

Západočeská univerzita v Plzni
Fakulta právnická

Katedra veřejné správy

Bakalářská práce

Zpracování a ochrana osobních údajů a veřejná správa

Předkládá: Simon Mertlů

Vedoucí bakalářské práce: JUDr. Tomáš Louda, CSc.

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Simon MERTLŮ**

Osobní číslo: **R16B0072P**

Studijní program: **B6804 Právní specializace**

Studijní obor: **Veřejná správa**

Název tématu: **Zpracování a ochrana osobních údajů a veřejná správa**

Zadávací katedra: **Katedra veřejné správy**

Z á s a d y p r o v y p r a c o v á n í :

1. Úvod
2. Obecné seznámení s problematikou
3. Právo na informace a princip publicity
4. Zákonná úprava podle zákona č. 101/2000 Sb., o ochraně osobních údajů
5. Úřad pro ochranu osobních údajů
6. General Data Protection Regulation (GDPR)
7. GDPR v praxi
8. Závěr

Rozsah grafických prací:

Rozsah kvalifikační práce: **cca 40 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

viz zvláštní seznam

Vedoucí bakalářské práce: **JUDr. Tomáš Louda, CSc.**

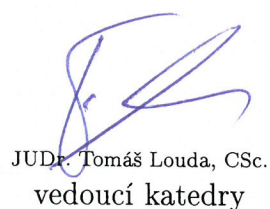
Katedra veřejné správy

Datum zadání bakalářské práce: **31. března 2018**

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



Doc. JUDr. Jan Pauly, CSc.
děkan



JUDr. Tomáš Louda, CSc.
vedoucí katedry

V Plzni dne 17. srpna 2018

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma "Zpracování a ochrana osobních údajů a veřejná správa" zpracoval samostatně a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal způsobem pro vědeckou práci obvyklým.

V Plzni dne 30. března 2019

.....

Simon Mertlů

Poděkování

Rád bych touto cestou poděkoval JUDr. Tomáši Loudovi, CSc., za odborné vedení práce, cenné rady, věcné připomínky a vstřícnost při konzultacích a vedení práce.

Obsah

Úvod	8
1. Obecné seznámení s problematikou	9
1.1 Vymezení pojmů	10
1.2 Veřejná správa	12
1.3 Legislativa upravující ochranu a zpracování osobních údajů	13
1.4 Ústavní základy	15
2. Právo na informace a princip publicity	17
2.1 Kolize v rámci veřejné správy	19
2.1.1 Kolize v rámci činnosti územních samosprávných celků	21
2.2 Test proporcionality	23
3. Zákonná úprava podle zákona č. 101/2000 Sb., o ochraně osobních údajů	25
3.1 Práva a povinnosti při zpracování	27
3.2 Přestupky	31
4. Úřad pro ochranu osobních údajů	33
4.1 Organizační struktura	35
5. General Data Protection Regulation (GDPR)	37
5.1 Cíle, nové přístupy a povinnosti	40
5.1.1 Cíle	40
5.1.2 Nová práva, povinnosti a přístupy	41
5.2 Zásady zpracování osobních údajů podle GDPR	43
5.2.1 Zásada zákonnosti	44
5.2.2 Zásada korektnosti a transparentnosti	46
5.2.3 Zásada účelového omezení	47
5.2.4 Zásada minimalizace údajů	48
5.2.5 Zásada omezení uložení	49
5.2.6 Zásada přesnosti	50

5.2.7 Zásada integrity a důvěrnosti	51
5.2.8 Zásada odpovědnosti	51
5.3 GDPR a role Úřadu pro ochranu osobních údajů	52
5.3.1 Pravomoci	53
5.4 Správní pokuty	55
5.5 GDPR a vztah k právu na informace	57
5.6 Pověřenec pro ochranu osobních údajů	58
6. GDPR v praxi	62
Závěr	65
Summary	67
Seznam použité literatury	69
Seznam příloh	72

Úvod

V dnešní moderní společnosti jsou osobní údaje neodmyslitelnou součástí každodenního života, komunikace a pohybu nejen v soukromé ale především veřejné sféře ať už v reálném či virtuálním prostoru, v kterém musíme osobní údaje poskytovat z důvodu, abychom dosáhli svého cíle, jímž může být např. získání určitého povolení, licence aj. dokladů od pověřeného úřadu nebo účast na správě věcí veřejných a možnost ovlivnění cíle, jenž správa státu sleduje.

Pod osobními údaji si můžeme představit širokou škálu informací, jež mohou být veřejně známé a nejčastěji uváděné jako např. pouhé jméno a příjmení, ale dají se chápat i jako údaje, které danou osobu identifikují a zároveň definují ve vztahu k ní samotné např. zdravotní stav, náboženské vyznání, sexuální orientace apod. a mohou ovlivnit nazírání na ni ostatních subjektů pohybujících se v prostoru a zapříčinit vznik negativních dopadů např. cestou diskriminace, která je dnešní společnosti citelně známá, ačkoliv společnost sleduje záměr zamezení a předcházení takových situací. Děje se tak především cestou ochrany rovnosti práv a ochrany těchto práv samotných ve vztahu ke konkrétním jedincům, neboť je zásadní aby na svých osobnostních právech čítaje právo na ochranu osobních údajů nikdo nebyl zkrácen.

Ochrana osobních údajů je rozsáhlou problematikou a je jedním ze základních práv přiznávaným občanům v podobě práva na ochranu soukromí každého demokratického státu, jenž tyto demokratické zásady upravuje a zajišťuje již v základním zákoně tj. u nás ústavním pořádku. Zároveň o objemnosti tohoto tématu svědčí existence celé řady dalších poměrně v krátkých časových intervalech novelizovaných právních norem, jež jsou vydávané nejen na úrovni národní, nýbrž se můžeme setkat i s právní úpravou na úrovni mezinárodní, neboť vyspělost informačních a komunikačních technologií překonává omezení prostoru a času a je nutno řešit danou problematiku ve souvztáznosti s dalšími státy.

Cílem bakalářské práce je problematiku přiblížit nejen z hlediska právní úpravy již navržené, schválené a vydané na území České republiky, ale bude se snažit o seznámení s inovacemi, které ji provázejí v současné době se zahrnutím pohledu osob pracujících ve veřejné správě, které osobní údaje zpracovávají popř. jsou odpovědné za jejich ochranu, a zároveň tak je úkolem nastínit úskalí zmíněné problematiky, která s sebou přináší inovativní procesy v rámci legislativy resp. oblasti nové právní úpravy.

1. Obecné seznámení s problematikou

Jak už bylo v samotném úvodu přibliženo osobní údaje, jejich zpracování a ochrana poskytují hodně prostoru pro popisování a zpracování tématu z různých úhlů pohledu. Informace mají důležitou roli v životě každého a ještě důležitější ve fungování veřejné správy a společnosti jako takové. Osobní údaje jsou informace speciálního charakteru, jež jsou neoddělitelným a nezczitelným vlastnictvím naprosto každého člověka bez ohledu na jeho společenské postavení a ekonomickou situaci.

Již samotná otázka “Co je to osobní údaj?” nabízí více variant pro odpověď. Mezi nejběžnější odpovědi může patřit vysvětlení, že osobní údaj je takový údaj, který charakterizuje konkrétní osobu a na jehož základě je možné danou osobu identifikovat a vytvořit tak její osobnostní profil. Pak se tedy musíme zabírat tím, na které všechny informace by se příkladné vysvětlení vztahovalo. Samotný pojem informace může působit interpretační potíže.¹

U některých údajů jako jsou např. záznamy osob na kamerovém systému či obdobné videonahrávce se můžeme dohadovat, zda do kategorie osobních údajů spadají a pokud ano, za jakých podmínek a tudíž jejich zařazení může být problematické. V takových případech je třeba se ohlížet na judikaturu Nejvyššího správního soudu popř. Ústavního soudu a stanoviska Úřadu pro ochranu osobních údajů, které v tomto konkrétním případě přisvědčují spíše skutečnosti, že v otázce kamerových systémů jsou tyto obrazové záznamy osob pokládány za osobní údaje a tudíž spadají pod ochranu osobních údajů.² Konkrétně rozsudek Nejvyššího správního soudu sp. z. NSS 1 As 113/2012 označuje provozování kamerových systémů za automatizované zpracování osobních údajů prostřednictvím technického systému. Ovšem musíme počítat s otázkou nahodilého shromáždování osobních údajů, kdy se nepoužije právní úprava České republiky obsahující ochranu osobních údajů.³

Pro správnou orientaci v problematice je vzhledem k rozsáhlosti tématu vhodné prvotně, než práce začne pojednávat detailněji o daném tématu a rozebírat jeho složitější úskalí, definovat, upřesnit a vysvětlit dle zákonných či obecně používaných jiných právnických a učebnicových definic základní pojmy jako je např. už jen samotné slovní spojení osobní údaj a zpracování osobních údajů.

¹ MATOUŠKOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. Praha: ASPI, 2008, s. 18 - 19.

² MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 123.

³ MORÁVEK, J. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Praha: Wolters Kluwer, a.s., 2015, s. 84 - 88.

1.1 Vymezení pojmů

Veřejná správa může být definována jako správa a řízení záležitostí veřejných ve veřejném zájmu.⁴

Osobní údaj je podle zákona jakákoliv informace týkající se určené nebo určitelné fyzické osoby, k níž se osobní údaj vztahuje. Taková osoba je v zákoně označována jako **subjekt údajů**. Subjekt údajů se považuje za určený a určitelný, jestliže ho lze identifikovat přímo či nepřímo a to zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní či sociální identitu.⁵ Subjektem údajů nejsou právnické osoby. V předchozí právní normě byl používán pojem dotčená osoba.

Osobní údaj by měl mít identifikační povahu ve vztahu k subjektu údajů bez nutnosti vynaložení většího úsilí, potřeby zvláštních technických prostředků a vyžadování delšího časového intervalu.

Zvláštní kategorií osobních údajů jsou osobní údaje označované jako citlivé, jenž jsou taxativně vymezené zákonnou úpravou. **Citlivým osobním údajem** se rozumí údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, údaj o odsouzení za trestný čin, zdravotním stavu a sexuálním životě dané osoby nebo její genetický údaj. Za citlivý údaj se též považuje biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.⁶

Naproti tomu stojí **anonymní údaj**, který nelze vztáhnout ke konkrétní určené nebo určitelné osobě v původním stavu ani po zpracování údaje. Na základě anonymního nebo anonymizovaného údaje by nemělo být možné identifikovat určitou osobu ani ve spojení s dalším údajem či informací.

Zveřejněný osobní údaj je údaj zpřístupněný především hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu např. katastru nemovitostí. Takový údaj je následně přístupný neomezenému počtu adresátů, kteří mají přístup k těmto sdělovacím prostředkům, veřejným seznamům aj. místu jejich umístění dle zvoleného způsobu zveřejnění.

⁴ POMAHÁČ, Richard a Olga VIDLÁKOVÁ. *Veřejná správa*. Praha: C.H.Beck, 2002, s. 57.

⁵ § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁶ § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Osoba, které je osobní údaj zpřístupněný a zároveň není zpracovatelem osobních údajů, je dle zákonné definice označována jako **příjemce**.

Zpracovatelem se rozumí zvláštním zákonem či správcem ke zpracování osobních údajů zmocněný nebo pověřený subjekt. **Správce** představuje každý subjekt, který provádí zpracování, odpovídá za něj a určuje účel a prostředky při zpracování osobních údajů.⁷

Zpracování osobních údajů je zákonem charakterizováno jako jakákoliv operace nebo soustava operací, které systematicky s osobními údaji provádí správce nebo zpracovatel, a to automatizovaně nebo jinými prostředky. Zpracování osobních údajů označuje zpravidla operace jako jejich shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.⁸

Shromažďováním osobních údajů se rozumí systematický postup či soubor postupů, který má za cíl získání osobních údajů za účelem jejich dalšího uložení na nosič informací, aby bylo možné tyto údaje okamžitě nebo později dále zpracovávat.⁹

Blokování je operace nebo jejich soustava, kterými se na určitou dobu omezí způsob nebo prostředky zpracování osobních údajů, pokud se nejedná o nezbytné zásahy potřebné pro jejich ochranu. Nicméně osobní údaje je možné po uplynutí časového omezení resp. po ukončení blokování dále zpracovávat, přičemž v případě **likvidace** se jedná o postup, jež označuje fyzické zničení nosiče osobních údajů, fyzické vymazání nebo trvalé vyloučení z dalších zpracování a to například formou skartace listinného dokumentu nebo skartace CD, DVD aj. nosiče dat. Likvidace neumožňuje další zpracování osobních údajů určených k likvidaci, pakliže nebude místo likvidace použita anonymizace, která má v porovnání s efektem likvidace podobné účinky, neboť anonymizovaný údaj už není osobním údajem ve smyslu zákona o ochraně osobních údajů.¹⁰

Ochrana osobních údajů znamená ochranu osobních údajů stanovením práv a povinností při zpracování, shromažďování a jiným nakládání s osobními a citlivými údaji, které mají zabránit jejich zneužití, jež může být postihnuto pokutou.

⁷ § 4 písm. j) a k) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁸ § 4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁹ § 4 písm. f) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

¹⁰ § 4 písm. h) a i) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

1.2 Veřejná správa

Charakter výkonu veřejné správy se váže již na samotné vymezení pojmu veřejná správa, který označuje regulaci a řízení veřejných záležitostí ve veřejném názvu tedy cílevědomou činností, přičemž procesy výkonu veřejné správy mají primárně sloužit občanům a nikoliv naopak. Aby bylo zamezeno zneužití veřejné moci a situace, kdy by činnost veřejné správy neplnila svůj účel, je v širším měřítku vázána právem a nemůže činit nad rámec zákona resp. nesmí provádět takové úkony, které nejsou zákonem stanoveny a na rozdíl od správy soukromé tak nemůže jednat *praeter legem* tzn. v souladu se zákonem, ačkoliv jím není výslovně dovoleno.

Za předpokladu potřeby vymezení důležitosti veřejné správy vzhledem k zpracování a ochraně osobních údajů je třeba brát v potaz množství informací, které jsou pro zajištění jejich funkcí potřebné a se kterými musí pracovat, aby bylo možné veřejného zájmu dosáhnout.

Údaje zpracovávané v rámci veřejné správy lze dělit do několika skupin, přičemž základní skupinou jsou osobní údaje fyzických osob, které jsou získávány především v rámci vyřizování žádostí občanů např. vydávání občanských a řidičských průkazů, ale zároveň se jedná o informace v povinně vedených rejstřících. Pokud by správní orgány v rámci výkonu veřejné správy neměly možnost zpracovávat osobní údaje v této oblasti, nemohlo by občanům být vyhověno, neboť bez poskytnutí jména, příjmení, data narození aj. potřebných nejčastěji uváděných informací se dnes žádná z žádostí neobejde.

S rejstříky a vedenými databázemi se váže další kategorie informací právního charakteru, které se více dotýkají soukromí dané osoby např. pokud se jedná o vedení záznamů v rejstříku trestů nebo o vlastnictví nemovitostí uvedených v katastru nemovitostí. Podstatnou kategorií údajů tvoří dále údaje z oblasti sociálního zabezpečení, neboť pokud by stát neměl informace o majetkových aj. poměrech svých občanů vypovídajících o jejich situaci, nemohl by jim v nouzi poskytnout potřebnou pomoc a postarat se o přiměřené zabezpečení, pokud dané osoby nedokáží samy sebe zajistit. Mezi informace potřebné pro možnost správné péče o občany jsou informace o zdravotním stavu, zaměstnání stávajícím i předchozím a s tím spjaté informace o příjmu občana a dále i příjmech členů rodiny.¹¹

S velkým objemem zpracovávaných dat ve veřejné správě je nutné tato data řádně zabezpečit, aby nedošlo k jejich zneužití, což s sebou přináší zabývání se oblastí přizpůsobení prostředí vzhledem k postupu informačních technologií. Jejich rozvoj se totiž nevyhnutelně

¹¹ MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 29.

dotýká i funkcí veřejné správy, neboť ta je s postupem času modernizována v zájmu občanů, aby poskytované služby a činnost veřejné správy disponovaly potřebnou kvalitou a efektivitou odpovídající poměrům současné doby a společnosti.

Modernizace sebou přináší i ulehčení některých úkonů při práci s osobními údaji např. využívání elektronických databází, ačkoliv stinnou stránkou zůstává fakt, že s využíváním a vývojem informačních technologií přibývá možných rizik a hrozeb např. pokud se jedná o neoprávněné nabourávání se do informačních systémů hackery apod. Proto musí vedle využívání inovativní technologie být zajištěna potřebná odpovídající ochrana a její rozvoj v návaznosti na rostoucí nebezpečí a z hlediska vázanosti veřejné správy právem by měla být tato oblast dostatečně reflektována i v legislativě.

1.3 Legislativa upravující ochranu a zpracování osobních údajů

Jelikož je téma, kterým se práce zabývá, široké, existuje logicky i obsáhlá právní úprava, jež danou problematikou řeší. Kromě níže zmíněné Listiny základních práv a svobod musíme především zmínit zákon č. 101/2000 Sb., o ochraně osobních údajů, který v historických souvislostech nahradil zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech zaměřující se na automatizované zpracování osobních údajů disponující nedostatky z hlediska absence dozorového orgánu a správních pokut.

Mezi zákony důležité pro problematiku zpracování a ochrany osobních údajů patří:

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, který upravuje pravidla pro poskytování informací, podmínky práva svobodného přístupu k informacím a zapracovává příslušné předpisy Evropské unie.

- zákon č. 89/2012 Sb., občanský zákoník.¹²

-zákon č. 500/2004., správní řád, především ve vztahu k činnosti Úřadu pro ochranu osobních údajů a nahlížení do spisů.

Na mezinárodní úrovni se jedná o směrnici Evropského parlamentu a Rady 95/46/ES o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, úmluvu Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat.¹³

¹² Zakotveno v rámci práva na soukromí zejména v § 86 občanského zákoníku.

¹³ Předpisy o ochraně osobních údajů. *Ochrana osobních údajů* [online]. oou.cz, ©2014 [cit. 1.2.2019] Dostupné z: <http://www.oou.cz/predpisy>

Do současné jednak mezinárodní právní úpravy i do vnitrostátních právních předpisů dané problematiky zasáhla především nová legislativa EU a to konkrétně Obecné nařízení na ochranu osobních údajů neboli zkratkou “GDPR”, kterému bude věnována samostatná kapitola níže a které nahrazuje předchozí výše zmíněnou směrnici.

Dále nemůžeme pominout směrnici Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) a směrnici Evropského parlamentu a Rady 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (Směrnice o elektronickém obchodu), které jsou v rámci oblasti zpracování a ochrany osobních údajů též souvisejícími právními předpisy na mezinárodní úrovni, jež ovlivňuje legislativu České republiky.

Mezi zákony na vnitrostátní úrovni dotýkající se i mimo jiné zpracování, shromažďování a uchovávání osobních údajů patří:

- zákon č. 480/2004 Sb., zákon o některých službách informační společnosti.
- zákon č. 127/ 2005 Sb., o elektronických komunikacích.
- zákon č. 133 /2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel).
- zákon č. 158/1999 Sb., o sčítání lidu, domů a bytů v roce 2001.
- zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon).
- zákon č. 301/2000 Sb., o matrikách, jménu a příjmení.
- zákon č. 586/1992 Sb., o daních z příjmů.
- zákon č. 21/1992 Sb., o bankách.
- zákon č. 284/2009 Sb., o platebním styku.
- zákon č. 563/1991 Sb., o účetnictví.
- zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon).
- zákon č. 89/1995 Sb., o státní statistické službě.
- zákon č. 328/1999 Sb., o občanských průkazech.
- zákon č. 134/2016 Sb., o zadávání veřejných zakázek.
- zákon č. 242/2016 Sb., celní zákon.
- zákon č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů (zákon o cestovních dokladech).¹⁴
- zákon č. 48/1997 Sb., o veřejném zdravotní pojištění.
- zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení.

¹⁴ Právní předpisy. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 2.2.2019]. Dostupné z: <https://www.uouu.cz/pravni-predpisy/ds-1257/archiv=0&p1=1657>

- zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů.

