data processing under Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR)*" deals with the GDPR phenomenon. In any case, the thesis does not have the ambition to analyze in detail every aspect of the new EU legislation. On the contrary, the aim is to focus on the basic institutes of the existing legislation on the processing of personal data in the Czech Republic, and to compare them with the corresponding institutes regulated under GDPR. Part of the diploma thesis is also the definition of the key approaches of the new regulation. The target is to analyze how the rights of data subjects and the responsibilities of administrators and processors in the processing of personal data, as well as sanctions for their violation, are changing. The position of the Czech Supervisory Authority after the entry into force of GDPR has also been examined. The diploma thesis uses the information gained from Czech and foreign monographs, journal articles, internet sources, court decisions and other sources. Relevant sources include the most recent interpretative opinions of the Supervisory Authorities, WP29 as well as the current opinions of legal doctrine.

The work is divided into four chapters in addition to the introduction and conclusion. Firstly, it deals with the protection of personal data in relation to the protection of privacy and briefly also with the development of the legal framework for the protection of personal data. It then deals with the sources of personal data protection. Following is the definition of basic concepts, such as "*personal data*", where the interpretation also affects its objective or subjective conception. The core of the diploma thesis is the analysis of selected issues of the legal regulation of the processing of personal data in the Czech Republic and their comparison with GDPR. In this chapter I focus on the analysis of the processing principles, legal titles of processing, the rights and obligations of data subjects, administrators and processors, the status of the Czech Supervisory Authority and sanctions under GDPR and Czech Data Protection Act. The thesis is conducted in the spirit of the real impact of the new legal regulation on small to medium-sized enterprises. The diploma thesis also includes some specifics of the draft law on the processing of personal data, which is to adapt the Czech legal order in relation to the GDPR.

The diploma thesis is based on the current legislation as of 25th March 2019.

Klíčová slova

Zpracování osobních údajů, GDPR, subjekt údajů, správce, zpracovatel, zásady zpracování, důvody zpracování, zpracování veřejně přístupných údajů, objektivní a subjektivní pojetí pojmu osobní údaj, záznamy o činnostech zpracování, příležitostné zpracování, vysoké riziko, pověřenec pro ochranu osobních údajů, posouzení vlivu na ochranu osobních údajů, přístup založený na riziku, zbytkové riziko, postavení ÚOOÚ, sankce dle GDPR, adaptační zákon, malý a střední podnik.

Keywords

Data Processing, GDPR, Data Subject, Administrator, Processor, Processing Principles, Legal Grounds for Data Processing, Processing of Public Data, Objective and Subjective concept of Personal Data, Records of Processing, Occasional Processing, High Risk, Actitivites, Personal Data Protection Officer, Data Protection Impact Assessment, Risk Based Approach, Residual Risk, Position of the Czech Supervisory Authority, Sanctions under GDPR, Adaptation Act, small and medium-sized entreprise.