Univerzita Palackého v Olomouci

Právnická fakulta

Kristián Ženatík

Dopady Obecného nařízení o ochraně osobních údajů ve veřejné správě

Diplomová práce

Olomouc 2019

„Prohlašuji, že jsem diplomovou práci na téma *„Dopady Obecného nařízení o ochraně osobních údajů ve veřejné správě"* vypracoval samostatně a citoval jsem všechny použité zdroje."

V Olomouci dne 25. června 2019

Kristián Ženatík

Tímto chci vyjádřit vděčnost a poděkování doc. JUDr. Kateřině Frumarové, Ph.D. za ochotu, veškeré rady a poznatky a především za čas, který mi věnovala v souvislosti s vedením mé diplomové práce.

Obsah

Seznam použitých zkratek

Adaptační zákon	**Zákon č. 110/2019 Sb., o zpracování osobních údajů**
ČNB	**Česká národní banka**
ČTÚ	**Český telekomunikační úřad**
DPIA	**Data Protection Impact Assessment**
DPO	**Data Protection Officer**
ESLP	**Evropský soud pro lidská práva**
EU	**Evropská unie**
Komise	**Evropská komise**
MPO	**Ministerstvo průmyslu a obchodu**
Nařízení	**Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)**
NSS	**Nejvyšší správní soud**
NKÚ	**Nejvyšší kontrolní úřad**
SDEU	**Soudní dvůr Evropské unie, Evropský soudní dvůr**
Úmluva 108	**Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat**
ÚoOÚ	**Úřad pro ochranu osobních údajů**
ÚS	**Ústavní soud**
ZEK	**Zákon č. 127/2005 Sb., o elektronických komunikacích**
ZoEO	**Zákon č. 133/2000 Sb., o evidenci obyvatel**
ZoOÚ	**Zákon č. 101/2000 Sb., o ochraně osobních údajů**

Úvod

Zhruba v polovině loňského roku nabyla účinnosti bezesporu zásadní právní úprava, která významným způsobem ovlivní agendu zpracování osobních údajů. O její významnosti hovoří mj. i skutečnost, že adresáti, která tato legislativní změna ovlivní, měli více než dva roky na seznámení se s ní a byli tak schopni dostát svých povinností v okamžiku nabytí její účinnosti. Přesto vzhledem ke komplexnosti předmětného nařízení z "legislativní dílny" Evropské unie lze předpokládat, že ne ve všech případech byl k dnešnímu dni zajištěn soulad s touto právní úpravou. Řeč není o ničem jiném, než o Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen "Nařízení").

Protože záměrem práce je především pohlížet na tuto úpravu v souvislosti s veřejnou správou, spatřuji seznámení s Nařízením jako nezbytnost. To, že Evropské společenství nebere ochranu osobních údajů na lehkou váhu, značí i skutečnost, že ochrana osobních údajů je považována za základní lidské právo dle Listiny základních práv Evropské unie. Historickému vývoji právní úpravy, na kterou Nařízení navazuje, bude následovat objasnění právního rámce na úrovni českých zákonů. Zásadním pramenem je zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který byl více než dvacetkrát novelizován. A právě reforma právní úpravy z dubna tohoto roku jdoucí ruku v ruce s GDPR, kterou představuje tzv. Adaptační zákon, zcela zásadně mění koncept stávající legislativy. Přiblížení ZoOÚ v dřívější podobě je ovšem podstatný prvek pro srovnání právního rámce před a po účinnosti GDPR, potažmo Adaptačního zákona. Proto je příhodné seznámit se v úvodní kapitole se ZoOÚ, a to konkrétně s požadavky, které klade na zpracování osobních údajů, užívanou terminologií a také vztahu práva na ochranu osobních údajů s právem na informace. Získané poznatky pak budou komparovány s Adaptačním zákonem a GDPR, což poslouží k zodpovězení výzkumné otázky. Následovat pak bude kapitola zkoumající konkrétní aspekty Nařízení. O rozsáhlosti normy svědčí fakt, že k jejímu ozřejmění bylo vydáno nespočet publikací a komentovaných znění. Přesto si v této části vystačíme s porozuměním motivu přijetí, zaměřením a v neposlední řadě také nově zavedených povinností. Konečně pak budou analyzovány důsledky GDPR v oblasti veřejné správy, a to na konkrétních činnostech. Zde již budou uplatněna východiska osvětlena v předchozích částech, proto tak půjde o zásadní kapitolu.

Nicméně i jí předcházející odstavce budou hrát důležitou roli pro zodpovězení výzkumné otázky, *zda GDPR představuje efektivní zvýšení ochrany zpracování osobních údajů ve veřejné správě*, jelikož se zde přímo nabízí užití právě komparační metody. Ať už pod pojem veřejné správy subsumujeme

činnost státní správy nebo samosprávu, v obou případech dochází ke zpracovávání obrovského množství údajů. Zvýšená ochrana zpracování se pak může projevit v různých ohledech. Jedním z nich je snížení rizik zneužití osobních dat například zavedením nových postupů. Můžou být poskytnuty nové a účinnější nástroje pro odstranění negativních následků vzniklých porušením ochrany zpracování. Nebo může dojít k posílení postavení dozorového orgánu apod. To vše jsou prvky, které by ovlivnily zpracování údajů a posílily by tak celkovou bezpečnost tohoto procesu. Vyjma komparace pak bude pro dosažení cíle práce užito metody analytické a popisné.

Primárním zdrojem budou právní předpisy, které souvisí s tématem diplomové práce a zároveň jsou potřebné pro nalezení odpovědi na výzkumnou otázku. Neméně důležitou roli pak bude představovat judikatura. Ta bude tvořena nejen soudními rozhodnutími, ale také rozhodnutími úřadu pro ochranu osobních údajů, jakožto dozorového orgánu. Úřad, kromě rozhodnutí vydávaných ve věcech, kde mu náleží rozhodovací pravomoc, pravidelně zveřejňuje na svých webových stránkách výkladová stanoviska, metodické postupy a další materiály, které budou v práci reflektovány. Mimo Úřad vydává materiály podobného charakteru Evropský sbor pro ochranu osobních údajů, dříve pojmenován jako Pracovní skupina WP29. I tyto budou dále použity jako jeden ze zdrojů. A jak už bylo zmíněno, rozhodně není nouze o publikace, ať už o komplexní komentáře či literaturu zaměřenou na specifické oblasti Nařízení. I proto využiji v deskriptivních částech práce odbornou literaturu. Příspěvky v odborných časopisech, stejně tak jako další internetové zdroje, budou použity jako doplňkové zdroje.

1. Ochrana osobních údajů ve veřejné správě

Úvodní kapitola bude pojímat proces zpracovávání osobních údajů v oblasti veřejné správy a jejich ochranu. Ačkoliv byl ZoOÚ nahrazen Adaptačním zákonem a pozbyl tak účinnosti, byl od počátku tisíciletí hlavním předpisem ve věci ochrany osobních údajů. Jak bude rozvedeno dále, jeho vznik byl ovlivněn evropským právem, které si také prošlo svým vývojem. Rovněž GDPR je dalším nástupcem, který má původ v již rozvinuté a užívané právní úpravě. Analýza ZoOÚ má svůj význam pro pochopení právního rámce v době předcházející Nařízení. Samotnému pojmu veřejné správy, resp. jeho vymezení, by mohla být věnována celá samostatná kapitola. Částečně to již bylo nastíněno v úvodu, přesto pro ujasnění bude veřejnou správou myšlena v této práci činnost veřejných institucí, a zároveň nepůjde o legislativní či justiční činnost. Zejména se budu věnovat vybraným oblastem státní správy, například školství, tak i samosprávy, zejména územní.

Na začátku je vhodné vymezit pojmy, které budou dále v práci užívány. Definování těchto pojmů bude vycházet z právní úpravy přiblížené níže, případně následných výkladů poskytnutých v rozhodnutích nejvyšších soudů či stanoviscích Úřadu. Základem problematiky je porozumění termínu "osobní údaj", který definuje ZoOÚ jako informaci, za pomocí které lze přímo či nepřímo určit konkrétní fyzickou osobu, tedy subjekt údajů. Za osobní údaje lze společně považovat i pouhý iniciál spolu s adresou trvalého bydliště, pakliže na této adrese bydlí jediná osoba s takovými iniciály[1]. Identifikovatelnost lze dovodit i v případě, kdy lze dovodit konkrétní osobu za využití dodatečné informace, třeba veřejně dostupné[2]. Podle výkladu Úřadu je osobním údajem *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. E-mailová adresa jako součást souboru informací vztažených k nějaké osobě, která je předmětem obchodního zájmu, je nepochybně osobním údajem"*[3]. Naopak o osobní údaje se nebude jednat za předpokladu, že pro identifikaci konkrétní osoby je nutné vynaložit nepřiměřeného nebo rozumně neočekávatelného úsilí[4]. Specifickou kategorií pak tvoří údaje, jejichž charakter odpovídá § 4 písm. b) ZoOÚ. Tyto jsou považovány za citlivé údaje. Posledním specifickým osobním údajem, se kterým česká právní úprava pracuje, je tzv. nahodile shromážděný osobní údaj. Příkladem nahodile shromážděného údaje je uvedení místa narození respondentem, ačkoliv formulář neobsahoval tuto dotazovanou

[1] ÚŘAD PRO OCHRANU OSOBNÁCH ÚDAJŮ. *Pojem osobní údaj* [online] uoou.cz, 13. prosince 2013 [cit. 19. listopadu 2018]. Dostupné z: < https://www.uoou.cz/pojem-osobni-udaj/d-1751/p1=2427>.
[2] NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 79.
[3] ÚŘAD PRO OCHRANU OSOBNÁCH ÚDAJŮ. *Nevyžádaná obchodní sdělení* [online] uoou.cz, 13. prosince 2013 [cit. 19. listopadu 2018]. Dostupné z: <https://www.uoou.cz/nevyzadana-obchodni-sdeleni/d-6273>.
[4] Tamtéž.

položku. Pakliže tento údaj nebude dále zpracováván, podle § 3 odst. 4 ZoOÚ nelze tento předpis aplikovat.

Od subjektu údajů je potřeba odlišovat správce a zpracovatele osobních údajů. Na rozdíl od něj jimi mohou být kromě fyzických osob, také právnické osoby nebo orgány veřejné moci. Z § 4 písm. j) ZoOÚ vyplývá, že správce určuje účel a prostředky zpracování osobních údajů a odpovídá za zpracování dat. Pokud neprovádí samotné zpracování, pověří tímto zpracovatele. Zpracovatel zpracovává data z pověření správce nebo na základě zvláštního zákona. Zatímco soukromoprávní subjekty v roli správce si mohou volit účel a způsob zpracování osobních údajů samy, subjekt veřejného práva musí vždy reflektovat čl. 2 odst. 3 Ústavy a čl. 2 odst. 2 Listiny, tedy uplatňování státní moci jen v případech, mezích a způsobem stanoveným zákonem. Pakliže orgán veřejné moci zpracovává osobní údaje jediným možným zákonným způsobem, který mu je umožněn, nikdy nemůže dojít k zásahu do legality. Orgán veřejné moci tak se v takovém případě nedopouští neoprávněného zásahu a Úřad nemůže takové zpracování postihovat svými dozorovými kompetencemi[5].

Činností spočívající v jakékoliv operaci s osobními údaji rozumíme dle § 4 písm. e) ZoOÚ jejich zpracováním. Bez ohledu na to, zda k ní dochází automatizovaně či jinak. Zákonodárce pak dále přibližuje zpracování jako shromažďování, ukládání na nosiče informací, zpřístupňování, úpravu nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace údajů. Toto vymezení pojmu zpracování vychází z Úmluvy 108[6]. Se zpracováním také úzce souvisí zabezpečení dat. Zabezpečení není v ZoOÚ subsumováno pod zpracování. Nejvyšší správní soud se vyjádřil v rozsudku ze dne 10.5.2006, čj. 3 As 21/2005-105 tak, že obě aktivity, ač přes jejich druhovou odlišnost, jsou ve vzájemném vztahu, *kdy povinnost zabezpečení dopadá na veškeré úkony zahrnované pod zákonný pojem zpracování osobních údajů*. Ačkoliv pojem "zabezpečení" dat není v zákoně výslovně definován, v ust. § 13 ZoOÚ jsou stanoveny povinnosti správců a zpracovatelů při jejich zpracování. Tento termín však více souvisí s principem bezpečnosti zpracování, na kterém podrobněji přiblížíme jednotlivé aspekty. Zde je vhodné uvést jen v krátkosti, že zákon nikterak nerozlišuje způsoby zabezpečení u orgánů veřejné moci a soukromými subjekty. Nicméně z rozhodovací činnosti Úřadu vyplývá, ačkoliv je zde stejná povinnost přijmout dostatečná bezpečnostní opatření pro správce i zpracovatele bez ohledu, zda se jedná o soukromou nebo veřejnou sféru, tak dále uvádí že *"v případě státních orgánů, které vedou rozsáhlé evidence obsahující velké množství osobních údajů včetně citlivých dat, je*

[5] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014, s 115.
[6] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 86.

důsledná ochrana zpracovávaných osobních údajů, vzhledem k možným následkům v případě jejich zneužití, snad ještě významnější než u subjektů soukromoprávní sféry"[7].

1.1. Právní úprava

1.1.1 Evropská právní úprava

V rámci Evropského společenství bychom hledali regulaci výše uvedené problematiky na několika místech. Elementárním pramenem je Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat. Kromě toho, že tento dokument vymezoval základní pojmosloví jako osobní údaj, subjekt údajů, automatizovaný soubor dat, automatizované zpracování nebo správce souborů, tak především poskytuje garance v oblasti ochrany dat všem subjektům údajů[8]. Působnost Úmluvy 108 je stanovena v čl. 3, který ukládá povinnost smluvních států jejího uplatnění na automatizované soubory osobních údajů a jejich automatizované zpracování ve veřejném a soukromém sektoru. Úmluva 108 je doplněna dodatkovým protokolem Rady Evropy z 8. listopadu 2001 č. 181 k úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice[9]. Dodatkový protokol je reakcí na technologický postup a komplikace vyvstávající v souvislosti s předáváním informací[10]. Významnost ochrany osobních údajů potvrzuje i reflexe této agendy ve Smlouvě o fungování Evropské unie (TFEU) zaručující každému právo na ochranu těch údajů, které se ho týkají. Listina základních práv Evropské unie pak de facto přiznává ochraně osobních údajů statut základního práva. Na komunitární úrovni je potřeba zmínit směrnici Evropského parlamentu a Rady č. 95/46/ES, jejímž účelem je kromě ochrany soukromí v souvislosti se zpracováním dat také harmonizace vnitrostátní legislativy jednotlivých států EU[11].

1.1.2 Česká právní úprava

V české legislativě zaštiťuje ochranu osobních údajů na ústavní úrovni Listina základních práv a svobod, a to konkrétně v čl. 7 odst. 1, který zaručuje nedotknutelnost soukromí osob. Ochrana před neoprávněným zasahováním do soukromého a rodinného života či neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě, je pak zakotvena v čl. 10 odst. 2, resp. 3 Listiny. Na zákonné úrovni je pak klíčový zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který vychází do značné míry z Úmluvy 108. Tato

[7] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. K dodržování povinnosti přijmout a provést bezpečnostní opatření k ochraně osobních údajů ve veřejnoprávní sféře [online]. uoou.cz, 21. března 2013 [cit. 12. března 2019]. Dostupné na <https://www.uoou.cz/k-dodrzovani-povinnosti-prijmout-a-provest-bezpecnosti-opatreni-k-ochrane-osobnich-udaju-ve-verejnopravni-sfere/d-1597>.
[8] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 44.
[9] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 34.
[10] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 45.
[11] Tamtéž.

norma stanovila sankce za spáchané přestupky podle tohoto zákona, ale především zřídila úřad pro ochranu osobních údajů (dále jen Úřad). Úřad představuje dozorový orgán, jehož činnost spočívá zejména v dozorové, legislativní a rozhodovací činnosti. Zároveň je ústředním správním úřadem pro oblast ochrany osobních údajů. Je vhodné ovšem poznamenat, že Český telekomunikační úřad, zřízený zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, je ústředním správním orgánem vykonávajícím státní správu ve věcech stanovených tímto zákonem. Jednou z nich je ochrana osobních údajů ve spojení s elektronickými komunikacemi. Činnost ČTÚ pak mj. spočívá v přispívání k zajištění vysoké úrovně ochrany osobních údajů a soukromí. K tomuto vychází také ze ZoOÚ[12]. V § 87 odst. 3 je však přímo dána působnost Úřadu ve věcech dozoru nad ochranou osobních údajů podle ZEK.

1.2. Principy zpracování a ochrany osobních údajů

Principy vyplývají z mezinárodních pramenů, a to konkrétně z Úmluvy 108. Ta ve svém čl. 4 ukládá povinnost všem smluvním stranám provést nutná opatření, která uvedou v platnost tyto základní zásady. Právě ZoOÚ představuje takové opatření, které tyto principy provádí do českého právního řádu.

