ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PRÁVNICKÁ

DIPLOMOVÁ PRÁCE

Srovnání zákona o ochraně osobních údajů s nařízením GDPR

Sabina Pardusová

Plzeň 2019

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci zpracovala samostatně, a že jsem vyznačila všechny prameny, z nichž jsem pro svou práci čerpala způsobem ve vědecké práci obvyklým.

V Horním Jelení dne 20. 3. 2019 Sabina Pardusová

Poděkování

Tímto bych chtěla poděkovat, vedoucímu mé diplomové práce, JUDr. et PhDr. Janu Malastovi, Ph.D. za její odborné vedení, vstřícný přístup a za pomoc, rady a připomínky při zpracování této práce.

Obsah

1. Úvod

Jako téma své práce jsem si vybrala velmi aktuální a živou problematiku, a to problematiku ochrany osobních údajů. Téma osobních údajů a zejména jejich ochrany je spolu s masivním rozvojem především sociálních sítí hodně diskutované téma. Čím dál častěji můžeme v médiích zaznamenat rozsáhlé zneužití osobních údajů, a to jak při jejich zpracování či uchování. Vzhledem k nedostačující právní úpravě bylo potřeba jít s dobou a zareagovat na tento extrémně rychlý růst a současné tendence jejich zneužití.

V polovině roku 2016 Evropská unie schválila poslední variantu očekávané velkolepé právní úpravy právě v oblasti ochrany osobních údajů. V platnost vstoupilo Obecné nařízení GDPR, kterému byla stanovena více než dvouletá legisvakanční lhůta, a to proto, aby se s ní všichni mohli náležitě vypořádat. Toto nařízení by mělo představovat komplexní úpravu v oblasti ochrany osobních údajů, jež definuje mnoho nových pojmů a zejména pak i povinnosti z něj plynoucí.

Cílem mé práce bude zhodnotit dosavadní právní úpravu ve světle práva evropského a zejména porovnání těchto dvou právních regulací. Chtěla bych vyzdvihnout především oblasti, ve kterých došlo k největším změnám a těm, které jsou pro nás úplnou novinkou, nebo které my jako jeho adresáti můžeme nejvíce pocítit. Je ale nutné podotknout, že se jedná o velmi obsáhlé téma, jež zahrnuje celou řadu pojmů a institutů, které by si zasloužily větší pozornost. Já však s ohledem na požadovaný rozsah práce si chci vytyčit za cíl na tyto pojmy zejména upozornit a vyzdvihnout vždy to nejdůležitější nebo nejběžnější. To vše čistě z mého subjektivního pohledu.

Úvodní kapitolu zaměřím a věnuji definicím základního pojmosloví, především tedy samotnému pojmu „osobní údaj.“ Tento pojem si rozebereme od jeho definice až po jeho velmi široký obsah. Přiblížíme si pojmy zvláštních kategorií osobních údajů, také označovaných jako citlivé údaje. Cílem práce rozhodně není podrobně definovat veškeré pojmy, které jsou za osobní údaj považovány, podrobněji zmíníme jen ty hlavní, přímo definované nařízením, jako jsou údaje genetické, biometrické a údaje o zdravotním stavu. Z dalšího nepřeberného množství údajů si vyberu pouze ty, jež jsou nejběžnější a vzbuzují řadu diskuzí. Dále si pak

přiblížíme pojmy anonymních údajů a pseudonymizace, které se mohou na první pohled zdát synonymy.

Další část práce bude zaměřena na okolnosti vzniku ochrany osobních údajů, jejich historický vývoj, a to jak celosvětový, tak náš vnitrostátní. U kapitoly věnované vnitrostátní právní úpravě logicky narazíme na úpravu Evropské unie, jež je do našeho právního řádu inkorporována a je z pohledu této práce stěžejním prvkem. Touto kapitolou se tak dostáváme k samotnému jádru problému, a to případu Obecného nařízení GDPR, které se v uplynulém roce stalo, troufám si tvrdit, nejdiskutovanějším pojmem.

Subjekt údajů je rozhodně pojem, jenž v tomto tématu hraje jednu z hlavních rolí, a potřebujeme se zaměřit na jeho postavení a zejména nově definovaná poměrně rozsáhlá práva, která mu obecné nařízení přiznává.

Stěžejní kapitola práce bude věnována procesu zpracování osobních údajů. Nejprve z pohledu naší právní úpravy, tedy zákona o ochraně osobních údajů. Druhá část bude logicky věnována zpracování z pohledu Obecného nařízení, bude zahrnuta zcela novými instituty, jež nařízení zavádí. V této kapitole se budu zabývat jak základními zásadami, které celý tento proces ovládají, tak právy a povinnostmi správců a zpracovatelů, jakož jejich vzájemný vztah. Značnou pozornost věnuji i institutu souhlasu se zpracováním, od něhož se poměrná část zpracování zcela odvíjí. Pověřenec pro ochranu osobních údajů je zcela novým institutem, který si rovněž zaslouží náležitou pozornost.

S procesem zpracování úzce souvisí i jejich ochrana v rámci zabezpečení osobních údajů, která z pohledu GDPR zaznamenala taktéž značné změny, zejména konkretizací jednotlivých pojmů. Za zmínku stojí i institut posouzení vlivu, jež jsme doposud v našem právním řádu neznali.

Dozorčí činnost v ochraně osobních údajů je prováděna nezávislými správními orgány, které si v této části definujeme z pozice jejich postavení, působnosti a pravomoci. Následující část se bude zabývat přeshraničním předávání osobních údajů, a to znovu nejprve z pohledu vnitrostátní právní úpravy a poté z pohledu GDPR, která se hodně věnuje předávání informací do třetích zemí.

Poslední část této práce se bude zabývat správními tresty za porušení ochrany osobních údajů. Úvodní část kapitoly bude věnována definici samotného přestupku. Přestupky si opět přiblížíme nejprve z pohledu stávající právní úpravy. Sankce stanovené GDPR vyvolaly po svém zveřejnění mnohé diskuse a můžeme říct i paniku, čemuž se nelze divit, sankce, jež Obecné nařízení stanovuje, jsou opravdu vysoké.

S ohledem na to, že se, jak už jsem zmiňovala, jedná se o novou právní úpravu. Potýkala jsem se s horší dostupností zdrojů, zejména pak co se týká judikatury, která samozřejmě ještě není k dispozici. Ve své práci jsem pracovala s právní úpravou platnou a účinnou k co nejaktuálnějšímu datu, avšak pro účely práce uzavřenou ke dni 31. 12. 2018. Nicméně i přesto stále sleduji vývoj adaptačního zákona, jenž podle dostupných informací nebude ke dni odevzdání práce mít dokončený celý legislativní proces, který je nad očekávání velmi komplikovaný a jenom jemu samotnému by se dala věnovat celá diplomová práce.

2. Základní pojmy

Informace je základním pojmem, který je podkladem pro další odvozené definice pracující s tímto pojmem, definice primárního pojmu informace je obsažena v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím následovně: „*Informací se pro účely tohoto zákona rozumí jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního.“*[1] Právní řád České republiky upravuje a definuje několik konkrétních druhů, a to informace o právu na informace o životním prostředí, definice utajované informace a samozřejmě definici osobního údaje, kterou se budeme dále zabývat. Právo na informace tak nemůžeme stavět do protipólu s pojmem ochrany osobních údajů, ale musíme jej chápat jako jeho prvotní předpoklad.

Právo na informace je jedním z politických práv zakotveným Listinou základních práv a svobod. Svoboda projevu je dalším příbuzným právem, kdy jejich vývoj byl společný, stejně tak jako jejich zakotvení v čl. 17 odst. 1 Listiny: *„Svoboda projevu a právo na informace jsou zaručeny.“*[2] Jedná se o právo občanů vůči státu, orgánům veřejné moci, jež mají povinnost reagovat na jednotlivé žádosti o poskytování informací, ale i o svých činnostech samostatně informovat. Z poskytnutí informací jsou informačním zákonem v § 7 až § 11 vyloučeny informace utajované, informace týkající se osobnosti, které spadají do působnosti občanského zákoníku nebo zákona o ochraně osobních údajů, obchodní tajemství apod.