1.4 Ústavní základy

Základní právní úpravou a pramenem ochrany osobních údajů je definitivně Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD (dále jen „Listina“), která je součástí ústavního pořádku České republiky a to dle znění čl. 3 Ústavy ČR, z čehož můžeme vyvodit zařazení práva na ochranu osobních údajů v rámci práva na ochranu soukromého života mezi základní ústavně zaručená lidská práva, jež jsou elementární a neodmyslitelná pro existenci právního státu respektujícího svobodu, rovnost a důstojnost lidu dle článku 1 Listiny.¹⁵

Listina upravuje danou problematiku hned v několika člancích a to v čl. 7, čl. 10 a čl. 13 Listiny.

Čl. 7 odst. 1 Listiny zaručuje právo na integritu neboli nedotknutelnost osoby a jejího soukromí a připouští možnost omezit dané právo pouze v případě, pakliže tak stanoví zákon, tudíž zabráňuje svévolným zásahům.

Čl. 10 odst. 1 Listiny zajišťuje právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a zaručuje ochranu jména. Odst. 2 téhož článku Listiny zajišťuje ochranu soukromého a rodinného života před neoprávněným zasahováním, a pro ochranu osobních údajů je nejdůležitější částí článku 10 Listiny odst. 3, který uznává právo každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Čl. 13 Listiny stanoví zákaz porušení listovního tajemství, tajemství jiných písemností a záznamů, ať již uchovaných v soukromí, nebo zasílaných poštou či jiným způsobem s výjimkou případů a způsobem, které stanoví zákon. Dále zaručuje tajemství zpráv podaných telefonem, telegrafem nebo jiným podobným zařízením.¹⁶

Právo na soukromý život a jeho ochranu tedy není komplexně shrnuto v jednom výhradním článku Listiny, ale utváří jej více ustanovení, která se vzájemně doplňují a navazují na sebe, neboť spolu souvisí a představují společně osobní prostor jedince potřebný pro rozvoje jeho individua a důstojné vedení života. Pokud bychom se měli zaměřit jen

¹⁵ MORÁVEK, J. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Praha: Wolters Kluwer, a.s., 2015, s. 12.

¹⁶ čl. 13 Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

na právo na ochranu osobních údajů, pak je zaručeno nejen ve výše zmíněném článku 10 odst. 3 ale váže se na něj uvedený čl. 13 Listiny, který zprostředkovává nedotknutelnost soukromí z hlediska obsahu dokumentů v tištěné, elektronické aj. podobě, kde se z principu často osobní údaje vyskytují a tudíž tento článek poskytuje jeden ze způsobů, jímž musí být zamezeno, aby osobní údaje byly poskytnuty neoprávněným osobám nebo jimi zjištěny.¹⁷

Listina zakotvuje řadu dalších důležitých práv a demokratických principů a jedním z těchto práv je právo na svobodu projevu společně s právem na informace v čl. 17 odst. 1 Listiny a s ním související princip publicity v čl. 17 odst. 5 a čl. 35 odst. 2 Listiny, kvůli čemuž zde vzniká možnost konfliktu práva na informace a práva na ochranu soukromí. Obě zmíněná práva jsou pro správný chod demokratické společnosti zásadní a je tedy velice důležité dbát na to, aby k jejich střetu nedocházelo, a dohlížet, aby při realizaci práva na informace bylo respektováno právo na ochranu osobních údajů.¹⁸

¹⁷ MORÁVEK, J. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Praha: Wolters Kluwer, a.s., 2015, s. 13 - 14.

¹⁸ Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

2. Právo na informace a princip publicity

Jak bylo výše zmíněno právo na informace je jedním z nejdůležitějších práv v demokratickém státě a v našem státě je součástí tzv. materiálního ohniska ústavnosti, které je dle čl. 9 odst. 2 Ústavy nezměnitelné a představuje zásadní demokratické principy. Na zákonné úrovni je právo na informace zakotveno zákonem č. 106/1999 Sb., o svobodném přístupu k informacím a zákonem č. 123/1998 Sb., o právu na informace o životním prostředí.

Z principů demokracie a samotného významu daného pojmu, který označuje vládu lidu, lze snadno vyvodit, že stát neboli veřejná moc by měla především sloužit občanům, kteří tvoří společnou vůli a vládou prostřednictvím svých volených zástupců resp. zastupitelských orgánů. Pro správné fungování musí existovat určitý systém kontroly veřejné správy, který by měl občanům dávat přehled o naplňování veřejného zájmu a informovat je, zda systém slouží skutečně v jejich prospěch a nikoliv naopak. Občanům musí být tedy zaručena určitá politická práva, mezi které právo na informace patří společně s právem na svobodu projevu aj. dalšími právy. Zároveň se předpokládá, že lidé informace potřebují, aby se mohli svobodně rozhodovat a orientovat v rámci konkrétních otázek, situací a jejich vývoje a proto k nim tedy nutně potřebují mít přístup, neboť v opačném případě by byla občanům ztížena možnost se zapojovat do správy veřejných záležitostí v podobě hlasování popř. při vnitřní participaci formou výkonu veřejné funkce např. člena zastupitelstva obce.¹⁹

Povinnými subjekty, které musí poskytovat informace o své činnosti dle čl. 17 odst. 5 Listiny a § 2 odst. 1 zákona o svobodném přístupu informacím, jsou státní orgány, orgány územní samosprávy a veřejné instituce.

Ačkoliv má občan zaručené právo na přístup k informacím, nemá právo na přístup ke všem informacím, neboť informace mají být poskytovány přiměřeným způsobem a zároveň lze právo na přístup k informacím omezit, pokud je omezení řádně přijatelně odůvodněno, má zákonnou oporu resp. naplňuje-li princip legality a legitimacy.

Princip legality neboli zákonnosti vyjadřuje vázanost veřejné správy zákony a stejně tak i dalšími příslušnými obecně závaznými právními předpisy.

Podle principu zákonnosti nemůže být do práva na informace zasaženo jinak, než zákonným způsobem, čímž je eliminována libovůle státních orgánů a zároveň zohledněno hledisko právní jistoty, jelikož zákon taxativně vymezuje právní důvody zásahů do práva na informace

¹⁹ MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 36.

a nelze stanovit jiné na základě obecného odkazu na potřebu ochrany určitého zájmu ani podzákoným právním předpisem.²⁰

Princip legitimacy můžeme popsat jako ospravedlnění či odůvodnění (podle představy demokratické společnosti) omezení ve veřejném zájmu určitého jednání s cílem ochrany před zneužití poskytnutých informací.

Ani jeden ze zmíněných dvou principů nemůže existovat samostatně a tudíž musí princip legality existovat vedle principu legitimacy a naopak, musí fungovat v souladu a vzájemně se doplňovat. Omezení práva na informace se může stát akceptovatelné až po naplnění obou principů, neboť pokud by nebyly naplněny oba principy, nebyla by vyloučena svévole státních orgánů.²¹

V Listině je možnost omezení uvedena v čl. 17 odst. 4, který připouští omezení přístupu a šíření informací pouze zákonem a v případě, je-li to nezbytné pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost či ochranu veřejného zdraví a mravnosti.²² Velice blízkým způsobem tak stanoví i článek 10. odst. 2 Úmluvy o ochraně lidských práv a základních svobod, kde jsou navíc za další možné omezení pokládány ty omezení a sankce, jichž je potřeba pro ochranu územní celistvosti, ochranu před nepokoji a zločinnosti a její předcházení, zabránění úniku důvěrných informací či zachování autority a nestrannosti soudní moci.

Nicméně s právem na informace i právem na ochranu soukromí souvisí velice úzce nejen jejich vymahatelnost podle článku 3 Listiny a čl. 4 Listiny, v kterém je schovaný i princip rovnosti a přiměřenosti a který konkrétně říká, že omezení daných práv musí platit pro všechny stejně a zároveň při omezení musí být šetřena jejich podstata a smyslu a nesmí být užita jinak, než pro jaké účely byla stanovena. Zároveň si od zmíněných aj. lidský práv nemůžeme odmyslet právo na soudní a jinou právní ochranu.²³

O právu na soudní a jinou právní ochranu pojednává Hlava pátá Listiny a zaručuje jej občanům v článku 36 Listiny. V odst. 1 je zmíněna samotná možnost každého domáhat se svého práva u nezávislého a nestranného soudu popř. u jiného orgánu v zákonem stanovených případech. Odst. 2 uvádí, že každý může požádat soud o přezkum zákonnosti rozhodnutí

²⁰ BREJCHA, Aleš. *Právo na informace a povinnost mlčenlivosti v českém právním řádu*. Praha: CODEX Bohemia, 1998, s. 17.

²¹ BREJCHA, Aleš. *Právo na informace a povinnost mlčenlivosti v českém právním řádu*. Praha: CODEX Bohemia, 1998, s. 16.

²² čl. 17 odst. 4 Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

²³ Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

orgánu veřejné správy, za předpokladu, že tvrdí, že byl takovým rozhodnutím zkrácen na svých právech. Stane-li se, že orgán veřejné správy, soud či jiný státní orgán vydal nezákonné rozhodnutí, má dotčená osoba právo na náhradu škody. Stejně tak na náhradu škody má poškozená osoba právo, pokud byla způsobena nesprávným úředním postupem a to podle čl. 36 odst. 3 Listiny. V rámci daného práva pokud dojde ke kolizi práva na informace s právem na ochranu soukromí nastává situace, kdy se soudy tímto střetem musí zabývat.

Konflikt práva na informace popř. práva na svobodu projevu a ochrany soukromí je řešen v různých státech různě. Na území České republiky vychází především z koncepce vyvažování práv a zájmů, která primárně vychází a je rozvedená v rozhodovací praxi Ústavního soudu.

Výchozím ustanovení vztahující se ke kolizi daných práv v rámci národní zákonné úpravy je § 8a zákona o svobodném přístupu k informacím, který stanoví, že poskytovat osobní údaje lze jen za předpokladu, pokud podání informací neodporuje zákonné úpravě ochrany osobních údajů tzn. tedy zákonu o ochraně osobních údajů, dalším právním předpisům a legislativě mezinárodní na základě čl. 10 Ústavy, která tuto oblast upravuje.²⁴

2.1 Kolize v rámci veřejné správy

V České republice se často jedná o střety těchto práv při zveřejňování platů veřejných činitelů.

Zveřejnění platů úředníků nesmí být samoúčelné a každý jednotlivý případ musí být zvážen individuálně. V každém řešeném případě musí být použit tzv. princip proporcionality, což znamená, že musí být posouzeno, zda v konkrétním sporu převažuje zájem veřejný ve smyslu práva na informace a nebo zájem na ochranu práva na ochranu soukromého života pracovníka, v jehož případě bylo o informace požádáno. Odůvodnitelnou situací může být např. vyžádání údajů o příjmu, pokud je zjevné, že daná osoba pobírá mimořádně velké odměny, dary či příspěvky navíc ke svému platu, nicméně jestliže se bude jednat o žádost o poskytnutí informace v situaci, kdy se výše příjmů zásadně neliší od tabulkových hodnot dle zákona č. 234/2014 sb., o státní službě, není důvod takový údaj poskytovat.²⁵

Příkladem v rámci konkrétního procesu může být poměrně nedávný náleží Ústavního soudu TZ 121/2017, kdy Ústavní soud shledal, že statutární město Zlín porušilo poskytnutím

²⁴ § 8a zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

²⁵ JANEČKOVÁ, Eva a Václav BARTÍK. *Zpracování osobních údajů obcemi*. Praha: Wolters Kluwer, 2013, s. 58.

osobních informací o platech svých zaměstnanců jejich základní právo na ochranu před neoprávněným zasahováním do soukromého života a právo na ochranu před neoprávněným zveřejňováním osobních údajů. Ústavní soud zakázal pokračování v takovém porušování práv.

Se stížností byl spojen i návrh na zrušení ustanovení § 8b zákona o svobodném přístupu k informacím, který byl odmítnut s odůvodněním, že posuzované ustanovení se dá vykládat konformním způsobem ve vztahu k ústavě.

Ústavní soud sám uvedl, že právo na informace ve veřejném zájmu není absolutní, pokud jeho výkon zasahuje do práva na ochranu soukromého života, které je ustanoveno v článku 10 Listiny. Dále Ústavní soud přiznal povinnost všem subjektům aplikující právní úpravu zákona o svobodném přístupu k informacím poměřovat všechna zmíněná práva v každém jednotlivém případě a docílit mezi nimi spravedlivé rovnováhy, neboť jsou to práva rovnocenná. Jedná se o subjekty poskytující informaci tedy správní orgány a soudy v systému správního soudnictví.²⁶

Zaměstnavatel dle zákona o svobodném přístupu k informacím jakožto povinný subjekt může odmítnout poskytnutí informace o platu zaměstnance, pokud nejsou splněny všechny zákonné podmínky. Takovými podmínky je rozuměn prvotně účel, kterým musí být dosažení přínosné hodnoty k diskusi o věcech veřejného zájmu. Informace samotná se musí týkat veřejného zájmu, musí existovat a být dostupná. Další podmínkou je, aby žadatel o údaj plnil úkoly či poslání dozoru veřejnosti či roli tzv. “společenského hlídacího psa”.

Pokud zaměstnavatel neposkytne požadované údaje žadateli o informace týkajících se platů jeho zaměstnanců a žadatel nesplnil všechny uvedené podmínky, pak nevydání takových údajů není bráno jako porušení povinnosti státních orgánů a orgánů územní samosprávy poskytnout přiměřeným způsobem informace o své činnosti, která je zakotvena v článku 17 odst. 5 Listiny.²⁷

V některých oblastech v rámci střetů práv převažuje upřednostňování spíše práva na svobodný přístup k informacím z hlediska důležitosti transparentnosti veřejné správy a to

²⁶ SEDLÁČKOVÁ, Miroslava. Zaměstnavatel jako povinný subjekt podle zákona o svobodném přístupu k informacím může za určitých podmínek odmítnout poskytnutí informací o platu zaměstnance (ústavně konformní výklad § 8b zákona o svobodném přístupu k informacím). *Ústavní soud České republiky*. [online]. Ústavní soud, ©2015. 1.11.2017. [cit. 11.11.2018]. Dostupné z: <https://www.usoud.cz/aktualne/zamestnavatel-jako-povinnny-subjekt-podle-zakona-o-svobodnem-pristupu-k-info-rmacim-muze-za-u/>

²⁷ Nález Ústavního soudu ze dne 17.10. 2017, sp. zn. IV. ÚS 1378/16 publikován pod č. 121/2017 Sb., [cit. 11.11. 2018] Dostupné z: https://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/Publikovane_nalezky/2017/IV._US_1378_16_an.pdf

zejména pokud jde o nakládání s veřejnými finančními prostředky resp. jedná-li se o žádosti o základní osobní údaje osob, kterým byly povinným subjektem poskytnuty veřejné prostředky tzn. veřejné finance, věci, majetková práva a jiné majetkové hodnoty patřící státu, státnímu fondu, územnímu samosprávnému celku, či jinému veřejnému subjektu, přičemž podobný přístup zastává i Soudní dvůr Evropské unie (SFEU), který judikoval, že je zájmem EU, aby při poskytování a využívání financí EU bylo dbáno na princip průhlednosti správy, ačkoliv v tomto případě nesmí být zveřejněna jména fyzických osob a přesné částky finanční podpory, neboť to by již znamenalo neodůvodnitelný zásah do soukromého života. Tudíž se tak musí dít způsobem, aby nebyla narušena rovnováha jednotlivých práv a informace nebyly zveřejňovány bez oprávněného důvodu.²⁸

Výjimku ve vztahu k poskytování informací o osobách, jimž byly poskytnuty veřejné prostředky v rámci vnitrostátních poměrů, tvoří informace vztahující se k poskytování veřejných prostředků v rámci právní úpravy sociální oblasti, poskytování zdravotních služeb, hmotného zabezpečení v nezaměstnanosti, státní podpory stavebního spoření a státní pomoci při obnově území, které se dle § 8b odst. 2 zákona o svobodném přístupu k informacím neposkytují.

2.1.1 Kolize v rámci činnosti územních samosprávných celků

Z hlediska práva na informace a zároveň práva na ochranu soukromí mají výjimečné postavení i obce jako veřejnoprávní korporace a to především z důvodu jejich blízkému přímému vztahu k občanům, jelikož obec je ve vztahu ke své samosprávné působnosti jednotkou, která má dbát na zájmy svého společenství, jenž tvoří už dle článku 100 Ústavy. Obce jsou významným základním stupněm, v rámci kterého se mohou občané participovat na správě věcí veřejných a který se jich osobně nejvíce dotýká.

Zaměstnanci obce se při výkonu svých činností setkávají s velkým množstvím osobních údajů ať se již jedná o výkon samosprávy nebo státní správy v přenesené působnosti a logicky se tedy musí zabývat i ochranou osobních údajů a zajišťovat ji dle příslušných právních předpisů, což může být problematické z hlediska organizace některých početně menší úřadů a odborných znalostí pracovníků, kteří na nich působí např. v případě obcí základního typu tzv. “jedničkových obcí”.

Podle zákona o svobodném přístupu k informacím jsou obce jako územní samosprávné celky povinnými subjekty ačkoliv dle principu transparentnosti a principu

²⁸ MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 58.

publicity mají povinnost poskytovat informace o své činnosti již dle článku 17 odst. 5 Listiny. V souvislosti s ochranou osobních údajů při přihlédnutí k celkovému počtu všech typů obcí je patrné, že obce jsou zároveň nejpočetnější skupinou správců a zpracovatelů osobních údajů.²⁹

Tyto skutečnosti mohou v rámci povinností obcí a práv občanů tvořit základ pro vznik konfliktu daných práv.

Podle správního řádu jsou obce povinny zřídit úřední desku způsobem, aby byla všem nepřetržitě přístupná, přičemž se tak děje většinou umístěním úřední desky na budovách obecního úřadu.³⁰ Na úřední desce jsou povinně vyvěšovány dokumenty dle zákona o obcích především obecně závazné vyhlášky a další písemnosti dle zvláštních zákonů nebo oznámení o možnosti určitou písemnost převzít. V takto zveřejňovaných typech dokumentů je možné, že dojde s jejich vyvěšením na úřední desce též k uveřejnění osobních údajů, které tyto dokumenty obsahují, což znamená možný vznik konfliktu práva na informace a práva na ochranu osobních údajů.³¹

I v tomto případě platí výchozí § 8a zákona o svobodném přístupu k informacím, který odkazuje na nutnost při zveřejňování informací osobní povahy souladu se zákonem o ochraně osobních údajů a dalšími normativními právními akty, které tuto problematiku upravují. V rámci zákona o ochraně osobních údajů tak lze odůvodnit zveřejňování osobních údajů ve vyvěšených dokumentech na základě právního titulu, kdy je možné zpracovávat osobní údaje bez souhlasu subjektů údajů, pokud je to nezbytné k dostání právní povinnosti správce v tomto případě tedy povinnosti obce tyto dokumenty zveřejnit.³² Nicméně vždy musí být zváženo, zda není vhodné dokumenty obsahující osobní údaje zveřejňovat jen formou oznámení o možnosti převzetí písemnosti u správního orgánu, pokud to povaha dokumentu umožňuje, přičemž v případě obsažení citlivých údajů se tak musí dít jediné touto cestou.

K zveřejňování osobních údajů v rámci činnosti územních samosprávných celků resp. obcí a krajů může docházet taktéž cestou záznamů formou zápisů z jednání zastupitelstev obcí či krajů uložených na obecním či krajském úřadu, kdy jsou jednání zastupitelstva obce či kraje ze zákona veřejné. Občané dané obce či kraje starší 18 let nebo fyzické osoby starší 18 let vlastníci nemovitost na územní obce či kraje jsou oprávněny do nich nahlížet dle § 16 odst. 2 písm. e) zákona o obcích a dle § 12 odst. 2 písm. c) zákona o krajích. Ostatní osoby mohou do zápisu nahlížet, jen za předpokladu, že nebude narušen zákon o ochraně

²⁹ JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů z pohledu zvláštních právních úprav k 1. 8. 2012*. Olomouc: ANAG, 2012, s. 142

³⁰ § 26 odst. 1 zákona č. 500/2004 Sb., správní řád.