1.2.1 Princip legality

Tento princip, který zakotvuje Úmluva 108 v čl. 5 bodě a), se vztahuje na zpracování a způsob, jakým byly osobní údaje získány. K obojímu musí docházet poctivě a současně musí absentovat jakýkoliv rozpor se zákonem. ZoOÚ jej promítá v ust. § 5 odst. 1 písm. c), ve kterém je stanoven požadavek souladu se zákonem v případě nabytí osobních údajů. Princip legality je dále doplněn v ust. § 5 odst. 3, který ukládá povinnost dbát práva na ochranu soukromého a osobního života subjektu údajů v případě zpracování na základě zvláštního zákona. Těmito mohou být například zákon č. 154/1994 Sb., o Bezpečnostní informační službě nebo zákon č. 289/2005 Sb., o Vojenském zpravodajství. S přihlédnutím k povaze těchto předpisů a jejich účelu, lze dovodit odlišný režim co do práv a povinností v souvislosti se zpracováváním údajů. Přesto je však vždy potřeba zohlednit § 5 odst. 3 ZoOÚ a nelze bezmezně ignorovat právo na ochranu soukromého a osobního života.

Dalším aspektem legality je kritérium přesnosti dat, které je vyžadováno. Atribut přesnosti lze vyjádřit ve dvou rovinách. Zaprvé správnost osobních údajů bez gramatických či jiných chyb vzniklých přepisem. Druhá rovina pak představuje faktickou nepřesnost, kdy je například vedena v registru dlužníků osoba, která reálně není dlužníkem[13]. Je však třeba uvést, že povinnost

[12] VANÍČEK, Zdeněk a kol. *Zákon o elektronických komunikacích: komentář.* 2. vydání. Praha: Linde Praha, 2014, s. 95.
[13] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář.* V Praze: C.H. Beck, 2012, s. 112.

zpracovávat přesné údaje není bezmezná, neboť nepřesnosti můžou nastat i jinak, než ze správcova přičinění. V takovém případě nelze dovozovat správcovu odpovědnost, nýbrž je žádoucí pravidelná aktualizace v případě nezbytnosti vzhledem k účelu zpracování[14].

Se zásadou legality je úzce spjato pravidlo důvodu zpracování[15]. Každý správce či zpracovatel může získat nebo zpracovávat osobní data pouze se souhlasem subjektu údajů nebo na základě jiného důvodu uvedeného v taxativním výčtu v § 5 odst. 2 písm. a) až g). Právní tituly budou přiblíženy více v samostatné části.

1.2.2 Princip omezení účelem a přiměřenosti

Oba tyto principy jsou stanoveny v čl. 5 písm. b) a c) Úmluvy 108. V domácí úpravě bychom našli jejich vyjádření v § 5 odst. 1 písm. d) ZoOÚ, který umožňuje shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Smyslem tohoto ustanovení je přiměřené zpracování osobních údajů, které nepřesahuje míru stanovenou účelem zpracovaní[16]. Jak vidno, zákonodárce vtěsnal obě zásady do jednoho bodu, přesto je však pohlížet na tyto z obou hledisek.

Prvním rozměrem je shromažďování osobních údajů pro stanovený účel, k jehož stanovení dochází před samotným shromažďováním[17]. Zároveň by spolu se stanovením účelu měl správce vytyčit rozsah osobních údajů, který bude shromažďován, a to z důvodu následného zkoumání přiměřenosti rozsahu a stanoveného účelu zpracování. V případě shromažďování osobních údajů státem a jeho orgány bude rozsah osobních údajů vyplývat ze zákona[18]. Ke každému určenému účelu bude odpovídat jiný rozsah nezbytných osobních údajů[19]. Nezbytnost rozsahu osobních údajů definoval Úřad ve své rozhodovací činnosti takto: *"Jednou ze základních povinností správce osobních údajů je dle § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. povinnost shromažďovat osobní údaje odpovídající* ***pouze stanovenému účelu*** *a* ***v rozsahu nezbytném pro naplnění stanoveného účelu****. Toto ustanovení zákona je přitom dle názoru správního orgánu nutno vykládat tak, že je-li z hlediska stanoveného účelu příslušný osobní údaj nadbytečný, dochází vždy k porušení této povinnosti."*[20]

Druhým rozměrem pak rozumíme zákaz zpracovávání osobních údajů k rozdílnému účelu, než pro který byly sdruženy[21]. Jako příklad lze uvést situaci, kdy pojišťovna disponuje osobními údaji svého klienta, pro účely případného plnění smlouvy. Součástí těchto budou i kontaktní údaje.

---

[14] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 112.
[15] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 10.
[16] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 115.
[17] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 11.
[18] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 116.
[19] Tamtéž.
[20] ÚŘAD PRO OCHRANU OSOBNÁCH ÚDAJŮ. *K rozsahu osobních údajů shromažďovaných subjektem veřejné správy* [online] uoou.cz, 13. listopadu 2013 [cit. 12. března 2019] Dostupné z: <https://www.uoou.cz/k-nbsp-rozsahu-osobnich-udaju-shromazdovanych-subjektem-verejne-spravy/d-5519/p1=1099>.
[21] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008, s. 41.

Jestliže ovšem takový klient neposkytnul souhlas se zpracováním osobních údajů pro marketingový účel, nemůže pojišťovny použít sdružené kontaktní údaje pro zasílání reklamních nabídek. Takovou situaci si už jde hůře představit ve veřejném právu, ale jako příklad lze uvést obec, která by rozesílala pozvánky na události pořádané na svém území za účelem zvýšení informovanosti a tím by podpořila potenciální nárůst zisku. Kontaktní údaje by získala z informačního systému evidence obyvatel.

Dle mého názoru působí tyto zásady prevenčně, neboť se lze ztotožnit s komentářovou literaturou, která spatřuje smysl[22] principu omezení účelem v tendenci snižovat rozsah zpracování dat již při jejich shromáždění a po celou dobu jejich zpracování je klíčový stanovený účel.

1.2.3 Princip časového omezení

Časová omezenost je vyjádřena v čl. 5 písm. e) Úmluvy 108, když ukládá povinnost uchovávat osobní údaje pouze po dobu potřebnou pro naplnění účelu jejich shromáždění. Z takové dikce vyplývá, že není vhodné stanovit konkrétní časový úsek, po který lze uchovávat osobní data. Stejně tak lze usuzovat, že maximální doba se bude lišit v závislosti na jednotlivých účelech jejich shromáždění. ZoOÚ přenáší toto pravidlo v § 5 odst. 1 písm. e), když k základní substanci doplňuje výjimky z tohoto pravidla. A to konkrétně pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví může dojít k dalšímu uchování osobních údajů, ačkoliv pominul prvotní účel jejich zpracování. Tyto specifické situace přináší již Směrnice 95/46/ES spolu s povinností smluvních stran zajistit vhodná ochranná opatření, která zajistí řádnost takového zpracování. Český zákonodárce označil jednání, které spočívá v uchování osobních dat po dobu delší, než nezbytnou k účelu zpracování podle § 5 odst. 1 písm. e) ZoOÚ, za přestupek. Úřad tak může v mezích své rozhodovací činnosti následně uložit sankci. Vzhledem k nemalým nákladům vydaným na samotné zpracování jsou správci náchylní k oddálení likvidace dat a uchovat je pro neupřesněné budoucí potřeby[23]. Takové tendence si však lze opět spíše představit v soukromoprávní sféře, než ve veřejné správě. Samozřejmě nelze absolutně vyloučit takové snahy ani tady, ale v praxi si těžko představuji takové nezákonné uchování dat založeném na úmyslném jednání. Spíše pak půjde o nedbalostní porušení jednotlivců. Naopak v oblasti veřejné správy bude pravděpodobněji docházet k uchování dat pro účely archivnictví a spisové agendy. Zde tak bude potřeba klást důraz na ochranu soukromí a případnost anonymizace.

1.2.4 Princip nezávislého dozoru

Jednou z nejzásadnějších povinností členských států je zřízení dozorového orgánu, jehož úkolem bude kontrola dodržování předpisů v oblasti ochrany osobních údajů. Čl. 28 Směrnice

[22] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 116.
[23] Tamtéž s. 119.

95/46/ES charakterizuje tuto složku aparátu jako nezávislý orgán veřejné moci. Již výše bylo zmíněno, že tímto je Úřad zřízený ZoOÚ. V souvislosti s tím došlo ke zúžení pravomoci civilních či správních soudů ve věcech sporů týkajících se ochrany osobních údajů podle tohoto zákona, když tato pravomoc přešla právě na Úřad[24]. V souvislosti s touto otázkou je však třeba vymezit situaci, kdy nastal soukromoprávní spor mezi subjektem údajů a správcem. Věc byla judikována v rámci kompetenčního sporu, když zvláštní senát opřel své rozhodnutí o určení pravomoci okresnímu soudu o ust. § 21 ZoOÚ[25]. Předmětem sporu bylo nevydání žadatelce kopie zdravotnické dokumentace nemocnicí v Opavě. Nemocnice své jednání zdůvodnila skutečností, že požadovaná dokumentace obsahovala osobní údaje třetích osob. Z rozhodnutí vyplývá, že pakliže stěžovatel nenapadá postup správce osobních údajů nebo mu nejde o výkon kontrolní či dozorové pravomoci nad správcem údajů, ale požaduje vydání kopií určitých dokumentů, přísluší o této otázce rozhodovat soudu.

Právním řádem akcentována nezávislost má mít povahu především funkční nezávislosti na jiných orgánech veřejné moci včetně vlády[26]. Může dokonce nastat situace, kdy Úřad bude rozhodovat o porušení povinnosti při zpracování osobních údajů jiným ústředním úřadem. V tomto případě tak lze mít dle mého důvodně za to, že by se tento ústřední orgán nacházel ve vztahu podřízenosti vůči Úřadu. Další projevy nezávislosti spatřuje odborná veřejnost v personální a materiální samostatnosti[27].

Dozorová činnost Úřadu dále spočívá v monitoringu a vymáhání uplatňování právní úpravy, rozhoduje o stížnostech subjektů údajů, provádí šetření a kontroly vymezené nejen v ZoOÚ, ale i ve zvláštních předpisech[28].

1.2.5 Princip transparentnosti (právo na informace)

Každý subjekt údajů má právo být obeznámen se skutečnostmi týkající se zpracování jeho osobních údajů. Právu subjektu údajů odpovídá povinnost správce - informační povinnost. Maštalka dělí informační povinnost dle okamžiku jejího plnění, tedy při shromažďování osobních údajů a v průběhu jejich zpracování[29]. V prvním případě dle § 11 ZoOÚ je správce povinen seznámit subjekt údajů s účelem, rozsahem a způsobem zpracování, včetně určení okruhu osob, které k těmto budou mít přístup. To neplatí v případě, že se jedná o některou z výjimek, které zákon uvádí v § 11 odst. 3. Dle § 12 ZoOÚ pak na žádost subjektu údajů musí zpracovatel

[24] rozsudek Nejvyššího soudu ze dne 30. září 2004, sp. zn. 30 Cdo 1183/2004
[25] usnesení zvláštního senátu zřízeného podle zákona č. 131/2002 Sb., o rozhodování některých kompetenčních sporů, ze dne 17. 10. 2011, čj. Konf 11/2011-6
[26] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 6.
[27] Tamtéž.
[28] ÚŘAD PRO OCHRANU OSOBNÁCH ÚDAJŮ. *Dozorová činnost* [online] uoou.cz, 13.12.2013 [cit. 24.2.2019]. Dostupné z: <https://www.uoou.cz/dozorova-cinnost/ds-1277/p1=1277>.
[29] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008, s. 85.

informovat o skutečnostech vymezených ve druhém odstavci téže ustanovení. V takovém případě mu vzniká nárok na přiměřenou úhradu až do výše nákladů na poskytnutí informace. Pokud by se jednalo o typově obdobné žádosti o informace, kdy jsou informace zpracovávány stejným způsobem v elektronické databázi, lze stanovit v sazebníku jednotný poplatek[30]. Dovedu si představit tuto situaci právě v případě plnění informační povinnosti správních úřadů. V obou případech může povinnost splnit zpracovatel osobních údajů namísto správce.

1.2.6 Princip bezpečnosti

Zjednodušeně řečeno se dá tvrdit, že podstatou ochrany údajů je jejich bezpečné zpracování. O tomto principu bychom mohli také říct, že vágně stanovuje ráz zabezpečení dat. Vyjádření bychom hledali v § 13 ZoOÚ, který zakotvuje povinnost správce, potažmo zpracovatele, k přijetí takových bezpečnostních opatření, která zabrání neoprávněnému a nahodilému přístupu ke zpracovávaným datům, či dokonce k jejich změně, likvidaci apod. Forma bezpečnostních opatření závisí do značné míry na prostředcích a způsobech zpracování osobních údajů[31]. Teoreticky by se dalo zabezpečení rozdělit na čtyři oblasti. Personální bezpečnost spočívající v určení osob s přístupem k osobním údajům a kontroly jejich zpracování, fyzická, chcete-li objektová bezpečnost, dále pak administrativní bezpečnost, jež směřuje ke způsobu spisové a archivní činnosti a konečně pak technologická bezpečnost, do které budou spadat například informační systémy[32].

1.2.7 Princip práva na opravu a výmaz údajů

Konečně je potřeba vymezit zásadu, která souvisí s několika výše uvedenými tezemi. Přesto jsem se rozhodl ji začlenit jako samostatný princip, protože přes zmíněnou spojitost by měla plnit roli principu a minimálně při tvorbě legislativy brána na vědomí.

Konkrétní vyjádření práva na opravu či výmaz poskytuje Úmluva 108 v čl. 8 písm. c), jako jednu ze záruk, které se dostává subjektu údajů. ZoOÚ pak poskytuje tuto záruku přímo pod ochranu práv subjektu údajů v § 21 odst. 1 písm. b). Pokud má subjekt údajů podezření o možném rozporu mezi zpracováním a ochranou osobního a soukromého života, může požádat o opravu údajů či dokonce jejich vymazání, tedy likvidaci. První spojitost spatřuji s principem transparentnosti, neboť na základě jeho uplatnění si subjekt údajů může verifikovat, zda opravdu dochází ke zpracování nepřesných údajů a správci nebo zpracovateli vzniká informační povinnost. Nepřesnost údajů nás pak dostává k principu legality, neboť správnost dat je jejím žádoucím

[30] KUČEROVÁ, Alena, NONNEMANN, František. *Ochrana osobních údajů v praktických příkladech*. Praha: BOVA POLYGON, 2013, s. 92.
[31] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 19.
[32] KUČEROVÁ, Alena, NONNEMANN, František. *Ochrana osobních údajů v praktických příkladech*. Praha: BOVA POLYGON, 2013, s. 100.

atributem. Z dikce zákona dále vyplývá povinnost neprodleně odstranit závadný stav v případě jakýchkoliv nesrovnalostí. Pokud by k žádoucí aktivitě správce či zpracovatele nedošlo, je možné se obrátit na Úřad, který takový podnět vyhodnotí, případně zasáhne[33]. Je však třeba zdůraznit, že Úřad nemůže provádět žádná konkrétní opatření, která by vedla k vymazání nebo změně dat, nýbrž zahájí řízení o uložení nápravných opatření dle § 40 ZoOÚ[34].

1.3. Právo na ochranu osobních údajů proti právu na informace

Státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce jsou dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím povinnými subjekty, které mají povinnost poskytovat informace vztahující se k jejich působnosti. To však může být někdy v konfliktu s ochranou osobních údajů. Zákonná úprava neposkytuje jasné řešení a v minulosti se tato otázka stala předmětem soudního rozhodování. Obě práva, jak právo na informace, tak právo na ochranu osobních údajů řadíme mezi základní. Právo na informace navíc nabourává právo na ochranu soukromí, což je také právo garantované Listinou. V případě kolize ústavně zaručených práv dochází k jejich poměřování uplatněním principu proporcionality (srov. nálezy ÚS Pl. ÚS 4/94, Pl. ÚS 24/07 nebo Pl. ÚS 3/02).