2.1. Osobní údaj

Poměrně široké definice osobního údaje nalezneme v obou účinných právních úpravách takřka v totožném znění, a dokonce i na shodném místě, a to v § 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále také jen Zákona č. 101/2000, Zákona nebo ZoOÚ), kdy se pod tímto pojmem rozumí *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt*

[1] §3 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím

[2] Čl. 17, odst. 1 Usnesení č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky

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.“[3] a článku 4 Obecného nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně osobních údajů (dále také jen Obecné nařízení nebo GDPR), kdy pro účely nařízení rozumíme *„osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*[4] Zde si tedy úpravy nikterak neodporují, což je vcelku pochopitelné, a je nutné si uvědomit, že aplikace výše zmíněných úprav nastává až při zpracování osobních údajů.

Úřad pro ochranu osobních údajů ve svém stanovisku č. 3/2012 speciálně upozorňuje na pojem projevu osobní povahy, jež je upraven v § 81 a násl. občanského zákoníku. Je podstatné tyto pojmy nezaměňovat, neb se jedná o dva samostatné právní instituty, přestože projev osobní povahy může v některých případech obsahovat osobní údaj a dochází tak k jejich překrývání. V konkrétních případech se může jednat o podobiznu, písemnost osobní povahy či zvukový projev.[5]

Osobním údajem je tedy každá informace, která není zákonnou úpravou přesně definována a není tak ani omezena. Z toho vyplývá, že zde není předpoklad pravdivé informace, s čímž se musíme vyrovnat, a to pomocí rozlišení na informace objektivní, soudy, hodnocení, závěry apod.[6] Pokud je tedy fyzická osoba na základě shromážděných údajů či jiným způsobem identifikovatelná, jedná se o údaj osobní. Samotná definice je pak velmi široká, ale odpovídá rozmanité agendě při zpracování osobních údajů v praktickém životě. Z tohoto nám vyplývá

[3] § 4 písm. a, zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[4] Čl. 4 odst. 1, Obecného nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně osobních údajů.
[5] Stanovisko č. 3/2012, k pojmu osobní údaj, ÚOOÚ, březen 2012, dostupné z www.uoou.cz/stanovisko-c-3-2012-k-pojmu-osobni-udaj/d-1535/p1=1863
[6] BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012*. Olomouc: ANAG, 2012. Právo (ANAG), str. 15.

poznatek, že na základní definici nelze pohlížet izolovaně a bez znalosti dalších okolností týkajících se zpracování osobních údajů.[7]

Je důležité si uvědomit, že výše popsaná identifikace fyzické osoby může nastat mnoha způsoby. Ne vždy jen pomocí „tradičních" způsobů, a to dle jména, příjmení, adresy, data narození či rodného čísla. Naproti tomu lze subjekt údajů rozpoznat i na základě přiděleného zaměstnaneckého kódu či IP adresy.

Základním hlediskem pro posouzení, zda se jedná o osobní údaj, je pojem určenosti nebo určitelnosti, tedy okolnosti zjištění identity subjektu údajů. Jde tudíž o to, že správce nebo další osoba vytvoří přímou vazbu mezi údajem a fyzickou osobou, a to především pomocí identifikátorů.[8] Vztah informace ke konkrétní osobě se vytváří pomocí identifikátorů, které nám umožní jednoznačně potvrdit, že se jedná o onu konkrétní osobu. Základní identifikátory můžeme rozdělit na identifikátory, jež nám byly přiděleny pro obecnou identifikaci, jako je jméno a příjmení. Další kategorií jsou identifikátory vrozené, což jsou např. biometrické údaje. Poslední kategorií jsou identifikátory účelně přidělené, jako např. PIN, platební karta, adresa našeho bydliště.[9]

V zásadě identifikaci rozlišujeme na přímou a nepřímou. Přímá zahrnuje údaje o jméně, příjmení a adrese. Jakákoliv jiná identifikace subjektu údajů se označuje za nepřímou. Příklad běžné kombinace osobních údajů obsahuje navíc datum narození, kdy tato „velká čtyřka" údajů ve valné většině jednoznačnou identifikaci umožní. Při zpracování více údajů v takovýchto kombinacích je nutno dodržovat jejich minimum, některé údaje vzhledem k účelu zpracování mohou být nadbytečné.[10] V běžném společenském životě se ale setkáme i s dalšími identifikátory, mezi které patří třeba povinné viditelné nošení jmenovek. Tato základní identifikace však souvisí pouze se specifickou situací, zejména v rámci výkonu profesní činnosti, ale nelze je plošně rozšiřovat do běžného života.[11]

Obecné nařízení nám v dalších odstavcích č. 4 nabízí definice neméně podstatných pojmů, jež jsou subsumovány do oné hlavní definice osobních údajů. Jedná se o pojmy genetických a biometrických údajů, údaj o zdravotním stavu,

[7] Stanovisko č. 3/2012, k pojmu osobní údaj, op. cit.
[8] Stanovisko č. 3/2012, k pojmu osobní údaj, op. cit.
[9] BARTÍK, Václav a Eva JANEČKOVÁ, 2012, op. cit., str. 16.
[10] Stanovisko č. 3/2012, k pojmu osobní údaj, op. cit.
[11] BARTÍK, Václav a Eva JANEČKOVÁ, 2012, op. cit., str. 17.

pseudonymizace a profilování. Tyto pojmy jsou povinně zavedeny právě až obecným nařízením GDPR, ale naše právní úprava s těmito prvky počítala a pracovala i doposud. Tyto definice však neobsahují úplné, tedy taxativní výčty osobních údajů, ale pouze demonstrují ty nejčastěji užívané a zpracovávané. Z působnosti GDPR jsou také vyloučeny údaje získané v rámci činností osobní povahy, jež nemají obchodní ani institucionální charakter, tedy údaje, které zpracováváme výhradně pro osobní potřebu.

2.2. Kategorie osobních údajů

Osobní údaje můžeme pro snadnější orientaci rozdělit na adresné a identifikační, citlivé, popisné a údaje o jiné osobě. Do skupiny adresných a identifikačních údajů řadíme údaje, jako jsou jméno, příjmení, datum a místo narození, rodinný stav, rodné číslo, státní příslušnost, adresa trvalého bydliště, ale i adresa doručovací, telefonní spojení, e-mail apod. Nesmíme opomíjet ani skupinu dalších přidělovaných číselných kódů, jako jsou identifikační čísla, DIČ, čísla občanského a řidičského průkazu nebo cestovního pasu. A v neposlední řadě kategorie záznamů fotografických, kamerových a audio.

Kategorie citlivých údajů, jak již z názvu vyplývá, zahrnuje údaje, jež si zasluhují zvláštní péči. Spadají sem informace o národnostním, rasovém, etnickém původu, sexuální orientace, náboženské příslušnosti apod. Do třetí skupiny tzv. popisných údajů řadíme údaje o odborných znalostech, dovednosti, dosažené vzdělání, kulturní profil, zaměstnání, mzdu, příjem z důchodu, údaje o zdravotní pojišťovně bankovní spojení a další. Jako poslední skupinu označíme údaje o jiné osobě, mezi které spadají např. adresní a identifikační údaje člena rodiny, partnera, manžela, dítěte a jiné.

2.2.1. Citlivé údaje

Zákonnou definici pojmu citlivý údaj nalezneme v § 4 odst. 1, písm. b zákona č. 101/2000 Sb., o ochraně osobních údajů*: „Citlivým údajem je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj,*

který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.“[12] Obecné nařízení ve svém čl. 9, odst. 1 obsahuje negativní definici, kdy zakazuje zpracování zvláštních kategorií osobních údajů, konkrétně: „*Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.“*

Pokud se podíváme na porovnání obou výše uvedených definic, nalezneme jeden patrný rozdíl, a to ten, že podle Obecného nařízení údaj o odsouzení za trestný čin již nebude považován za zvláštní kategorii osobních údajů, neboť je nově upraven v samostatném článku 10 GDPR *„zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů“*. Další, možná méně nápadnou odchylkou od úpravy v zákoně č. 101/2000 Sb., Obecné nařízení za zvláštní kategorii nepovažuje údaj o národnostním původu. Novinkou naproti tomu je zařazení údaje o sexuální orientaci. Zařazení genetických a biometrických údajů pod tuto kategorii máme nově omezenou jen v určitých situacích, a to jsou-li zpracovávány pro účely jedinečné identifikace fyzické osoby. Ze zvláštní kategorie citlivých údajů je taktéž vyňata skupina, jež zasluhuje vyšší stupeň ochrany, jako jsou údaje zpracovávané výhradně pro zdravotní účely. V dalších výše popsaných údajích nedošlo k žádné změně a byla zachována kontinuita jejich charakteru.