³¹ JANEČKOVÁ, Eva a Václav BARTÍK. *Zpracování osobních údajů obcemi*. Praha: Wolters Kluwer, 2013, s. 44.

³² § 5 odst 2 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

osobních údajů, kdy míru možného zásahu do práva na ochranu osobních údajů posuzuje v jednotlivých případech příslušný správní orgán.

Základní vyvoditelnou myšlenkou je omezení okruhu osob, které mají možnost se k osobním údajům uvedených v záznamech z veřejných jednání zastupitelstva dostat, neboť zákonné explicitní vymezení oprávněných osob nezkracuje dané osoby na jejich právu být informován tzn. je zachován princip publicity a transparentnosti veřejné správy a zároveň jsou osobní údaje chráněny před přístupem neoprávněnou osobou.

Ovšem jiná situace nastává jedná-li se o záznamy z neveřejných schůzí rady obce či kraje, kdy jsou oprávněnými osobami k nahlížení pouze členové zastupitelstva, neboť tato možnost nahlížení do zápisů uložených u obecního úřadu slouží především k výkonu jejich zastávané funkce. Problém střetu práv by se mohl objevit především vzhledem k zveřejnění umožňující dálkový přístup, a proto tak může být provedeno pouze s anonymizovanými veškerými osobními údaji, neboť tento způsob zveřejnění nemá stanovený okruh osob a stává se tak neomezeným.³³

Anonymizace je nutná i v případě zveřejňování nahrávek, vysílání aj. záznamů ze zasedání zastupitelstev na elektronických platformách resp. internetových stránkách obcí, aby nebylo narušeno právo na ochranu osobních údajů třetích osob, jejichž osobní údaje mohou v rozmluvě být zmíněny. Anonymizace se provádí dále i v rámci vyvěšování programů jednání zastupitelstva obce či kraje, neboť zveřejňování programů jednání daných zastupitelstev sleduje primární cíl informovat pouze o činnosti obce a jejích záměrech, v rámci kterého je zveřejňování identit konkrétních fyzických osob zbytečné a nežádoucí.³⁴

2.2 Test proporcionality

Pokud by nebylo poměřováno mezi výše zmíněnými právy individuálně, mohla by nastat situace, kdy bude bez adekvátního důvodu zasaženo do základních práv a svobod dotčených osob, což je z hlediska právního státu a demokratických hodnot nepřijatelné, neboť zásahy do základních práv jsou možné pouze za cílem ochrany jiného základního práva. V případě potřeby posouzení kolize dvou ústavně zaručených práv je využíván test proporcionality. Ústavní soud stanovil ve svém nálezu Pl. ÚS 4/94 jednotlivé aspekty, které je

³³ JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů z pohledu zvláštních právních úprav k 1. 8. 2012*. Olomouc: ANAG, 2012, s. 150 - 151.

³⁴ MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 80.

nutno zhodnotit a z kterých se test proporcionality skládá. Jsou jimi tři kritéria konkrétně vhodnost, potřebnost a porovnání závažnosti obou práv.³⁵

Při zvažování z hlediska vhodnosti je nutné položit a nalézt odpověď na otázku, zda je možné daným omezením či zásahem dosáhnout sledovaného cíle, kterým by měla jednoznačně být ochrana jiného základního práva.

Potřebnost je úvaha, zda by nebylo možné stejného cíle dosáhnout jiným stejně efektivním právem upraveným a povoleným způsobem, který by nezasahoval vůbec nebo v takové míře do základních práv a svobod a tudíž by nemuselo dojít ke kolizi dvou základních práv.³⁶

Třetí kritérium porovnání je porovnání obou základních práv stojících proti sobě z hlediska jejich závažnosti. Jedná-li se o práva rovnocenná, jakož tomu je i v případě práva na informace s právem na ochranu soukromí, jak je již uvedeno na základě nálezu Ústavního soudu o poskytování informací o platech veřejných zaměstnanců, pak je nutné přihlédnout k empirickým, systémovým, kontextovým a hodnotovým argumentům.

Empirickým argumentem je myšlena míra závažnosti skutečnosti spojené s ochranou určitého základního práva, která by mohla ono právo narušovat resp. intenzita negativního působení na základní právo, pokud by nemělo být daným opatřením chráněno. V rámci systémového argumentu se jedná o snahu zařadit dané základní právo do systému základních práv a svobod jako celku, neboť je důležité ujasnit, na jaké místo základní právo patří vzhledem k ostatním právům a svobodám a posoudit jeho smysl vzhledem k danému uspořádání. Kontextový argument v sobě zahrnuje v důsledku určitého opatření s cílem ochrany jednoho práva cestou omezení jiného základního práva další možné negativní dopady. Poslední hodnotový argument se zakládá na hodnocení pozitiv obou práv, jejichž střet je zkoumán, ve vztahu k hierarchii hodnot.³⁷

³⁵ Nález Ústavního soudu ze dne 12.10. 1994, čj. Pl. ÚS 4/94.

³⁶ MORÁVEK, J. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Praha: Wolters Kluwer, a.s., 2015, s. 20.

³⁷ Nález Ústavního soudu ze dne 12.10. 1994, čj. Pl. ÚS 4/94.

3. Zákonná úprava podle zákona č. 101/2000 Sb., o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů, v platném znění k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanovuje podmínky, za nichž se uskutečňuje předávání osobních údajů do jiných států a to v souladu s právem Evropské unie a dalšími mezinárodními smlouvami, kterými je Česká republika vázána.

Zákon přiznává právo na ochranu osobních údajů každému a není tedy podstatné, zdali se jedná o občana České republiky nebo cizince a zároveň zákon neuznává důležitost věku ani způsobilosti k právním úkonům. Zákon tedy správně reflektuje skutečnost, že problematika ochrany osobních údajů se týká každého z nás bez rozdílu rasy, pohlaví, věku aj. charakteristik osobnosti obzvlášť v době rozvoje a hojného využívání informačních technologií, které jsou schopny naše údaje přenést během velmi krátkého časového úseku a to na libovolnou vzdálenost po celém světě.

Fyzickým osobám neboli dle zákona subjektům údajů nejsou uloženy na základě zákona povinnosti, ačkoliv stejně jako všechny osoby, které na základě zmíněného zákona mohou přijít do styku s osobními údaji druhých, mají obecnou povinnost dbát, aby druzí jakožto subjekty údajů neutrpěly újmu na svých právech s ohledem zejména na právo na zachování lidské důstojnosti a právo na ochranu před neoprávněným zasahováním do soukromého života.

Předmětem úpravy dle § 2 je dále zřízení Úřadu pro ochranu osobních údajů se sídlem v Praze, kterému bude věnována samostatná kapitola.

Zákon se vztahuje na veškeré zpracování osobních údajů a to bez zřetele, zda k tomu dochází automatizovaně např. prostřednictvím výpočetní techniky nebo jinými prostředky. Zohledňuje tedy nejen osobní údaje vedené automatizovaně v informačních systémech, jak tomu bylo v dřívější právní úpravě.³⁸

Jedná se o zpracování takových osobních údajů, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby,

³⁸ ŠMÍD, Vladimír, *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 227/2000 Sb., zákona č. 177/2001 Sb., zákona č. 450/2001 Sb., zákona č. 107/2002 Sb., zákona č. 310/2002 Sb., zákona č. 517/2002 Sb., zákona č. 439/2004 Sb., zákona č. 480/2004 Sb., zákona č. 626/2004 Sb. a zákona č. 413/2005 Sb.* Brno, 2005. Komentář. Masarykova univerzita v Brně.

s výjimkou fyzických osob, které zpracovávají osobní údaje výlučně pro osobní potřebu. Fyzické osoby, jež zpracovávají osobní údaje pouze pro vlastní potřebu, nesmí shromážděné informace dále zveřejňovat, využívat v rámci obchodních aktivit či jinak vystavit subjekt údajů neoprávněnému zásahu do soukromí.³⁹

Zároveň se zákon dle § 3 odst. 4 nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány. Většinou jde o shromažďování individuálně a jednoúčelně. Jako příklad lze uvést např. záznam adresy zákazníka při poskytování konkrétní služby a dále speciální povolání, ke kterému se váže povinnost mlčenlivosti např. zdravotnický pracovník. Naproti tomu jiná situace nastává, pokud jde o systematicky vedené adresáře zákazníků, kterým jsou pak následně zasílány nabídky jiných služeb apod.

Zákon se vztahuje i na situace, kdy se právní řád České republiky použije přednostně na základě mezinárodního práva veřejného, i jestliže správce nesídlí na území České republiky. Další situace nastává jestliže správce, který sídlí mimo území Evropské unie, provádí zpracování na území České republiky a nejedná se pouze o předání osobních údajů přes území Evropské unie. Ve zmíněném případě je správce povinen zmocnit na území České republiky zpracovatele postupem uvedeném v § 6 daného zákona. Pokud správce provádí zpracování osobních údajů prostřednictvím svých organizačních jednotek nacházejících se na území Evropské unie, je správce povinen zajistit, že dané organizační jednotky budou zpracovávat osobní údaje v souladu s národním právem příslušného členského státu Evropské unie.⁴⁰

V působnosti zákona v § 3 odst. 6 jsou explicitně zákonem určené výjimky, kterých situací se která konkrétní ustanovení zákona netýkají. Ustanovení § 5 odst. 1, § 11 a § 12 se nepoužijí pro zpracování osobních údajů, které jsou nezbytné pro plnění povinností správce stanovených zvláštními zákony pro zajištění: bezpečnosti a obrany České republiky; veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského zájmu České republiky nebo Evropské unie; významného finančního zájmu České republiky nebo Evropské unie, kterým je zejména stabilita finančního trhu a měny, fungování peněžního oběhu a platebního styku, jakož i rozpočtová a daňová opatření; výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci v některých výše uvedených příkladech; činností spojených se zpřístupňováním svazků bývalé Státní bezpečnosti nebo činností spojených s vedením

³⁹ § 3 odst. 3 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁴⁰ § 3 odst. 5 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

centrální evidenci účtů.⁴¹

3.1 Práva a povinnosti při zpracování

Práva a povinnosti při zpracování osobních údajů jsou upravena v zákoně o ochraně osobních údajů v hlavě II. a to konkrétně v ustanoveních § 5 až § 26. Povinnosti daný zákon přiznává správcům a zpracovatelům, kteří odpovídají za práva fyzických osob, jejichž osobní údaje zpracovávají. Fyzickým osobám, jejichž osobní údaje jsou předmětem zpracování, neboli subjektům údajů zákon nestanovuje žádné povinnosti ale pouze jejich práva.

Zákon v první řadě vymezuje povinnosti správce a to v § 5. Dle daného zákona je správce povinen stanovit prostředky, způsob zpracování a především účel, za kterým jsou osobní údaje zpracovány. Správce musí zpracovat pouze přesné osobní údaje, které získal v souladu s daným zákonem, a pokud je to nezbytné, musí osobní údaje aktualizovat. Za situace, kdy nejsou osobní údaje přesné vzhledem ke stanovenému účelu zpracování, musí správce nepřesné osobní údaje označit a provést opatření přiměřeného charakteru. Z pravidla to znamená zablokování zpracování a následná oprava osobních údajů, jejich doplnění nebo v jiných případech likvidace. Správce je povinen sdělit informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů všem příjemcům tedy všem osobám, kterým jsou osobní údaje zpřístupněny a nezpracovávají osobní údaje podle § 3 odst. 6 písm. g) zákona o ochraně osobních údajů.

Správce je dále povinen shromažďovat pouze takové osobní údaje odpovídající stanovenému účelu a v rozsahu, který je pro naplnění účelu nezbytný. Stejně tak správce uchovává osobní údaje pouze po takovou dobu, která je pro účel zpracování nezbytná. Po uplynutí dané doby mohou být osobní údaje pouze pro účely státní statistické služby, vědecké a archivní, přičemž je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života osob, jejichž osobní údaje jsou uchovávány. V souvislosti s ochranou před neoprávněným zasahováním do soukromého a osobního života, je nutno osobní údaje anonymizovat hned, jak je to možné.⁴² Po uplynutí účelu, pro který byly údaje zpracovány, je správce nebo na základě jeho pokynu také zpracovatel povinen provést jejich likvidaci pokud se nejedná o výše zmíněné výjimky. Stejně tak osobní údaje musí zlikvidovat, pokud o to sám subjekt údajů požádá.

⁴¹ § 3 odst. 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁴² § 5 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Osobní údaje jsou správcem, jak už bylo zmíněno, dle jeho povinností zpracovávány jen v souladu s účelem, za kterým byly shromážděny a pokud by byly zpracovávány jinak, je nutné aby k tomu dal subjekt údajů předem souhlas a nebo aby takové zpracování bylo v souladu s již dříve zmíněnými ustanoveními § 3 odst. 6 daného zákona.

Není povoleno, aby správce shromažďoval údaje pod záminkou jiného účelu nebo jiné činnosti a stejně tak je zakázáno správci sdružovat osobní údaje, které byly získány k rozdílným účelům.⁴³

V rámci svých povinností v první řadě správce nesmí osobní údaje zpracovávat bez souhlasu subjektů údajů, pokud se tak neděje za zákonem stanovených výjimek, kdy může dojít ke zpracování správcem i bez souhlasu. Mezi výjimky patří situace kdy správce provádí zpracování nezbytné pro dodržení své právní povinnosti⁴⁴, plnění smlouvy, jejíž smluvní stranou je subjekt údajů nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů.

Další případy, kdy může správce zpracovávat osobní údaje bez souhlasu subjektu údajů jsou takové, jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem⁴⁵ (nesmí být však dotčeno právo na ochranu soukromého a osobního života subjektu údajů), jedná-li se o zpracování pouze pro účely archivní podle zvláštního zákona taktéž s ohledem na ochranu práva na ochranu soukromého a osobního života subjektu údajů, a jedná-li se o poskytování osobních údajů o veřejně činné osobně, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti, funkčním nebo pracovním zařazení.

Další výjimkou je nezbytnost zpracování kvůli ochraně životně důležitých zájmů subjektu údajů. V tomto případě však je třeba bez zbytečného odkladu získat jeho souhlas, není-li dán pak správce zpracování ukončí a údaje zlikviduje. Další nezbytností je ochrana

⁴³ § 5 odst. 1 písm. g) a h) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁴⁴ Například zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zákon č. 564/1990 Sb., o státní správě a samosprávě ve školství, ve znění pozdějších předpisů, zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, zákon č. 154/2000 Sb., o šlechtění, plemenitbě a evidenci hospodářských zvířat a o změně některých souvisejících zákonů (plemenářský zákon), ve znění pozdějších předpisů, zákon č. 166/1999 Sb., o veterinární péči a o změně některých souvisejících zákonů (veterinární zákon), ve znění pozdějších předpisů, zákon č. 246/1992 Sb., na ochranu zvířat proti týrání, ve znění pozdějších předpisů, zákon č. 147/1996 Sb., o rostlinolékařské péči a změnách některých souvisejících zákonů, ve znění pozdějších předpisů, a zákon č. 219/2003 Sb., o uvádění do oběhu osiva a sadby pěstovaných rostlin a o změně některých zákonů (zákon o oběhu osiva a sadby).

⁴⁵ Zákon č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích, ve znění pozdějších předpisů.

práv a právem chráněných zájmů správce, příjemce a jiné dotčené osoby v souladu s ochranou soukromého a osobního života subjektu údajů.⁴⁶

Subjekt údajů má výhradní právo nejen na ochranu práva na ochranu svého soukromého a osobního života, ale musí být zároveň při udělení souhlasu informován o účelu zpracování, za kterým je souhlas dáván, a dále jakému správci a na jaké období souhlas dává.⁴⁷ Správce musí být v souvislosti s tím schopen po celou dobu zpracování souhlas prokázat.

Správce nebo zpracovatel mohou zpracovávat osobní údaje za účelem nabízení obchodu nebo služeb osobě, jejíž osobní údaje zpracovává. V takovém případě lze použít jméno, příjmení a adresu dané osoby, za předpokladu, že správce nebo zpracovatel dané údaje získal z veřejného seznamu či v souvislosti s vlastní činností. Pokud daná osoba vyjádří písemně svůj nesouhlas, nesmí správce ani zpracovatel dále údaje zpracovávat ani k nim přiřazovat údaje další.⁴⁸

Je možné aby správce zpracování osobních údajů předal jinému správci, pokud budou využity pouze k nabízení obchodu a služeb a subjekt údajů nevyslovil písemně nesouhlas poté, co byl předem informován. Jiný správce tyto údaje dále již nesmí předávat jiné osobě.

Všechny zmíněné povinnosti platí jak pro správce tak obdobně také pro zpracovatele, jehož zmocnění ke zpracování osobních údajů vyplývá z právního předpisu. Pokud není zmocnění stanoveno právním předpisem musí správce se zpracovatelem o zpracování osobních údajů uzavřít smlouvu, která musí mít písemnou formu a musí uvádět, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů. Z toho vyplývá, že zpracovatel navzdory podobnosti vlastních povinností povinnostem správce nikdy není příslušný k určení účelu zpracování, neboť povinnost stanovení účelu náleží výhradně správci.⁴⁹

Zpracovatel má povinnost upozornit bez prodlení na vzniklou situaci, kdy správce porušuje povinnosti stanovené daným zákonem, a ukončit zpracování. Pokud tuto povinnost poruší, odpovídá společně a nerozdílně se správcem za škodu vzniklou subjektu údajů.

⁴⁶ § 5 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁴⁷ § 11 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁴⁸ MATOUŠKOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. Praha: ASPI, 2008, s. 300.

⁴⁹ MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 102.

Mnohem přísněji jsou stanoveny povinnosti při zpracování citlivých údajů. Oblasti možného zpracování citlivých údajů jsou ustanoveny v § 9 zákona a jsou dále upraveny zvláštními zákony.⁵⁰

Při zpracování citlivých údajů je důležitá zejména ochrana práva na zachování lidské důstojnosti a právo na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, na kterou musí dbát správce i zpracovatel a zajistit, aby osoba, jejíž údaje zpracovávají na svých právech neutrpěla újmu, neboť se zneužitím citlivých osobních údajů neoprávněnou osobou se ve většině případů pojí vážnější následky a to zejména v souvislosti s diskriminací.

Každá fyzická osoba, jejíž citlivé aj. osobní údaje jsou zpracovávány nebo shromažďovány, má dle § 11 zákona o ochraně osobních údajů právo na informace o svých právech, o účelu, rozsahu, způsobu zpracování, o zpřístupnění údajů nebo příjemcích, o svých právech k opravě a přístupu k osobním údajům. Zákon o ochraně osobních údajů stanovuje případy, kdy správce nebo zpracovatel není povinen informace poskytnout a to v § 11 odst. 3.

Zákon se dále v § 13 zabývá povinnostmi osob při zabezpečení osobních údajů a uděluje tak další povinnosti správcům a zpracovatelům osobních údajů, kteří musí přijmout a provést taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich zničení, změně či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování nebo jinému zneužití a to i při automatizovaném zpracování. Tato povinnost přetrvává i po ukončení zpracování osobních údajů. Zároveň je správce a zpracovatel povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů.

Osoby, které nejsou zpracovatelem nebo správcem, ale jsou jejich zaměstnanci popř. i jiné osoby zpracovávající osobní údaje tak činí na základě smlouvy se správcem nebo zpracovatelem a to pouze za podmínek a v rozsahu, jenž je správcem nebo zpracovatelem stanoven. Takové osoby jsou vázány povinností zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, vyjímaje informační povinnost osob podle zvláštních zákonů např. § 167 a § 168 zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů. Povinnost mlčenlivosti trvá i po

⁵⁰ Například zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů, zákon č. 218/2002 Sb., o službě státních zaměstnanců ve správních úřadech a o odměňování těchto zaměstnanců a ostatních zaměstnanců ve správních úřadech (služební zákon).

skončení zaměstnání či příslušných prací, v rámci kterých se daná osoba s osobními údaji setká.⁵¹

Zákon upravuje také oznamovací povinnost, která dává za úkol správcům a zpracovatelům oznámit před zahájením zpracování nebo změnou osobních údajů písemně se všemi potřebnými informacemi uvedenými v § 16 odst. 2 daného zákona Úřadu pro ochranu osobních údajů danou skutečnost a svůj záměr mimo výjimky ustanovené v § 18. Při splnění zákonných podmínek je Úřadem pro ochranu osobních údajů provedena registrace. Vznikne-li však z oznámení důvodná obava, že při zpracování osobních údajů by mohlo dojít k porušení daného zákona, zahájí Úřad pro ochranu osobních údajů z vlastního podnětu řízení.