Ve veřejné správě může mezi výše zmíněnými právy docházet ke kolizi v případech, kdy je zde požadavek k podání informací o činnosti veřejné správy. S ohledem na dikci zákona mám za to, že pokud jde o informace zahrnující údaje související s činností veřejné správy, právo na ochranu soukromí a ochranu osobních údajů ustupuje právu na informace. NSS konstatoval, že *"..co do střetu práva na svobodný přístup k informacím a práva na ochranu osobních údajů Nejvyšší správní soud konstatuje, že právo na ochranu osobních údajů není neomezené, když čl. 10 odst. 3 Listiny základních práv a svobod má každý právo na ochranu před neoprávněným shromažďováním, zveřejňováním a jiným zneužíváním údajů o své osobě. Stanoví-li pak zákon o svobodném přístupu k informacím povinnost poskytnout některé osobní údaje (jinak chráněné zákonem o ochraně osobních údajů), jedná se o jejich poskytnutí podle práva, tj. o poskytnutí oprávněné"*[35]. Jako odlišnou situaci vnímám žádost o informace týkající se odměn zaměstnanců veřejné správy. Tuto argumentaci opírám především o rozsudek rozšířeného senátu Nejvyššího správního soudu ze dne 22. 10. 2014, č.j. 8 As 55/2012-62, který kromě sjednocení dosavadní judikatury uvádí, že *"povinný subjekt neposkytne informace o platu zaměstnance poskytovaném z veřejných prostředků jen výjimečně, pokud se tato osoba na podstatě vlastní činnosti povinného subjektu podílí jen nepřímo a nevýznamným způsobem a zároveň nevyvstávají konkrétní pochybnosti o tom, zda v souvislosti s*

[33] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 25.
[34] rozsudek Nejvyššího správního soudu ze dne 16.3.2010, čj. 1 As 93/2009-126
[35] rozsudek Nejvyššího správního soudu ze dne 27.5.2011, čj. 5 As 57/2010-79

odměňováním této osoby jsou veřejné prostředky vynakládány hospodárně." Vliv na posuzování této otázky má také zákon č. 89/2012 Sb., občanský zákoník, který přinesl změny v oblasti ochrany soukromí a tyto by se měly promítnout do testu proporcionality[36]. V tomto případě bude záležet na konkrétních okolnostech, na základě kterých bude upozaděno buď právo na informace nebo právo a ochranu osobních údajů.

1.4. Projevy ochrany osobních údajů

Vzhledem ke skutečnosti, že výše popsané principy jsou v podstatě zákonné záruky pro subjekty údajů, i tyto se dají považovat za projev ochrany osobních údajů. Cílem této kapitoly je však blíže analyzovat zákonnost zpracování dat a posléze prostředky, kterými disponuje Úřad v případě zákonného nesouladu. Tato podkapitola tak bude obsahovat dvě části - první bude zahrnovat právní důvod zpracování osobních údajů, načež druhá výkon dozorové činnosti Úřadu.

1.4.1 Právní titul pro zpracování osobních údajů

Někdy se užívá také pojem právní důvod zpracování, představuje v nejužším slova smyslu legalitu zpracování osobních údajů[37]. Proto v případě, kdy zde takový titul absentuje, nelze považovat zpracování osobních údajů za zákonné. Seznam titulů je veden v § 5 odst. 2 ZoOÚ a je seznamem taxativním.

Protože zpracováním osobních údajů rozumíme zásah do soukromí jednotlivce, mělo by k němu primárně docházet tehdy, když s tím subjekt údajů souhlasí[38]. Souhlas se zpracováním je tak základním titulem. Souhlasem rozumíme právní jednání, jehož vlastnosti odpovídají § 4 písm. n) ZoOÚ. Především je projevem vůle subjektu údajů, který je svobodný a vědomý, přičemž tímto se dovoluje zpracovávat konkrétní osobní údaje. Požadavek konkrétnosti lze dovodit z ust. § 5 odst. 4 ZoOÚ, který je rozšířen o informovanost subjektu údajů pro jaký účel dochází ke zpracování, kdo je správcem a také dobu zpracování. Pokud nebude sdělen účel zpracování, osoba správce a v některých případech kategorie osobních údajů, které vzniknou až v průběhu zpracování a k jejichž zpracování rovněž bude docházet ze strany správce, postrádá takový souhlas platnost a legitimitu[39]. Ze stejného ustanovení vychází povinnost správce schopnost prokázat takový souhlas po celou dobu zpracování. Historicky obsahoval ZoOÚ ustanovení o možném odvolání poskytnutého souhlasu. Nicméně z důvodu komplikaci, které v praxi nastávaly, se tato možnost z právní úpravy vytratila. Aspoň do doby účinnost zák. č. 89/2012 Sb., nového občanského zákoníku, který

[36] KRECHT, Jaroslav. Právo na informace a ochrana soukromí. *Právní rozhledy*, 2016, roč. 14, č. 23-24, s. 845.
[37] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008, s. 46.
[38] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 99.
[39] NONNEMANN, František. Náležitosti souhlasu se zpracováním osobních údajů. *Právní rozhledy*, 2011, roč. 142, č. 19, s. 526.

obsahuje úpravu právních jednání, čímž souhlas se zpracováním osobních údajů bezesporu je. Odvolání souhlasu tak možné je, ovšem vždy je potřeba u takového právního jednání posoudit otázku souladu odvolání s dobrými mravy[40]. V oblasti veřejné správy bude vyžadován souhlas se zpracováním osobních údajů také. S tímto lze nastínit stav, kdy obec zveřejňuje uzavřené smlouvy s fyzickými osobami na svých webových stránkách za předpokladu, že tyto obsahuji jejich údaje a zároveň nejde o plnění zákonné povinnosti, jak bude popsáno níže. V případě absence právního předpisu přímo a výslovně umožňující či dokonce nařizující zveřejnění smluvní dokumentace, je předem poskytnutý výslovný souhlas nepostradatelný[41]. O jinou situaci půjde ve výběrovém řízení podle § 9 odst. 5 zákona č. 312/2002 Sb., o úřednících územních samosprávných celků, dle kterého mají všichni uchazeči právo nahlédnout do závěrečné zprávy výběrové komise, která může obsahovat i osobní údaje dalších uchazečů. Na rozdíl od prvního případu zde není vyžadován souhlas se zpřístupněním, protože zde správce plní zákonnou povinnost[42].

Pokud je však právo jednotlivce na soukromí převáženo legitimním zájmem jiného subjektu nebo vyváženo jiným základním právem, přicházejí v úvahu sekundární právní tituly[43]. Jedním z nich je takové zpracování, které nezbytné pro dodržení právní povinnosti správce dle § 5 odst. 2 písm. a) ZoOÚ. Právě tento titul zpracování bude typický v oblasti veřejné správy, když vzpomeneme, že veřejnou moc je možno vykonávat pouze na základě a v mezích zákona[44]. Maštalka tak na základě tohoto zmiňuje, že jiný případný titul zpracování osobních údajů by znamenal nepochopení zákona nebo dokonce překročení pravomoci a působnosti. S tímto závěrem se nelze bez dalšího ztotožnit. Již při zkoumání primárního právního titulu byl uveden příklad, kdy například i obec bude potřebovat k zákonnosti zpracování souhlas. Stejně tak si lze představit zpracování dat, ke kterému v rámci veřejné správy dochází na základě plnění smluvní povinnosti (pozn. tento právní titul bude zpracován dál níže). Zákonné zmocnění musí být vždy zcela dostatečně určité, tedy příslušný zvláštní zákon stanoví správci údajů povinnost či oprávnění, které by nešlo splnit bez zpracování údajů nebo dokonce zpracování přímo výslovně ukládá[45].

Další scénář, který může nastat, a bezesporu k němu nebude docházet zřídka, je zpracování v souvislosti se smluvní agendou. Ust. § 5 odst. 2 ZoOÚ vymezuje rozsah oprávnění poměrně široce, když kromě zpracování nezbytného pro plnění smlouvy dopadá tento titul i na kontraktační proces včetně následných změn. Je však podstatné upozornit, že tento právní titul se týká pouze

[40] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 99.
[41] KUČEROVÁ, Alena, NONNEMANN, František. *Ochrana osobních údajů v praktických příkladech*. Praha: BOVA POLYGON, 2013, s. 62.
[42] Tamtéž, s. 64.
[43] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 99.
[44] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008, s. 54.
[45] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 99.

subjektu údajů, který je zároveň smluvní stranou[46]. Pokud smluvní dokumentace obsahuje údaje i třetích osob, například subdodavatelů, mám za to, že pakliže by i tyto osoby dostály statusu subjektu údajů, je zapotřebí k legálnímu zpracování takových údajů jiného právního titulu. Tento právní titul je možným odrazem obecného pravidla pro sjednávání smluv, když je legitimní seznámit se se všemi údaji a významnými informacemi potřebných k rozhodnutí o uzavření smlouvy[47]. Ve veřejné správě pak lze uvést jako příklad zpracování osobních údajů nezbytných pro plnění smlouvy v případě nájmu obecních bytů. V tomto případě by bylo vhodné zohlednit doporučení veřejného ochránce práv, který označil požadavek žadatele o obecní byt na informaci o státním občanství, pohlaví, rasu a etnickou příslušnost za diskriminační kritéria porušující zásadu rovného zacházení při přístupu k bydlení[48].

Následuje právní titul v § 5 odst. 2 písm. c), který zakotvuje oprávnění zpracovávat data, pokud to vyžaduje ochrana životně důležitých zájmů subjektu údajů. Tento musí být nahrazen souhlasem s dalším zpracováním v okamžiku, kdy jej subjekt údajů může udělit. Z takového vyjádření jasně vyplývá provizornost zpracování. Dle komentářové literatury nedochází k časté aplikaci tohoto titulu v praxi a jako modelovou situaci uvádí stav nezvěstnosti subjektu údajů[49].

V dnešní době dochází ke zveřejňování osobních údajů také z mnoha legitimních důvodů. ZoOÚ obsahuje výčet v § 4 písm. i) určení, co se rozumí zveřejněným údajem. Jsou jimi data zpřístupněná zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu. K dalšímu zpracování dat tak může docházet ve spojení s § 5 odst. 2 písm. d) ZoOÚ. Kromě skutečnosti, že zveřejnění údajů musí být oprávněné, vždy musí mít správce na paměti ochranu soukromého a osobního života subjektu údajů. Za oprávněně zveřejněné osobní údaje nelze považovat např. osobní údaje ve správním spise, neveřejnou část živnostenského rejstříku nebo centrální evidence závětí. V těchto případech jde právo se s nimi seznámit ruku v ruce s právním zájmem ze strany nahlížejícího[50]. ZoOÚ stanovuje tři výjimky, na které nebude možné bez dalšího uplatnit tento právní titul. Zaprvé jsou to citlivé údaje, pokud k jejich zveřejnění nedošlo samotným subjektem údajů v souladu s § 9 písm. g). Dále pak zpracování rodného čísla, jehož podmínky zpracování upravuje zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech. A konečně pak zpracování z marketingových účelů podle § 5 odst. 5 ZoOÚ. Za zveřejněné údaje půjde také v případě zveřejnění na žádost oprávněných osob. K tomu může dojít právě na základě ZoEO. Poskytnutí osobních údajů o osobách, které mají nahlášený trvalý pobyt

[46] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008, s. 53.
[47] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 139.
[48] Doporučení veřejného ochránce práv k naplňování práva na rovné zacházení s žadateli o pronájem obecního bytu ze dne 9.3.2010, sp. zn. 22/2010/DIS/AHŘ, dostupné na https://www.ochrance.cz/fileadmin/user_upload/DISKRIMINACE/Doporuceni/Obecni_byty.pdf
[49] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 141.
[50] Tamtéž, s. 142.

na adrese domu s vymezenými bytovými jednotkami vlastníkům jednotlivých bytových jednotek a v relevantním rozsahu je legitimní i z pohledu ochrany osobních údajů[51].

Kromě ochrany subjektu údajů je také namístě ochrana správce, leč za současného respektu práv subjektu údajů k ochraně jeho soukromého a osobního života. Kromě správce přisuzuje § 5 odst. 2 písm. e) záštitu také příjemci osobních údajů a jiných dotčených osob. V praxi lze poukázat na uplatnění tohoto titulu při užití kamerových záznamů. Zachycení vizuální podoby lze považovat za osobní údaj ve smyslu ZoOÚ. Tímto způsobem také dochází ke zpracování osobních údajů v rámci veřejné správy, když budovy úřadů disponují kamerovými zařízeními v rámci bezpečnostních opatření. Takové zpracování subsumujeme pod písm. e), neboť ani v případě informování subjektu o skutečnosti, že je objekt monitorován, nelze považovat za udělení souhlasu konkludentním způsobem[52]. Na základě judikatury lze uvést, že ustanovení dopadá i na představitele veřejných institucí, přičemž v případě posuzování, zda se jedná o veřejnou či soukromou instituci, je potřeba zkoumat, zda převahují soukromoprávní či veřejnoprávní aspekty[53].

Z pohledu veřejné správy se dostáváme k relevantnímu právnímu titulu, který umožňuje poskytnout osobní údaje o veřejně činné osobě, funkcionáři nebo zaměstnanci veřejné správy i bez jejich souhlasu. Dle § 5 odst. 2 písm. f) ZoOÚ je povaha těchto údajů stanovena tak, že tyto musí souviset s veřejnou nebo úřední činností subjektu údajů, či o jeho funkčním nebo pracovním nasazení. Co se týče veřejné činnosti, tak její projevy lze spatřovat v různých oblastech jako politika, kultura nebo sport[54]. V otázce zveřejnění "mimořádné odměny" se v minulosti vyjádřil NSS, který došel k závěru, že i tento údaj může být za určitých okolností zveřejněn, resp. zpracováván i jinou osobou než správcem. To však zpochybňuje Furek[55], který se domnívá, že NSS nedostatečně odůvodnil své rozhodnutí. Takový závěr však ve světle aktuální judikatury[56] již nemůže obstát a ve spojení se zákonem o svobodném přístupu k informacím lze zveřejnit i údaj zahrnující mimořádnou odměnu.

Posledním důvodem zpracování aprobovaným zákonem, je zpracování pro účely archivnictví podle zvláštního zákona. Jedná se tak o zbytkovou oblast. Komentářové znění však považuje toto ustanovení za obsolentní, protože totéž stanovuje zákon o archivnictví[57]. Ačkoliv

[51] GABRIŠOVÁ, Veronika. Poskytování osobních údajů z evidence obyvatel. *Právní rozhledy*, 2013, roč. 21, č. 10, s. 364.
[52] KUČEROVÁ, Alena, NONNEMANN, František. *Ochrana osobních údajů v praktických příkladech*. Praha: BOVA POLYGON, 2013, s. 57.
[53] rozhodnutí Nejvyššího správního soudu ze dne 29.5.2008, čj. 8 As 57/2006-67.
[54] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 148.
[55] FUREK, Adam, Informace o platech pracovníků veřejné správy. *Právní rozhledy*, 2011, roč. 19, č. 17, s. 626.
[56] rozsudek rozšířeného senátu Nejvyššího správního soudu ze dne 22. 10. 2014, č.j. 8 As 55/2012-62
[57] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 153.

jeho autoři doporučují jeho zrušení v rámci novelizace z důvodu přehlednosti, ZoOÚ jej obsahuje i k dnešnímu dni v § 5 odst. 2 písm. g).

1.4.2 Činnost Úřadu

Již v předchozích kapitolách byl zmíněn Úřad, jakožto ústřední orgán vykonávající dozor ve věcech ochrany osobních údajů. Cílem této kapitoly není kompletní rozbor tohoto orgánu, nýbrž popsání jeho aktivity. Ačkoliv se nebude jednat o primární účel, přesto by měl Úřad vystupovat v roli asistenta zákonodárce a napomáhat formování legislativy[58]. Tím určitě není myšleno, aby mu byla přisouzena zákonodárná moc v tomto rozsahu, ale svou autoritou a odborností by měl spolupracovat s orgány ovlivňující legislativní proces[59].

Pro konání Úřadu je klíčový ZoOÚ, který v hlavě VI. stanovuje rozsah jeho činnosti. Mimo jiné Úřad vede registr zpracování osobních údajů. Jedná se o veřejný rejstřík, do kterého jsou zapisovány informace vymezené v § 16 odst. 2 ZoOÚ. Tímto zároveň správce plní svou zákonnou oznamovací povinnost. Subjekt údajů může po celou dobu zpracování kontrolovat jeho řádnost a v souladu se zásadou transparentnosti je každý správce povinen poskytnout řádnou kooperaci. V případě nesrovnalostí nebo i jen jejich podezření, má subjekt údajů právo v souladu s § 21 ZoOÚ na vysvětlení. Pakliže se potvrdí závadný stav, může subjekt vyžadovat jeho odstranění, ke kterému dojde blokováním dat, provedením oprav, doplněním či v krajním případě i likvidací osobních údajů. Volba řešení závadného stavu je plně v kompetenci subjektu údajů[60]. V případě, že nedojde ke kladnému vyřízení žádosti subjektu údajů, může uplatnit v souladu s § 21 odst. 1 písm. c) právo podat podnět Úřadu o možném rozporném zpracování osobních údajů. Zákon ovšem nepodmiňuje podnět Úřadu adresováním žádosti o nápravu či vysvětlení správci nebo zpracovateli, takže subjekt údajů jej může podat spolu s žádostí nebo dokonce i bez ní[61]. Podnět pak může vést k zahájení správního řízení ve spojení se zákonem č. 500/2004 Sb., správním řádem, které je plně v kompetenci Úřadu[62]. V případě, že Úřad vykonává svou dozorovou činnost ve smyslu § 21 odst. 1 písm. a), vykonává tuto formou kontroly s aplikací zákona č. 255/2012 Sb., kontrolního řádu (dále jen "Kontrolní řád")[63]. I v tomto případě, pokud by shledal porušení zákona, zahájí o tomto správní řízení. Výsledkem správního řízení může být uložení sankce v souladu se ZoOÚ nebo uložení satisfakčního opatření. Co se týká sankcí, tak ZoOÚ umožňuje uložení peněžitého trestu až do výše pěti milionů korun ve věcech přestupků fyzických osob nepodnikajících, které zastávají roli správce a deseti milionů korun v případě spáchaní přestupků u právnické osoby nebo fyzické

[58] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008, s. 174.
[59] Tamtéž.
[60] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 126.
[61] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012, s. 281.
[62] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018, s. 129.
[63] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008, s. 176.

osoby podnikatele. Nutno podotknout, že tato hranice je stanovena pro nejzávažnější porušení, kterými jsou dle zákona ohrožení soukromého života většího počtu osob nebo došlo k porušení povinnost v souvislosti se zpracováním osobních údajů. Co se týče satisfakčních opatření, tak mezi tyto bude patřit zdržení se škodlivého jednání, vydání bezdůvodného obohacení subjektu, likvidace informace nebo zamezení přístupu k informacím v průběhu sporu[64].