Jedná se o taxativně vymezenou množinu údajů, které jsou charakteristické zejména tím, že samy o sobě mohou uškodit v běžném životě, a to jak ve společnosti, zaměstnání, škole, a mohou být především příčinou diskriminace. Jejich neoprávněné zpracování může výrazně ohrozit či zasáhnout do jiných práv a soukromí, a proto jim je poskytována zvýšená ochrana, a to především zákaz jejich zpracování.

2.2.2. Genetický údaj

Genetický údaj, jak již bylo řečeno výše, řadíme do zvláštní kategorie osobních údajů, a konkrétně tímto pojmem rozumíme *„osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné*

[12] § 4, písm. b zákona č. 101/2000 Sb.

informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby".[13] Konkrétně jde zejména o informace chromozomů, kyseliny deoxyribonukleové (DNA) nebo ribonukleové (RNA), krevní skupinu, RH faktor krve.

Podkategorií genetických údajů jsou osobní údaje o zdravotním stavu, jímž se rozumí *„osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu."*[14] Tyto údaje zahrnují všechny informace, jež vypovídají o minulém, současném a budoucím tělesném či duševním zdraví subjektu údajů. Jsou zde zahrnuty veškeré informace o fyzických osobách shromážděné pro účely zdravotní péče a jejího poskytování, jako jsou vyšetření, tělesné látky, genetické údaje, biologické vzorky a jakékoliv informace o nemoci, postižení, anamnéze, rizicích nezávisle na jejich původu, a bez ohledu na to, zda pocházejí od lékaře či jiného zdravotníka, nemocnice, zdravotnických prostředků, diagnostických testů apod.[15]

2.2.3. Biometrický údaj

Rovněž biometrické údaje spadají do zvláštní kategorie osobních údajů. Vnitrostátní úprava zákona č. 101/2000 Sb. zařazovala biometrické údaje do skupiny citlivých údajů uvedených v § 9. Díky rozšíření používání biometrických znaků zejména v pracovněprávních vztazích reagoval Úřad pro ochranu osobních údajů vydáním stanoviska č. 3/2009, jež upravilo zpracování takových údajů do dvou kategorií.[16] První kategorie zahrnovala biometrické údaje, které byly okamžitě převedeny na číselnou řadu, a jejich zpětná rekonstrukce byla vyloučena. Proto tyto údaje mohly být považovány za zpracování běžných osobních údajů. Do druhé kategorie se řadily systémy, jež aktivně s biometrickými údaji pracovaly, např. ověřování podpisů, spuštění nebo aktivace mobilního telefonu, počítače apod. Tyto údaje pak podléhaly režimu zpracování jako citlivé údaje.

Díky vstupu Obecného nařízení v platnost, jež tyto údaje výslovně konkretizuje a řadí pod kategorii zvláštních osobních údajů, Úřad upravil své stanovisko

[13] Čl. 4 bod 13 Obecného nařízení GDPR
[14] Čl. 4 bod 15 Obecného nařízení GDPR
[15] Recitál 35 Obecného nařízení GDPR
[16] Stanovisko č. 3/2009, biometrická identifikace nebo autentizace zaměstnanců, ÚOOÚ, červen 2017, dostupné z www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=23858

ve světle nové platné právní úpravy, a to tak, že obě kategorie sjednotil pod jednotná pravidla spadající pod zpracování zvláštních kategorií osobních údajů.[17]

V Obecném nařízení GDPR jsou definovány jako *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“*.[18] Dalšími příklady mohou být snímky oční duhovky a sítnice, podpis, zabarvení hlasu, chůze apod. S ohledem na to, že jsou biometrické údaje jedinečné a téměř neměnné, jsou tak vždy vztahovány k jednoznačnému určení konkrétní osoby a jejich další zpracování je podřízeno ochraně osobních údajů.

Nejčastější použití v pracovněprávních vztazích nastává při užívání přístupových karet a docházkových systémech, kde se třeba pomocí identifikačních karet snaží omezit klamání zaměstnavatele nebo otiskem prstu má dojít k zajištění přístupu oprávněných osob do chráněných prostor či chráněných informací.[19] Samotné zpracování údajů v docházkových systémech je nutné posuzovat za nepřiměřené, a to ve vztahu rozsahu i účelu zpracování. Pokud je však zaměstnanci přiděleno osobní číslo, které vystupuje jako druhý identifikátor, potom už tyto údaje mohou být zpracovávány ve světle účinných právních úprav na ochranu osobních údajů. Je ovšem třeba také brát zřetel na povinnost zaměstnavatele plynoucí z § 316 zákona č. 262/2006 Sb., zákoník práce, o zákazu sledování zaměstnance.

2.2.4. Anonymní údaj

Zákon č. 101/2000 Sb. ve svém § 4 písm. c) upravuje další odchylku ze základního pojmu osobní údaj, kterým rozumíme údaj *„buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů“*.[20] Obecné nařízení v úvodním recitálu č. 26 uvádí, že „*zásady ochrany osobních údajů by se proto neměly vztahovat na anonymní informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani*

[17] Nonnemann František, Skácelová Michaela, Zpracování biometrických údajů ve světle obecného nařízení osobních údajů (GDPR), dostupné z www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-ve-svetle-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-106028.html
[18] Čl. 4 bod 14 Obecného nařízení GDPR
[19] Stanovisko č. 1/2017, biometrická identifikace nebo autentizace zaměstnanců, ÚOOÚ, červen 2017, dostupné z www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29089
[20] § 4, písm. c) zákona č. 101/2000 Sb.

na osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným.“[21]

V případě, že se budou zpracovávat informace, které byly anonymní již na samém počátku, tedy při získávání takových informací, a nelze je přiřadit ke konkrétní fyzické osobě, jež není ani z dalších shromážděných informací určitelná, nebude se vůbec jednat o osobní údaj ve smyslu tohoto zákona, potažmo Obecného nařízení.[22] Takovýto údaj neobsahuje žádné informace o fyzické osobě či možnosti jiné identifikace a zároveň je vyloučena možnost zpětného spojení.[23] Obě právní úpravy se tak shodují, že pro ně tyto informace v podstatě nejsou natolik relevantní a nepředstavují takové riziko, které by zasluhovalo větší pozornost v podobě ochrany osobních údajů. Ani jedna právní úpravě se tak nezabývá zpracováním těchto anonymních informací, a to včetně zpracování pro statistické nebo výzkumné účely. V těchto případech dochází k tomu, že správce údajů, jenž shromažďuje údaje o jméně, příjmení, věku a dosaženém vzdělání, vymaže jméno a příjmení. Zbývající údaje tak může bez problému a omezení zpracovávat, neboť povaha takových informací je natolik vágní, že není potřeba jejich ochrana výše uvedenými předpisy.

2.2.5. Pseudonymizace

Pseudonymizace je nový pojem zavedený Obecným nařízením a obsahuje údaje, jež nejsou anonymizovanými údaji, a proto se na ně vztahuje regulace GDPR. Pseudonymizací označujeme činnosti *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě“*.[24]

Použití tohoto institutu má za cíl omezit rizika pro dotčené subjekty údajů a být nápomocen při řádné činnosti správců a zpracovatelů. Informace, na něž je tento institut použit, jsou považovány za informace o fyzických osobách a rozhodně není primárním cílem předem vyloučit jakákoliv opatření týkající se ochrany osobních

[21] Recitál 26 Obecného nařízení GDPR
[22] BARTÍK, Václav a Eva JANEČKOVÁ, 2012, op. cit., str. 17.
[23] Kohútová Zuzana, Anonymizace, pseudonymizace a šifrování osobních údajů jako bezpečnostní opatření dle GDPR, dostupné z fly-eye.cz/blog-detail-1.html
[24] Čl. 4 bod 5 Obecného nařízení GDPR

údajů.[25] Použití identifikovaných prostředků podléhá objektivním faktorům, mezi které řadíme náklady a čas potřebné k identifikaci, a to vzhledem k dostupným technologickým prostředkům v době zpracování.[26] Nařízení stanoví, že se nevztahuje na zpracování anonymních informací, a to ani pro statistické či výzkumné účely.