Každý subjekt údajů, který zjistí nebo má podezření, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může požádat správce nebo zpracovatele o vysvětlení nebo požadovat, aby správce nebo zpracovatel odstranil vzniklou skutečnost a to blokováním, provedením opravy, doplněním nebo likvidací osobních údajů. Pokud subjektu údajů vznikla újma majetková i jiná nejen, že správce nebo zpracovatel je povinen odstranit nežádoucí stav, ale je dále povinen nahradit vzniklou škodu a to správce a zpracovatel společně a nerozdílně, pokud zpracovatel neupozornil na porušení správcových povinností na základě viz výše uvedené vlastní povinnosti.⁵²

3.2 Přestupky

Zákon o ochraně osobních údajů vymezuje přestupky v hlavě VII. v ustanoveních § 44 až § 46. V zákoně jsou vymezeny jednak druhy přestupků a jejich pokuty, ale také jsou rozděleny podle osob fyzických, podnikajících fyzických, právnických, podle toho zda jsou zpracovateli a správci či zaměstnanci správce nebo zpracovatele. Projednávání přestupků přísluší Úřadu pro ochranu osobních údajů, který zároveň vybírá za přestupky následné pokuty.

Zaměstnanci správce nebo zpracovatele neboli fyzické osoby, které jsou ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru, vykonávají pro správce nebo zpracovatele činnosti na základě dohody, nebo v rámci plnění zvláštním zákonem uložených

⁵¹ § 14 a 15 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁵² § 8 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

oprávnění a povinností přichází u správce nebo zpracovatele do styku s osobními údaji, se mohou dopustit přestupku porušením povinnosti mlčenlivosti, za který lze uložit pokutu do výše 100 000 Kč.

Správce nebo zpracovatel jakožto fyzická osoba se může dopustit přestupků následujícím vyjmenovaným chováním. Mezi takové nežádoucí chování při zpracování osobních údajů patří nestanovení účelu, prostředků nebo způsobu zpracování nebo stanoveným účelem zpracování porušení povinnosti. Dále se za přestupky považuje zpracování nepřesných osobních údajů, shromáždění nebo zpracování osobních údajů v rozsahu nebo způsobem, který neodpovídá stanovenému účelu, uchování osobních údajů po dobu delší než nezbytnou k účelu zpracování, zpracování osobních údajů bez souhlasu subjektu údajů mimo případy uvedené v daném zákoně, neposkytnutí nebo odmítnutí poskytnutí subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem, nepřijetí nebo neprovedení opatření pro zajištění bezpečnosti zpracování osobních údajů, nesplnění oznamovací povinnosti.

Za vyjmenované přestupky je možné uložit pokutu do výše 1 000 000 Kč. Za situace, že by v případě výše zmíněných přestupků správce nebo zpracovatel ohrozil svým neoprávněným zasahováním do soukromého a osobního života větší počet osob, či porušil dříve zmíněné povinnosti pro zpracování citlivých údajů, pokuta může dosahovat výše až 5 000 000 Kč.

Všeobecně u fyzických osob může dojít k porušení zákazu zveřejnění osobních údajů, které je sankcionováno pokutou do 1 000 000 Kč. Pakliže je tento přestupek spáchán prostřednictvím tisku, filmu, televize, rozhlasu, veřejně přístupné počítačové sítě či jiným obdobným způsobem, lze udělit pokutu do 5 000 000 Kč. Právnícké osoby a podnikající fyzické osoby jsou stejně jako fyzické osoby vázány zákazem zveřejnění osobních údajů, za jehož porušení jim hrozí stejná pokuta jako v případě osob fyzických.

V případě právníckých nebo podnikajících fyzických osob, které jsou správcem nebo zpracovatelem, zákon stanovuje stejné přestupky jako v případě osob fyzických, které jsou správcem nebo zpracovatelem, s rozdílem pokutových sazeb, jenž jsou až 5 000 000 Kč a v případě ohrožení svým neoprávněným zasahováním do soukromého a osobního života větší počet osob, či porušení povinnosti pro zpracování citlivých údajů pak až 10 000 000 Kč. Tyto osoby se mohou navíc dopustit přestupku, kdy daná osoba nevede přehled případů porušení ochrany osobních údajů podle § 88 odst. 7 zákona o elektronických komunikacích.⁵³

⁵³ § 44 až 46 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

4. Úřad pro ochranu osobních údajů

Úřad pro ochranu osobních údajů jinak zkratkou “ÚOOÚ” (dále také “Úřad”) je nezávislý orgán se sídlem v Praze, který ve své činnosti postupuje nezávisle a je vázán pouze zákony a jinými právními předpisy. Vázanost Úřadu pouze zákony a jinými právními předpisy znamená, že do činnosti Úřadu pro ochranu osobních údajů lze zasahovat pouze na základě zákona. Činnost Úřadu je hrazena ze samostatné kapitoly státního rozpočtu České republiky.⁵⁴

Do činnosti a působnosti úřadu patří provádění dozoru nad dodržováním povinností stanovených zákonem při zpracování osobních údajů, vedení registru povolených zpracování osobních údajů (GDPR pozměňuje povinnosti předchozích konzultací), přijímání podnětů a stížností občanů na porušení povinností stanovených zákonem při zpracování osobních údajů a zároveň informuje o vyřizování daných stížností a podnětů.⁵⁵ Dále má Úřad na starosti projednávání přestupků a udělování pokut za porušení podle zákona o ochraně osobních údajů, zpracování a zpřístupňování výroční zprávy o své činnosti.

V rámci mezinárodních vztahů a mezinárodní spolupráce má Úřad pro ochranu osobních údajů na starosti zajišťování plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána, a z přímo použitelných předpisů Evropské unie, mezi které patří především GDPR, a zároveň Úřad pro ochranu osobních údajů spolupracuje s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působící v oblasti ochrany osobních údajů. Úřad pro ochranu osobních údajů v souladu s právem Evropské unie plní oznamovací povinnost vůči orgánům Evropské unie.⁵⁶

Dále Úřad poskytuje konzultace v oblasti ochrany osobních údajů a vykonává další působnosti stanovené mu zákonem. Při výkonu dozoru ve formě kontroly postupuje Úřad podle zákona č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů (nahrazen kontrolním řádem) a správním řádem.

Kontrolní činnost Úřadu je uskutečňována v rámci kontrolního plánu nebo na základě podnětů a stížností.⁵⁷

Úřad pro ochranu osobních údajů je dále dle zákona o svobodném přístupu k informacím povinností poskytovat informace o své činnosti na základě podaných žádostí.

⁵⁴ § 28 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁵⁵ Úřad. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 11.2.2019]. Dostupné z: <https://www.uouu.cz/urad/ds-1059/p1=1059>

⁵⁶ § 29 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁵⁷ § 31 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Žádost musí disponovat určitými náležitostmi, aby mohla být vyřízena. Zejména musí být ze žádosti jasně zřetelné, že je určena Úřadu pro ochranu osobních údajů a že požaduje poskytnutí informace dle zákona o svobodném přístupu k informacím. Dále musí být žádost srozumitelná, musí obsahovat všechny zákonem stanovené údaje o žadateli a musí být jasné, jaká informace je vyžadována. Formulace žádosti nesmí být formulována příliš obecně. Pokud se ukáže některý z nedostatků, Úřad pro ochranu osobních údajů vyzve žadatele k doplnění či upřesnění a to ve lhůtě sedmi dnů od podání žádosti. Jestliže žadatel nezjedná nápravu žádosti do třiceti dnů, Úřad pro ochranu osobních údajů žádost odloží.

Opravným prostředkem proti rozhodnutí o odmítnutí žádosti je odvolání k předsedkyni Úřadu ve lhůtě patnácti dnů ode dne doručení rozhodnutí.

Úřad pro ochranu osobních údajů zveřejňuje poskytnuté informace dle ustanovení § 5 odst. 3⁵⁸ zákona o svobodném přístupu k informacím.⁵⁹

Úřadu pro ochranu osobních údajů poskytuje Ministerstvo vnitra nebo Policie České republiky pro výkon jeho působnosti stanovené zákonem 101/2000 Sb., o ochraně osobních údajů a dalšími právními předpisy referenční údaje ze základního registru obyvatel, údaje z agendového informačního systému evidence obyvatel a údaje z agendového informačního systému cizinců. Takovými údaji se rozumí příjmení popř. rodné příjmení, jméno popř. jména, druh a adresa místa pobytu popř. předchozí adresy místa trvalého pobytu či číslo a platnost oprávnění k pobytu (s tím související počátek pobytu, popř. datum ukončení pobytu) a datum narození.

Poskytnuté údaje lze ve vztahu ke konkrétním případě použít vždy jen takové, které jsou nezbytné ke splnění daného úkolu.⁶⁰

⁵⁸ “Do 15 dnů od poskytnutí informací na žádost povinný subjekt tyto informace zveřejní způsobem umožňujícím dálkový přístup. O informacích poskytnutých způsobem podle § 4a odst. 2 písm. e) a f), informacích poskytnutých v jiné než elektronické podobě, nebo mimořádně rozsáhlých elektronicky poskytnutých informacích postačí zveřejnit doprovodnou informaci vyjadřující jejich obsah.”

⁵⁹ Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 12.11.2018]. Dostupné z:

<https://www.uouu.cz/zakon-c-106-1999-sb-o-svobodnem-pristupu-k-informacim/ds-2571/p1=2571>

⁶⁰ § 29a zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

4.1 Organizační struktura

Struktura Úřadu je tvořena zaměstnanci, kterými jsou předseda nebo předsedkyně, inspektoři a další zaměstnanci. Kontrolní činnost Úřadu provádějí inspektoři a pověření zaměstnanci označení zákonem o ochraně osobních údajů jako kontrolující.

Předseda nebo předsedkyně Úřadu má nárok na plat, náhradu výdajů, naturální plnění a odchodné jako prezident Nejvyššího kontrolního úřadu podle zákona č. 236/1995 Sb., o platu a dalších náležitostech spojených s výkonem funkce představitelů státní moci a některých státních orgánů a soudců, ve znění pozdějších předpisů. Podobné nároky jako předseda mají i inspektoři ovšem s výjimkou odchodného a v postavení nikoliv prezidenta ale členů Nejvyššího kontrolního úřadu podle stejného zvláštního zákona.

Předseda řídí Úřad pro ochranu osobních údajů, je jmenován a odvoláván prezidentem republiky na návrh Senátu Parlamentu České republiky. Předseda je jmenován na dobu 5 let a to maximálně na 2 po sobě jdoucí období. Z funkce je předseda Úřadu odvolán, přestal-li splňovat některou z podmínek pro jeho jmenování nebo pokud nevykonává svou funkci po dobu 6 měsíců.

Předpokladem pro jmenování do funkce předsedy Úřadu je státní občanství České republiky, způsobilost k právním úkonům, bezúhonnost⁶¹, splnění podmínek stanovených zákonem č. 451/1991 Sb., ukončené vysokoškolské vzdělání a další znalosti, zkušenosti a morální vlastnosti, které jsou předpokladem pro řádné zastávání své funkce.

Předseda Úřadu se považuje za služební orgán a je oprávněn dávat státnímu zaměstnanci příkazy k výkonu státní služby podle zákona o státní službě.

Vzhledem k faktu nezávislosti Úřadu musí být tato nezávislost respektována i v rámci výkonu klíčových pozic jako je funkce předsedy Úřadu a to prostřednictvím stanovení neslučitelnosti s funkcemi, které by byly s nezávislostí v přímé či nepřímé kontradikci. Předseda nesmí zastávat funkci poslance nebo senátora, soudce, státního zástupce, jakákoliv funkce ve veřejné správě, funkce člena orgánů územní samosprávy a členství v politických stranách a hnutích. Předseda Úřadu nesmí zastávat jinou placenou funkci, být v dalším pracovním poměru ani vykonávat výdělečnou činnost s výjimkou správy vlastního majetku a činnosti vědecké, pedagogické, literární, publicistické a umělecké, pokud tato činnost nenarušuje důstojnost nebo neohrožuje důvěru v nezávislost a nestrannost Úřadu.⁶²

⁶¹ Za bezúhonnou je v tomto případě považována fyzická osoba, která nebyla pravomocně odsouzena pro úmyslný trestný čin nebo i trestný čin spáchaný z nedbalosti v souvislosti se zpracováním osobních údajů.

⁶² § 32 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Stejně jako v případě předsedy inspektoři do funkce jmenuje a odvolává prezident republiky na návrh Senátu Parlamentu České republiky, ačkoliv inspektoři jsou jmenováni na období 10 let a mohou být jmenováni opakovaně. Inspektorů je 7 a náplní jejich činnosti je řízení kontroly a další úkony, které jsou v působnosti Úřadu.

Do funkce inspektora může být jmenován občan České republiky, který je způsobilý k právním úkonům, bezúhonný, splňuje podmínky stanovené zákonem č. 451/1991 Sb., a má ukončené odborné vysokoškolské vzdělání.

Výkon funkce inspektora je neslučitelný s dalšími funkcemi srovnatelně jako v případě funkce předsedy a zároveň inspektor taktéž nesmí zastávat jinou placenou funkci, být v pracovním poměru ani vykonávat výdělečnou činnost s výjimkou správy vlastního majetku a činnosti vědecké, pedagogické, literární, publicistické a umělecké, pokud tato činnost nenarušuje důstojnost nebo neohrožuje důvěru v nezávislost a nestrannost Úřadu. Přestal-li inspektor splňovat některou z podmínek pro jeho jmenování, je z funkce odvolán.⁶³

⁶³ § 33 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

5. General Data Protection Regulation (GDPR)

V Bruselu 27. dubna 2016 byla schválena nová legislativní úprava Evropské unie v oblasti zpracování a ochrany osobních údajů, která si obecně klade za cíl výrazné zvýšení ochrany osobních údajů a zprůsňení podmínek při zpracování. Jedná se o Obecné nařízení o ochraně osobních údajů z anglického překladu General Data Protection Regulation (dále také “GDPR” nebo “Nařízení”), jehož celý název je 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).

Platnost započala dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie a to k datu 24. května 2016, zatímco účinnosti Obecné nařízení o ochraně osobních údajů nabylo až 25. května 2018 a stalo se tak k tomuto dni závazným a přímo použitelným na území všech členských států Evropské unie.⁶⁴

Dlouhý časový odstup mezi platností a účinností tzv. legisvakantní lhůta byl stanoven s ohledem na přípravu na nové povinnosti a s tím spjaté náročné úkoly, které GDPR přináší svým uživatelům. Byla tak poskytnuta všem osobám, které pracují s osobními údaji, více než dvouletá lhůta na uvedení své správy zpracování osobních údajů do souladu s novou právní úpravou v podobě GDPR.

Struktura GDPR je tvořena dvěma částmi, preambulí a zvláštní částí. GDPR ve svém znění zakotvuje úsek věnující se nepřímému výkladu jednotlivých ustanovení zvláštní části GDPR a to konkrétně ve své preambuli. Preambule čítající 173 článků označovaných též jako recitály lze být brána a používána obdobně jako důvodová zpráva k zákonům. Zvláštní část je tvořena 99 články a společně s preambulí se tvoří velmi rozsáhlou a komplexní právní úpravu.

Z hlediska rozsáhlosti a členění GDPR je důležité znát nejen samotnou zvláštní část, ale věnovat pozornost oběma částem GDPR současně. Aby bylo umožněno správné porozumění jednotlivých ustanovení ale i GDPR jako celku je třeba si příslušné recitály vzhledem k jejich vysvětlující povaze spojovat s odpovídajícími články zvláštní části.⁶⁵

Nutnost vytvoření a vydání nové právní úpravy spočívala především v reakci na rozmach nových technologií a zastaralost směrnice oblast ochrany osobních údajů upravující, celým označením směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995

⁶⁴ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 551.

⁶⁵ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 30.

o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen “směrnice 95/46/ES”), která přestala vyhovovat současné době vzhledem k rozsáhlosti prostředků využívaných k zpracování osobních údajů např. profilování a monitorování fyzických osob.

GDPR tak dnem své účinnosti zrušilo a nahrazuje směrnicí 95/46/ES.⁶⁶

Z hlediska prudce se rozvíjejícího informačního prostředí nebylo možné řešit dostatečné zabezpečení osobních údajů dalšími novelizacemi původní směrnice, ale byla upřednostněna a použita forma unijního nařízení.

Vydání nové právní úpravy formou nařízení má jednoznačně unifikační efekt a nařízení Evropské unie je tak přímo použitelné a bezpodmínečně závazné pro všechny státy, které jsou členy EU tzv. členské státy a dále pro Island, Norsko a Lichtenštejnsko. Dá se tedy mluvit o charakteristickém rysu univerzální použitelnosti v členských státech a cíleném sjednocujícím účinku GDPR.⁶⁷

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 komunikací) (dále také “směrnice e-Privacy” nebo “směrnice 2002/58/ES”) zůstává zachována v platnosti, přičemž probíhá příprava na nové právní úpravě v podobě e-Privacy nařízení, na které se následně též bude vztahovat ustanovení čl. 95 GDPR a které bude vůči GDPR v postavení zvláštní úpravy.⁶⁸

Článek 95 stanoví, že v souvislosti se směrnicí e-Privacy GDPR neukládá žádné další povinnosti fyzickým nebo právnickým osobám, pokud se jedná o zpracování ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v Unii a to konkrétně ve vztahu k záležitostem, u nichž se na ně vztahují konkrétní povinnosti s tímž cílem stanovené ve směrnici e-Privacy.⁶⁹ Úprava GDPR se tedy použije jen v situacích, které směrnice e-Privacy neupravuje za předpokladu splnění podmínky souladu cíle stanovených povinností v GDPR s cílem povinností upravených směrnicí e-Privacy.

⁶⁶ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 547.

⁶⁷ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 29.

⁶⁸ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 548.

⁶⁹ čl. 95 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Mezinárodní dohody, které byly uzavřeny přede dnem 24. května 2016 a jsou v souladu s právem Evropské unie použitelným před tímto dnem, zahrnující předávání osobních údajů do třetích zemí či mezinárodním organizacím, zůstávají v platnosti, dokud nebudou změněny, nahrazeny či zrušeny.⁷⁰

GDPR se nevztahuje na zpracování osobních údajů fyzickou osobou uskutečňované pro výhradně vlastní osobní potřeby, které nemají souvislost s profesní nebo obchodní činností, a nebo pod téže podmínkou činnosti prováděny čistě jen v domácnosti. Jedná se o situace v rámci osobní korespondence, využívání sociálních sítí pokud daná osoba není zároveň správcem těchto sítí, vedení osobních adresářů či vedení jiných záznamů obdobného charakteru. Podmínkou je nevyužívání osobních údajů z těchto činností k návazné podnikatelské činnosti.⁷¹

GDPR nepřísluší řešit některé otázky v souvislosti s činnostmi, které stojí mimo působnost práva EU, jako jsou činnosti ve vztahu k národní bezpečnosti aj. situace v oblasti ochrany základních lidských práv a svobod či volného pohybu osobních údajů. Při zpracování osobních údajů členskými státy jako součást výkonu činností v oblasti společné zahraniční a bezpečnostní politiky EU, se na tyto procesy GDPR též nevztahuje.

GDPR dále neupravuje ochranu osobních údajů zesnulých osob a ponechává vzhledem k této problematice prostor členským státům, aby si samy vymezily podmínky týkající se zpracování osobních údajů zesnulých osob, které jsou v právním řádu České republiky řešeny zejména v občanském zákoníku, autorskými aj. právními předpisy. Právní úprava jiných právních odvětví se ochrany osobních údajů dotýká i v dalších zvláštních předpisech na unijní i vnitrostátní úrovni upravující např. vyšetřování, odhalování, stíhání nebo výkon trestných činů a jejich předcházení včetně ochrany před hrozbami pro veřejnou bezpečnost, kdy jsou tyto situace z působnosti GDPR vyňaty.