[64] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008.

2. Nařízení Evropského parlamentu a Rady (EU) 2016/679

Jak již bylo předestřeno v úvodu, část práce bude věnována rozboru nařízení o ochraně osobních údajů. Co je důvodem přijetí této legislativy, terminologie a konkrétní novinky s sebou přinášející, které jsme doposud neznali. Protože budu vycházet v této kapitole především z právních předpisů, je vhodné zmínit specifikum GDPR. Tímto jsou recitály, které předchází samotnému textu nařízení a je možné je přirovnat k preambuli. Při aplikaci nařízení je vhodné s recitály pracovat, neboť do určité míry suplují důvodovou zprávu předpisu.

2.1. Požadavek GDPR s ohledem na dosavadní legislativu

Přestože cílem práce není zkoumat nezbytnost Nařízení, objasnění potřeby tohoto předpisu má relevanci pro jeho správný výklad a především žádanou aplikaci. Jak již bylo zmíněno, ochrana fyzických osob v souvislosti se zpracováním osobních údajů má statut základního práva. Výkon této ochrany však může být poněkud obtížný s přihlédnutím k dosaženému technologickému rozvoji. V době internetového obchodování, elektronického bankovnictví nebo enormního rozvoje sociálních sítí je potřeba zohlednit rozsáhlost sběru a zpracování osobních údajů, monitoring a profilování osob apod.[65] Je třeba dodat, že i míra globální integrace přidává na intenzitě těchto činností.

V rámci EU se uplatňovala ochrana osobních údajů již od konce minulého století, když byla účinná Směrnice 95/46/ES. Kromě toho, že již přestala odpovídat současným trendům, tak především jí nebylo dosaženo požadované míry sjednocení právní úpravy ve všech členských státech.[66] Jednotlivé země měly uzákoněnou vlastní legislativu pro tuto oblast. Tímto tak absentoval jednotný standard. GDPR je proto nařízením, a tedy musí být aplikováno přednostně před právní úpravou všech států[67]. Kromě všech členských států se Nařízení uplatní také na Islandu, v Norsku a Lichtenštejnsku[68]. GDPR de facto nahrazuje vnitrostátní normu[69]. Tuzemská právní úprava byla doposud zajištěna ZoOÚ, nicméně od 24. dubna 2019 nabyl účinnosti zákon č. 110/2019 Sb., o zpracování osobních údajů, který je plně kompatibilní s Nařízením. Z důvodové zprávy tohoto adaptačního zákona plyne, že "*hlavním cílem předloženého návrhu zákona a novelizace právních předpisů je tedy provést implementaci shora uvedeného sekundárního předpisu Evropské unie* (pozn. autora: směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016, o ochraně fyzických osob

[65] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 29.
[66] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017, s. 28.
[67] Soudní dvůr: Rozhodnutí ze dne 15. července 1964, *Flaminio Costa proti E.N.E.L., věc 6/64 Sb. rozh.*
[68] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 30.
[69] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017, s. 16.

v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV), *včetně adaptace na nařízení, zajistit soulad vnitrostátní právní úpravy s těmito předpisy a tím splnit povinnost, která plyne České republice z členství v Evropské unii"*[70].

2.2. Cíle nařízení

Již z názvu podkapitoly je zřejmé, co bude jejím obsahem. Zamýšlené cíle jsou vyjádřeny hned v čl. 1 GDPR. Těmito je ochrana fyzických osob v souvislosti se zpracováním osobních údajů a zároveň zabezpečit, aby tato ochrana neomezila či dokonce znemožnila volný pohyb osobních údajů v EU. Pohyb osobních údajů v rámci EU mezi jednotlivými orgány bude častý v případech trestněprávních věcí nebo justiční spolupráce. V oblasti veřejné správy k němu bude docházet minimálně, jestli vůbec. Nařízení přiznává fyzickým osobám práva, kterými můžou kontrolovat využití svých osobních údajů a navíc stanovuje okolnosti, za kterých je možné osobní údaje zpracovávat. S tím souvisí také zavedení povinností těm, kdo osobní údaje zpracovávají[71].

2.2.1 Ochrana fyzických osob

Skutečnost, že GDPR poskytuje ochranu fyzickým osobám vyplývá implicitně z Nařízení. Ze 14 recitálu také vyplývá, že zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby není chráněno nespadá do působnosti Nařízení. V souvislosti s těmito dvěma okolnostmi je však potřeba zdůraznit, že fyzické osoby ve vztahu k právnické osobě požívají ochranu v souladu s Nařízením. Ať už jsou to zaměstnanci či osoby zastupující právnickou osobu. Nulíček považuje i služební email zaměstnance, který může být veřejně dostupný jako kontaktní údaj na webu, za osobní údaj a přisuzuje mu tak řádnou ochranu osobních údajů[72]. Zaměstnanci veřejné správy jsou běžně uvedení na internetových stránkách státních institucí včetně kontaktních informací. Zveřejnění těchto informací má své opodstatnění a účelem je možnost kontaktovat tyto osoby ve věcech jejich agendy. Dle mého i tito zaměstnanci požívají ochrany v případě, že zveřejněné informace jsou použity v rozporu s účelem jejich zveřejnění. Pokud by tak například byli kontaktováni v rámci marketingové činnosti, jednalo by se o zneužití osobních údajů.

Praktický problém nastává u otázky, zda se GDPR vztahuje i na fyzické osoby podnikající a osoby vykonávající svobodná povolání. Dle ÚS nelze přisuzovat fyzickým osobám, které jsou

[70] Důvodová zpráva k zákonu č. 110/2019 Sb., o zpracování osobních údajů. Dostupná na: < https://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=138&CT1=0>.
[71] NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 60.
[72] Tamtéž, s. 62.

podnikateli, ochranu osobních údajů dle zákona o ochraně osobních údajů, neboť z hlediska jejich statusu je nutno za rozlišovací kritérium považovat jejich podnikatelskou činnost[73]. Úřad ve svém stanovisku dospěl k závěru že "*údaje týkající se určitých nebo určitelných osob, živnostníků či příslušníků svobodných povolání, jsou osobními údaji ve smyslu zákona o ochraně osobních údajů. Jejich zpracování ve formě vedení veřejně dostupných registrů je sice upraveno řadou zvláštních zákonů, ovšem zákon o ochraně osobních údajů jako obecný předpis je nutno rovněž aplikovat, a to v těch částech daného zpracování, které zvláštními předpisy upraveny nejsou.*[74]" Svou argumentaci opírá o rozsudek ESLP ze dne 16. Amann proti Švýcarsku (stížnost č. 27798/95), ze dne 16. 2. 2000 či Rozsudek SDEU ve spojených věcech Österreichischer Rundfunk a další (C-465/00, C-38/01 a C-139/01), ze dne 20. května 2003. Kromě toho, že výše zmínění ústavní nález lze považovat za judikatorně překonaný, tak především není v souladu s GDPR. To může praktický dopad s ohledem na evidenci v živnostenském rejstříku. Tento informační systém veřejné správy, jehož správcem je Ministerstvo průmyslu a obchodu ČR obsahuje osobní údaje fyzických podnikajících osob. Přestože jsou provozovateli jednotlivé obecní živnostenské úřady, odpovědnost za zpracování nese vždycky MPO. Otázkou je, zda může být takový zpracovatel sankcionován v případě, že se dopustil porušení zabezpečení osobních údajů. S přihlédnutím k nedávnému legislativní postupu, ve kterém budou spadat obce a kraje do režimu, dle kterého nebudou moct být sankcionovány[75], dovozuji stejný postup i v tomto případě.

2.2.2 Volný pohyb osobních údajů

Jedna z výhod EU spočívá v integraci, která se projevuje v několika směrech. Jedním z těchto směrů je právě umožnění volného pohybu osobních údajů mezi správci v různých členských státech, což odpovídá ideje vnitřního trhu a volného pohybu zboží[76]. Pakliže dochází k předávání osobních údajů mimo země EU, je zde požadavek na zajištění institucionální ochrany při předávání. Tento požadavek pramení z recitálu 101. K takovému pohybu údajů může dojít předáním založeném na rozhodnutí o odpovídající ochraně. Z čl. 45 GDPR vyplývá, že Komise vydala rozhodnutí, kterými stanovuje, která třetí země či mezinárodní organizace zajišťuje odpovídající úroveň ochrany zpracování osobních údajů. Pokud absentuje rozhodnutí Komise podle čl. 45, lze předávat údaje proti záruce správce či zpracovatele a také musí být k dispozici vymahatelná práva subjektu údajů a možnost účinně se jich domáhat[77]. Poslední alternativou jsou tzv. specifické situace, jejichž taxativní výčet je uveden v čl. 49 odst. 1. Podle třetího odstavce na

[73] Nález Ústavního soudu ze dne 9. března 2004, sp. zn. Pl. ÚS 38/02.
[74] Stanovisko Úřadu č. 3/2011 z listopadu 2011 k ochraně osobních údajů podnikajících fyzických osob. Dostupné na: <https://www.uoou.cz/files/stanovisko_2011_3.pdf>
[75] Přiblíženo dále ve 3. kapitole.
[76] NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 64.
[77] Čl. 46 GDPR

činnost prováděnou orgány veřejné moci při výkonu jejich pravomocí se bude aplikovat katalog výjimek pouze v rozsahu čl. 49 odst. 1 pododstavec písm. d) až g), neboť zbylé výjimky se na tuto situaci nebudou vztahovat.

2.3. Vymezení pojmů

Samotné Nařízení obsahuje článek, ve kterém vymezuje a definuje pojmy dále užívané. Nutno dodat, že z velké části se nejedná o žádné novoty či dosud neznámé pojmy. I proto budou v této podkapitole rozebrány pouze ty, které nebyly prozatím vymezeny ZoOÚ a zavádí je tak až Nařízení, případně rozšiřuje již existující koncepty. Zároveň níže budou analyzovány pouze nejrelevantnější pojmy s ohledem na cíle této práce.

Začněme samotným osobním údajem, u kterého došlo k rozšíření jeho významu. Ačkoliv již v minulosti bylo judikováno SDEU, že dynamická IP adresa se rovněž považuje za osobní údaj[78], Nařízení nově považuje za osobní údaj také lokační údaje či síťový identifikátor. Lze tak spatřovat snahu vykládat tento pojem ještě extenzivněji než doposud.

První novinkou je tzv. omezení zpracování osobních údajů. Podstatou je označení osobních údajů za účelem omezení jejich zpracování v budoucnu. Návod na způsoby omezení představuje recitál 67, dle kterého lze omezení zpracování docílit přesunem údaje do jiného systému zpracování, zamezením přístupu osobních údajů uživatelům nebo dočasně odstranit informace zveřejněné na webu. V případech automatizovaného zpracování dochází k omezení technickými prostředky zajišťující zastavení dalších operací zpracování osobních údajů a také zabezpečení nemožnosti změnit údaje. Omezení zpracování úzce souvisí s čl. 18 Nařízení, které v taxativním výčtu vymezuje důvody, na základě kterých se může subjekt údajů dožadovat omezení zpracování. Jedná se o případy, kdy subjekt údajů popírá přesnost osobních údajů, odmítá jejich výmaz, odpadl původní účel zpracování a zároveň nelze prozatím odstranit z právních důvodů nebo doposud nebylo vyřízeno rozhodnutí o námitce proti zpracování. Právo na omezení zpracování konkretizuje a rozpracovává již známý pojem "blokování" osobních údajů[79]. Zjednodušeně řečeno k omezení dojde tehdy, když dochází k nezákonnému zpracování a zároveň subjekt nevyžaduje výmaz údajů a nebo dočasné pozastavení zpracování, než dojde k vyřešení sporu[80]. Ke zrušení omezení dochází neprodleně po tom, co pominou důvody jeho omezení[81]. V

[78] Soudní dvůr: Rozsudek Soudního dvora EU ze dne 19.října 2016, *Patrick Breyer proti Spolkové republice Německo*, věc C-213/15
[79] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018, s. 191.
[80] Tamtéž.
[81] NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 238.

souvislosti s omezením je třeba poznamenat povinnost vyznačení této skutečnosti v systému, ve kterém dochází ke zpracování v souladu s recitálem 67.

Novým institutem, který GDPR zavádí, je profilování. To definuje v čl. 4 bodě 4 jako jakoukoliv formu automatizovaného zpracování údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě. Touto činností dochází k utváření profilu rozborem aspektů konkrétního subjektu údajů. Těmito hledisky můžou být dle GDPR údaje o ekonomické situaci, zdravotním stavu, spolehlivosti, chování apod. Profilování je typické pro marketingové účely, kdy na základě historických nákupů je utvořen profil zákazníka a následně jsou mu nabízeny další produkty. Co se týče automatizovaného zpracování, tak o takové zpracování půjde tehdy, když dojde k využití automatizovaných prostředků či postupů k alespoň některým operacím zpracování[82]. Význam profilování se promítá v čl. 22 GDPR, který zakládá právo subjektům údajů nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, a to včetně profilování, které by mělo pro tento subjekt právní účinky nebo by se ho obdobným způsobem významně dotýkalo. Výjimky z tohoto pravidla jsou uvedeny v bodě 2 téže článku a jsou jimi nezbytnost kontraktačního procesu či plnění smlouvy, právo EU či členského státu to povoluje proti vhodným opatřením zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů a konečně pak výslovný souhlas subjektu údajů k takovému jednání.

Nařízení rozlišuje mezi i) profilováním, ii) rozhodováním založeným na profilování a iii) výhradně automatizovaným rozhodováním, včetně profilování. GDPR cílí na stav, kdy o právech a povinnostech rozhoduje výhradně algoritmus bez přispění lidského faktoru[83]. Jako možné příklady uvádí Nulíček webovou aplikaci banky, která na základě algoritmu vyhodnocuje žádost o úvěr po zjištění údajů o subjektu z rejstříků a rozhoduje o konečném poskytnutí či neposkytnutí úvěru nebo software využívaný zaměstnavatelem pro určování výše prémií na základě hodnocení výkonnosti zaměstnanců. Přestože se nabízí výhradně automatizované rozhodování v soukromé sféře, nelze čl. 22 GDPR vztahovat výlučně jen na ni. Jako příklad lze uvést praktiky úřadů Čínské lidové republiky[84], které na základě několika vstupních údajů, včetně úředních záznamů, vyhodnocují "kredit" občanů, na jehož základě pak dochází k determinaci jejich práv, jako nákup letenek, možnost úvěrování či dokonce koupě bytu. Tento proces není transparentní, takže nelze zcela vyloučit lidský faktor na konečném vyhodnocení. Stejně tak takové jednání zcela nepřiměřeně

[82] RADIČOVÁ, Zuzana, Burian, David. *Profilování ve světle nového obecného nařízení o ochraně osobních údajů (GDPR)* [online]. epravo.cz, 2. února 2017 [cit. 5. března 2019]. Dostupné na <https://www.epravo.cz/top/clanky/profilovani-ve-svetle-noveho-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-104926.html>.
[83] NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 255.
[84] VACHTL, Jiří. *Čína zakázala milionům neposlušných občanů cestovat, mají nízké skóre* [online]. idnes.cz, 3. března 2019 [cit. 7. března 2019]. Dostupné na <https://www.idnes.cz/zpravy/zahranicni/cina-kamery-zakaz-cestovani.A190302_213230_zahranicni_chtl>.

zasahuje do práv a svobod občanů a v případě stejného postupu úřadů v rámci evropského prostoru by bylo zcela nekompatibilní s celkovým právním rámcem, nikoliv jen s Nařízením. V tuzemském prostředí tak prozatím nevnímám automatizované individuální rozhodování ve veřejné správě jako aktuální riziko vyvstávající pro subjekty údajů.