Klasickým příkladem může být nahrazení identifikačních údajů, jako je třeba jméno a příjmení, kódovaným údajem pomocí klíče, tedy nějakým bezvýznamným identifikátorem, např. číslem. Vzniknou tak dva soubory dat, které mají být uchovány odděleně, a ten, kdo má přístup k oběma zároveň, podléhá výše uvedené ochraně.

2.2.6. Fotografie

Fotografie, audiozáznamy, kamerové záznamy a ostatní patří mezi skupinu nejběžněji používaných osobních údajů, které si zasluhují zvláštní pozornost. Jedná se o dokumenty, jež často umožňují identifikaci osob na základě podoby či hlasu. Portrétní fotografie sama o sobě vypovídá o rasovém, etnickém původu a případná pokrývka hlavy může zobrazovat i informace o náboženském vyznání apod. Fotografie nebo jiný záznam člověka je dokumentem osobní povahy, který obsahuje charakteristiky subjektů údajů, mimo jiné i biometrické údaje, jež spadají pod úpravu § 4 ZoOÚ a případně pro ně může být stanoven i přísnější režim ochrany. Jedním z častých dotazů je úprava právního režimu při pořizování, používání, šíření nebo zveřejňování fotografií a jiných záznamů. Odpovědí na tuto problematiku může být stanovisko Úřadu pro ochranu osobních údajů č. 12/2012.

Zpracování takovýchto údajů může probíhat v režimu zpracování osobních údajů, jakož i pouze v režimu zákona č. 89/2012 Sb., občanský zákoník. Pro odlišení těchto dvou variant hraje roli, zda fyzická osoba jedná sama ze své vůle, a to za použití svých vlastních záznamů, nebo se na straně druhé jedná o záznamy jiných osob. Dále je také důležité brát zřetel na to, zda je tu zvýšené nebezpečí zneužití či se záznamy veřejně zpřístupňují na internetu.

Jedná se o téma velmi často diskutované, přesto si jej každý vykládá trošku po svém a jsou mu přikládány i různé významy. My je můžeme rozčlenit do čtyř

[25] Recitál č. 28 Obecného nařízení GDPR
[26] Recitál č. 26 Obecného nařízení GDPR

režimů. První dva režimy zpracování podléhají čistě občanskému zákoníku. První režim se věnuje úpravě časově omezených nebo příležitostných pořízení a následného použití fotografických a jiných záznamů. Tyto záznamy nejsou použity při vytváření evidence o fyzických osobách, a kromě běžné identifikace, jako je jméno a příjmení, k nim nejsou přiřazovány další osobní údaje. Zde se jedná nejčastěji o případy pořizování záznamů ze schůzí, jednání, kulturních, společenských nebo sportovních akcí. Tento přístup podporuje i recitál 51 Obecného nařízení GDPR, který uvádí, že zpracování fotografií nemá být systematicky považováno za zpracování zvláštních kategorií, neboť na fotografie se úprava biometrických údajů vztahuje pouze v některých případech, kdy je za použití technických prostředků umožněna jednoznačná, autentická identifikace fyzické osoby. Druhý režim potom zahrnuje operace prováděné výlučně pro svou osobní potřebu nebo výkon domácích činností, a to např. zpracování a shromažďování fotografií pro rodinnou potřebu nebo třeba monitorování vlastního domu kamerovým systémem. V těchto případech, ačkoliv režim ochrany údajů nespadá pod zákon o ochraně osobních údajů, nelze ovšem vyloučit odpovědnost za soukromoprávní delikt v souvislosti s porušením práva na ochranu osobnosti, případně potom i trestněprávní odpovědnost.

Třetí způsob již zahrnuje zpracování osobních údajů podléhající režimu ochrany stanovený zákonem o ochraně osobních údajů, potažmo Obecným nařízením GDPR. Jedná se o zpracování osobních údajů zachycených pomocí monitorování prostor podléhající úpravě stanovené zvláštním zákonem. V konkrétních případech může jít o zpracování fotografií v informačních systémech Policie ČR, uchovávání podobizen, vydávání služebních průkazů a podobně. Tento režim může být v některých případech omezován nutností souhlasu subjektu údajů, a to například se zveřejňováním fotografií zaměstnanců na internetových stránkách. Oproti tomu informace o pracovním zařazení požadavku souhlasu již nepodléhá.

Posledním režimem je kategorie zpracování citlivých údajů, jež je samozřejmě chráněna, jak zákonem č. 101/2000 Sb., konkrétně ustanovením § 9, tak nařízením GDPR. Zde se jedná o zpracování snímků, obrazových a zvukových záznamů o zdravotních údajích pacienta, léčebných postupů, které mohou být součástí zdravotnické dokumentace. V ostatních případech zpracování takto citlivých údajů podléhá nutnosti souhlasu dotčeného subjektu údajů.

Závěr nám tedy vyplývá takový, že ne každé pořizování fotografií či nahrávek podléhá režimu ochrany osobních údajů. Zároveň zde není vyloučena ani ochrana prostřednictvím soukromoprávní žaloby, jež v některých případech může dostat přednost před veřejnoprávním zásahem ze strany Úřadu.

2.2.7. Rodné číslo

Rodné číslo je jednoznačný číselný identifikátor přidělovaný obyvatelům České republiky a je do takové míry zvláštním osobním údajem, že má dokonce svou vlastní zvláštní právní úpravu v zákoně č. 133/2000 Sb., o evidenci obyvatel a rodných čísel a o změně některých zákonů (dále jen ZoEO). Je tvořeno jedinečnou řadou čísel, která mají přesně definovaný svůj význam a můžeme z něj odvodit údaje, jako jsou datum narození a pohlaví dané osoby. Díky povaze takového identifikátoru jej řadíme mezi osobní údaje, avšak podle Obecného nařízení GDPR jej nezačleňujeme do kategorie citlivých údajů. Vazbu mezi právními úpravami nalezneme v § 5 odst. 2 věta první a v § 13 odst. 9 a § 13c odst. 1 ZoEO, primárně však užití rodného čísla musíme posuzovat z pohledu ZoEO.

Podobná jednoznačná identifikace je užívána v mnoha dalších zemích, shodný formát ale nalezneme pouze na Slovensku. Ekvivalenty tohoto identifikátoru jsou používány převážně pro účely sociálního, důchodového nebo zdravotního pojištění. Využití rodného čísla je však i v soukromoprávní sféře, a to především pro označení stran soudních sporů, tedy účastníků řízení. Z tohoto hlediska je takováto identifikace pouze alternativa, nikoliv povinnost. Dále podle § 28 exekučního řádu využívá exekutor rodné číslo při provádění své činnosti.

Díky tomu, že rodné číslo řadíme mezi osobní údaje, je jeho zpracování možné pouze se souhlasem jeho nositele nebo v případech zákonem dovolených. V případě neoprávněného užití rodného čísla se dopouštíme správního deliktu, který může být Úřadem pro ochranu osobních údajů potrestán pokutou.

Čísel a číselných kódů spojovaných s konkrétní fyzickou osobou existuje nespočet, mezi ty nejčastější řadíme PIN, jež chrání platební karty, přístupové kódy do různých informačních a obdobných systémů. Tyto kódy však nemají trvalý charakter, neboť je lze poměrně lehce změnit. Naproti tomu rodné číslo je s danou fyzickou osobou spojeno natolik pevně, že splňuje požadavky vyjádřené v § 4 ZoOÚ.

3. Právní úprava

Ochrana osobních údajů je úzce spojena s ochranou soukromí, která se vyvíjí od samého počátku společnosti. Veškeré záležitosti na dnešní dobu, i poměrně intimní, se často odehrávaly veřejně a k ochraně docházelo až zhruba od středověku, kdy se ochrana začala rozvíjet nejen u významných osob z nejbohatších vrstev společnosti.

Z tohoto historického exkurzu můžeme sledovat, jak byly osobní údaje v minulosti hojně zneužívány a měly na svědomí řadu nehezkých historických událostí. Zde se vyvinuly základní principy, které se přizpůsobovaly trendům společnosti, technickému pokroku a sociálním jevům.