Přestože se GDPR vztahuje na činnost soudů a dalších justičních orgánů, nesmí být při výkonu jejich soudních pravomocí narušena jejich nezávislost a to včetně rozhodovacích činností, tudíž by měl být dozor nad takovými soudními funkcemi, kdy zároveň dochází ke zpracování osobních údajů, svěřen a ponechán zvláštním subjektů v rámci justičního systému daného členského státu.⁷²

⁷⁰ čl. 96 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

⁷¹ body preambule 18 až 20 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

⁷² NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 68.

5.1 Cíle, nové přístupy a povinnosti

5.1.1 Cíle

Z hlediska cílů, které GDPR sleduje se jedná především o sjednocení právní úpravy a v ní stanovených pravidel a způsobů ochrany osobních údajů ve všech zemích Evropské unie a dalších mimo členských zemích, na které GDPR dopadá. S tím souvisí cíl posílení důvěryhodnosti Evropské unie a jejích členských zemí a těch zemí, na které GDPR působí, pro další země, které mají nebo potenciálně mohou mít zájem na rozvoji obchodu s Evropskou unií a toho se dotýkajícím předáváním osobních údajů mezi zeměmi. Neopomenutelným by mělo být i sjednocení výkladu GDPR dozorovými úřady jednotlivých zemí Evropské unie.⁷³

Sjednocená právní regulace by však postrádala význam bez přizpůsobení právní regulace ochrany osobních údajů poměrům dnešní doby respektive rozvoji informačních technologií a tím většímu rozsahu možných zneužití, kdy se jedná o jeden z hlavních cílů viz zmínění o nutnosti revize právního rámce výše.

Dalším přímo výše nezmiňným cílem ačkoliv snadno vyvoditelným je posílení práv v oblasti ochrany osobních údajů všech osob, jejichž údaje jsou zpracovávány resp. subjektů údajů. GDPR má ve svém právním rámci ochrany osobních údajů hájit práva občanů na celém území EU proti neoprávněnému zacházení s jejich osobními údaji a daty.

Posíleno je zejména právo na získávání informací a právo být informován o tom, jaké údaje dané osoby jsou zpracovávány a proč, neboli subjektu údajů by měl být znám účel zpracování, a dále se jedná o posílení práva domáhat se dodržování pravidel a s tím související právo na nápravu stavu.

GDPR zahrnuje všechny dosavadní zásady ochrany a zpracování údajů, na kterých je postavený unijní systém ochrany osobních údajů a dokládá skutečnost, že ochrana by měla cestovat a cestuje přes hranice současně s osobními údaji.

⁷³ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 30.

5.1.2 Nová práva, povinnosti a přístupy

GDPR i přes vlastní rozsáhlost a významnost pro právní řád navazuje na dosavadní právní úpravu a práva a povinnosti mění v různé míře, v některých případech zavádí i zcela nové věci.

Ve snaze lepšího zajištění vymahatelnosti práv občanů a upravení povinností správců či zpracovatelů, jenž jsou odpovědní za zpracování, obsahuje GDPR propracovanější a náročnější pravidla pro zvláštní kategorie údajů a zpracování a současně vymáhá od správců a zpracovatelů výrazně aktivnější přístup. Při nastavování povinností správců je brán zřetel zejména na rizikovost, která je dovozována z rozsahu zpracování a při něm používaných technologií.

GDPR v tomto ohledu zavádí dva nové přístupy, kterými jsou přístup založený na riziku a princip odpovědnosti správce.

Z principu odpovědnosti správce vyplývá odpovědnost správce za dodržení souladu zpracování obecně s GDPR a souladu se zásady zpracování osobních údajů, které GDPR uvádí ve svém čl. 5 odst. 1. Zároveň má správce v rámci tohoto principu povinnost doložit tento soulad zpracování s GDPR a již zmíněnými zásadami prostřednictvím tzv. kodexů, osvědčení, certifikace nebo případně záznamů o činnostech zpracování a to po celou dobu průběhu zpracování.⁷⁴

Přístup založený na riziku se dá chápat z hlediska širšího a užšího pojetí, přičemž v širším slova smyslu má správce povinnost od počátku koncipování zpracování osobních údajů brát v úvahu povahu, kontext, rozsah a účel zpracování a musí dbát na možná rizika narušující práva a svobody fyzických osob a musí tomu přizpůsobit i způsob zabezpečení osobních údajů, jak je již zmíněno výše. V tomto širším pojetí funguje přístup založený na riziku již dle zákonné úpravy zákona č. 101/2000 Sb., o ochraně osobních údajů.

V užším slova si můžeme vykládat přístup založený na riziku jako upotřebení některých povinností pouze v takovém případě, pokud by bylo důvodné dané povinnosti aplikovat. Odůvodnitelnou situací pro aplikaci je stav, kdy by zpracování osobních údajů či porušení zabezpečení znamenalo riziko nebo vysoké riziko pro práva a svobody fyzické osoby. V tomto pojetí se princip založený na riziku uplatňuje především u některých nových povinností.

⁷⁴ GDPR upravuje tuto povinnost v čl. 24, kodexy v čl. 40, osvědčení v čl. 42 a záznamy o činnostech zpracování v čl. 30. Certifikace GDPR ve svém právním textu neupravuje.

Novými povinnostmi v tomto smyslu se rozumí zejména povinnost ohlašovací, která spočívá v ohlašování porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů jakožto dozorovému úřadu a také dotčeným osobám, o jejichž informace se jedná resp. subjektům údajů, a to nejpozději do 72 hodin od doby, kdy se správce osobních údajů o narušení bezpečnosti dozvěděl.⁷⁵

Dále jsou zavedeny relativně nové významné povinnosti jako povinnost vypracování posouzení vlivu zpracování na ochranu osobních údajů. Tato povinnost je upravena v čl. 35 GDPR a ve vztahu k ní odpadá a je nahrazena zákonem č. 101/2000 Sb., o ochraně osobních údajů, stanovená povinnost zpracování dokumentace dle § 13 odst. 2.

Posouzení musí zahrnovat hned několik aspektů a to především systematický popis zamýšlených úkonů zpracování a jeho jednotlivých kroků od okamžiku získání osobních údajů, přes uchovávání, využití nebo přenos, až po jejich likvidace např. formou skartace či výmazu z informačního systému a to i z hlediska použitých technických prostředků. V této části nesmí chybět ani srozumitelný a pravdivý popis účelů zpracování, přičemž není nutné popisovat účely konkrétních jednotlivých kroků za předpokladu, že dané operace nebudou představovat zvýšení rizika pro subjekty údajů aniž by byl zřejmý důvod nutnosti takové operace.⁷⁶

Posouzení by mělo obsahovat i analýzu nezbytnosti a přiměřenosti operací zpracování ve vztahu k účelům zpracování, což znamená povinnost správce posoudit, zda jsou výše zmíněné postupy při zpracování přiměřené a nezbytné ve smyslu, zda nelze daných účelů dosáhnout jinými způsoby, které budou disponovat stejnou měrou efektivitivy a zároveň budou v menší míře zasahovat do soukromí subjektu údajů.⁷⁷

Dalším dílčím důležitou oblastí dokumentu je posouzení rizik pro práva a svobody subjektů údajů, tedy jaké jsou možné dopady na práva a svobody subjektů údajů za situace, kdy by osobní údaje unikly a dostaly se k rukám nežádoucích osob. Míra rizikovosti se zvyšuje zejména pokud se jedná o citlivé osobní údaje, jejichž únik by mohl subjektu údajů způsobit vážnější následky.

Správce musí nakonec vylíčit možná opatření k řešení daných rizik, včetně záruk, bezpečnostních opatření a mechanismů, které by měly nejen zajistit ochranu osobních údajů

⁷⁵ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 80.

⁷⁶ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 103.

⁷⁷ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 349.

a dokládat soulad s GDPR, ale zároveň brát ohled na práva a oprávněné zájmy subjektů údajů a dalších dotčených osob.⁷⁸

Nově jsou zavedeny povinné konzultace s Úřadem na ochranu osobních údajů a to výhradně před samotným zpracováním osobních údajů, které nahrazují a ruší povinnost registrace správců a zpracovatelů u Úřadu pro ochranu osobních údajů.

Mezi vzniklé povinnosti patří také řádné vedení záznamů o zpracování osobních údajů a povinnost umožnit přenositelnost osobních údajů od jednoho správce k jinému.⁷⁹

GDPR neopomenutelně zavádí nezávislou kontrolní a poradní funkci resp. povinnost jmenování Pověřence pro ochranu osobních údajů, jakožto zcela nový institut v právním řádu České republiky, který je jinak zvaný Data Protection Officer (dále také “DPO”).

GDPR mimo jiné dále výslovně upravuje nezávislost, obecné podmínky pro členy, úkoly a pravomoci dozorových úřadů v členských státech Unie, EHP i Švýcarska, tj. u nás Úřadu pro ochranu osobních údajů. GDPR neopomíjí ani úpravu vzájemné spolupráce jednotlivých dozorových úřadů, kterou může být např. jednotný přístup k sankcím.⁸⁰

5.2 Zásady zpracování osobních údajů podle GDPR

GDPR přináší jakožto nová právní úprava ve vztahu k dosavadní vnitrostátní právní úpravě České republiky z hlediska kontinuity práva některé zcela nové aspekty již výše uvedené, ale zároveň upravuje již dříve zakotvené skutečnosti, které se týkají samotných principů, na kterých zpracování a ochrana osobních údajů stojí již dle zákona č. 101/2000 Sb., o ochraně osobních údajů a v tomto ohledu je GDPR ve vztahu k zásadám ve vnitrostátním i evropském právním rámci spíše deklaratorní, doplňující a zpřesňující povahy.

GDPR upravuje základní zásady zpracování osobních údajů v článku 5 a veškerý výklad obsahu všech ostatních částí GDPR musí být s těmito základními principy v souladu, neboť z hlediska jejich významnosti a povahy, kdy jsou zásadními východisky a mantinely pro správce při výkonu své činnosti, je dodržování těchto zásad nejdůležitější povinností.

⁷⁸ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 349.

⁷⁹ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 33.

⁸⁰ GDPR (Obecné nařízení). *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 13.1.2019]. Dostupné z: <https://www.uouu.cz/gdpr-obecne-nbsp-narizeni/ds-3938/archiv=0>

Do základních principů dle právní úpravy GDPR patří zákonnost, korektnost a transparentnost, kdy správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně. Patří sem i zásady dobře z dnešní legislativy známé jako minimalizace, přesnost a omezení uložení osobních údajů, které znamenají, že osobní údaje musí být přiměřené a relevantní ve vztahu k účelu zpracování, musí být přesné a uloženy ve formě umožňující identifikaci subjekt údajů jen po nezbytnou dobu pro dané účely zpracování. Ve výčtu nesmí chybět ani neopomenutelná zásada, kterou je integrita a důvěrnost, jež zahrnuje nutnost technického a organizačního zabezpečení osobních údajů a zásada odpovědnosti zavazující správce.

Členské státy mají možnost v rámci čl. 23 GDPR omezit práva a povinnosti vyplývající z těchto základních principů a to v rámci potřeby zajištění důležitých veřejných cílů. Přijatá omezení musí být nezbytná a přiměřená a nesmí narušovat podstatu základních práv a svobod a odporovat demokratické povaze společnosti. Omezení mohou být provedena za předpokladu sledování některého z cílů taxativně vymezených v uvedeném článku GDPR např. zajištění národní bezpečnosti, obrany či ochrany nezávislosti soudnictví.⁸¹

5.2.1 Zásada zákonnosti

První a především výchozí zásada je zásada zákonnosti, která stanoví, že zpracování osobních údajů je možné realizovat pouze na základě určitého definovaného právního titulu a je vyloučeno, aby bylo zpracování v rozporu se zákonem, tudíž aby bylo vykonáváno na základě nelegálního či nelegitimního účelu. Průběh zpracování musí být v souladu se všemi zákonnými i podzákonnými právními předpisy dle právního řádu. Je nedostačující, aby bylo respektované pouze GDPR, ale zároveň je nezbytné dodržovat soulad s právním řádem obecně včetně dodržování smluvní povinnosti, povinnosti mlčenlivosti a dbát na základní lidská práva v rámci problematiky zejména na právo na soukromí.

Z logiky věci vyplývá, že pokud by nebylo předpokladem a nutností dodržovat zákonem stanovené meze, nová legislativní úprava by postrádala smysl stejně jako každá stanovená pravidla, pokud by se dle nich nebylo nutné řídit.

V dosavadní právní úpravě dle zákona č. 101/2000 Sb., o ochraně osobních údajů nenalezneme zásadu zákonnosti přímo vyjádřenou, ačkoliv její podstatu namísto explicitního stanovení obstarávají v § 5 zakotvené povinnosti správce. Prioritně se jedná o povinnost

⁸¹ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 122.

zpracovávat osobní údaje vždy na základě alespoň jednoho ze stanovených zákonných titulů v § 5 odst. 2.

Zákonnost zpracování je dále upravena v GDPR v článku 6, kde jsou vymezeny právní tituly, na kterých musí zpracování osobních údajů stát.

Právní tituly jakožto právní podmínky pro zpracování osobních údajů jsou velice blízké účelům zpracování a v některých situacích zejména v oblasti zvláštních kategorií údajů se mohou překrývat. V průběhu zpracování je stanovení právního titulu vedle stanovení účelu zpracování nejdůležitějším krokem, který by měl předcházet všem ostatním úkonům správce a musí existovat před zamýšleným zpracováním. Za předpokladu že by zpracování osobních údajů začalo probíhat bez jediného platného právního titulu, bylo by zpracování od počátku nelegální.⁸²

Nejnámějším právním titulem je souhlas subjektu údajů, který byl dle dřívější vnitrostátní úpravy a směrnice 96/45/ES chápán jako hlavní a nejvíce využívaný právní titul ve srovnání s ostatními právními tituly, na které bylo nahlíženo jako na druhořadá řešení, pokud by nebylo možné souhlas od subjektu údajů získat.⁸³

Nařízení staví veškeré právní důvody na stejnou úroveň, ačkoliv zpřísňuje podmínky pro užívání právního titulu souhlasu subjektu údajů, aby správce byl nucen uvažovat nejprve nad možností použití jiného zákonného důvodu pro zpracování a souhlas využít pakliže nebude možné aplikovat na zpracování jiný titul.

Správce, který by zvolil zpracování osobních údajů za použití právního titulu souhlasu, bude povinen prokázat, že mu subjekt údajů tento souhlas poskytnul, přičemž se musí jednat o svobodný, informovaný, konkrétní a jednoznačný projev vůle, kterým dává subjekt údajů prohlášením či zjevným potvrzením souhlas se zpracováním svých osobních údajů. Z definice souhlasu je zřejmé, že jeho dokládání předvídá písemnou formu souhlasu, neboť ústní forma by se stala obtížně prokazatelnou, pokud by se nejednalo o záznam ve formě např. audionahrávky se všemi potřebnými náležitostmi jako jsou údaje o čem byl subjekt údajů informován před udělením souhlasu a kdo a kdy souhlas udělil resp. musí být uveden identifikátor osoby a časový indikátor.⁸⁴

Pokud bychom měli dále srovnávat právní tituly stanovené v GDPR s úpravou dle zákona o ochraně osobních údajů, GDPR některé právní tituly ve svém výčtu postrádá.

⁸² NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 125.

⁸³ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 127.

⁸⁴ Definice souhlasu je uvedena v čl. 4 odst. 11 Nařízení a podmínky vyjádření souhlasu v čl. 7 Nařízení.

V GDPR tedy nenalezneme možnost zpracovávat ty osobní údaje, které byly již oprávněně zveřejněné a to v souladu se zvláštním zákonem č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích, ve znění pozdějších předpisů.⁸⁵ Dalším opomenutým titulem je zpracování osobních údajů, pokud správce poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení.⁸⁶

Není však zcela vyloučeno, aby taková zpracování nebylo možné dále provádět, jen je bude nutno podřadit pod jiný právní titul. Nalezení vhodného právního titulu, který by tyto nahradil, může zajistit např. skutečnost rozšíření právního titulu oprávněného zájmu v GDPR a zároveň GDPR přináší nový právní titul dle čl. 6 odst. 1 písm. e, který zajišťuje možnost správce zpracovávat osobní údaje, pokud je to nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci.

5.2.2 Zásada korektnosti a transparentnosti

Zásada korektnosti spočívá v poctivém resp. férovém přístupu a postupu při zpracování osobních údajů, kdy by se měl správce vyvarovat bezdůvodnému přehlížení zájmů a rozumných očekávání dotčených osob a měl by naopak dbát na jejich zohlednění. Naprosto nepřijatelnou situací by bylo záměrné využití mylných představ a domněnek subjektu údajů aj. dotčených osob a zneužití vzniklého omylu např. k zastření pravého účelu zpracování osobních údajů a sledování jiného v horším případě nelegálního účelu, než který byl stanoven.

Zásada transparentnosti představuje princip otevřenosti ohledně toho, jakým způsobem je s osobními údaji nakládáno. V zásadě se současně skrz tento princip projevuje právo na informační sebeurčení resp. subjekty údajů sami rozhodují o tom, jaké údaje o sobě poskytnou a měly by být zároveň informovány o tom, že jim přísluší právo na informace vztahující se k skutečnosti, jaké údaje o nich byly a jsou zpracovávány a o budoucích způsobech zpracování.⁸⁷

Zásada transparentnosti se především uskutečňuje informačními povinnostmi správce, který by měl subjekty údajů informovat o zpracování osobních údajů v rozsahu dle čl. 13 GDPR a způsobem stanoveným v čl. 12. Informace musí být jednoduše dostupné a ve srozumitelné, jasné a jednoduché řeči s ohledem na osoby nebo skupiny osob, ke kterým

⁸⁵ § 5 odst. 2 písm. d) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁸⁶ § 5 odst. 2 písm. f) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

⁸⁷ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 40.

informace směřují, neboť forma informací se musí přizpůsobit subjektům údajů, aby nebyly uvedeny v omyl.

Subjekt údajů má zároveň právo na přístup zakotvené v čl. 15 GDPR, jeho odepření by znamenalo porušení této zásady. V rámci svých práv by subjekty údajů měly být seznámeny s možnými riziky, předpisy a právy, která jim náleží a v jakém rozsahu a za jakých podmínek mohou svá práva uplatnit. S tím souvisí i právo na to být informován, pokud by došlo k závažnému porušení zabezpečení osobních údajů dle čl. 34 GDPR.⁸⁸

V zákoně o ochraně osobních údajů je zásada korektnosti a transparentnosti zakotvena v § 5 odst. 1 písm. g) a v § 11 téhož zákona, který upravuje informační povinnost správce k subjektům údajů, a dále v § 16, kde je zakotvena informační povinnost správce k Úřadu pro ochranu osobních údajů.

5.2.3 Zásada účelového omezení

Další neméně důležitou zásadou je zásada účelového omezení, která určuje správci osobních údajů, který tyto údaje zpracovává, povinnost postupovat při svém výkonu pouze v souladu s tím účelem, který sám určil jako důvod zpracování. Důležitost této zásady spočívá i v jejím vlivu na zásady další, které se od účelového omezení odvíjejí, jedná se o zásady např. minimalizace údajů nebo omezení uložení.

Až na několik výjimek nelze později zpracovávat osobní údaje za jiným účelem, než který byl správcem určen, přičemž správce musí účel stanovit nejpozději při shromažďování osobních údajů. Výjimky, při kterých dochází ke zpracování osobních údajů za jiným účelem, než který byl stanoven při jejich shromažďování jsou označovány jako tzv. další zpracování. Jedná se pouze o čtyři případy uvedené v čl. 5 odst. 1 písm. b) a čl. 6 odst. 4 GDPR.⁸⁹

Stanovení účelu musí splňovat náležitosti, kterými je určitost, výslovné vyjádření a legitimita. Z účelu musí být zcela zřejmé, jaká zpracování na základě něj budou prováděna a jaká naopak ne a zároveň musí jeho určitost poskytovat možnost posouzení, zda je či není účel v souladu s GDPR. Účel musí zároveň být legitimní a naplňovat zásadu zákonnosti, s kterou je úzce spjat, jak je již popsáno výše. Stanovení určitého a legitimního účelu správcem a vědomí správce o tomto účelu však samo o sobě nestačí a správce musí účel sdělit subjektům údajů a zároveň by měl účel dokumentovat nejlépe v záznamech o činnostech

⁸⁸ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 108 - 109.