Následuje termín pseudonymizace zpracování osobních údajů. Z výkladu čl. 4 bodu 5) lze dovodit, že se jedná o bezpečnostní prvek, který zajišťuje vyšší míru ochrany osobních údajů. Pseudonymizovaný údaj je takový údaj, který bez dodatečné informace nelze spojit se subjektem údajů. Nejen že dodatečná informace musí být podrobena technickým a organizačním opatřením, které zajistí nemožnost identifikace fyzické osoby, ale také musí být odděleně uchovávána. Dle recitálu 26 jsou pseudonymizované údaje považovány i nadále za osobní a i nadále spadají do působnosti GDPR na rozdíl od anonymizovaných údajů. Anonymizace údaje má za následek nemožnost zpětného propojení s konkrétní osobou, zatímco v případě pseudonymizace je identifikace osob možná po přiřazení dodatečných údajů[85]. Proces pseudonymizace je spojen s prováděním archivace, když čl. 89 GDPR reflektuje potřebu archivace ve veřejném zájmu. I v tomto případě je potřeba dbát práv a svobod údajů. Za předpokladu, že by pseudonymizace splnila tento účel, může být vhodným opatřením. Právě proto spatřuji uplatnění pseudonymizace v rámci veřejné správy, když dle zákona č. 499/2004 Sb., o archivnictví a spisové službě provádí archivní službu organizační složky státu, územní samosprávné celky, vysoké školy a další.

Kromě terminologie došlo také ke změnám důvodů zpracování. Nedošlo však k rozšíření o žádný právní titul, který by opravňoval zpracování osobních důvodů. Naopak Nařízení implicitně neuvádí zpracování výlučně pro účely archivnictví a takové zpracování spadá pod právní titul splnění právní povinnosti nebo plnění úkolu prováděného při výkonu veřejné moci. Fakticky se tak spíše jedná o kosmetické změny.

2.4. Nové povinnosti podle GDPR

Aniž bych snižoval význam pojmového vymezení, zásadní změny pro správce a zpracovatele nastávají v povinnostech, které jim Nařízení nově ukládá. Tyto úkoly, které čerstvě budou spadat do jejich kompetence, lze považovat za konkrétní složky právní ochrany zpracování osobních údajů a teoreticky by tak měly přispívat k bezpečnějším procesům zpracování. Zda tomu tak fakticky je, se pokusím přiblížit u jednotlivých povinností.

[85] KOHÚTOVÁ, Zuzana. *Anonymizace, pseudonymizace a šifrování osobních údajů jako bezpečnostní opatření dle GDPR* [online]. flye-eye.cz, 13. září 2017 [cit. 7. března 2019]. Dostupné na <https://fly-eye.cz/blog-detail-1.html>.

2.4.1 Povinnost vést záznamy o činnostech zpracování

Kromě správců a zpracovatelů osobních údajů, jsou povinni též jejich případní zástupci vést záznamy o činnostech zpracování. Tato povinnost vyplývá z čl. 30 GDPR odst. 1., resp. 2. Obsah záznamů je srozumitelně vymezen na témže místě. Kromě účelu zpracování musí záznamy zahrnovat kategorické vymezení osobních údajů, jejich subjektů a příjemců. Dále informace o možném předávání do třetích zemí nebo mezinárodním organizacím. Pokud to situace umožňuje, je součástí záznamů obecný popis zabezpečení dat uvedených v čl. 32 GDPR a plánované lhůty výmazu údajů. Nesmí chybět ani identifikace správce, zpracovatele nebo jejich zástupců a pověřence. Povinnost správce je širší, když zpracovatel má povinnost vést záznamy v menším rozsahu. Neuvádí například účel zpracování, protože tento stanovuje správce. Záznamy zpracování nahrazují notifikační povinnost dle ZoOÚ[86]. GDPR stanovuje také formu vedení záznamů, když v odst. 3 je vyjádřen požadavek písemnosti. Úřad pak v rámci své dozorové činnosti bude využívat záznamy, které mu vždy musí relevantní osoba vydat. V posledním odstavci čl. 30 je pak dána výjimka z této povinnosti, a to v případě i) absence pravděpodobnosti rizika pro práva a svobody subjektů, ii) jedná se o příležitostné zpracování a konečně pak iii) zpracování nezahrnuje zvláštní kategorii údajů jako citlivé údaje nebo osobní údaje vztahující se k rozsudkům v trestních věcech a k trestním činům. Kromě těchto tří bodů je pak kumulativně nutné splnit podmínku počtu zaměstnanců správce a zpracovatele, který nesmí přesáhnout 250. I proto lze usoudit, že splnění všech těchto podmínek bude méně časté a výjimka je poměrně přísná. V případě zpracování osobních údajů ve veřejné správě dle mého je nereálné splňovat veškeré podmínky a orgány veřejné moci tak budou muset dostát této povinnosti. Pokud by správce nebo zpracovatel měl za to, že zpracování, které provádí, by mohlo spadat do výjimečného režimu, měl by disponovat detailní analýzou, která by takové zpracování obhájila v případě kontroly s dozorovým úřadem[87]. Nejsem úplně přesvědčen, že plnění této povinnosti povede k bezpečnějšímu zpracování, nýbrž jen fakticky administrativně zatíží správce či zpracovatele. Taková administrativní zátěž dle mého nepřispěje k dobré správě.

2.4.2 Posouzení vlivu na ochranu osobních údajů

Pro následující povinnost budeme užívat zkratku DPIA (Data Protection Impact Assessment). Pokud je zde zvýšená rizikovost zpracování pro práva a svobody subjektů, vyžaduje se dle čl. 35 odst. 1 GDPR právě DPIA. Rizikovost se posuzuje s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování. Ve třetím odstavci téže článku obsahuje GDPR demonstrativní

---

[86] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018, s. 246.

[87] MALIŠ, Petr. *GDPR - 3. díl: Vedení záznamů o činnostech zpracování osobních údajů* [online]. pravoit.cz, 22. listopadu 2017 [cit. 11. března 2019]. Dostupné na <http://www.pravoit.cz/novinka/gdpr-3-dil-vedeni-zaznamu-o-cinnostech-zpracovani-osobnich-udaju>.

výčet, kdy se vyžaduje z důvodu vysokého rizika posouzení vlivu. Jedná se i) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad, ii) rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů nebo iii) rozsáhlé systematické monitorování veřejně přístupných prostorů. Takovéto to mantinely jsou poměrně vágní, a proto vydala pracovní skupina WP29 pokyny (dále jen "Pokyny k DPIA"), ve kterých konkrétněji vymezuje kritéria, která mají být zohledněna při vyhodnocení rizikovosti zpracování. Další případná konkretizace vychází z čl. 35 odst. 4 GDPR, a to když je založena pravomoc Úřadu zveřejnit seznam druhů operací zpracování, které budou podléhat DPIA. Jedná se tak v podstatě o konkretizaci právní úpravy dozorovým úřadem. Úřad dne 7.2.2018 zveřejnil dokument v této věci, ve kterém vymezil parametry, na základě kterých lze hodnotit jednotlivé zpracování. Hodnocení na základě těchto parametrů pak určí, zda je zpracování vysoce rizikové, rizikové nebo ostatní[88]. Nejedná se však o právně závazný dokument, nýbrž o pouze návrh, k němuž lze podávat připomínky a je podroben veřejné diskuzi. DPIA není jednorázový proces, ale je dlouhodobý kontinuální proces, který by měl být započat již před samotným zahájením zpracování osobních údajů[89]. V čl. 35 odst. 7 GDPR jsou stanoveny pak minimální obsahové požadavky na posouzení vlivu. Jedná se o systematický popis zamýšlených operací zpracování a účely zpracování, posouzení nezbytnosti a přiměřenosti operací s ohledem na účely zpracování, posouzení rizik pro práva a svobody subjektů údajů a plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k prokázání souladu s GDPR. Obsahové přiblížení rozvádí Příloha č. 2 k Pokynům k DPIA[90]. Z takto vymezených bylo prakticky nemožné, aby se orgány veřejné moci vyhnuly posouzení vlivu na ochranu zpracování. Nicméně Adaptační zákon stanovuje v § 10 výjimku z této povinnosti, pakliže se jedná o zpracování z důvodu plnění zákonné povinnosti. A protože v rámci tohoto režimu bude docházet ke zpracování dat v rámci veřejné správy, právě na tu bude dopadat výjimka. Ovšem stejně jako v předchozím bodě i zde to považuji za zatížení správců a zákonem stanovenou výjimku kvituji.

[88] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)* [online]. uoou.cz, 7. února 2018 [cit. 12. března 2019]. Dostupné na <https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385>.

[89] KARTNER, Martin, PROUZA, Jiří. *Posouzení vlivu na ochranu osobních údajů podle GDPR* [online]. epravo.cz, 17. května 2017 [cit. 12. března 2019]. Dostupné na <https://www.epravo.cz/top/clanky/posouzeni-vlivu-na-ochranu-osobnich-udaju-podle-gdpr-105892.html>.

[90] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018, s. 274.

2.4.3 Předchozí konzultace

Konzultovat zpracování osobních údajů s Úřadem by měl správce tehdy, když z posouzení vlivu na ochranu osobních údajů vyplyne, že by dané zpracování mělo za následek vysoké riziko. Zároveň by správce nepřijal opatření ke zmírnění tohoto rizika. Tato povinnost tak přímo navazuje na DPIA. Podstatné je, že zahájení zpracování osobních údajů není závislé na předchozím povolení Úřadu a uplynutím lhůty, kterou dozorový úřad má na vyjádření, je správce oprávněn zahájit zpracování[91].

2.4.4 Ohlašovací a oznamovací povinnost

Předmětem těchto povinností je porušení zabezpečení osobních údajů. Elementární rozdíl spočívá v tom, vůči komu je vyrozumění o porušení činěno. Čl. 33 GDPR ukládá ohlašovací povinnost správce vůči dozorovému úřadu, zatímco čl. 34 GDPR stanovuje oznamovací povinnost vůči subjektu údajů. V obou případech musí jít o takové porušení, které ohrožuje práva a svobody subjektu údajů. Ohlášení musí být učiněno do 72 hodin od porušení. Případné nedodržení lhůty musí správce vždy zdůvodnit. Lhůta začíná běžet od okamžiku, kdy se správce dozvěděl o riziku[92]. Na rozdíl od ohlášení je možné se vyhnout oznamovací povinnosti, pokud je naplněn některý z předpokladů v čl. 34 odst. 3 písm. a) - c). První případ se vztahuje na porušení zabezpečení osobních údajů, které jsou chráněné dostatečnými opatřeními a bez dalšího je nelze plnohodnotně přiřadit k subjektům údajů[93]. Zadruhé se jedná o situaci, kdy není nutné notifikovat subjekt, protože následná opatření zamezují vysokému riziku pro jeho práva a svobody. A konečně pak situace, kdy by oznamovací povinnost představovala nepřiměřené úsilí. V takovém případě se oznamuje veřejným oznámením. Tyto povinnosti lze vnímat jako posílení bezpečného zpracování. Posílení spatřuji jednak v následné součinnosti s Úřadem po ohlášení skutečnosti, že došlo k porušení zabezpečení. S touto rovinou souvisí hrozba sankcí, které mohou působit na zpracovatele či správce pozitivně ve vztahu k nápravě nastalé situace. A dále se zde vzniká nárok subjektům údajů uplatňovat svá práva vůči správci či zpracovateli.

2.4.5 Jmenování pověřence pro ochranu osobních údajů

Poslední povinnost se váže na nový institut, který zavádí Nařízení. Tato podkapitola bude zaměřena na povinnost jmenovat pověřence, nikoliv rozboru tohoto institutu a jeho postavení. S ohledem na skutečnost, že pověřenec je velmi relevantní pro orgány veřejné moci, je vhodnější

[91] NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 354.
[92] Tamtéž, s. 321.
[93] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018, s. 267.

blíže rozvést tuto funkci v následující kapitole spolu s dalšími konkrétními dopady GDPR na veřejnou správu.

Dle čl. 37 odst. 1 písm. a) jmenuje pověřence správce nebo zpracovatel vždy, pokud zpracování provádí orgán veřejné moci či jiný veřejný subjekt. Jinými veřejnými subjekty lze chápat veřejnoprávní korporace[94].Výjimkou jsou soudy v rámci svých soudních pravomocí. Nicméně pro personální agendu či ostrahu budovy soudu kamerovým systémem již musí být pověřenec jmenován[95]. Podle odst. 3 téže článku, umožňuje GDPR jmenovat jediného pověřence pro několik orgánů nebo subjektů veřejné správy v případech, kdy je to vhodné s ohledem k přihlédnutí k jejich organizační struktuře a velikosti. Vždy je však nutné, aby společný pověřenec byl schopen tuto funkci adekvátně vykonávat[96]. Pověřenec je zároveň osoba odlišná od správce a zpracovatele. V písm. b) je uložena povinnost jmenování pověřence všem správcům a zpracovatelům, jejichž hlavní činnost spočívá v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů. Nulíček uvádí jako příklady nemocnici, která zpracovává osobní údaje pacientů pro následující poskytnutí zdravotní péče nebo agenturu, která dohlíží v nákupních centrech nad veřejnými prostory za užití kamer. Poslední případ, kdy je nutnost mít pověřence pro ochranu osobních údajů, je v případě hlavní činnosti správce nebo zpracovatele spočívá v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10 Nařízení.

[94] NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 362
[95] Tamtéž.
[96] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018, s. 288.

3. Dopady GDPR ve vztahu k činnosti veřejné správy

Závěrečná kapitola by měla tvořit nosnou část práce, ve které se pokusíme vyvodit závěry k výzkumné otázce, která byla vytyčena v úvodu. Tato část bude členěna do dvou podkapitol. První z nich budou důsledky implicitně vyplývající z Nařízení. Protože tyto byly již částečně popsány v předchozí kapitole jakožto nové povinnosti podle GDPR, nyní budou analyzovány pro účely veřejné správy. Následovat pak bude podkapitola zkoumající dopady adaptačního zákona na současný právní stav. Ačkoliv je adaptační zákon také důsledkem GDPR, představuje především zákonné uspořádání, které v mezích stanovených Nařízením nastavil český zákonodárce. Takové uspořádání pak bude zcela jistě odlišné ve všech státech, ve kterých je aplikováno GDPR. Konkrétně česká úprava pak představuje legislativu, která může značně ovlivnit ochranu osobních údajů v gesci orgánů veřejné moci a jiných veřejných subjektů.

Kromě samotných důsledků nové legislativy, které se odrazí v právech a povinnostech jednotlivých subjektů, je třeba mít na paměti také implementační proces, který budou muset provést všichni správci a zpracovatelé, tedy i orgány veřejné moci, veřejnoprávní korporace a další. Implementačním procesem rozumíme činnost, kterou dochází ke změně postupů v oblasti zpracování osobních údajů, v posuzování možných rizik, potažmo následných řešení negativních následků spočívajících v nedodržení svých povinností. Cílem implementačního procesu by měl být vznik mechanismu, který bude odpovídat standardu stávající právní úpravy. Nejprve by mělo dojít k právní analýze současného stavu ochrany osobních údajů a následně k porovnání s požadavky Nařízení[97]. V rámci implementace také dochází k revizi všech procesů týkající se zpracování.

3.1. Důsledky GDPR

Není pochyb, že Nařízení představuje v oblasti zpracování osobních údajů legislativní změnu značného rozsahu. V této podkapitole se již budeme zaobírat vybranými hledisky pro oblast státní správy a samosprávy. Specifických aspektů ve veřejné správě bychom jistě nalezli více, ovšem pro účely a zejména rozsah práce postačí níže vybrané.

3.1.1 Osobní údaje a registr smluv

Zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen "zákon o registru smluv") vymezuje okruh soukromoprávních smluv, na které dopadá povinnost jejich uveřejnění. Vymezující kritérium je existence smluvní strany korespondující taxativnímu výčtu v § 2 odst. 1 tohoto zákona ve spojení s § 3 stanovujícím výjimky z této povinnosti. Ač se jedná o případy, kdy smluvní stranou bude např.

[97] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. s. 140.

obec, veřejná vysoká škola či Česká televize, se zřetelem k povaze soukromoprávních smluv je jisté, že obsahem mohou být v mnoha případech osobní údaje fyzických osob. Jaký vliv bude mít na dosavadní stav Nařízení?