Za první milník ochrany soukromí můžeme považovat náboženské války, z nichž vyvstala potřeba uchovávat své soukromí. Dalším milníkem by mohla být Velká francouzská revoluce, kde mírně řečeno nepokoje způsobené rozdílnými názory vedly ke snaze o uchování svého soukromí. Tím největším impulsem k ochraně soukromí a uplatnění ochrany osobních údajů bylo nepochybně období nacismu, ruku v ruce s uplatňováním rasových zákonů.

Prvním psaným dokumentem dotýkajícím se zčásti ochrany osobních údajů byla Deklarace práv člověka a občana z roku 1789. Na tuto Deklaraci nám nepřímo navázala Všeobecná deklarace lidských práv z roku 1948, která je považována za katalog právních obyčejů, a to přesto, že nikdy nenabyla právní závaznosti. Zde nás zajímá zejména čl. 12: *„Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst.“* Každý by měl mít proti takovýmto zásahům právo na zákonnou ochranu. Následný, již právně závazný Mezinárodní pakt o občanských a politických právech, jenž do svého čl. 17 převzal doslovné znění výše zmíněného čl. 12 Všeobecné deklarace lidských práv.

3.1. Vývoj ochrany osobních údajů

Ochrana osobních údajů ve svém pravém významu je tak poměrně novým právním odvětvím, které se objevuje od 70. let 20. století, a to zejména v západních státech, jež začaly reagovat na současnou problematiku. Nový směr ochrany nastal spolu s rozvojem výpočetní techniky. Rozvoj elektronické komunikace, vznik sociálních sítí, obchodování v elektronické podobě otevřelo velký prostor dat,

která se shromažďovala, často pro nežádoucí účely. Druhou stranou mince je také obrovská možnost jejich zneužití, z čehož vzniklo např. obchodování s osobními údaji pomocí falešných identit.

Z počátku se jednalo převážně o jakýsi evropský boom, postupně však ochrana osobních údajů a její hlavní principy začaly pronikat do právních úprav mimoevropských zemí. Naproti tomu značná území tuto úpravu stále neakceptují nebo alespoň ne v takové míře, jako např. USA.

Spolu se zvyšující se životní úrovní, globalizací, technologizací vystávala čím dál větší potřeba centralizované úpravy pro ochranu osobních údajů, neméně potřebnou i pro účely ekonomické. Na druhou stranu tato ochrana způsobovala postupnou izolaci a získávání informací klasickým způsobem, tedy prostým sociálním kontaktem se stávala stále obtížnější. Zároveň se jakékoliv shromažďování osobních údajů začíná posuzovat jako nevhodný zásah do osobní sféry.

Základním evropským dokumentem, z něhož se následně začaly odvozovat vnitrostátní právní úpravy, se stala Úmluva Rady Evropy č. 108/1981, o ochraně osob, se zřetelem na automatizované zpracování osobních dat.[27]

3.2. Vnitrostátní právní úprava

Na našem území se úprava ochrany osobních údajů začala poprvé řešit v první polovině 90. let. Během vlády komunismu se touto problematikou nikdo zvlášť nezabýval, pouze v zákoně č. 40/1964 Sb., občanský zákoník byly zakotveny základní principy ochrany soukromí v úpravě vztahující se k ochraně osobnosti.

Právní zakotvení však nalezneme i v ústavním pořádku, a to v ústavním zákoně č. 2/1993 Sb., Listina základních práv a svobod, konkrétně v článcích 7, 10 a 13, a samozřejmě v novelizovaném zákoně č. 89/2012 Sb., občanský zákoník.

V porevolučním období byl v návaznosti na Úmluvu Rady Evropy č. 108/1981, o ochraně osob (dále jen Úmluva 108) vydán zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Na tuto právní regulaci byla poměrně pozitivní reakce, neb se jednalo o vcelku rychlou a zdařilou úpravu nedávno

[27] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi, str. 25-27.

rozpuštěného tzv. východního bloku. Zákon ovšem trpěl podstatným nedostatkem, díky kterému nebyl v praxi příliš akceptován. Díky nestabilní politické situaci totiž nedošlo ke zřízení nezávislého kontrolního úřadu, jenž by dohlížel na zpracování osobních údajů.

Nová právní úprava byla přijata v podobě zákona č. 101/2000 Sb., o ochraně osobních údajů, a to v souvislosti se vstupem do Evropské unie. Tímto zákonem se tak Česká republika úplně vyrovnala s úpravou Úmluvy 108. V době vzniku našeho zákona č. 101/2000 Sb. však již existovala zpřesňující a konkretizující Směrnice Evropského Parlamentu a Rady 95/46/ES ze dne 24. 10. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů. Zákon o ochraně osobních údajů byl v této souvislosti stejně jako v několika dalších případech novelizován např. tzv. schengenské dohody, a také z důvodu praktické aplikace.[28]

3.3. Obecné nařízení o ochraně osobních údajů / GDPR

V souvislosti s rapidním rozvojem IT technologií se stále zvyšuje potřeba zajištění lepšího fungování systému ochrany osobních údajů. Evropská unie musí jít s dobou a reagovat na současné požadavky společnosti spočívající především v internetových nabídkách, elektronickém bankovnictví, masivním rozvoji sociálních sítí, monitorování fyzických osob, zaměstnanců apod.

Díky větší důležitosti a kladení důrazu na ochranu těchto práv je přistoupeno k formě nařízení, které je tím nejúplnějším nástrojem sbližování práva, jež mají orgány EU k dispozici. Nařízení jsou unifikačního charakteru a jsou pro členské státy závazná a přímo použitelná, tudíž není třeba jejich implementace do vnitrostátních právních řádů.

Obecné nařízení o ochraně osobních údajů, v angličtině General Data Protection Regulation neboli GDPR, je představitelem nového právního základu ochrany osobních údajů v Evropě, které výrazně zvyšuje ochranu osobních dat občanů. Dopad nařízení však nebude směřovat jen proti jeho členům, ale bude mít i mimoevropský přesah.

---

[28] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008. Beckova edice ABC., str. 11, 12.

Mezi hlavní cíle nařízení patří přizpůsobení právní regulace ochrany osobních údajů dnešní společnosti, unifikace ochrany osobních údajů v EU, posílení práv a sjednocení výkladu GDPR pomocí dozorových úřadů a v neposlední řadě posílení důvěryhodnosti EU a jejích členů pro předání osobních údajů mezi sebou. Právní rámec ochrany osobních údajů se týká všech jednotlivců, institucí a firem, dokonce i online služeb, které zpracovávají data uživatelů. Nařízení GDPR hrozí především zavedením astronomických pokut za porušení pravidel a některým správcům či zpracovatelům nařizuje zřídit nezávislou kontrolní funkci DPO, tedy Data Protection Officer, tj. Pověřence pro ochranu osobních údajů.[29]

Vzhledem k velkým změnám, jež GDPR přináší, zde byla stanovena více než dvouletá legisvakanční lhůta, neb v platnost vstoupilo v dubnu 2016, účinnosti však nabylo až 25. 5. 2018.[30] Během tohoto období museli všichni, kterých se nařízení dotýká zrevidovat své informační systémy a postupy nakládání s osobními údaji. Jednotlivé členské státy EU tak měly čas přijmout prováděcí neboli adaptační zákon, jímž se upřesní více než padesát bodů, které Obecné nařízení ponechává a nadále svěřuje do národních pravomocí.

3.4. Pracovní skupina 29

Pracovní skupina 29 byla ustanovena již směrnicí 95/46/EC, která účinností GDPR pozbyla platnost. Vznikla jako nezávislý evropský poradní orgán pro ochranu dat a soukromí. Pracovní skupina byla složena z vedoucích zástupců dozorových úřadů jednotlivých členských zemí Evropské unie. Po vstupu Obecného nařízení v účinnost se změnila v Evropský sbor pro ochranu osobních údajů (dále jen EPDB).

Úkolem tohoto Sboru je především zajišťování jednotného uplatňování Obecného nařízení, a to za účelem monitorování uplatňování GDPR. Sbor má vydávat pokyny, doporučení a osvědčené postupy, a to i pro některé stanovené oblasti a instituty Obecného nařízení.[31] Sbor jím vydané materiály veřejně diskutuje, a to za účelem adresátovi maximálně vysvětlit a co nejblíže ho seznámit s jednotlivými pasážemi Obecného nařízení.