⁸⁹ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 41.

zpracování. Správce by měl své sdělení účelu formulovat tak, aby subjekty údajů jakožto i všechny zúčastněné osoby např. zpracovatelé měly jasnou a ucelenou představu o účelu, která by se neměla rozcházet s představou správce ani s porozuměním ostatních zúčastněných osoba na zpracování mezi sebou.⁹⁰

Z hlediska právní kontinuity zůstává zákonná úprava zásady účelového omezení neměnná.

5.2.4 Zásada minimalizace údajů

Zásada minimalizace údajů omezuje činnost správce při zpracování způsobem, aby správce mohl shromažďovat a zpracovávat pouze takové osobní údaje, které jsou podstatné pro naplnění účelu a pouze v nezbytném rozsahu. Z negativního hlediska správce ani zpracovatel nejsou oprávněni a nesmí zpracovávat osobní údaje irelevantní vzhledem k účelu, který byl předem stanoven, a každé zamýšlené nakládání s osobními údaji by mělo být předem posouzeno z hlediska nezbytnosti pro splnění účelu.⁹¹

Situace, kdy by správce zpracovával osobní údaje bez zřejmé shody s účelem tudíž zcela nevhodné popř. by rozsah shromážděných informací přisvědčoval skutečnosti, že je nepřiměřený účelu, by znamenala porušení zásady minimalizace údajů a zároveň bychom mohli hovořit o porušení zásady účelového omezení, od které se minimalizace údajů odvíjí, za předpokladu, že by z jednotlivých kroků zpracování bylo znatelné, že mohou být využívány nejen nadbytečně ale zároveň pro účel jiný, než který byl stanoven.

Ve vztahu k právní úpravě zákona o ochraně osobních údajů je zásada minimalizace údajů vyjádřena v § 5 odst. 1 písm. d) a tudíž se nejedná o žádnou novou GDPR zavedenou skutečnost.

⁹⁰ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 110 - 111.

⁹¹ Čl. 5 odst. 1 písm. c) NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

5.2.5 Zásada omezení uložení

Zásada omezení uložení osobních údajů upravuje časový interval, po který je možné uchovávat osobní údaje. Stejně jako zásada minimalizace údajů se i tato zásada váže na stanovený účel zpracování osobních údajů, avšak tato zásada omezení uložení se netýká rozsahu z hlediska četnosti zpracování osobních údajů, neboť stanoví povinnost zpracovávat osobní údaje pouze po dobu, která je nezbytná k naplnění účelu zpracování.⁹²

V praxi správce musí vymazat nebo anonymizovat veškeré osobní údaje, které pozbyly potřeby pro naplnění účelu a jejich zpracování ve vztahu k účelu dále není nezbytné. Doba stanovená pro zpracování osobních údajů nesmí být zcela neurčitá, ačkoliv může být stanovena relativně ve vztahu k rozhodné události např. ukončení poskytování určitých služeb. Nutnost vymazání osobních údajů se může objevit ještě dříve, před uplynutím doby potřebné pro naplnění účelu a to v případě, pokud bude naplněna některá z podmínek pro uplatnění práva na výmaz upraveného v čl. 17 GDPR např. pokud zpracování bude protiprávní.

Tato zásada je již zakotvena v zákoně o ochraně osobních údajů v § 5 odst. 1 písm. e) a v zásadě se nijak nemění. Nicméně GDPR formuluje ve vlastním právním textu zásadu omezení uložení tak, že správce nesmí uchovávat osobní údaje po dobu delší, než je pro účely zpracování nezbytné, ve formě umožňující identifikaci. Vymezením formy, ve které po uplynutí doby nesmí být údaje dále uchovávány resp. formy umožňující identifikaci, tak v podstatě GDPR deklaruje přípustnost anonymizace osobních údajů jako dalšího zpracování.

Anonymizací se rozumím proces, kterým má za cíl, aby z uchovávaných údajů nebylo dále možné identifikovat subjekt údajů tj. spojovat tyto údaje s žádnou individuální fyzickou osobou, které se tyto údaje týkají. Anonymizované údaje nejsou považovány za osobní údaje a ochrana osobních údajů se na ně nevztahuje, z čehož vyplývá, že anonymizace v konečném důsledku disponuje srovnatelným efektem s efektem výmazu.⁹³

Oba právní předpisy současně uvádějí tutéž výjimku z této zásady, kdy se jedná o zpracování za účelem vědeckého či historického výzkumu či pro statistické účely, a zároveň stanoví opatření a podmínky, které jsou v GDPR uvedeny v čl. 89 odst. 1.

⁹² Čl. 5 odst. 1 písm. e) NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

⁹³ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 117.

5.2.6 Zásada přesnosti

Zásada přesnosti požaduje, aby zpracovávané osobní údaje byly přesné, aktuální a odpovídaly skutečnosti. Přesnost zpracovaných osobních údajů je třeba hodnotit ve vztahu k účelu, jelikož k rozličným účelům postačí jiná míra přesnosti, aby bylo účelu dosaženo. Chybné údaje z důvodu gramatických, výpočetních chyb či údaje které v souvislosti s danou osobou nevypovídají o pravdivém stavu, ačkoliv jsou formálně správné jsou považovány jako nepřesné a správce musí přijmout veškerá možná opatření, aby tyto údaje opravil, v případě potřeby aktualizoval nebo zlikvidoval. Správce však neodpovídá za nepřesné údaje, které mu byly v nesprávné podobě poskytnuty samotným subjektem údajů. Subjekt údajů má právo podle čl. 16 GDPR na opravu, které se od zásady přesnosti odvíjí a je jedním z jejích projevů v praxi. To znamená, že sám subjekt údajů může správci podat žádost, aby jeho údaje opravil a aktualizoval.⁹⁴

Právní řád výslovně nestanoví jakým způsobem má být dosažení přesnosti provedeno, ani jak často má být správcem přesnost údajů kontrolována a zajišťována. Správce by měl přesnost informací ověřovat s ohledem na zamýšlené operace s osobními údaji a rizika vztahujícím se k těmto jednotlivým úkonům resp. v souladu s čl. 24 odst. 1 GDPR. Reálná újma např. nehrozí při pouhém ukládání osobních údajů a z toho důvodu není nezbytné přesnost a aktuálnost kontrolovat nepřetržitě, ačkoliv pokud se při komunikaci se subjektem údajů správce dozví o zastaralosti či jiné nepřesnosti osobních údajů nebo subjekt údajů sám požádá o opravu a není právní důvod, který by předpokládal nutnost uchování původní podoby osobních údajů, pak je nutné data aktualizovat či opravit.

V případě pokud by správce prováděl zpracování osobních údajů, při kterém by hrozil vznik újmy subjektu údajů z důvodu nepřesnosti údajů, měl by jejich přesnost ověřovat pravidelně a před samotným provedením operace zpracování osobních údajů. Úřad pro ochranu osobních údajů, ačkoliv je ponecháno na správci jakým způsobem se s touto povinností vypořádá, předpokládá, že každý správce či zpracovatel by měl přijmout systém opatření, kterým bude předcházet zpracování nepřesných a nesprávných osobních údajů, a to v závislosti na rozsahu a okolnostech předmětného zpracování. Díky danému systému opatření by správce měl být schopen včas zjistit nedostatky v přesnosti osobních údajů.⁹⁵

⁹⁴ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 114.

⁹⁵ K problematice aktualizace zpracovávaných osobních údajů. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 27.02.2019]. Dostupné z: https://www.uouu.cz/vismo/dokumenty2.asp?id_org=200144&id=1595&n=k-problematice-aktualizace-zpracovanych-osobnich-udaju

Zásada přesnosti je v zákoně o ochraně osobních údajů již vyjádřena v § 5 odst. 1 písm c) a zůstává i s účinností GDPR neměnná.

5.2.7 Zásada integrity a důvěrnosti

Zásada integrity a důvěrnosti vyjadřuje nutnost zpracování osobních údajů způsobem, který bude bezpečný a bude chránit osobní údaje před jejich zneužitím tj. neoprávněným či nezákonným zpracováním a zároveň před neplánovanou ztrátou, zničením nebo poškozením, což zahrnuje povinnost správce osobní údaje technicky a organizačně zabezpečit vhodnými opatřeními. Integrita znamená tedy nedotknutelnost osobních údajů a zamezení jejich neoprávněné změně či zničení, zatímco důvěrnost značí ochranu před nežádoucím zjištěním osobních údajů tudíž ochranu před získáním daných dat neoprávněnými osobami, jež by mohly osobní údaje zneužít.⁹⁶

GDPR vnímá zabezpečení osobních údajů jako klíčovou povinnost a proto ji řadí mezi základní zásady, přičemž konkrétním požadavkům na zabezpečení osobních údajů se GDPR věnuje v čl. 32.

5.2.8 Zásada odpovědnosti

Zásada odpovědnosti již byla zmíněna mezi novými přístupy a povinnostmi, jako princip odpovědnosti správce. Odpovědnost správce za dodržení všech povinností vyplývajících z popsaných zásad, je již známá zákonu o ochraně osobních údajů i směrnici 95/46/ES, nicméně důležitým aspektem je především povinnost správce být schopen doložit tento soulad, o níž byla tato zásada v GDPR obohacena.⁹⁷

Správce vzhledem k rozšíření této zásady novou právní úpravou musí přistupovat ke svým povinnostem iniciativně a sám dbát na důkladnou dokumentaci a zavádění vhodných systémů ochrany, aby řádně a včas předcházel různorodým nebezpečím a hrozbám pro osobní údaje a zamezil jejich zneužití. Princip odpovědnosti správce je podrobněji upraven v čl. 24 GDPR.

⁹⁶ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 43.

⁹⁷ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 121.

5.3 GDPR a role Úřadu pro ochranu osobních údajů

Role Úřadu pro ochranu osobních údajů se ve souvztažnosti k GDPR v zásadě nijak razantně nemění oproti zákonem o ochraně osobních údajů zavedené praxi a hlavním úkolem zůstává výkon dozoru a nadále disponuje při plnění svých úkolů a uplatňování jednotlivých pravomocí nezávislostí. Úřad pro ochranu osobních údajů jakožto dozorový úřad provádí kontrolu nad dodržováním GDPR, zákona o ochraně osobních údajů a dalších souvisejících právních předpisů a vymáhá uplatňování práv a povinností vyplývajících z této právní úpravy při zpracování a ochraně osobních údajů.

Úřad pro ochranu osobních údajů by měl dle GDPR nejen monitorovat, zda správci při zpracování osobních údajů řádně plní své povinnosti a postupují v souladu s GDPR a vnitrostátními právními předpisy a za jakých podmínek, ale měl by zároveň rozvíjet uvědomělost a znalost správců a zpracovatelů o jejich právech a povinnostech a stejně tak na požádání poskytovat informace subjektům údajů co se týče jejich práv a jejich samotného výkonu. Úřad se podílí i na některých vzdělávacích projektech.⁹⁸

V rámci zvyšování povědomí veřejnosti laické i odborné o ochraně osobních údajů Úřad zároveň zveřejňuje na vlastních webových stránkách v samostatné rubrice o GDPR informace o novinkách v dané problematice např. šířeji využitelné výstupy z konzultační činnosti nebo návrhy výkladových materiálů k jednotlivým otázkám aplikace GDPR, na jejichž vypracování se ÚOOÚ podílí s dozorovými úřady ostatních členských zemí EU jako člen Evropského sboru pro ochranu osobních údajů. Evropský sbor pro ochranu osobních údajů nahradil Pracovní skupinu WP29, která vykonávala tuto činnost před účinností GDPR dle čl. 29 směrnice 95/46/ES.

Do prací na výkladu Obecného nařízení jsou zapojeny konzultační útvarů ÚOOÚ a už od počátku 2017 má ÚOOÚ k dispozici pět tabulkových míst obsazovaných odborníky na GDPR a to konkrétně pro zahraniční a vládní agendu, legislativu, analytickou činnost a kontrolní odbor. S novými dozorovými agendami a zaměřením GDPR na nové technologie, přeshraniční dozor a jiné bezpečnostní otázky, které v důsledku zvyšují nároky na personální obsazení, se účinnost GDPR promítla i v personální a organizační struktuře Úřadu.⁹⁹

⁹⁸ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 451.

⁹⁹ Role ÚOOÚ: GDPR (Obecné nařízení). *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 9.2.2019]. Dostupné z: <https://www.uouu.cz/gdpr-a-role-uouu/ds-4726/archiv=0&p1=3938>

Prvotně se Úřad zaměřoval především na nové či zásadně inovované oblasti, které musí správci a zpracovatelé osobních údajů doplnit do mechanismů zpracování osobních údajů. Velkou změnou je zřízení funkce osob pověřených ochranou osobních údajů tzv. pověřenců a proto byl výklad této nové role ve veřejném i soukromém sektoru mezi prvními. Další výklad se týkal návodu k právu na přenositelnost údajů, což je jedna ze zásadních novinek především pro sektor soukromý, a dále byl např. zveřejněn dokument vysvětlující určení tzv. vedoucího dozorového úřadu, jelikož GDPR stanoví nový mechanismus celoevropského, přeshraničního dozoru nad zpracováním osobních údajů a to relativně dost detailním způsobem.¹⁰⁰

Úřad pro ochranu osobních údajů odborně podporoval práci vlády a ministerstev při přípravách adaptace právního prostředí České republiky na změny spojené s GDPR jako člen vládní pracovní skupiny skrze své odborníky, která od podzimu 2016 tzn. ještě před nabytím účinnosti GDPR projednávala problematiku a dopady GDPR. Dle GDPR by měl Úřad pro ochranu osobních údajů poskytovat Parlamentu ČR, vládě a dalším orgánům a institucím, zejména v souvislosti s legislativní činností a správními opatřeními vztahujícím se k ochraně práv a svobod fyzických osob v rámci zpracování poradenskou činnost.

Ve vymezených úkolech v čl. 57 GDPR se projevují i některé nové skutečnosti odrážející se zároveň i v kompetencích dle čl. 58 GDPR, které vychází jednak z nutnosti spolupráce správců a zpracovatelů s dozorovým úřadem při plnění jeho stanovených úkolů upravené v čl. 31 GDPR a zároveň nových povinností správců např. vypracování posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR, povinnosti předchozí konzultace dle čl. 36 nebo povinnosti ohlašovací dle čl. 33 GDPR.

5.3.1 Pravomoci

GDPR na jedné straně upravuje pravomoci nové vycházející z nově zřízených výše zmíněných právních institutů, ačkoliv z velké části zahrnuje klasické pravomoci shodné s úpravou zákona o ochraně osobních údajů, kontrolního a správního řádu, kdy postavení Úřadu zůstává bez výrazného posílení. Veškeré stanovené kompetence může Úřad vykonávat pouze způsobem, který nesmí narušovat soulad s právní úpravou vnitrostátní zejména pokud se jedná o procesní záruky a základní zásady stanovené procesním právem konkrétního členského státu. Tento soulad má být dodržován již na základě preambule GDPR a jejího bodu 129, kde jsou současně uvedeny základní zásady výkonu pravomocí Úřadu, kam patří

¹⁰⁰ GDPR a role ÚOOÚ. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 27.02.2019]. Dostupné z: <https://www.uouu.cz/gdpr-a-role-uouu/d-23082>

neustrannost, spravedlivost a výkon bez zbytečných průtahů tj. stanovení a dodržování přiměřených lhůt. Zásahy do práv a povinností musí být vhodné, nezbytné a přiměřené v rámci posouzení individuálních okolností jednotlivých případů.¹⁰¹

Pravomoci Úřadu jsou v GDPR rozděleny na vyšetřovací, nápravné a povolávací a poradní.

Vyšetřovací pravomoci dle GDPR jsou již upraveny kontrolním řádem a nejsou typově žádnou novinkou, ačkoliv se mezi nimi objevuje nový pojem, kterým je audit jako forma kontroly využívaná Úřadem pro vyšetřování za účelem zjišťování skutečného stavu při zpracování. V rámci již zavedených kompetencí má Úřad právo nařídit správčům a zpracovatelům poskytnutí informací ohledně komplexního procesu zpracování či přezkoumat osvědčení vydaných v souladu s čl. 47 odst. 7 GDPR.

Relativně novou kompetencí je v rámci vyšetřovacích pravomocí ohlášení správci či zpracovateli ze strany Úřadu údajné porušení GDPR, pokud získá Úřad důvodné podezření např. na základě stížnosti subjektu údajů, že k takovému porušení došlo. Současné procesní předpisy vnitrostátní právní úpravy tuto možnost neupravují a nejde o opatření, které by mělo za následek vznik, zánik či změnu práv a povinností správců a zpracovatelů a zároveň nemá potvrzovací charakter, zda k porušení GDPR skutečně došlo či nikoliv. Přestože forma této kompetence není zákonem přímo stanovena, obdobným způsobem Úřad již postupuje např. v rámci stížností na nevyžádaná obchodní sdělení.¹⁰²

Nápravné pravomoci jsou v obecné rovině totožné s dříve zavedenými pravomocemi Úřadu, nicméně se nápravné pravomoci úzce vážou na povinnosti správců a zpracovatelů a jejich dodržování či případné porušování a proto je třeba zohlednit změny v nich zavedené.

Výraznější povinností ovlivňující nápravné pravomoci je již z výše zmíněných nových institutů zejména povinnost předchozí konzultace, při kterých může Úřad shledat, že správce nedostatečně zohlednil možná rizika pro průběh zpracování osobních údajů a jejich ochranu a následně má Úřad právo upozornit správce či zpracovatele na skutečnost, že zamýšlené zpracování představuje porušení GDPR. Dále v souvislosti s ohlašovací povinností za předpokladu, že by došlo k narušení bezpečnosti osobních údajů, může Úřad správci nařídit, aby vzniklou situaci oznámil subjektu údajů.

¹⁰¹ bod preambule 129 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

¹⁰² NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 459.

Úřad pro ochranu osobních údajů je oprávněn ukládat sankce resp. správní pokuty dle článku 83 a to buď současně s využitím dalšího opatření např. nařízení opravy či výmazu osobních údajů nebo omezení zpracování podle příslušných článků GDPR, nebo namísto jiného prostředku.¹⁰³ Ovšem místo pokuty může být uděleno pouze napomenutí, pokud je to vhodné vzhledem ke konkrétním okolnostem daného případu např. pokud stačí sankce napomenutí z hlediska dostatečnosti společenské odpovědnosti, kdy je veřejnosti zpřístupněna informace, že daný správce porušil stanovená pravidla pro zpracování osobních údajů a pro společnost se stane méně věrohodnou osobou a je ohrožena reputace daného správce. Nicméně kvůli omezené efektivitě napomenutí se nelze vyhnout v oprávněných případech opatření ve formě pokut, přičemž udělená pokuta musí být vždy přiměřená jednotlivým skutečnostem individuálního případu.

Povolávací a poradní kompetence zahrnují např. poskytování poradenství, schvalování návrhů kodexů a schvalování kritérií pro vydávání osvědčení, vydávání stanovisek ke kodexům a vydávání osvědčení nebo akreditace jiné osoby k jeho vydání, vydávání stanovisek na základě podnětu nebo vlastního rozhodnutí určených vnitrostátnímu parlamentu, vládě aj. subjektům včetně veřejnosti v souladu s právem konkrétního členského státu.¹⁰⁴

5.4 Správní pokuty

Ukládáním správních pokut je pověřen v rámci svých pravomocí dozorový úřad viz výše uvedené shrnutí pravomocí stanovených v GDPR, ačkoliv tato možnost Úřadu pro ochranu osobních údajů náleží již dle zákona o ochraně osobních údajů, kde nalezneme upravené přestupky a maximální sazby ukládaných pokut, o kterých již práce pojednává v samostatné podkapitole. K zajištění dodržování povinností, ochrany práv a efektivity vzhledem k vymahatelnosti GDPR stanoví v článku 83 vlastní výše pokut, které hranice vymezené vnitrostátním právním předpisem o ochraně osobních údajů značně přesahují.