Na problematika osobních údajů v souvislosti s registrem smluv je nutné pohlížet ve dvou rovinách. První z nich souvisí se svobodným přístupem k informacím. Na základě ust. § 3 odst. 1 zákona o registru smluv se prostřednictvím registru smluv neuveřejňují informace, které nelze poskytnout při postupu podle předpisů upravujících svobodný přístup k informacím. Zákon č. č. 106/1999 Sb., o svobodném přístupu k informacím stanovuje povinnost povinnému subjektu ve svém § 8b poskytnout základní osobní údaje o osobě, které poskytl veřejné prostředky, ledaže došlo k vyplacení veřejných prostředků podle zákonů v oblasti sociální, poskytování zdravotních služeb, hmotného zabezpečení v nezaměstnanosti, státní podpory stavebního spoření. Druhá rovina pak představuje případy, kdy bude namísto zákona o svobodném přístupu k informacím vyžadována aplikace GDPR. Takový závěr vyplývá z metodického návodu k aplikaci zákona o registru smluv vydaným ministerstvem vnitra. *"Je proto nutné vycházet z obecné úpravy ochrany osobních údajů stanovené zejména nařízením GDPR a zákonem o zpracování osobních údajů. Osobní údaje je možné zpracovat (v tomto případě uveřejnit) jen na základě některého z právních titulů vymezených v čl. 6 nařízení GDPR. Pokud ke zpracování osobních údajů jejich zveřejněním právní titul k dispozici není, je nezbytné osobní údaje v dané smlouvě anonymizovat. V opačném případě by se jednalo o nezákonné zpracování osobních údajů, za které může být Úřadem pro ochranu osobních údajů odpovědnému subjektu uložena peněžitá sankce, nebo se fyzická osoba, jejíž údaje byly neoprávněně zpracovány, může domáhat náhrady újmy v rámci práva na ochranu osobnosti."*[98]

Jinými slovy dle tohoto metodického pokynu není dovoleno bez dalšího zveřejnit osobní údaje v registru smluv, pakliže není dán žádný právní titul pro zveřejnění. Pokud by tak nastala situace, kdy obec uzavře smlouvu, která bude podléhat evidenci registru smluv, je možné zveřejnit osobní údaje pouze v odpovídajícím a nutném rozsahu pro plnění právní povinnosti podle zákona o registru smluv. Údaje navíc je pak možno zveřejnit, jen lze-li uplatnit jiný důvod dle čl. 6 Nařízení. Typicky se souhlasem subjektu. Názorně to lze demonstrovat na situaci, kdy obec v rámci environmentální politiky vyplácí žadatelům příspěvky na pořízení a instalaci solárních panelů. V takovém případě dojde k uzavření smlouvy o poskytnutí účelové dotace občanovi Josefovi Novákovi. Ač tato smlouva bude předmětem evidence registru smluv, může obec zveřejnit údaje pouze v takovém rozsahu, jaký je vyžadován zákonem o registru smluv. Ten mj. vyžaduje identifikaci smluvních stran. Pro identifikaci Josefa Nováka je pak dostačující jeho jméno a datum narození. Rozhodně není nutné zveřejnit kontaktní údaje včetně adresy. Obec, jakožto smluvní

[98] Metodický návod ministerstva vnitra k aplikaci zákona o registru smluv ze září 2018, č.j. MV-37683-1/EG-2018, s. 51.

strana, je oprávněna zpracovávat veškeré osobní údaje uvedené ve smlouvě, včetně kontaktních údajů, zejména pak pro své oprávněné zájmy. Ovšem povinnost zveřejnit tyto údaje v registru smluv nelze dovodit a obec tak není oprávněna je zveřejnit. Okamžik účinnosti GDPR má tak poměrně zásadní dopad na registr smluv, neboť zveřejněné údaje, které nejsou v souladu s GDPR pro absenci řádného právního titulu, je potřeba okamžitě anonymizovat. Pokud k datu účinnosti anonymizace nebyla provedena, došlo k porušení ochrany osobních údajů a tím tak ke spáchání přestupku. Subjekt údajů je oprávněn uplatnit své právo na omezení zpracování. Tímto tak dojde k nápravě závadného stavu. Právo na náhradu škody tímto není dotčeno.

3.1.2 Zveřejňování na úřední desce

Povinnost správních orgánů zřídit úřední desku a zveřejňovat její obsah způsobem umožňujícím dálkový přístup je zakotvena v § 26 správního řádu. Prostřednictvím úřední desky může docházet k povinnému zveřejnění údajů, typicky doručování veřejnou vyhláškou dle správního řádu, a nebo k nepovinnému zveřejňování jehož cílem je např. zvýšení transparentnosti jednání obce[99]. Pokud obec bude doručovat veřejnou vyhláškou, může zvolit jednu z následujících variant. Buď zveřejní samotnou písemnost nebo pouze oznámení o možnosti převzetí písemnosti, ve které budou publikovány pouze nezbytné identifikační údaje dotčené osoby[100].

Legalita takového zpracování vychází z čl. 6 odst. 1 písm. c) GDPR, neboť jde o plnění právní povinnosti, případně se též může jednat o zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci obce dle čl. 6 odst. 1 písm. e) GDPR. Nicméně přikláním se k názoru Janečkové[101], která uvádí, že pakliže se doručuje konkrétní fyzické osobě, která není neznámá, mělo by se vždy zvolit zveřejnění oznámení o možnosti převzetí písemnosti, kdy jsou na úřední desce uvedeny osobní údaje potřebné pouze k identifikaci. Pokud se má tento konkrétní adresát dozvědět o existenci písemnosti z úřední desky, není nutné zveřejnit konkrétní písemnost a tedy její obsah a vystavit jej tak nebezpečí zneužití osobních údajů.

3.1.3 Zpracování osobních údajů zaměstnanců veřejné správy

Zaměstnanecký poměr představuje vztah dvou subjektů, z nichž alespoň jeden z nich je fyzickou osobou. Zaměstnaneckým poměrem rozumíme pracovněprávní vztahy nebo také různé druhy služebních vztahů týkajících se státních zaměstnanců, úředníků územních samosprávných celků, příslušníků bezpečnostních sborů, soudců apod. Tyto jsou pak zvláště upraveny podle zákona č. 234/2014 Sb., o státní službě, zákona č. 361/2003Sb., o služebním poměru příslušníků bezpečnostních sborů nebo zákona č. 6/2002 Sb., o soudech a soudcích, ve znění pozdějších

[99]Příloha k Průvodci pro přípravu obcí na požadavky GDPR. Dostupná na: <https://www.mvcr.cz/gdpr/soubor/gdpr-modelove-situace-zverejnovani-v-obecnim-periodiku.aspx>.
[100] Tamtéž.
[101] JANEČKOVÁ, Eva. *GDPR - řešení problémů v praxi obcí.* Praha: Grada Publishing, a.s., 2019, s. 230.

předpisů. Je zřejmé, že v těchto vztazích dochází k zpracování osobních údajů ve značném množství. Z toho jasně rezultuje, že všechny osoby spadající do působnosti Nařízení požívají ochrany osobních údajů. A protože správní úřady, územně samosprávné celky a další orgány veřejné správy disponují úřednickým aparátem, je pro ně nová legislativa bezesporu relevantní i z tohoto hlediska.

Ze stanoviska ke zpracování osobních údajů na pracovišti[102] klade Pracovní skupina WP29 důraz na řádné zpracovávání osobních dat bez ohledu na užité technologie, informovanost zaměstnanců o probíhajícím monitoringu nebo nemožnost zpracování na základě uděleného souhlasu, pokud zaměstnanec nemohl bez negativních následků pro sebe odmítnout. V této věci dále dodává možnost zpracovávat údaje na základě titulů v souladu s GDPR - nezbytnost zpracování pro plnění smlouvy (čl. 6 odst. 1 písm. b), nezbytnost zpracování pro plnění právní povinnosti, typicky sociální a zdravotní pojištění (čl. 6 odst. 1 písm. c) nebo oprávněné zájmy zpracovatele či třetí osoby čl. 6 odst. 1 písm. c).

Zaměstnancům náleží škála práv v souvislosti s procesem zpracování jejich osobních údajů. Naproti těmto právům zaměstnanců náleží povinnosti zaměstnavatelů. Ti jsou především povinni dostát své informační povinnosti vůči zaměstnanci. Obsahem těchto informací bude především uvedení totožnosti zaměstnavatele a jeho kontaktních údajů, účelu zpracování, pro který jsou osobní údaje určeny, a právním základu pro zpracování, oprávněných zájmů zaměstnavatele, případných příjemců osobních údajů[103]. Jedním z faktorů, který může ovlivnit bezpečnost zpracování, je doba, po kterou k němu dochází. V případě zaměstnání závisí maximální možná doba zpracování jednotlivých dat na účelu jejich zpracování. Pokud dochází ke zpracování na základě souhlasu, mám za to, že by nejpozději k okamžiku skončení pracovního poměru odpadl důvod dalšího zpracování. Takový závěr vyvozuji z toho, že pakliže zaměstnanec může udělit informovaný a svobodný souhlas ke zpracování osobních údajů svému zaměstnavateli, vždy se tento bude vázat k výkonu tohoto zaměstnání. Stejně tak souhlas může kdykoliv odvolat, a to i v průběhu trvání zaměstnaneckého poměru. Po skončení pracovního poměru tak může zaměstnavatel uchovávat po dobu odpovídající účelu zpracování, po dobu trvání povinnosti dalšího uchování dat nebo po dobu, která je nezbytná k vypořádání vzájemných práv a povinností mezi stranami[104]. Již v tomto spatřuji snížení rizika zneužití dat, když po odpadnutí účelu zpracování vzniká povinnost zaměstnavatele zlikvidovat data. V tomto ohledu tak bezesporu půjde o zvýšení

[102] Stanovisko Pracovní skupiny WP29 2/2017 ke zpracování osobních údajů na pracovišti ze dne 8. června 2017, dostupné na: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30203
[103] FRANTIŠOVÁ, Petra. *GDPR a některé povinnosti zaměstnavatelů.* [online]. epravo.cz, 20. listopadu 2017 [cit. 13. června 2019]. Dostupné na <https://www.epravo.cz/top/clanky/gdpr-a-nektere-povinnosti-zamestnavatelu-106526.html>.
[104] KUBÍČKOVÁ, Alice, Veronika, PATÁKOVÁ. *Zpracování osobních údajů po skončení pracovního poměru.* [online]. incompliance.cz, 7. března 2018 [cit. 13. června 2019]. Dostupné na <https://www.incompliance.cz/cz/blog/zpracovani-osobnich-udaju-po-skonceni-pracovniho-pomeru >.

bezpečnosti zpracování osobních údajů zaměstnanců, a to nikoliv jen ve sféře veřejné správy. K tomu je třeba mít na paměti ohlašovací a oznamovací povinnost zakotvenou v čl. 33, resp. 34 GDPR, které se týkají všech správců a zpracovatelů osobních údajů včetně orgánů veřejné moci.

3.1.4 Zvláštní činnosti obce

V krátkosti se budeme zaobírat specifickými situacemi v gesci obce. Jako první je povinnost obce vést kroniku dle § 1 zákona č. 132/2006 Sb., o kronikách obcí. Dle tohoto předpisu má každá obec za úkol zaznamenávat zprávy o důležitých a pamětihodných událostech v obci pro informaci i poučení budoucím generacím. Takové zápisy pak budou mít bezesporu povahu osobních údajů a vzhledem k tomu, že každý může nahlížet do takové obecní kroniky podle § 4 zákona o kronikách, není vhodné zapomínat na požadavky GDPR. Obecně se lze opřít o čl. 6 odst. 1 písm. c) GDPR - zpracování nezbytné pro splnění právní povinnosti, případně pak o čl. 6 odst. 1 písm e) GDPR - zpracování nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce. Přesto je však potřeba evidovat vždy takové údaje, které jsou nezbytné pro plnění povinnosti podle zákona o kronikách a v případě možného překročení je namístě vyžádat si řádný souhlas od subjektu údajů.

Jako další specifickou oblast lze uvést kontrolní činnost různého charakteru. Pakliže dochází k takové kontrolní činnost například u obce, není možné odmítnout poskytnutí dokumentů s odůvodněním, že tyto obsahují osobní údaje. Kontrolující je oprávněn v souladu s § 8 písm. c) Kontrolního řádu požadovat poskytnutí údajů, dokumentů a věcí vztahujících se k předmětu kontroly nebo k činnosti kontrolované osoby. I v tomto případě dochází k plnění zákonné povinnosti a souhlas subjektu se nevyžaduje. Vždy je však třeba dbát na účel zpracování, kterým je v tomto případě provedení kontroly, a po jejím dokončení je třeba ukončit další zpracování[105].

Poslední oblastí, kterou se budeme zabývat, je ochrana osobních údajů v rámci správního řízení. V případě správních řízeních v režii obcí je dle Janečkové[106] klíčové stanovit rozsah zpracovávaných osobních údajů, přičemž stanovení nezbytného rozsahu pak bude nutné ve třech dimenzích. Jsou jimi identifikace účastníků či jiných dotčených osob, dále pak osobní údaje vzešlé z provádění důkazů či jiných úkonů během řízení a konečně pak hledisko zveřejnění meritorního rozhodnutí ve správním řízení. Aby došlo k souladu s GDPR, bude muset obec dbát na řádné zpracování v nutném rozsahu, který nebude nadbytečný. Co se týče identifikace, tak její rozsah vyplývá z § 18 odst. 2 správního řádu, který stanovuje, že údaji umožňující identifikaci fyzické osoby se rozumí jméno, příjmení, datum narození a místo trvalého pobytu, popřípadě jiný údaj

[105] JANEČKOVÁ, Eva. *GDPR - řešení problémů v praxi obcí*. Praha: Grada Publishing, a.s., 2019, s. 328.
[106] Tamtéž, s. 323.

podle zvláštního zákona. Rozsah zjišťování je pak poněkud vágně stanoven v § 52 správního řádu, který umožňuje provést takové důkazy, které jsou potřebné ke zjištění stavu věci. V obou případech tak půjde o zákonné zpracování, které lze zařadit pod čl. 6 odst. 1 písm. c) - plnění zákonné povinnosti, případně pak podpůrně lze využít čl. 6 odst. 1 písm. e) - zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce. Přesto mám za to, že v praxi nedojde v této agendě k žádným změnám, když obce nejsou vystaveny rizikům jakékoliv sankce za porušení těchto povinností, jak bude blíže rozvedeno v následující podkapitole. Specifikum u správního řízení vnímám také v jeho účelu, kterým je dle § 9 správního řádu určení právních poměrů konkrétní osoby. Zároveň není možno opomíjet zásadu materiální pravdy, k níž by se měl rozhodující orgán pokud možno co nejvíce přiblížit. Z tohoto důvodu si myslím, že se nebude omezovat ve zjišťování podstatných skutečností, což by mohlo vést k nadbytečnému zpracování, na úkor ochrany osobních údajů. Zvlášť bez rizika následné sankce. Avšak jiná situace nastane v případě zveřejňování správních rozhodnutí. Zde by bylo teoreticky možné zveřejnit rozhodnutí, pokud by k tomu subjekt údajů dal výslovný souhlas.

Se správním řízením je také spojeno právo nahlížet do spisu. Primárně je toto umožněno v souladu s § 38 odst. 1 správního řádu všem účastníkům řízení. Vyjma účastníků může být spis zpřístupněn dalším osobám, kteří prokáží svůj právní zájem nebo jiný vážný důvod a zároveň a tím nebude porušeno právo některého z účastníků, popřípadě dalších dotčených osob anebo veřejný zájem. Tato oprávnění GDPR nijak nemění. Otázkou pak je, kdo bude zodpovědný za případné zneužití údajů, k nimž následně získal přístup neoprávněný prostřednictvím opisů ze spisu, které provedl oprávněný. Jsem toho názoru, že takové provinění nemůže být přičítáno správnímu orgánu a to ani za předpokladu, že o tomto oprávněné osoby nepoučil. Taková poučovací povinnost není nikde zakotvena, a proto dovozuji odpovědnost u konkrétního subjektu, který opisy nezákonně zpracovával. Ten je totiž může zpracovávat pouze v takovém rozsahu, který odpovídá jeho oprávnění, typicky uplatňování svých práv v rámci správního řízení. Není možné takto získané údaje zpřístupnit třetím stranám, byť bez úmyslu, natož je pak zveřejnit.

Závěrem jen doplňuji, že tato pravidla se uplatní obecně ve všech správních řízeních.

3.1.5 Pověřenec pro ochranu osobních údajů

Povinnost jmenovat pověřence, chcete-li DPO (Data Protection Officer), již byla předestřena v předchozí kapitole. Orgány veřejné moci či veřejný subjekt musí jmenovat pověřence, a to bez výjimky. Pod takové vymezení lze zahrnout ústřední orgány státní správy, obce všech kategorií a kraje, státní podniky, veřejné školy nebo také ČNB či NKÚ[107]. Přesto je možné, aby jediná osoba vykonávala funkci pověřence pro více zpracovatelů či správců, je-li to vhodné.

[107] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. s. 244.

Typicky tak několik sousedních menších obcí může jmenovat téhož pověřence. Dále bude tento nový institut rozebrán z pohledu jeho postavení a úkolů mu náležejících. Závěrem se také pokusíme zhodnotit reálný přínos pro ochranu osobních údajů v rámci veřejné správy.