[29] Obecné nařízení o ochraně osobních údajů prakticky, dostupné z www.gdpr.cz/blog/
[30] NAVRÁTIL, Jiří. GDPR pro praxi, 2018, op. cit., str. 29 - 31.
[31] Pracovní skupina 29, dostupné z www.gdpr.cz/gdpr/heslo/pracovni-skupina-29/

Sbor má přispět k zajištění konzistentního uplatnění právního předpisu týkajícího se ochrany osobních údajů po celé Evropské unii a má usilovat o zajištění efektivní spolupráce mezi jednotlivými úřady pro ochranu osobních údajů. V případě sporů má zajistit jednotné uplatňování pravidel pomocí přijímání závazných rozhodnutí pro případy, aby se stejný případ neřešil různorodě v jiných jurisdikcích.

Andrea Jelinek, předsedkyně EDPB: *„Tato velmi očekávaná legislativa dává jednotlivcům větší kontrolu nad jejich osobními údaji a stanoví ucelený soubor pravidel pro každého, kdo v EU zpracovává osobní údaje jednotlivců. Ve světě, kde se s daty zachází jako s platidlem, jsou práva jednotlivců často přehlížena nebo dokonce zlehčována. Ze zřetele bychom neměli ztrácet skutečnost, že osobní údaje neoddělitelně patří k lidským bytostem. Jsem přesvědčena, že GDPR dává jednotlivcům i dozorovým úřadům prostředky pro účinnou ochranu a prosazování tohoto základního práva.“*

3.5. Adaptační zákon

Adaptační zákon má reagovat zejména na přibližně shora již zmíněných padesát bodů, ve kterých Obecné nařízení ponechává jednotlivým členským státům možnost vlastní právní regulace. Adaptační zákon nejenže se nepodařilo schválit do účinnosti Obecného nařízení, nicméně jeho legislativní proces se ukázal nad očekávání velmi komplikovaný a teprve 12. března 2019 Poslanecká sněmovna *„vyslovuje souhlas s návrhem zákona o zpracování osobních údajů podle sněmovního tisku 138/14, ve znění schváleném Senátem, podle sněmovního tisku 138/15“.*[32]

[32] Usnesení Poslanecké sněmovny z 27. schůze ze dne 12. března 2019, dostupné z www.psp.cz/sqw/text/tiskt.sqw?o=8&v=US&ct=561

4. Subjekt osobních údajů

Subjektem údajů je fyzická osoba, na níž se osobní údaje vztahují. Osoba, která je nositelem, musí být určená nebo určitelná, jak již bylo popsáno v předchozích kapitolách.[33] Co se týká pojmu fyzické osoby, zde vycházíme z ustanovení § 23 OZ, které říká, že: *„Člověk má právní osobnost od narození až do smrti.“* Již z tohoto ustanovení nám vyplývá závěr, že se působnost zákona bude vztahovat zejména k živým fyzickým osobám. Výjimku tvoří § 25 OZ, kde se hovoří o právech a povinnostech počatého dítěte, za podmínky, že se narodí živé.

Nařízení GDPR nám na problematiku subjektu osobních údajů odpovídá hned v úvodních ustanoveních. Jejich definice je totožná s naší právní úpravou. Subjektem údajů je tedy pouze fyzická osoba, k níž se osobní údaje vztahují, a to bez ohledu na její státní příslušnost či bydliště.[34] Nařízení ve svých úvodních recitálech dále vysloveně stanoví, že se vztahuje pouze k žijícím fyzickým osobám, a působnost nařízení na osobní údaje zesnulých osob je zcela vyloučena.[35] GDPR zde však připouští vlastní vnitrostátní úpravu týkající se zpracování osobních údajů zesnulých osob.

Na právnické osoby se toto nařízení nevztahuje, dopadá jen na jednání jejich zaměstnanců nebo členů čistě v soukromoprávní sféře. Z důvodu, že se s touto problematikou setkáváme v každodenním životě, a to prostřednictvím zaměstnanců, členů apod., kteří jsou označeny identifikátory, např. jmenovkami, je potřeba se s těmito vztahy vypořádat. Náš zákon se však tímto vztahem výslovně nikterak nezabývá, možnost působnosti zákona č. 101/2000 Sb. by se dala vztáhnout třeba v případě, že by byl pracovník na svém pracovišti osloven nabídkou týkající se pouze soukromé záležitosti. Pokud by ale byl zaměstnanec osloven v souvislosti s činností právnické osoby, zde je aplikace právních předpisů pro ochranu osobních údajů vyloučena. V běžné praxi však často narážíme na situace, kdy předmětem téhož zpracování jsou jak osobní údaje, tak údaje o právnické osobě. V tomto případě se tedy aplikovatelnost vyloučí jen na osobní údaje.[36]

[33] § 4 písm. d) zákona č. 101/2000 Sb.
[34] Recitál 14 Obecného nařízení GDPR
[35] Recitál 27 Obecného nařízení GDPR
[36] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008. Beckova edice ABC. ISBN 978-80-7400-033-1, str. 34, 35.

Jakousi snahou o diskreci zákona o ochraně osobních údajů byl zcela jistě prosazovaný názor rozšíření působnosti zákona i na údaje zvířat, tento názor vyplynul ze snahy zavedení cestovního dokladu pro přepravu psa. Zde by se však jednalo o propojení dokladu psa s jeho majitelem, a byla by tak potřebná dvojí identifikace, tedy jak zvířete, tak osobních údajů jeho vlastníka.[37]

4.1. Práva subjektů

Práva subjektů údajů jsou nedílnou součástí a pilířem unijní ochrany osobních údajů, jelikož vyvažují často nerovný vztah mezi správcem a subjektem údajů. Subjekt často musí zpracování osobních údajů strpět, a to typicky v případech vrchnostenského zpracování orgánů veřejné moci nebo veřejnými subjekty.

Tato skupina práv je nařízením GDPR upravena v samostatné kapitole III. „práva subjektu údajů“ a jsou jim věnovány články 12 až 22. Zde si můžeme na první pohled všimnout velmi značného rozdílu od stávající právní úpravy, tedy Směrnice 95/46/ES, resp. zákona č. 101/2000 Sb., který se této problematice výslovně věnuje pouze v jediném § 12 „Přístupu subjektu údajů k informacím“. Výrazně podrobnější právní úprava přímo reflektuje jeden z důvodů přijetí nového právního rámce. Výkon práv subjektu je podle nařízení vysoce chráněný zájem, jehož porušení je dokonce podmíněno vyšší sazbou pokuty, než je tomu u ostatních povinností stanovených nařízením. Každý správce tak má vyvíjet aktivitu k řádnému zajištění výkonu práv subjektu údajů.[38]

4.1.1. Základní postupy a transparentnost

Mezi základní povinnost správce patří přijmutí vhodných opatření, aby subjektu údajů mohl snadno poskytnout stručným, transparentním, srozumitelným a lehce přístupným způsobem za použití jednoduchých jazykových prostředků všechny informace. Poskytnutí probíhá v písemné formě, ve vhodných případech ve formě elektronické a na žádost subjektu i ústně. Správce tradičně zveřejňuje obecné informace o zpracování na internetových stránkách.[39] K zajištění plnění výše uvedených požadavků musí správce využít různých vizualizací, metod psaní a členění textu. Doporučuje se využívání hypertextových odkazů, psaní

[37] MAŠTALKA, Jiří, 2008, op. cit., str. 35.
[38] ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG), str. 130.
[39] ŽŮREK, Jiří, 2018, op. cit., str. 131.

jednoduchým stylem, využívání metody otázek a odpovědí, vyhýbání se právnickým, technickým a dalším odborným termínům. Dále se doporučuje informovat subjekt údajů až v přímo nezbytné době, dosáhne se tak toho, že subjekt údajů nebude zahlcen informacemi v době podpisu smlouvy, ale dostane je až před samotným využitím požadované služby. Další využívanou technickou může být tzv. vrstvení podmínek, jež znamená v první řadě krátké oznámení o klíčových informacích, v druhé vrstvě stručné oznámení, jež by už mělo obsahovat podrobnější relevantní informace, a poslední vrstva by pak měla být plným oznámením všech informací o zpracování osobních údajů.[40]

Vzhledem k plnění této povinnosti ÚOOÚ uvádí, že je nutné plnit svou informační povinnost tak, aby subjekt údajů skutečně porozuměl smyslu sdělovaných informacích. V případě, že bude podání informací nepřehledné nebo nesrozumitelné, nemusí být taková informační povinnost považována za splněnou, a to i pokud ke sdělení informací došlo.[41] Fyzické osoby mají právo být poučeny o existenci rizik, pravidel, záruk a dalších právech v souvislosti se zpracováním údajů. Informační povinnost je proti stávající úpravě zakotvené v § 12 zákona č. 101/2000 Sb. značně rozšířená. Nařízení striktně rozlišuje situace, kdy jsou osobní údaje získávány přímo od subjektu údajů a kdy ne.