Předchozí směrnice 95/46/ES na rozdíl od GDPR ponechávala členským státům možnost samostatného rozhodování o užívání opatření směřujících k řádnému uplatňování směrnice včetně stanovení výše ukládaných sankcí a jejich zakotvení v právních rádech, což mělo za důsledek vytváření rozdílů v právních úpravách i praxích jednotlivých členských

¹⁰³ čl. 58 odst. 2 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

¹⁰⁴ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 462.

států, v kterých se výše sankcí více či méně lišily nebo v některých případech nebylo možno správní pokuty ukládat vůbec. Správní pokuty jsou tedy jednou ze zásadních otázek GDPR, kde se neopomenutelně objevuje výrazný sjednocující efekt a rozdíl mezi užitím v dřívější právní úpravě formy směrnice nahrazené formou nařízení.

Základní maximální výše správní pokuty jsou ukládány za méně závažná porušení a její hranice činí 10 000 000 EUR, jedná-li se o podnik pak 2 % celkového ročního celosvětového obratu za předchozí finanční rok na základě toho, která hodnota je vyšší.

Za předpokladu, že dojde k závažnému porušení GDPR, může být odpovědné osobě uložena pokuta v dvojnásobné maximální výši 20 000 000 EUR nebo v rámci podniku 4 % celkového ročního celosvětového obratu za předchozí finanční rok na základě toho, která hodnota je vyšší.¹⁰⁵

Jako méně závažná porušení GDPR uvádí porušení povinností správců a zpracovatelů dle článků 8, 11, 25 až 39, 42 a 43, dále porušení povinností subjektu pro vydávání osvědčení v rámci článku 42 a 43 a povinností subjektu pro monitorování souladu s kodexem chování dle článku 41 odst. 4.

Závažnými proviněními jsou ta, která směřují proti základním zásadám a principům a v souvislosti s nimi i proti pravidlům týkajících se právního titulu souhlasu dle příslušných článků 5, 6, 7 a 9, nebo se jedná o počínání narušování práv subjektů údajů dle článků 12 a 22. GDPR považuje za závažné provinění i nesplnění příkazu uloženého dozorovým úřadem dle článku 58 odst. 2. Některé další skutečnosti, za které hrozí uložení až dvojnásobné maximální výše pokuty jsou dále uvedeny v článku 83 odst. 5.

GDPR kromě vymezení maximálních možných hranic ukládaných pokut zároveň vytyčuje v článku 83 odst. 1 základní principy při jejich ukládání, kterými je princip účinnosti, přiměřenosti a odrazující schopnosti a vyjmenovává polehčující a přitěžující okolnosti upravené v článku 83 odst. 2 písm. a) až k).

Účinnost, přiměřenost a odrazující schopnost vyjadřují základní aspekty, dle kterých má být správní pokuta ukládána adekvátně ve souvstažnosti na dané porušení GDPR. Už samotné rozdělení maximálních výší pokut podle závažnosti a podle faktu, zda odpovědnou osobou je fyzická nebo právnická osoba, napovídá, že v každé konkrétní události by měla být situace posouzena individuálně. Při určování pokuty by nemělo být opomínáno posouzení osobní situace osoby, která své povinnosti porušila nebo neoprávněně zasáhla do

¹⁰⁵ čl. 82 odst. 4 až 6 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

práv druhých osob, a to v rámci výše pokuty především s ohledem na situaci ekonomickou resp. příjmovou stránku, kdy nesmí pokuta působit na odpovědného likvidačně, ale zároveň se nesmí jednání v rozporu s GDPR vyplácet. Konkrétně odrazující požadavek na správní pokuty jako prvek preventivní povahy koresponduje s předepsanými vysokými maximálními částkami, kterými mohou být jednotlivci postihnuti.

S těmito znakovými rysy se váží polehčující a pohoršující okolnosti, které musí být zahrnuty do určování výše pokuty zejména ve vztahu k přiměřenosti. Většina skutkových okolností např. zda k porušení došlo úmyslně nebo z nedbalosti, míra způsobené škody, doba trvání s přihlédnutím k povaze, rozsahu a účelu se dají zahrnout do této kategorie dle logického odvození a znalostí přestupkového zákona. Nicméně GDPR uvádí další nutně zohlednitelná stanoviska, kterými jsou kategorie osobních údajů, jichž se týká porušení či míra spolupráce s dozorovým úřadem za účelem nápravy nebo zmírnění nežádoucích vlivů.

Do jaké míry zvýšené sankce ovlivní praxi ukládání pokut v rámci činnosti Úřadu pro ochranu osobních údajů, bude zejména ovlivněno implementačním zákonem, který by měl ponechat v rámci ukládání správních pokut orgánům veřejné moci a veřejnoprávním subjektům na hranici 10 000 000 Kč, avšak soukromému sektoru by se změna ani v takovém případě nevyhnula.¹⁰⁶

Veřejné orgány a veřejnoprávní subjekty disponují a rozhodují o užití veřejných prostředků a proto by nadměrné sankcionování těchto subjektů ve svém důsledku mohlo vést k nepřímému potrestání občanů prostřednictvím omezení činnosti těchto subjektů. Správní pokutu může v tomto smyslu dle uzpůsobení právní úpravy členského státu nahradit sankce dle článku 84, ačkoliv právní řád České republiky nevyklučuje možnost ukládání správních pokut veřejným orgánům aj. subjektům veřejného sektoru.

5.5 GDPR a vztah k právu na informace

Ochrana osobních údajů a její právní úprava nesmí opomíjet zásadu přístupu veřejnosti k úředním dokumentům a proto tuto zásadu musí zohledňovat při svém provádění i GDPR, jelikož ani právo na ochranu osobních údajů není absolutní a střetává se s dalšími klíčovými právy viz samostatná kapitola bakalářské práce pojednávající o právu na informace a principu publicity.

¹⁰⁶ NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. Praha: Wolters Kluwer, 2018, s. 516.

Přístup veřejnosti k úředním dokumentům je chráněn veřejným zájmem, z čehož vyplývá, že orgán veřejné moci či jiný veřejný subjekt by měl mít možnost zpřístupnit veřejnosti v dokumentech uvedené osobní údaje, které má takový subjekt v držení. Pro takový daný druh zveřejnění je nutný předpoklad, že je toto zpřístupnění stanoveno právem Evropské unie nebo právem určitého členského státu. V žádném případě však zpřístupňování osobních údajů v úředních dokumentech nesmí narušovat právo na ochranu osobních údajů ve smyslu právní úpravy GDPR.

V oblasti střetu zásady veřejného přístupu k informacím a ochrany osobních údajů v České republice již existuje nejméně jeden judikát v rámci této problematiky a GDPR ponechává členským státům nadále možnost, aby tuto oblast opatřily národními předpisy za předpokladu, že budou respektovat veškeré mezinárodní principy vyplývající ze základních práv a svobod a budou v souladu s GDPR.¹⁰⁷

Zajištění vyvažování práv na svobodný přístup k informacím a rovněž svobodu projevu s právem na ochranu osobních údajů členskými státy upravuje GDPR už v části preambule v bodě 153 a následně v článcích 85 a 86 zahrnutých v ustanoveních týkajících se zvláštních situací, které při zpracování mohou nastat. Z toho důvodu proto lze racionálně vyvodit téměř neměnný stav pro orgány veřejné moci aj. veřejné subjekty a především dosavadní praxi Úřadu pro ochranu osobních údajů ve vztahu k právní úpravě GDPR a zákonu o svobodném přístupu k informacím.

5.6 Pověřenec pro ochranu osobních údajů

Správčům a zpracovatelům GDPR stanovuje povinnost pověřence jmenovat a to konkrétně ve třech případech. Jmenování je podle ustanovení článku 37 odst. 1 GDPR nutné, pokud zpracování provádí orgán veřejné moci či veřejný subjekt kromě soudů v rámci výkonu jejich soudních pravomocí, dále za předpokladu že hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů, a nebo pokud hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů např. citlivých údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.¹⁰⁸

Mezi pravidelné a systematické monitorování občanů patří všechny formy sledování a profilování včetně prostřednictvím internetu a to i pro účely behaviorální reklamy. Patří sem

¹⁰⁷ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 92.

¹⁰⁸ Zvláštní kategorie v tomto smyslu upravuje čl. 9 GDPR a trestné činy čl. 10 GDPR.

případy jako provozování telekomunikačních sítí a služeb, stanovení výše pojistného, sledování polohy skrz internet či mobilní aplikace, věrnostní programy a kamerové systémy.

109

Za rozsáhle zpracování údajů se může považovat zpracování údajů o pacientech v rámci běžné činnosti nemocnice, zpracování obsahových, provozních či lokalizačních dat poskytovatelem telefonních a internetových služeb, zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu.

Subjekty zpracovávající osobní údaje v rámci činnosti ve veřejné správě mají povinnost jmenovat pověřence vždy bez výjimky, zatímco v soukromém sektoru záleží na uvážení správce či zpracovatele, zda pověřence jmenuje, pokud se nejedná o zpracování osobních údajů podle dalších dvou vymezených případů. Za všech okolností ať je pověřenec jmenován z povinnosti nebo na základě dobrovolného rozhodnutí, je však nezbytné postupovat dle GDPR, plnit všechny stanovené povinnosti a respektovat uvedené požadavky.

Požadavky na pověřence pro jmenování nejsou v GDPR přesně uvedeny resp. není stanovena požadovaná úroveň vzdělání či vymezení konkrétní délky potřebné praxe, ačkoliv GDPR předpokládá odpovídající úroveň odborných znalostí práva především vědomostí z oblasti národní a evropské legislativy, což zahrnuje i důkladnou znalost GDPR, a praxi v oboru ochrany osobních údajů pro řádný výkon úkolů stanovených článkem 39 GDPR s přihlédnutím k povaze a rozsahu zpracování. Přilepšit šanci na jmenování dané osoby na pozici pověřence zajisté může znalost systému veřejné správy, konkrétního oboru v rámci orgánu či podnikání a chodu organizace dle individuálního působení a správce, který má pověřence jmenovat. Dostatečná znalost možných prováděných operací zpracování, stejně jako znalost informačních systémů a technického zabezpečení osobních údajů aj. dat je jedním z dalších logických předpokladů, které GDPR exaktně neupravuje.¹¹⁰

Funkci pověřence je možné vykonávat na základě smlouvy o poskytování služeb, kterou lze uzavřít s jednotlivcem nebo externí organizací, jež je jiná než organizace správce nebo zpracovatele. Nejen státním orgánům ale i fyzickým a právnickým osobám může být svěřena na základně národních předpisů pravomoc vykonávat veřejnou moc a plnit úkoly ve veřejném zájmu. V tomto smyslu se může jednat například o oblast veřejné dopravy, zásobování vodou a energiemi, silniční infrastrukturu nebo veřejnoprávní vysílání.

¹⁰⁹ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 252.

¹¹⁰ čl. 37 odst. 5 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Obecné nařízení dovoluje pověřenci jakožto jedné osobě být jmenován i pro několik státních orgánů, institucí či firem resp. pro více správců nebo zpracovatelů zároveň, které mají podobnou organizační strukturu a jejich velikost nebrání výkonu úkolů pověřence. Kvůli odbornosti úkolů pověřence musí být zajištěno, aby je jediný pověřenec zvládl plnit řádně a efektivně i přes jeho službu pro několik orgánů veřejné moci nebo veřejných subjektů zároveň. Občané by měli mít jistotu, že pověřence dokáží kontaktovat, jeho kontaktní údaje musí být dostupné a zároveň musí být také zajištěna osobní dosažitelnost pověřence fyzicky nejlépe ve stejných prostorách jako zaměstnanci, po telefonu nebo prostřednictvím jiného zabezpečeného komunikačního prostředku např. e-mailu či datové schránky.¹¹¹

Pověřenci jsou správcům nebo zpracovatelům důležitou nápomocnou osobou z důvodů potřeby odborných znalostí v oblasti právních předpisů a postupů týkajících se ochrany údajů, ale především jsou žádaným přínosem díky vlastní nezávislosti z hlediska plnění svých povinností a úkolů a to bez ohledu na to, zda je pověřenec zaměstnancem správce nebo poskytovatel externí služby. Při výkonu úkolů mu náležících tak pověřenci nemůže být ukládáno dalších pokynů tj. správce nebo zpracovatel nemohou a nesmí nařídít pověřenci, jakým způsobem má postupovat ve své činnosti. Zároveň se pověřenec nemusí řídit obchodním nebo jiným zájmem správce nebo zpracovatele, neboť jeho postavení odpovídá samostatnému poradnímu orgánu a naopak nesmí dojít ke střetu zájmů.

Pověřenci smějí zastávat i jiné funkce v rámci organizace správce a působit interně jako jeho zaměstnanci, kterými mohou být ještě před jmenováním do funkce pověřence, nemohou jim však být svěřeny takové úkoly a povinnosti, které by zapříčinily střet zájmů resp. by se dostali do situace, kdy by kontrolovali svou vlastní činnost. Pozice při jejichž výkonu by mohl střet zájmů nastat jsou zejména ty, na které by pověřenec stanovoval účel a prostředky zpracování osobních údajů. V rámci zamezení střetu zájmů je důležité vymezit tato pracovní místa, která jsou neslučitelná s funkcí pověřence a kterými mohou být především řídicí funkce např. ředitel IT oddělení nebo personálního oddělení nebo vlastník společnosti.¹¹²

Pověřenec je při výkonu své funkce vázán povinností mlčenlivosti v souladu s právem Unie nebo členských států. Pověřenci nejsou osobně zodpovědní za nedodržování GDPR při zpracování osobních údajů, jelikož Obecné nařízení stanoví, že povinnost zajistit a schopnost

¹¹¹ KALÍŠEK, Jindřich a VĚŽNÍKOVÁ, Petra. Pověřenec pro ochranu osobních údajů dle nařízení. In: *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. EPRAVO.CZ, a.s., ©1999-2019. 24.1.2017 [cit. 11.2.2019]. Dostupné z: <https://www.epravo.cz/top/clanky/poverenec-pro-ochranu-osobnich-udaju-dle-narizeni-gdpr-nove-pokyny-wp29-k-vykonu-funkce-104829.html>

¹¹² DPO čili Pověřenec pro ochranu osobních údajů. *Obecné nařízení o ochraně osobních údajů — prakticky* [online]. GDPR.cz. [cit. 15.11.2018]. Dostupné z: <https://www.gdpr.cz/gdpr/dpo/>

doložit provádění řádného zpracování v souladu s Obecným nařízením přísluší správcům a zpracovatelům. Nicméně správci či zpracovatelé jako zaměstnavatelé nebo klienti pověřence mohou požadovat v případě narušení bezpečnosti, jednání v rozporu s GDPR a vzniku újmy, aby jim poskytl náhradu škody, pokud prokáží zavinění ze strany pověřence.

113

Pověřenec pro ochranu osobních údajů má v náplni práce především poskytování informací a poradenství správcům, zpracovatelům a zaměstnancům, kteří se na zpracování osobních údajů podílejí, monitorování uplatňování posouzení vlivu na ochranu osobních údajů a monitorování souladu zpracování s GDPR a dalšími předpisy Evropské unie a vnitrostátními právními předpisy. Mezi stanovené úkoly patří i zvyšování povědomí a odborné přípravy osob zapojených do jednotlivých operací zpracování a souvisejících auditů, kdy tak může konat prostřednictvím školení pracovníků.

Ve výkonu své funkce by měl spolupracovat s Úřadem pro ochranu osobních údajů jako dozorovým úřadem v rámci České republiky a zároveň pro Úřad působit jako kontaktní místo v rámci záležitostí spadajících do oblasti zpracování např. předchozích konzultacích.¹¹⁴

Plnit veškeré v článku 39 GDPR uvedené úkoly by měl pověřenec způsobem, kdy bude brát v potaz povahu, rozsah, kontext a účel zpracování s patřičným ohledem na všechna možná rizika spojená s postupem zpracování osobních údajů. V praxi by se tak měl pověřenec zaměřit nejprve na ty oblasti, které mohou tvořit největší riziko a vytvořit si plán, který bude představovat postup v práci podle rizikovosti jednotlivých úkonů, i když by zásadně neměl přehlížet ani méně rizikové oblasti.

¹¹³ NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018, s. 241.

¹¹⁴ Základní příručka k GDPR: Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 11.11.2018]. Dostupné z: https://www.uouu.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=2571?fbclid=IwAR19peywXnYv1UqQLIkuMaWJQNURmvtGC4XHb6NOKy_YgvBHDMDkuyUAEO0

6. GDPR v praxi

Pro zjištění pohledu pracovníků ve veřejné správě na GDPR a především posouzení vlivu na výkon pracovních povinností v souvislosti s ochranou osobních údajů byl proveden rozhovor s Dagmar Mertlovou, která zastává funkci jako vedoucí odboru regionálního rozvoje a investic na Městském úřadě v Rumburku. Rozhovor byl uskutečněn 25. října 2017 tzn. před začátkem účinnosti GDPR, kdy probíhala legisvakanační lhůta v jejímž průběhu úředníci se stejně jako jiní správci a zpracovatelé měli připravit na příchod této nové zákonné úpravy a veškeré činnosti přizpůsobit patřičným požadavkům nové legislativy, aby nedošlo ke zpracování osobních údajů nezákonným způsobem při následném nabytí účinnosti GDPR.

Otázky využitě pro rozhovor sledovaly především zhodnocení pozitiv a negativ GDPR z pohledu osoby, která se zpracováním osobních údajů setkává v praxi a přímo ji zavedení nové zákonné úpravy ovlivňuje.

Z hlediska vhodnosti posouzení celkového vlivu GDPR v tomto případě bylo nutné zkoumat nejen situaci před účinností, ale zjistit případné změny a fungování GDPR v praxi i za situace, kdy již má schopnost zavazovat resp. ukládat povinnosti, především vzniká povinnost se tímto právním předpisem řídit. Z toho důvodu bylo od Dagmar Mertlové vyžádáno a následně bylo k datu 24. února 2019 poskytnuto celkové shrnutí stavu a popsání změn, v rámci Městského úřadu Rumburk vzhledem k dopadům, které mohou zaměstnanci pociťovat při výkonu svých každodenních pracovních aktivit.

Z rozhovoru provedeného před počátkem účinnosti viz příloha je patrné, že nejzásadnějším problémem, který dle názoru Dagmar Mertlové představoval největší hrozbu, mohl být samotný systém podrobného vedení záznamů o zpracování osobních údajů a systém jednotlivých bezpečnostních opatření, jehož řádné fungování může být společně s vyřizováním žádostí občana na poskytnutí informací ohledně zpracování jeho údajů či žádostí na opravu, anonymizace nebo výmaz jeho údajů časově náročné a při jeho nedostačujícím provedení resp. při špatném nastavení správného systému vedení evidence a zabezpečení zpracování osobních údajů může dojít k nežádoucí situaci např. ztrátě dat. Správně nastavený systém zpracování a ochrany osobních údajů tak vyžaduje určitý stupeň odbornosti, což pro úředníky v praxi znamenalo např. absolvování odborných školení.¹¹⁵

Na provoz Městského úřadu Rumburk se tak následně tato oblast potřeby zabezpečení osobních údajů po nabytí účinnosti GDPR promítla hned několika způsoby. Jedním z méně

¹¹⁵ Rozhovor s Dagmar Mertlovou, vedoucí odboru regionálního rozvoje a investic Městského úřadu Rumburk. Rumburk 25.10.2017

problémových provedených opatření je zabezpečení kanceláří a skříněk s dokumenty obsahující osobní údaje zámky a v případě úklidu nesmí být dokumenty volně ponechány na stolech pracovníků. Následná ačkoliv již více invazivní opatření ve vztahu k aktivitám úředníků je skutečnost, že ze spisové služby musely být vymazány všechny dříve využívané adresáře s daty o fyzických a právnických osobách, tudíž mají úředníci ztíženou práci nutností každou adresu opakovaně zadávat, pokud nemohou využít centrální registr osob.