Postavení pověřence pro ochranu osobních údajů je stanovena v několika odstavcích čl. 38 GDPR. Podstatou je náležité a včasné zapojení pověřence do veškeré agendy ochrany osobních údajů, přičemž správce a zpracovatel mu zajistí dostatečnou podporu a zdroje při plnění svých úkolů. Podle čl. 37 Nařízení může být DPO externista spolupracující na základě smlouvy o poskytování služeb nebo může jít také o zaměstnance. V případě obcí lze rozdělit případy, kdy je pověřenec zaměstnanec obce zařazený do obecního úřadu či mimo obecní úřad[108]. Odlišnost spočívá ve způsobu obsazení funkce, když na zaměstnance zařazeného do obecního úřadu dopadají ustanovení zákona č. 312/2002 Sb., o úřednících územních samosprávných celků[109]. Vyvstává pak otázka, zda může vykonávat funkci DPO zastupitel obce. Ministerstvo vnitra vydalo metodický pokyn[110], ve kterém v této věci uvádí, že zastupitel nemůže plnit tuto funkci z titulu své funkce zastupitele, ale nic mu nebrání stát se pověřencem, ať už jako externí či interní pracovník. Dále k tomu dodává, že musí být splněny další požadované předpoklady jako kvalifikovanost daného kandidáta a nezávislost a nestrannost. Právě aspekt nestrannosti shledávám poněkud problematický. Nejsem přesvědčen, že zastupitel obce bude vždy schopen zamezit střetu zájmů. Funkce zastupitele znamená mj. hájit zájmy občanů obce dle § 83 odst. 1 zákona o obcích a tyto zájmy mohou být někdy v protikladu s nestranností pověřence. Z tohoto důvodu bych tam raději nenechával žádný prostor pro slučitelnost funkce pověřence a zastupitele. Ba dokonce si myslím, že taková situace měla být implicitně vyloučena Adaptačním zákonem. Zároveň je dle čl. 38 odst. 3 GDPR dána nezávislost pověřence na správci a zpracovateli. Tito nemůžou pověřence nikterak sankcionovat. Další důležitým faktorem posilující nezávislost je zajištění, aby nedošlo ke vzniku střetu zájmů s jinými pověřencovými úkoly a povinnostmi, které plní. Případný střet zájmů musí být posouzen a vyhodnocen správcem a zpracovatelem a ve smlouvě o poskytování služeb by měly být smluvně stanoveny nástroje, které dostatečně zabrání takovému střetu zájmů[111]. Nicméně v případě zastupitele jsem poněkud skeptický, že by střetu zájmu bylo plně zabráněno prostřednictvím smluvních sankcí či jiných nástrojů.

---

[108] JANEČKOVÁ, Eva. *GDPR - řešení problémů v praxi obcí*. Praha: Grada Publishing, a.s, 2019, s. 164.
[109] Tamtéž.
[110] Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí podle právního stavu k 10. srpnu 2017. Dostupné na <https://www.mvcr.cz/gdpr/clanek/aktualizovana-metodika-k-poverencum-pro-ochranu-osobnich-udaju.aspx>.
[111] NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 375.

Čl. 39 odst. 1 obsahuje demonstrativní výčet úkolů pověřence. Již z tohoto vyplývá možný přínos tohoto institutu, když vezmeme v potaz kvalifikovanost pověřence v oblasti ochrany osobních údajů a jeho poradenskou úlohu vůči správcům, zpracovatelům či zaměstnancům provádějící zpracování osobních údajů. Jako nejdůležitější úkol pověřence považuji kontinuální monitoring souladu s GDPR. Pracovní skupina WP29 pak vydala pokyn[112], který vymezuje monitoring jako chování spočívající ve shromažďování informací pro určení činností zpracování, analýze a kontrole souladu činností zpracování nebo informování správce či zpracovatele včetně poskytování poradenství. Monitoring tak má značnou preventivní funkci. Nicméně pokud nelze hovořit o souladu s Nařízením v souvislosti se zpracováním osobních údajů, není za tento nesoulad zodpovědný pověřenec, nýbrž správce[113]. Je tak v zájmu každé obce či jiného veřejného subjektu jmenovat kompetentního DPO. Dále by měl pověřenec fungovat jako kontaktní místo pro Úřad v záležitostech týkajících se zpracování dle čl. 39 odst. 1 písm. e) GDPR. Pracovní skupina WP29 jej označuje také za jakéhosi zprostředkovatele. Myslím si, že takové opatření povede k usnadnění a celkovému zrychlení komunikace, což může být ku prospěchu všech. K tomuto se vztahují dvě povinnosti DPO. Zaprvé musí poskytnou v případě potřeby Úřadu veškerou potřebnou součinnost a zadruhé je vázán mlčenlivostí a všechny skutečnosti, které se dozví v souvislosti s výkonem této funkce jsou důvěrné[114]. Taková spolupráce může vést k minimalizaci škod v případě zneužití dat. Jako poslední z úkolů pověřence stojí za zmínku vedení záznamů podle čl. 30 odst. 1 a 2 GDPR. Z tohoto článků je nepochybné, že tato povinnost tíží samotné správce nebo zpracovatele. Nicméně Pracovní skupina WP29 ve svých pokynech uvádí, že tuto roli může převzít DPO. V případě veřejné správy pak lze tuto variantu maximálně doporučit. Jestliže bych měl zůstat u příkladu obce, dle mého by měl vykonávat agendu zpracování osobních údajů právě kvalifikovaný pověřenec, a to v co největším možném rozsahu. To znamená, že kromě úkolů stanovených Nařízením, by měla daná obec stanovit i další povinnosti a tyto vymezit co nejšíře. Ačkoliv se nikdy neoprostí od odpovědnosti za řádné a bezpečné zpracování, přenesením velké škály úloh na DPO může minimalizovat rizika spojená se zpracováním.

Souhrnně spatřuji v DPO zvýšení celkové bezpečnosti zpracování, neboť mám za to, že ve veřejné správě bude docházet spíše k nedbalostním porušení ochrany osobních údajů. Úředníci mnohdy nejsou v této agendě dostatečně znalí a tak vzniká prostor pro přestupky. Právě pověřenec může být klíčový faktor, který přinejmenším s sebou přinese snížení možných rizik. Jeho kompetence, jako monitoring legislativy v oblasti ochrany osobních údajů a následné zvyšování

[112] Pokyny Pracovní skupiny WP29 týkající se pověřenců pro ochranu osobních údajů naposledy revidované a přijaté dne 5. dubna 2017, dostupné na: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31880>.
[113] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. s. 277.
[114] NULÍČEK, Michal a kol. *GDPR/ obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, s. 378.

povědomí pracovníků zapojených do těchto operací, lze považovat za přínos. Ovšem abychom skutečně mohli hovořit o pozitivním dopadu pověřence, je nutné nekompromisně trvat na veškerých předpokladech a nepřipouštět možné mezírky. Taková právě může nastat v případě výkonu funkce DPO zastupitelem obce a potenciálního střetu zájmu. Ačkoliv k němu nemusí fakticky vůbec dojít, samotné riziko by mělo být dostačujícím argumentem pro volbu jiné vhodnější osoby, ač zákon tuto variantu nezakazuje.

3.2. Důsledky zákona č. 110/2019 Sb., o zpracování osobních údajů

Rozboru samotného Nařízení byla věnována celá druhá kapitola. V ní jsme také vymezily země, pro které je GDPR relevantní. Nicméně nelze říci, že by tato novelizace měnila právní rámec ochrany osobních údajů ve všech zemích shodně. Každý stát totiž může v rámci své vlastní zákonodárné iniciativy pomocí adaptačního zákona upravit určité oblasti dle svého uvážení. Český zákonodárce tak učinil přijetím zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen "Adaptační zákon"), kterým došlo fakticky k celkové změně stávajícího konceptu. Kromě toho, že Adaptační zákon derogoval ZoOÚ, tak současně s tímto byl přijat zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů (dále jen "Doprovodný zákon"). Doprovodný zákon tak reaguje na zrušení ustanovení zvláštních zákonů obsahující ochranu osobních údajů ve specifických situacích. Jako příklady lze uvést zákon č. 273/2008 Sb., o Policii České republiky, zákon č. 17/2012 Sb., o Celní správě České republiky nebo zákon č. 133/2000 Sb., o evidenci obyvatel. Celkově došlo k převážně drobnějším změnám v rozsahu několika ustanovení u 38 předpisů.

Adaptační zákon se kromě upřesnění zavedených ustanovení GDPR také odchyluje od nové úpravy a zavádí určité výjimky u povinnosti posuzování slučitelnosti účelů zpracování nebo oznamovací povinnosti správce či zpracovatele[115]. Za zmínku dále stojí stanovení způsobilosti dítěte v § 7 udělit souhlas se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti přímo jemu dovršením patnáctého roku věku. Nicméně jako důležitou vidím výjimku z povinnosti provést DPIA zakotvenou v § 10 Adaptačního zákona, dle kterého správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést. Jinými slovy jde o zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje. Právě orgány veřejné moci budou mnohdy zpracovávat osobní údaje pro tento účel a tak

[115] CETKOVSKÁ, Barbora, MÁLEK, Jakub. *Adaptační zákon k GDPR byl konečně přijat.* [online]. epravo.cz, 3. dubna 2017 [cit. 14. června 2019]. Dostupné na < https://www.epravo.cz/top/clanky/adaptacni-zakon-k-gdpr-byl-konecne-prijat-109122.htmll>

povolením takové výjimky z DPIA, jakožto nástroje, který by měl snížit rizika zpracování osobních údajů, nevnímám jako správný krok. Na jedné straně chápu, že nebude docházet ke zvyšování administrativní zátěže úřadů, ovšem v některých případech by měl zákonodárce na DPIA trvat. Jako příklad bych uvedl informační systém evidence obyvatel, ve kterém je vedena již zmíněná evidence, která obsahuje takové osobní údaje, které je potřeba chránit nejvíce. DPIA by tak měla být provedena i přes byrokratické břemeno s ní související.

Podstatná část nového předpisu, více než třetina ustanovení, se týká ochrany osobních údajů při jejich zpracování v souvislosti s trestnou činností od jejího odhalování, až po výkon trestů a ochranných opatření, včetně zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti (hlava III.) a ochrany osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky (hlava IV.). Následuje pak vymezení Úřadu, včetně jeho kompetencí. Konečně pak Adaptační zákon v ust. § 60 an. určuje přestupky a stanovuje horní hranici potenciální peněžité sankce. A právě zde je zcela zásadní úprava bezprostředně dopadající na veřejnou správu. Konkrétně mám na mysli § 61 odst. 5 Adaptačního zákona, který zakazuje uložit peněžitý trest orgánům veřejné moci či jiným veřejným subjektům. Pakliže by se takový správce nebo zpracovatel dopustil přestupku dle Adaptačního zákona, Úřad musí vždy upustit od uložení správního trestu. Takový přístup vnímám rozhodně negativně a nesouhlasím s odvodněním, že sankce nejsou na místě, protože by tak docházelo k přelévání peněz v rámci veřejných rozpočtů[116]. Stejně tak není pro mě argument možného dodatečného zavedení sankcí v případě zneužívání tohoto ustanovení[117]. Nerozporuji, že by hrazení takto uložených sankcí nevedlo k přelévání finanční prostředků v rámci jednotlivých rozpočtů, ale jsem přesvědčen, že tato skutečnosti by neměla vytlačovat práva subjektů údajů na adekvátní ochranu jejich zpracování. Takové přesuny finančních prostředků lze označit za negativní efekt, ovšem i tato skutečnost by měla stimulovat relevantní orgány k takovému přístupu, který zabezpečí ochranu dat a tím se tak vyhne jakýmkoliv správním sankcím. Vyhnout se těmto sankcím by bylo dle mého i jednoznačnou motivací vedoucích pracovníků orgánů veřejné moci, neboť by i jim osobně byl tento důsledek přičítán. A co se týče argumentu o dodatečném zavedení pokut až v okamžiku zneužívání této výjimky jsem toho názoru, že již vznikl prostor pro beztrestné porušení povinností a snížení bezpečného zpracování osobních údajů. Je třeba mít totiž stále na paměti, že i tyto subjekty nadále spadají do působnosti Nařízení a musí se řídit pravidly, které stanovuje. Výše jsme uvedly například institut pověřence pro ochranu osobních údajů, u které jsme došli k závěru jednoznačně

[116] mka. *Obcím a krajům nebudou za porušení GDPR hrozit pokuty, rozhodli poslanci.* [online]. ceskatelevize.cz, 12. března 2019 [cit. 17. června 2019]. Dostupné na < https://ct24.ceskatelevize.cz/domaci/2757596-zive-poslanci-maji-znovu-rozhodnout-o-zdaneni-nahrad-cirkvim-a-resit-mohou-i-faltynka>
[117] Tamtéž.

pozitivního dopadu v předmětné agendě. Nicméně tento efekt je značně otupěn, když v případě nejmenování pověřence nelze některým subjektům vůbec uložit sankci.

Závěr

Ač tomu tak vždycky historicky nebylo, významnost osobních údajů každého člověka je nesmírná. Kromě bezrozporné ekonomické hodnoty je obzvláště nutné vnímat jejich osobnostní význam. Osobní údaje jsou totiž úzce spjaty se soukromím a vůbec s osobností všech fyzických osob. Proto je nepochybné, že by tuto jejich hodnotu měla následně reflektovat odpovídající míra ochrany. Tím spíše v oblasti veřejné správy, v rámci jejíž činnosti se nakládá s údaji ve značném rozsahu. A zrovna orgány veřejné moci budou ze své povahy převážně zpracovávat osobní údaje ve veřejném zájmu nebo pro plnění své zákonné povinnosti, tedy nepotřebují souhlas subjektů údajů. Cílem práce tudíž bylo posoudit, zda nová legislativa reagující na novodobé trendy efektivně posiluje bezpečné zpracování osobních dat, které je prováděno veřejnou správou.

Pokud chceme docílit zvýšené bezpečnosti, musí dojít ke změnám práv a povinností správců a zpracovatelů osobních údajů, potažmo subjektů údajů. Potenciální změny pak představuje právě GDPR, které univerzálně ovlivňuje právní rámec uvedených států. Každý stát může následně přijmout domácí úpravu, která dílčím způsobem určí odchylky a výjimky z Nařízení. Povolené meze těchto odlišností plynou z Nařízení. V České republice tuto legislativu představuje Adaptační zákon. Abychom tak zjistili, zda došlo k posílení bezpečnosti zpracování osobních údajů, je nutné podrobit ZoOÚ komparaci GDPR s Adaptačním zákonem. V úvodu jsme také stanovili, že zvýšené efektivity ochrany zpracovávání lze docílit i) zavedením nových postupů během zpracování, ii) vytvořením nových nástrojů pro odstraňování negativní následků vzešlých z nesprávného či nezákonného zpracování ba dokonce předcházení jejich vzniku nebo iii) posílením postavení dozorového orgánu. Nutno dodat, že se nejedná o žádný taxativní výčet a zvýšit zabezpečení lze i jinými prostředky.

Základem veškeré činnosti závisející na uchovávání, pozměňování, zveřejňování či jiném úkonu, který spadá pod zpracování, je zákonnost takové aktivity. Podmínkou tak je dispozice některého ze zákonných titulů zpracování. A právě žádné radikální změny nová úprava v této oblasti nepřináší. Nově dle GDPR již neexistuje právní důvod zpracování osobních údajů pro účely archivnictví a právní titul pro zpracování osobní údajů o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení. V prvním případě došlo k formální změně, neboť povinnost archivace je zakotvena v zákoně č. 499/2004 Sb., o archivnictví a spisové službě. Takové zpracování pak představuje nezbytnost pro splnění právní povinnosti, která se na správce vztahuje dle čl. 6 odst. 1 písm. c) GDPR. Druhý případ bychom těžko subsumovali pod jediný právní titul v Nařízení. Povinnost sdělovat informace o výše uvedených osobách souvisí s právem na informace. Poskytnutí těchto informací pak lze považovat také za plnění právní povinnosti, anebo je jejich

zpracování nezbytné pro účely oprávněných zájmů správce či třetí osoby, pokud tyto zájmy mají přednost před zájmy nebo základními právy subjektu údajů dle čl. 6 odst. 1 písm. f) GDPR. Fakticky tak Nařízení neovlivní takové zpracování, a proto tak nelze hovořit o posílení bezpečnosti. Naopak přímý vliv na proces zpracování již bude mít povinnost vést záznamy dle čl. 30 GDPR. Taková povinnost ovlivní zpracování minimálně administrativně. Otázkou však je, zda záznamy garantují také větší míru bezpečnosti. Jsem spíše toho názoru, že záznamy vnesou větší přehlednost v procesu zpracování. A právě v případě veřejné správy a k přihlédnutí rozsahu zpracovávaných dat to lze kvitovat. Celkově to přispívá k větší systémovosti a spatřuji v tom tak preventivní účinek. Na druhou stranu nelze takovou aktivitu přeceňovat a bez dalších opatření sama o sobě nemá význam.