Nařízení nově stanoví lhůty pro splnění povinnosti. Základní lhůta pro získání osobních údajů má být přiměřená, ale ne delší než jeden měsíc. Za nejzazší okamžik je považována doba první komunikace se subjektem, je-li použití údajů předmětem komunikace, či nejpozději při prvním zpřístupnění příjemci. Recitál 61 nařízení toto ustanovení ještě zpřesňuje tím, že informování subjektu o zpracování by mělo proběhnout již v okamžiku jejich shromáždění od subjektu údajů, v ostatních případech v přiměřené lhůtě vzhledem k okolnostem případu. Lhůtu tak lze vzhledem k složitosti případu na žádost prodloužit o další 2 měsíce.[42] Výjimkami z této povinnosti jsou situace, kdy subjekt údajů již tyto informace má, poskytnutí informací vyžaduje nepřiměřené úsilí, jedná se o zájem EU či jeho člena nebo v případě povinnosti zachování důvěrnosti s ohledem na zachování služebního tajemství a povinnosti mlčenlivosti.

[40] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, str. 182.
[41] Rozhodnutí ÚOOÚ č.j. 26/05/SŘ-OSČ, č.j. 50/05/SŘ-OSČ a č.j. 70/05/SŘ-OSČ
[42] Čl. 12 odst. 3 Obecného nařízení GDPR

Nařízení stanoví, že poskytování informací podle následujících článků je v zásadě bezplatné. Výjimkou může být účtování administrativního poplatku za opatření další, nikoliv ale první kopie podle čl. 15. odst. 3. Právě zde je patrný rozdíl oproti úpravě v § 12 zákona č. 101/2000 Sb., kde poskytnutí informace mohlo být přiměřeně zpoplatněno. GDPR tuto možnost však zavrhuje, a proto lze očekávat zvýšení počtu žádostí. Z recitálu 63 nařízení nám dále vyplývá možnost správce poskytnout vzdálený přístup v rámci zabezpečeného systému subjektu údajů přímo do zpracovávaných údajů, zde se ovšem jedná spíše o ideální představu, nikoliv závaznou povinnost.

4.1.2. Právo na informace

Základním právem, které naplňuje zásadu transparentnosti zpracování osobních údajů, je právo na informaci, jež by mělo zajistit řádnou informovanost o zpracování osobních údajů. Do značné míry se jedná o pasivní právo, neboť pro správce se jedná o aktivní povinnost, kterou musí plnit automaticky, a nikoliv na požádání. *„Obecné nařízení rozlišuje obsah informace podle toho, zda správce získal či nezískal osobní údaje přímo od subjektu údajů.“*[43] Informace získané přímo od subjektu údajů se poskytují současně s jejich získáváním, tedy při samotném jednání se subjektem. Pokud takové setkání se subjektem není možné, dochází k postupuje se podle čl. 14 odst. 3 Obecného nařízení. Správce má tak povinnost poskytnout údaje v přiměřené lhůtě, nejpozději do jednoho měsíce, nebo v okamžiku první komunikace se subjektem či při prvním zpřístupnění osobních údajů. Podle výše uvedeného se nebude postupovat v případě, že dotčený subjekt, již informace má nebo by jejich poskytnutí vyžadovalo nepřiměřené úsilí či není možné vůbec.

Pokud správce zpracovává naše údaje, subjekt má právo být informován o totožnosti a kontaktních údajích správce nebo pověřence, účelu zpracování, dotčených kategorií, příjemci a všech, komu budou zpřístupněny, předání do třetí země, plánované době jejich uložení, možnosti požadovat jejich výmaz, vznést námitku a stížnost. Subjekt má právo vědět o všech dostupných informací a jejich zdrojích, pokud nejsou získány přímo od subjektu, stejně tak jako být informován o automatickém rozhodování.[44]

[43] ŽŮREK, Jiří, 2018, op. cit., str. 132.
[44] JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha 2018, str. 21.

4.1.3. Přístup k informacím

Toto právo máme zakotveno v článku 15 GDPR a jeho hlavním cílem je získat potvrzení od správce, zda jsou či nejsou jeho osobní údaje zpracovávány. Stejně jako předchozí uvedené právo na informace souvisí i tento přístup k informacím úzce se zásadou transparentnosti. Na rozdíl od předchozího práva se zde jedná o aktivní právo subjektu údajů, neboť subjekt jej využívá podle svého uvážení. Všechny tyto informace jsou zásadně poskytnuty na základě žádosti.

Subjekt má v čl. 15 odst. 3 Obecného nařízení zakotveno právo dostat kopii zpracovávaných údajů, kdy tato služba může být administrativně zpoplatněna do výše nákladů.[45] Právo získat kopii je však hned následujícím odstavcem do jisté míry omezeno. *„Tímto právem by neměla být nepříznivě dotčena práva ani svobody ostatních, například obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení.“*[46] Závěrem je potřeba zdůraznit, že se toto právo vztahuje pouze k takovým osobním údajům, jež se týkají dotčeného subjektu údajů.

4.1.4. Oprava, doplnění a výmaz

Právo na opravu a doplnění údajů pro nás není žádnou novinkou, neb ho máme zakotveno v § 21 ZoOÚ, a to v návaznosti na povinnost správce zpracovávat přesné osobní údaje. Obecné nařízení nám však tento institut zpřesňuje, a sice že dotčený *„subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.*[47] Práva na doplnění může subjekt využít i sám ze své vlastní vůle a poskytnout tak správci další osobní údaje. Správce při uplatnění tohoto institutu musí dbát zvýšené opatrnosti s ohledem na účel zpracování, aby nedocházelo ke zpracování údajů, jež nejsou pro dané účely potřebné.

„Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:“[48]

[45] Čl. 15 odst. 3 Obecného nařízení GDPR
[46] Recitál 63 Obecného nařízení GDPR
[47] Čl. 16 Obecného nařízení GDPR
[48] Čl. 17 odst.1 Obecného nařízení GDPR

údaje již nejsou účelně potřebné, subjekt odvolá svůj souhlas se zpracováním, existence námitky proti zpracování, zpracování bylo protiprávní, vyžaduje-li to splnění povinnosti stanovené v právu Unie či členského státu vztahující se ke správci nebo byly osobní údaje shromážděny na popud nabídky služeb v informační společnosti.

Právo subjektu na výmaz však není absolutní a existuje z něj řada výjimek, kdy se povinnost odstranit osobní údaje neuplatní. Takovými případy mohou být situace, kdy je zpracování nezbytné pro výkon práva na svobodu projevu a informace, pro splnění právní povinnosti na základě unijního práva nebo práva členského státu, jímž je správce vázán. Dále z důvodu existence veřejného zájmu v oblasti veřejného zdraví, archivace, statistiky a výzkumu, také pro určení, výkon či obhajobou právních nároků.[49] Pakliže správce již údaje zveřejnil, případně rozšířil, je povinen učinit přiměřená opatření k informaci ostatních správců, aby došlo k jejich veškerému výmazu na všech dostupných nosičích.

Právo na výmaz, také označováno jako právo být zapomenut, má význam v možnosti požadovat po správci zlikvidování osobních údajů, a především jejich další nezpracovávání. Jeho vývoj zaznamenáváme prostřednictvím soudních výkladů, a to z práva na opravu, blokování a práva na námitku. Obdobu nalezneme i v § 21 zákona o ochraně osobních údajů jako obecnou žádost o vysvětlení a odstranění nežádoucího stavu. Soudní dvůr Evropské Unie v květnu roku 2014 vydal přelomové rozhodnutí ve věci C 131/12 Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González, kterým definoval právo na opravu, výmaz nebo blokování údajů, jejichž zpracování zejména z důvodu neúplné nebo nepřesné povahy údajů není v souladu se směrnicí 95/46/ES. SDEU zde potvrdil, že Google opravdu zpracovává osobní údaje. Tady vyvstal problém a nutnost posouzení, zdali jedná v oprávněném zájmu a jestli komerční zájem Googlu ve spojení s veřejným zájmem společnosti na právo na informace převáží nad zájmem konkrétního subjektu údajů. V tomto případě se SDEU přiklonil na stranu pana Costeji Gonzálese a přikázal společnosti Google nežádoucí osobní údaje z vyhledávání odstranit. Díky tomuto rozsudku vyhledávač Google zavedl speciální webový formulář, který umožnuje podat žádost o výmaz osobních údajů z výsledků vyhledávání. Tento rozsudek se díky rozšíření v médiích

[49] Čl. 17 odst. 3 Obecného nařízení GDPR

vžil pod názvem právo být zapomenut, jež se následně dostalo do návrhu Nařízení a bylo schváleno v podobě, kdy subjekt údajů má možnost kontroly nad svými osobními údaji.