Přísnější bezpečnostní opatření ovlivnily práci úředníků také z hlediska využívání při plnění svých povinností elektronických zařízení tzn. pracovních počítačů, které musí být opatřeny heslem periodicky se po 3 měsících obměňujícím a na kterých bylo nastaveno pracovníky IT oddělení automatické vypínání po určité době nečinnosti, aby bylo zamezeno možnému přístupu neoprávněných osob k osobním údajům obsažených v dokumentech aj. nástrojích využívaných k práci, pokud by se příslušný úředník v tu chvíli u svého pracovního stolu nenacházel. “Při práci jsme neustále museli zadávat hesla někdy až 20x denně. Stačí zvednutý telefon, ústní dotaz občana v kanceláři a 2 min jsou pryč. Tento vypínací čas PC nakonec IT na žádost zaměstnanců prodloužil.”¹¹⁶

Pracovníci musí dále reagovat na dotazy občanů vztahující se k anonymizaci, jelikož občané namítají, že na smlouvách se jim nedostává požadovaných informací a působí neúplně resp. údaje jako telefonní čísla, bankovní účty a podpisy jsou a musí být začerněny.

Dalším bodem, který ovlivnil správu Městského úřadu Rumburk je jmenování pověřence, kterého ze zákona jako orgán veřejné moci jmenovat musí a ačkoliv v tomto konkrétním případě neřešil pověřenec zatím žádné spory, ani dotazy ze strany občanů, jsou na tuto funkci vynakládány finanční prostředky, jelikož pověřenec musí být jmenován a jeho činnost musí být finančně zajišťována vždy bez ohledu, zda je v určitém případě potřebné poradenství a využití odborné kvalifikace daného institutu a nikoliv na základě úvahy a potřeby jako tomu je ve správě soukromé.¹¹⁷

V porovnání obou zohledněných poměrů před a po nabytí účinnosti GDPR lze konstatovat zřejmý vliv na časovou náročnost jednotlivých prováděných úkonů způsobenou nejen vyřizováním písemností ale i samotnou úpravou dokumentů, které mají být zveřejněny tzn. anonymizací, tudíž nutnost a způsob provedení přísného bezpečnostního systému přináší zaměstnancům úřadu další povinnosti ovlivňující jejich výkon. Nepřehlednutelný zůstává i fakt jmenování pověřenců, kdy je zasahováno do finančních zdrojů, aniž by existovala

¹¹⁶ Informace poskytla Dagmar MERTLOVÁ, vedoucí odboru regionálního rozvoje a investic Městského úřadu Rumburk. Rumburk 24.2.2019.

¹¹⁷ Informace poskytla Dagmar MERTLOVÁ, vedoucí odboru regionálního rozvoje a investic Městského úřadu Rumburk. Rumburk 24.2.2019.

možnost institut pověřence nevyužívat, jelikož GDPR kogentně stanoví povinnost pověřence jmenovat.

Závěr

V současné době jsou informace včetně osobních údajů jedním ze základních faktorů důležitých pro fungování společnosti. S neustále stoupajícím významem informací a osobních údajů roste i využívání moderních technologií pro usnadnění a zefektivnění práce s nimi v rámci služeb občanům a dosažení kvalitního fungování veřejné správy potřebného pro poměry dnešní rychle se rozvíjející doby. Moderními technologiemi jsou data v hojném počtu každodenně přenášena, ačkoliv s nimi roste riziko zneužití osobních údajů jednotlivých osob, jelikož informace jsou také velmi výhodným obchodním artiklem.

S možností zneužití osobních údajů a narušení základních práv každé osoby na ochranu před neoprávněným zasahováním do jejich soukromého a osobního života, je nutno zabývat se otázkou ochrany těchto práv a ochrany osobních údajů. Nicméně tuto skutečnost reflektuje rozsáhlá právní úprava pomocí stanovených zásad, práv a povinností při zacházení s osobními údaji, která nepostrádá vymezení sankcí, jež jsou nezbytné z hlediska vymahatelnosti dodržování daných povinností, neboť ty zastupují vzhledem k zamezení vzniku nebezpečí pro práva jedinců jeden ze základních prvků vůbec. Tuto skutečnost taktéž zrcadlí rozsáhlá judikatura soudů a praxe či stanoviska dozorového úřadu, který v České republice působil ještě před GDPR.

Při bližším pohledu a shrnutí řešení ochrany osobních údajů dnešní legislativou je zřejmé, že si rozsáhlost a vážnost této problematiky dnešní společnost uvědomuje a podrobně se jí zabývá jak na úrovni České republiky tak i mezinárodní především Evropské unie, jak tomu přisvědčuje i objemnost a komplexnost nového právního předpisu GDPR, jenž zasahuje do oblastí vnitrostátní úpravy ve větší či menší míře, neboť ta již řeší problematiku poměrně dostatečně obsáhle a relativně rigorózně, ačkoliv se novým institutům i přesto nevyhne.

Česká republika jako demokratický stát zajišťuje zároveň právo na informace, které se v oblasti ochrany osobních údajů nemusí projevovat jen eventuálním střetem základních práv, neboť je nezbytné ohlížet se zároveň na důležitost principu transparentnosti veřejné správy a principu publicity pro vyloučení svévole orgánů veřejné moci, ale taktéž se projevuje v právu osob, aby byly informovány o tom, jak je zacházeno s jejich osobními údaji. V tomto ohledu můžeme přihlídnout k Obecnému nařízení ze strany Evropské unie, které zmíněné právo posiluje a tím přispívá zároveň i k ochraně osobních údajů.

Na druhé straně tato nová zákonná úprava v podobě GDPR utvrzováním povinností znamená více práce pro úředníky nejen ve veřejné správě ale i pro jiné fyzické a právnické osoby, které osobní údaje zpracovávají a zajišťují jejich ochranu, a to i za předpokladu že

přehlédneme nutnost zapracování GDPR do stávajícího právního řádu a mechanismů zpracování a ochrany osobních údajů a dále vypracování výkladu GDPR, jako tomu je u každé nové legislativy podobného charakteru.

Zda Obecné nařízení přináší více negativ nebo pozitiv v jeho fungování v praxi, je zatím jen nepřesně určitelné, jelikož názory se mohou lišit z pohledu úředníka veřejné správy a z pohledu občana, jehož osobní údaje jsou zpracovávány. Pro přesnější analýzu a podrobnější východiska by bylo potřeba delšího pozorování a více názorů osob, kterých se zavedení nové legislativy osobně dotkne bez ohledu na to, jakou roli budou v dané situaci zastávat. Podstatným ukazatelem také mohou být v budoucnu judikáty upravující oblasti, v kterých může GDPR ve vztahu k vnitrostátní úpravě činit potíže např. v rámci některých nových či pozměněných povinností správců či zcela nového institutu pověřence pro ochranu osobních údajů.

Summary

In the present time information is one of the essential factors of a working society. With the rise of importance of personal information and the usage of modern technologies for ease of use and higher work efficiency and to reach a higher quality of functionality of public administration necessary for the fastly growing modern society. Data are transferred using modern technologies at all times now, even though the risk of personal information misuse is higher than with other methods, this is due to information being a coveted resource.

With the possibility of misuse of personal information and breach of the fundamental human right of privacy, it is paramount to take into account the question of data protection. This is taken into account by a statutory definition which defines a fine, that is necessary from the perspective of data protection enforcement. It ensures security for data protection of individuals and is one of the most basic elements. This is reflected by the extensive judiciary structure of courts which has functioned before the introduction of GDPR.

Solving such issues with the legislature, the gravity of data protection is more than apparent. Such endeavors are present on the national level of the Czech Republic and in the European Union via the General Data Protection Regulation. It is even more apparent in the complexity and structure of GDPR which interferes with the national statute that solves the problems in an extensively rigorous way. The introduction of new legislative institutions is unavoidable, even if in a small enough quantity.

As a democratic country, the Czech Republic ensures the citizens' right to information which does not necessarily cause a breach of basic human rights given the fact it is necessary to take into account the principle of transparency of public administration and the principle of publicity for the exclusion of decisions made against the public interest. It is also shown in the citizens' right to be informed about how their information is handled. The general regulation of the European Union aid this right and in turn adds to the protection of personal data.

On the other hand, this reform in the form of GDPR means more work for administrative staff not only in the public administration but also for those in the private sector. This is under the assumption that the inclusion of GDPR is overlooked.

Whether the regulation by the European Union holds more positive or negative aspects in its practical application is impossible to say as opinions vary from one extreme to another, whether it is an opinion of an employee of public administration or an ordinary citizen whose data is being processed. Longer time of observation and more collected opinion would be

necessary for a more thorough analysis. A significant factor in the future may also be court decisions in this area, which can cause issues within the relation between GDPR and national statute.

Seznam použité literatury

Knižní literatura

BREJCHA, Aleš. *Právo na informace a povinnost mlčenlivosti v českém právním řádu*. Vyd. 1. Praha: CODEX Bohemia, 1998. 288 s. ISBN 80-85963-47-7.

JANEČKOVÁ, Eva a Václav BARTÍK. *Zpracování osobních údajů obcemi. Vybrané problémy*. Praha: Wolters Kluwer, 2013. 152 s. ISBN 978-80-7357-962-3.

JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů z pohledu zvláštních právních úprav k l. 8. 2012*. Vyd. 1. Olomouc: ANAG, 2012. 352 s. ISBN 978-80-7263-749-2.

MATOUŠKOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2. vydání. Praha: ASPI, 2008. 455 s. ISBN 80-7357-322-9.

MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Vyd. 1. Praha: Leges, 2018. 152 s. ISBN 978-80-7502-275-2.

MORÁVEK, Jakub. *Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům*. Vyd. 1. Praha: Wolters Kluwer, 2015. 360 s. ISBN 978-80-7552-018-0.

NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Vyd. 1. Plzeň: Aleš Čeněk, 2018. 339 s. ISBN 978-80-7380-689-7.

NULÍČEK, Michal. *GDPR/Obecné nařízení o ochraně osobních údajů: Praktický komentář*. 2., aktualizované. vyd. Praha: Wolters Kluwer, 2018. 559 s. ISBN 978-80-7598-068-7.

POMAHÁČ, Richard a Olga VIDLÁKOVÁ. *Veřejná správa*. Vyd. 1. Praha: C.H.Beck, 2002. 278 s. ISBN 80-7179-748-0.

ŠMÍD, Vladimír. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 227/2000 Sb., zákona č. 177/2001 Sb., zákona č. 450/2001 Sb., zákona č. 107/2002 Sb., zákona č. 310/2002 Sb., zákona č. 517/2002 Sb., zákona č. 439/2004 Sb., zákona č. 480/2004 Sb., zákona č. 626/2004 Sb. a zákona č. 413/2005 Sb.* Brno, 2005. Komentář. Masarykova univerzita v Brně.

Internet

Předpisy o ochraně osobních údajů. *Ochrana osobních údajů* [online]. oou.cz, ©2014 [cit. 1.2.2019] Dostupné z: <http://www.oou.cz/predpisy>

Právní předpisy. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 2.2.2019]. Dostupné z: <https://www.uouu.cz/pravni-predpisy/ds-1257/archiv=0&p1=1657>

SEDLÁČKOVÁ, Miroslava. Zaměstnavatel jako povinný subjekt podle zákona o svobodném přístupu k informacím může za určitých podmínek odmítnout poskytnutí informací o platu zaměstnance (ústavně konformní výklad § 8b zákona o svobodném přístupu k informacím). *Ústavní soud České republiky*. [online]. Ústavní soud, ©2015. 1.11.2017. [cit. 11.11.2018]. Dostupné z: <https://www.usoud.cz/aktualne/zamestnavatel-jako-povinnny-subjekt-podle-zakona-o-svobodnem-pristupu-k-info-rmacim-muze-za-u/>

Nález Ústavního soudu ze dne 17.10. 2017, sp. zn. IV. ÚS 1378/16 publikován pod č. 121/2017 Sb., [cit. 11.11. 2018] Dostupné z: https://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/Publikovane_nalezky/2017/IV._US_1378_16_an.pdf

Úřad. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 11.2.2019]. Dostupné z: <https://www.uouu.cz/urad/ds-1059/p1=1059>

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 12.11.2018]. Dostupné z: <https://www.uouu.cz/zakon-c-106-1999-sb-o-svobodnem-pristupu-k-informacim/ds-2571/p1=2571>

GDPR (Obecné nařízení). *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 13.1.2019]. Dostupné z: <https://www.uouu.cz/gdpr-obecne-nbsp-narizeni/ds-3938/archiv=0>

K problematice aktualizace zpracovávaných osobních údajů. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 27.02.2019]. Dostupné z: https://www.uouu.cz/vismo/dokumenty2.asp?id_org=200144&id=1595&n=k-problematice-aktualizace-zpracovavanych-osobnich-udaju

Role ÚOOÚ: GDPR (Obecné nařízení). *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 9.2.2019]. Dostupné z: <https://www.uouu.cz/gdpr-a-role-uouu/ds-4726/archiv=0&p1=3938>

GDPR a role ÚOOÚ. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 27.02.2019]. Dostupné z: <https://www.uouu.cz/gdpr-a-role-uouu/d-23082>

KALÍŠEK, Jindřich a VĚŽNÍKOVÁ, Petra. Pověřenec pro ochranu osobních údajů dle nařízení. In: *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. EPRAVO.CZ, a.s., ©1999-2019. 24.1.2017 [cit. 11.2.2019]. Dostupné z: <https://www.epravo.cz/top/clanky/poverenec-pro-ochranu-osobnich-udaju-dle-narizeni-gdpr-nove-pokyny-wp29-k-vykonu-funkce-104829.html>

DPO čili Pověřenec pro ochranu osobních údajů. *Obecné nařízení o ochraně osobních údajů — prakticky* [online]. GDPR.cz. [cit. 15.11.2018]. Dostupné z: <https://www.gdpr.cz/gdpr/dpo/>

Základní příručka k GDPR: Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, ©2013. [cit. 11.11.2018]. Dostupné z: https://www.uouu.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=2571?fbclid=IwAR19peywXnYv1UqQLIkuMaWJQNURmvtGC4XHb6NOKy_YgvBHDMDkuyUAEO0

Právní předpisy

Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. července 2017.

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Zákona č. 500/2004 Sb., správní řád.

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Judikatura

Nález Ústavního soudu ze dne 17.10. 2017, sp. zn. IV. ÚS 1378/16

Nález Ústavního soudu ze dne 12.10. 1994, čj. Pl. ÚS 4/94.

Ostatní

Rozhovor s Dagmar Mertlovou, vedoucí odboru regionálního rozvoje a investic Městského úřadu Rumburk. Rumburk 25.10.2017

Informace poskytla Dagmar MERTLOVÁ, vedoucí odboru regionálního rozvoje a investic Městského úřadu Rumburk. Rumburk 24.2.2019.

Seznam příloh

Příloha č. 1 - Rozhovor s vedoucí odboru regionálního rozvoje a investic před počátkem účinnosti ze dne 25.10. 2017

Jaké jsou hlavní problémy/nebezpečí při zpracování/ochraně osobních údajů?

“Problémy spočívají v pracnosti přípravy, evidence veškerých zpracovávaných údajů, tak aby bylo zmapováno a ošetřeno veškeré nakládání s nimi. Nebezpečí vždy spočívá ve špatně nastaveném a ošetřeném systému, kdy může dojít např. osobní chybou úředníka ke ztrátě osobních údajů, pak ke úmyslnému odcizení, nebo kybernetickému vstupu do databází hackery. Tedy nejen zmapování zpracovávání, ošetření, ale i zajištění IT bezpečnosti. Pak si myslím, že tento systém bude vyvolávat problémy při aplikace tzv. anonymizace (vymazávání údajů na žádost občana) nebo sdělování na žádost občana s jakými a proč jeho osobními údaji nakládáme. Zvýší se tím časová náročnost pro úředníky.”

Co vidíte jako pozitiva spjatá s novou zákonnou úpravou v podobě GDPR?

“K zajištění ochrany pro občany a subjekty, při současném trendu elektronizace a možnosti využívat databáze, je více než zřejmé, že by nebyl problém pro jakéhokoliv hackera, nebo i úředníka použít např. rodné číslo a vzít si půjčku na občana, který by toto ani netušil, nebo změnit údaje v katastru nemovitostí a po čase zjistíte, že nejste ani právoplatný majitel nemovitosti. Tedy jednoznačně pozitivum, aby nedocházelo ke zneužívání a trestným činům. Údaje jsou dnes zneužívány také hlavně velkými internetovými společnostmi, kdy se podíváte do webu, něco objednáte a na Váš e-mail chodí i nadále nevyžádané nabídky, nebo Vám dealeři volají a nabízí. Sama jsem se tím setkala, kdy mě neustále nejmenovaná firma nabízí změnu firmy na dodávku plynu. Jak je možné, že mají k dispozici údaje o mém místě na odběr plynu?”

Co vidíte jako negativa spjatá s novou zákonnou úpravou v podobě GDPR?

“Nastavený systém bude moci ochraňovat i záležitosti, kdy trestné činy, nebo nemožná identifikace občanů a subjektů budou činit problémy v dokazování nezákonné činnosti. Je zde mnoho otazníků, kdy je potřeba souhlas vlastníka osobních údajů, např. jestliže vstoupí do veřejné budovy a jsou zde umístěny kamery. Nebo ochrana osobního majetku právě kamerami, kdy nesmíte použít záznam z veřejné komunikace, či prostoru. Tyto případy budou vyvolávat potřeby tzv. judikátů, tedy dokud neproběhne správní řízení, či soud, budou nesrovnalosti ve výkladu GDPR, stejně jako u každé nové právní normy.”

Jak byste celkově shrnula danou problematiku z vašeho pohledu?

“Nastavené a schválené GDPR přináší mnoho povinností pro veřejné subjekty (města, obce, příspěvkové organizace..), ale více práv pro občany a soukromé subjekty. Dle mého názoru bude aplikace složitější než u jiné zákonné normy, kdy na vahách rozhodování je právo občana proti veřejnému zájmu.”

Příloha č. 2 - Poznámky k GDPR –MěÚ Rumburk, Odbor regionálního rozvoje a investic

Město Rumburk v rámci nového zákona vydalo několik směrnic a opatření – oběh písemností, IT používání osobních údajů, atd. Všichni zaměstnanci mají zabezpečeny kanceláře, uklízečky by neměly nalézt na stolech volně položené dokumenty, na skřínkách, kde jsou uloženy dokumenty, byly instalovány zámky.

Spisová služba VERA musela vymazat používaný adresář fyzických a právnických osob, zaměstnanci musí každou adresu opětovně zadávat, pokud nemohou využít centrální registr osob (zmocnění v zákoně).

Pracovníci IT oddělení nastavily vypínání PC zpočátku na 2 min, pokud úředník na PC souvisle nepracoval. Při práci jsme neustále museli zadávat hesla někdy až 20 x denně. Stačí zvednutý telefon, ústní dotaz občana v kanceláři a 2 min jsou pryč. Tento vypínací čas PC nakonec IT na žádost zaměstnanců prodloužil.

Každé tři měsíce musí zaměstnanci měnit hesla na svých PC, která nesmí obsahovat předchozí čísla, písmena a znaky (tzv. stanovená politika hesel). Služební telefony musí být také opatřeny heslem při každém otevření (buď znak, nebo otisk).

Na profilu zadavatele E-ZAKu jsou zveřejňovány dokumenty, které musí být před zveřejněním tzv. anonymizovány (zakrytí telefonních čísel, bankovních účtů, podpisů atd.). Občané naopak vznášejí dotazy, že na smlouvách není nic vidět, že se z nich nedozví požadované informace. Smlouvy takto zveřejněné působí nedoplněné, bez údajů.

Pověřenec zatím neřešil žádný dotaz, problém dotazů od občanů. V každém případě město stojí finanční prostředky, neboť musí být vždy ustanoven.

Závěr – vliv na dodržování DGPR

Zpomalení pracovních úkonů při vyřizování písemností, úprava zveřejňovaných dokumentů. Neustálé měnění hesel, kódování PC, zamykání telefonů.

V Rumburku 24.02.2019

Ing. Dagmar Mertlová, vedoucí ORRI MěÚ Rumburk