Ať už je legislativa sebelepší, nikdy není možné stoprocentně vyloučit možná porušení zpracování dat, a to ať už úmyslná či nedbalostní. Proto by měly existovat takové nástroje, které maximálně předchází negativním následků nelegálního zpracování, potažmo jsou způsobilé již nastalé negativní následky účinně odstranit. Do první kategorie bych zařadil dvě nové povinnosti. Jmenování pověřence a DPIA. Osoba pověřence by se dala označit za klíčový institut z následujících důvodů. Kvalifikovanost a odbornost, které jsou důležitým předpokladem pro výkon této funkce, jsou právě tím prvkem, který zde v minulosti absentoval. Pokud užijeme tuto premisu ve spojení s povinností všech orgánů veřejné moci či jiných veřejných subjektů zřízení této funkce, dojdeme k závěru, že tato novinka bezesporu zvyšuje bezpečnost zpracování. Pověřenec, jakožto nezávislá osoba, spravuje činnosti související se zpracováním, radí a konzultuje potřebné kroky s relevantními osobami nebo je kontaktní osobou v této agendě pro subjekty údajů i Úřad. Všechny tyto aktivity lze hodnotit jako přínos pro současnou praxi. Stejně tak pozitivně vnímám povinnost posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR, neboli DPIA. Úzce souvisí s institutem pověřence, když ten zpracovává posudek pro správce, kterého DPIA tíží. Posouzení spočívá v popsání všech operací zpracování včetně jejich účelu, posouzení nezbytnosti a přiměřenosti operací zpracování s ohledem na jejich účel, posouzení rizik pro práva a svobody subjektů údajů a konečně plánovaná opatření pro prevenci a zamezení těchto rizik. Při tomto procesu jsou zohledněny technologie užívané během zpracování, povaha, rozsah nebo druh zpracování. Jako kritický však vnímám zásah Adaptačního zákona, který v § 10 zakotvuje výjimku z této povinnosti. Správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést. A jak již bylo několikrát zmíněno, právě na základě tohoto titulu bude většinově docházet v rámci veřejné správy. Ač nelze říct, že by orgány veřejné moci vůbec nemuseli provádět DPIA, rozsah této povinnosti je pro mě užší, než pro jiné správce. Osobně se domnívám, že takové

zúžení povinnosti nebude ku prospěchu. Na druhou stranu plnění právní povinnosti není jediný právní titul užívaný pro zpracování vně veřejné správy, tudíž posouzení se úplně nevyhnou. V praxi tak může docházet k situacím, kdy i tito správci či správci údajů splní tuto povinnost nad rámec požadovaný zákonem. Co se týče druhé kategorie, tedy opatření vypořádávající se s nežádoucími následky, uvedl bych oznamovací povinnost správce či zpracovatele vůči subjektu údajů. Předmětem oznámení je vyrozumění subjektu údajů, že jsou jeho práva a svobody ohroženy. I z této povinnosti jsou však výjimky. Tou je například situace, kdy by oznámení představovalo nepřiměřené úsilí. V takovém případě však musí orgány veřejné moci alespoň provést oznámení veřejným oznámením prostřednictvím úřední desky. Byť se nejedná o žádnou převratnou změnu, lze ji vnímat kladně. Subjekty údajů jsou alespoň srozuměny s nastalým stavem a mohou provést další kroky ve spolupráci se správcem, zpracovatelem či Úřadem vedoucí k nápravě.

Konečně posledním aspektem, který byl zvažován, je postavení dozorového orgánu. Ten je v České republice představován Úřadem pro ochranu osobních údajů a byl ustaven již ZoOÚ. Adaptační zákon prakticky převzal stávající koncept bez značných změn. Z Nařízení však vyplývají nové kompetence, které vykonává v součinnosti se správci a zpracovateli údajů. Mám na mysli konzultaci, která předchází zpracování a iniciuje ji správce, pokud z DPIA vyplývá vysoké riziko daného zpracování. Mimo ni pak je nově zavedena ohlašovací povinnost správce či zpracovatele, pokud jsou dány předpoklady pro oznamovací povinnost. Oproti oznamovací povinnosti zde povinné osoby informují právě Úřad, nikoliv subjekt údajů o vzniklých rizicích. V rámci veřejné správy bude mnohdy ohlašovat tyto skutečnosti pověřenec.

Kdybych tak měl shrnout v krátkosti důsledek Nařízení na ochranu osobních údajů v souvislosti s veřejnou správou, vypíchl bych zejména povinnost jmenovat pověřence, který značně zvýší odbornou schopnost ve státní správě, tak i samosprávě. Ostatní nástroje nejsou nijak zásadní pro veřejnou správu. Byť DPIA mohl být také podstatnou ochrannou složkou nebýt jeho omezení Adaptačním zákonem, které se výrazně dotkne veřejné správy. A právě Adaptační zákon dle mého až hrubě otupuje celkový efekt GDPR, když navíc stanovuje výjimku z udílení sankcí orgánům veřejné moci či jiným veřejným subjektům. Pokud se však tito správci nebo zpracovatelé dopustí přestupku dle Adaptačního zákona, Úřad musí upustit od uložení správního trestu. Veškeré povinnosti tak výrazně ztrácí své vážnosti. Sankce je represivní prvek, jehož úkolem je působit na adresáty zastrašujícím způsobem. Pokud však nehrozí, neplní svůj účel. Argument o možném dodatečném zavedení sankci i pro orgány veřejné moci a další veřejné subjektu v případě, že bude docházet k jeho zneužívání, považuji za lichý. *Naopak zastávám postoj, že by sankce měly být zavedeny okamžitě. V opačném případě tak rozhodně nelze dospět k závěru, že GDPR představuje efektivní zvýšení ochrany zpracování osobních údajů ve veřejné správě.*

Seznam použitých zdrojů

LITERATURA

JANEČKOVÁ, Eva. *GDPR - řešení problémů v praxi obcí*. Praha: Grada Publishing, a.s., 2019. 341 s.

KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012. 516 s.

KUČEROVÁ, Alena, NONNEMANN, František. *Ochrana osobních údajů v praktických příkladech*. Praha: BOVA POLYGON, 2013. 167 s.

MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012. 206 s.

MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008. 212 s.

MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. 150 s.

NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. 339 s.

NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. 301 s.

NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. 484 s.

NULÍČEK, Michal a kol. *GDPR/obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018. 559 s.

PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018. 487 s.

VANÍČEK, Zdeněk a kol. *Zákon o elektronických komunikacích: komentář*. 2. vydání. Praha: Linde Praha, 2014. 559 s.

ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. 223 s.

LEGISLATIVA

Ústavní zákon č. 1/1992 Sb., Ústava

Ústavní zákon č. 2/1992 Sb., Listina

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

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

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

Zákon č. 255/2012 Sb., kontrolní řád, ve znění pozdějších předpisů

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

Zákon č. 312/2002 Sb., o úřednících územních samosprávných celků, ve znění pozdějších předpisů

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech, ve znění pozdějších předpisů

Zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů

Zákon č. 132/2006 Sb., o kronikách obcí, ve znění pozdějších předpisů

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat

Směrnice Evropského parlamentu a Rady č. 95/46/ES

JUDIKATURA

nález Ústavního soudu ze dne 9. března 2004, sp. zn. Pl. ÚS 38/02

nález Ústavního soudu ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94

nález Ústavního soudu ze dne 8. ledna 2008, sp. zn. Pl. ÚS 24/07

nález Ústavního soudu ze dne 13. srpna 2002, sp. zn. Pl. ÚS 3/02

rozsudek Nejvyššího soudu ze dne 30. září 2004, sp. zn. 30 Cdo 1183/2004

rozsudek Nejvyššího správního soudu ze dne 16.3.2010 čj. 1 As 93/2009-126

rozsudek Nejvyššího správního soudu ze dne 27.5.2011 čj. 5 As 57/2010-79

rozhodnutí Nejvyššího správního soudu ze dne 29.5.2008 čj. 8 As 57/2006-67

rozsudek Nejvyššího správního soudu ze dne 10.5.2006, čj. 3 As 21/2005-105

rozsudek rozšířeného senátu Nejvyššího správního soudu ze dne 22. 10. 2014, č.j. 8 As 55/2012-62

Usnesení zvláštního senátu zřízeného podle zákona č. 131/2002 Sb., o rozhodování některých kompetenčních sporů ze dne 17. 10. 2011, čj. Konf 11/2011-6

Soudní dvůr: Rozhodnutí ze dne 15. července 1964, *Flaminio Costa proti E.N.E.L., věc 6/64 Sb. rozh.*

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

ODBORNÉ ČLÁNKY

KRECHT, Jaroslav. Právo na informace a ochrana soukromí. *Právní rozhledy*, 2016, roč. 14, č. 23-24, s. 845.

GABRIŠOVÁ, Veronika. Poskytování osobních údajů z evidence obyvatel. *Právní rozhledy*, 2013, roč. 21, č. 10, s. 364.

FUREK, Adam, Informace o platech pracovníků veřejné správy. *Právní rozhledy*, 2011, roč. 19, č. 17, s. 626.

NONNEMANN, František. Náležitosti souhlasu se zpracováním osobních údajů. *Právní rozhledy*, 2011, roč. 142, č. 19, s. 526

INTERNETOVÉ ZDROJE

CETKOVSKÁ, Barbora, MÁLEK, Jakub. *Adaptační zákon k GDPR byl konečně přijat*. [online]. epravo.cz, 3. dubna 2017 [cit. 14. června 2019]. Dostupné na <https://www.epravo.cz/top/clanky/adaptacni-zakon-k-gdpr-byl-konecne-prijat-109122.htmll>.

FRANTIŠOVÁ, Petra. *GDPR a některé povinnosti zaměstnavatelů.* [online]. epravo.cz, 20. listopadu 2017 [cit. 13. června 2019]. Dostupné na <https://www.epravo.cz/top/clanky/gdpr-a-nektere-povinnosti-zamestnavatelu-106526.html>.

KARTNER, Martin, PROUZA, Jiří. *Posouzení vlivu na ochranu osobních údajů podle GDPR* [online]. epravo.cz, 17. května 2017 [cit. 12. března 2019]. Dostupné na <https://www.epravo.cz/top/clanky/posouzeni-vlivu-na-ochranu-osobnich-udaju-podle-gdpr-105892.html>.

KOHÚTOVÁ, Zuzana. *Anonymizace, pseudonymizace a šifrování osobních údajů jako bezpečnostní opatření dle GDPR* [online]. flye-eye.cz, 13. září 2017 [cit. 7. března 2019]. Dostupné na <https://fly-eye.cz/blog-detail-1.html>.

KUBÍČKOVÁ, Alice, Veronika, PATÁKOVÁ. *Zpracování osobních údajů po skončení pracovního poměru.* [online]. incompliance.cz, 7. března 2018 [cit. 13. června 2019]. Dostupné na <https://www.incompliance.cz/cz/blog/zpracovani-osobnich-udaju-po-skonceni-pracovniho-pomeru >.

MALIŠ, Petr. *GDPR - 3. díl: Vedení záznamů o činnostech zpracování osobních údajů* [online]. pravoit.cz, 22. listopadu 2017 [cit. 11. března 2019]. Dostupné na <http://www.pravoit.cz/novinka/gdpr-3-dil-vedeni-zaznamu-o-cinnostech-zpracovani-osobnich-udaju>.

mka. *Obcím a krajům nebudou za porušení GDPR hrozit pokuty, rozhodli poslanci.* [online]. ceskatelevize.cz, 12. března 2019 [cit. 17. června 2019]. Dostupné na <https://ct24.ceskatelevize.cz/domaci/2757596-zive-poslanci-maji-znovu-rozhodnout-o-zdaneni-nahrad-cirkvim-a-resit-mohou-i-faltynka>.

RADIČOVÁ, Zuzana, Burian, David. *Profilování ve světle nového obecného nařízení o ochraně osobních údajů (GDPR)* [online]. epravo.cz, 2. února 2017 [cit. 5. března 2019]. Dostupné na <https://www.epravo.cz/top/clanky/profilovani-ve-svetle-noveho-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-104926.html>.

ÚŘAD PRO OCHRANU OSOBNÁCH ÚDAJŮ. *Nevyžádaná obchodní sdělení* [online] uoou.cz, 13.12.2013 [cit. 19.11.2018]. Dostupné z: <https://www.uoou.cz/nevyzadana-obchodni-sdeleni/d-6273>.

ÚŘAD PRO OCHRANU OSOBNÁCH ÚDAJŮ. *Dozorová činnost* [online] uoou.cz, 13.12.2013 [cit. 24.2.2019]. Dostupné z: <https://www.uoou.cz/dozorova-cinnost/ds-1277/p1=1277>.

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)* [online]. uoou.cz, 7. února 2018 [cit. 12. března 2019]. Dostupné na <https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385>.

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *K dodržování povinnosti přijmout a provést bezpečností opatření k ochraně osobních údajů ve veřejnoprávní sféře* [online]. uoou.cz, 21. března 2013 [cit. 12. března 2019]. Dostupné na <https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385>.

ÚŘAD PRO OCHRANU OSOBNÁCH ÚDAJŮ. *Pojem osobní údaj* [online] uoou.cz, 13. prosince 2013 [cit. 19. listopadu 2018]. Dostupné z: < https://www.uoou.cz/pojem-osobni-udaj/d-1751/p1=2427>.

ÚŘAD PRO OCHRANU OSOBNÁCH ÚDAJŮ. K rozsahu osobních údajů shromažďovaných subjektem veřejné správy [online] uoou.cz, 13. listopadu 2013 [cit. 12. března 2019] Dostupné z: <https://www.uoou.cz/k-nbsp-rozsahu-osobnich-udaju-shromazdovanych-subjektem-verejne-spravy/d-5519/p1=1099>.

VACHTL, Jiří. *Čína zakázala milionům neposlušných občanů cestovat, mají nízké skóre* [online]. idnes.cz, 3. března 2019 [cit. 7. března 2019]. Dostupné na <https://www.idnes.cz/zpravy/zahranicni/cina-kamery-zakaz-cestovani.A190302_213230_zahranicni_chtl>.

JINÉ

Doporučení veřejného ochránce práv k naplňování práva na rovné zacházení s žadateli o pronájem obecního bytu ze dne 9.3.2010, sp. zn. 22/2010/DIS/AHŘ, dostupné na https://www.ochrance.cz/fileadmin/user_upload/DISKRIMINACE/Doporuceni/Obecni_byty.pdf

Stanovisko Úřadu č. 3/2011 z listopadu 2011 k ochraně osobních údajů podnikajících fyzických osob. Dostupné na: < https://www.uoou.cz/files/stanovisko_2011_3.pdf>

Důvodová zpráva k zákonu č. 110/2019 Sb., o zpracování osobních údajů. Dostupná na: < https://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=138&CT1=0>

Stanovisko Pracovní skupiny WP29 2/2017 ke zpracování osobních údajů na pracovišti ze dne 8. června 2017, dostupné na: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30203>.

Pokyny Pracovní skupiny WP29 týkající se pověřenců pro ochranu osobních údajů naposledy revidované a přijaté dne 5. dubna 2017, dostupné na: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31880 >.

Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí podle právního stavu k 10. srpnu 2017. Dostupné na <https://www.mvcr.cz/gdpr/clanek/aktualizovana-metodika-k-poverencum-pro-ochranu-osobnich-udaju.aspx>.

Metodický návod ministerstva vnitra k aplikaci zákona o registru smluv ze září 2018, č.j. MV-37683-1/EG-2018, s. 51.

Příloha k Průvodci pro přípravu obcí na požadavky GDPR. Dostupná na: <https://www.mvcr.cz/gdpr/soubor/gdpr-modelove-situace-zverejnovani-v-obecnim-periodiku.aspx>.

Abstrakt

Předmětem diplomové práce je zhodnocení právního stavu ochrany osobních údajů před a po účinnosti GDPR, a to především se zaměřením na projevy této legislativy v oblasti veřejné správy. První část práce tak analyzuje stav v době před účinnosti GDPR, zákon č. 100/2000 Sb., o ochraně osobních údajů představuje zásadní právní předpis v této oblasti. Na tento oddíl pak navazuje rozbor samotného Nařízení včetně nových povinností s ním souvisejících. Konečně je pak pohlíženo na konkrétní aspekty, které jsou pro veřejnou správu relevantní. Cílem práce je poté pokusit se vyhodnotit vlivy současné právní úpravy na činnost veřejné správy a vyhodnotit celkový přínos při procesu zpracování osobních dat.

Abstract

The subject of this diploma thesis is the evaluation of the legal status of personal data protection before and after the effectiveness of GDPR, especially with focus on display of this legislation in the area of public administration. The first part of the thesis analyzes the situation before the GDPR comes into effect, when Act No. 100/2000 Coll., on the protection of personal data represents an essential legislation regulation in this agenda. This section is followed by an analysis of the Regulation itself, including new related obligations. Finally, the specific aspects that are relevant to public administration are viewed. The aim of the thesis is to try to evaluate the effects of the current legislation on the activities of public administration and to evaluate the overall contribution in the process of personal data processing.

Seznam klíčových slov

Ochrana osobních údajů

GDPR

Úřad pro ochranu osobních údajů

Právo na informace

Pověřenec pro ochranu osobních údajů

Veřejná správa

Posouzení vlivu na ochranu osobních údajů

Key words

Personal data protection

GDPR

The office for personal data protection

Right to information

Data Protection Officer

Public administration

Data Protection Impact Assessment