4.1.5. Právo vznést námitku

Subjekt údajů má v konkrétní situaci kdykoliv možnost vznést námitku proti zpracování osobních údajů. Po vznesení námitky správce údaje dále nezpracovává, a to do doby prokázání závažných oprávněných důvodů pro zpracování, jež převažují nad zájmy, právy a svobodami subjektu údajů nebo pro určení, výkon a obhajobu právních nároků. V případě zpracování údajů pro účely přímého marketingu včetně profilování dochází po vznesení námitky k jejich okamžitému vyloučení z dalšího zpracování.[50] Na možnost vznést námitku má být subjekt výslovně a jednoznačně upozorněn.

Právo na námitku lze uplatnit zejména v situacích, kdy subjekt údajů neměl možnost ovlivnit fakt, že jsou jeho osobní údaje zpracovávány, a zároveň se nejedná o jednání v oprávněném zájmu. Rozlišujeme tři druhy námitek, jež může subjekt údajů uplatnit, a to námitky, které směřují proti „*zpracování na základě právního titulu oprávněného zájmu a plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, zpracování pro účely přímého marketingu na základě právního titulu oprávněného zájmu, a nakonec zpracování pro účely vědeckého či historického významu nebo pro statistické účely.“*[51]

Úprava práva na námitku, která byla zakotvená v čl. 14 Směrnice 95/46/ES se od úpravy v Obecném nařízení ve svých podstatných znacích nelišila, což se ovšem nedá říct o její implementaci do české právní úpravy pod § 21 zákona č. 101/2000 Sb. Subjekt údajů podle vnitrostátní právní úpravy měl doposud možnost podat pouze obecnou námitku, ale nemá možnost přezkumu zpracování na základě právních titulů oprávněného zájmu či plnění úkolů veřejné moci. Dalším rozdílem oproti Směrnici i nařízení je možnost námitky pro účely přímého marketingu, jež je do našeho zákona upravena pouze § 5 odst. 5 v rámci možnosti opt-outu pro zpracování nabídek obchodu nebo služeb.

[50] Čl. 21 Obecného nařízení GDPR
[51] NULÍČEK, Michal, 2017, op. cit., str. 227.

4.1.6. Automatizované rozhodnutí

„Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.“[52] Výše uvedený článek 22 Obecného nařízení nám tedy přímo zakotvuje právo nebýt předmětem výhradně automatizovaného zpracování, ale i z tohoto práva máme pár výjimek. Mezi první výjimku patří potřeba takovéhoto zpracování k uzavření, případně plnění smlouvy mezi subjektem a správcem, dále pokud to povoluje EU či její člen a také v případě výslovného souhlasu subjektu údajů.

Podobné ustanovení znala dosavadní úprava v čl. 15 směrnice 95/46/ES, které mohlo být do vnitrostátních úprav členských států transponováno dvěma způsoby. V České republice jej zákon o ochraně osobních údajů aplikoval ustanovením § 11 odst. 6 jako generální zákaz s výjimkami pro některé případy, druhým způsobem aplikace bylo povolení takového rozhodování a následná možnost uplatnění námitky. Právě díky rozdílným podobám národních úprav jsou ohledně tohoto institutu výkladové rozpory, a to s ohledem na současný článku 22 GDPR.[53]

Nařízení však oproti stávající úpravě chrání subjekty údajů mimo jiné i proti neprávním důsledkům, dalším rozdílem je zahrnutí důsledků pozitivních, ale i těch negativních. Největší změna však plyne z možnosti uložení sankcí, neboť Úřad pro ochranu osobních údajů takovou pravomoc neměl, jelikož náš výčet přestupků takovou skutkovou podstatu neznal.

Právní úprava směřuje proti situacím, kdy o právech a povinnostech subjektu údajů rozhoduje výlučně algoritmus. Algoritmus můžeme chápat jako předem stanovený postup, jenž je následně prováděn automatizovaně. Cílem úpravy stanovené GDPR je především regulace případu, ve kterých lze takovéto automatizované rozhodování připustit.[54]

Toto právo má obsahovat pojistku z plně automatizovaného rozhodování s právními účinky vůči fyzické osobě. V praxi by se jednalo např. v oboru silniční dopravy jednoduše uskutečnitelné plné automatizované zpracování.[55] Zvýšená

[52] Čl. 22 odst. 1 Obecného nařízení GDPR
[53] NULÍČEK, Michal, 2017, op. cit., str. 233.
[54] NULÍČEK, Michal, 2017, op. cit., str. 232.
[55] ŽŮREK, Jiří, 2018, op. cit., str. 148.

ochrana by se tak měla vztahovat pouze na právní účinky, jež jsou pro subjekt údajů nějakým způsobem významné, protože pokud bychom zastávali striktní výklad tohoto ustanovení, vztahovalo by se i na absurdní situace, jakým může být poskytování slevy na základě hodnoty nákupu v obchodě.

4.1.7. Omezení zpracování

Omezením rozumíme *„označení uložených osobních údajů za účelem jejich zpracování v budoucnu“.*[56] Subjekt údajů má právo požadovat po správci omezení v několika případech uvedených v článku 18 odst. 1 GDPR. Prvním případem je, kdy subjekt popírá přesnost osobních údajů, omezení tak trvá po dobu ověření údajů. Zpracování je protiprávní a subjekt místo výmazu požaduje omezení jejich použití. Dále také v případě, že správce již dosáhl zamýšleného účelu, ale subjekt ke zpracování požaduje k určení, výkonu, obhajoby právních úkonů. A rovněž v případě, kdy subjekt vznesl námitku, a to do doby, než bude o ní rozhodnuto.

Došlo-li k požadovanému omezení, osobní údaje mohou být nadále zpracovány mimo jejich uložení pouze na základě souhlasu subjektu, z potřeby určení, výkonu nebo obhajoby právních nároků, dále z nutnosti ochrany práv jiné fyzické nebo právnické osoby, případně v naléhavém veřejném zájmu Evropské unie nebo jejího členského státu.[57]

Po obdržení žádosti správce musí nejprve posoudit naplnění podmínek stanovených Obecným Nařízením. Výše zmíněné omezení znamená především označení, jež podle recitálu 67 GDPR může být provedeno mnoha způsoby. Mezi ty nejčastěji užívané patří dočasný přesun údajů do jiného systému zpracování, znepřístupnění údajů, dočasné označení zveřejněných údajů na internetových stránkách a další. Cílem takového označení je zejména zjištění, aby se všichni, kteří mají k takovým údajům přístup, dozvěděli o omezení zpracování.

Značnou podobnost práva na omezení máme i v současné právní úpravě, zakotvené v § 21 odst. 1 ZoOÚ v rámci blokace osobních údajů, o niž může subjekt údajů požádat, pokud se domnívá, že jsou jeho osobní údaje zpracovávány v rozporu se zákonem nebo s ochranou jeho soukromého a osobního života. Blokaci máme definovanou v § 4 písm. h) zákona č. 101/2000 Sb. *„blokováním je*

[56] Čl. 4 bod 3Obecného nařízení GDPR
[57] Čl. 18 odst. 2 Obecného nařízení GDPR

operace nebo soustava operací, kterými se na stanovenou dobu omezí způsob nebo prostředky zpracování osobních údajů, s výjimkou nezbytných zásahů.“ Obecné nařízení na rozdíl od vnitrostátní právní úpravy nestanoví obecnou možnost omezení zpracování osobních údajů, ale uvádí konkrétní případy, ve kterých to subjekt údajů může požadovat, jak již bylo výše uvedeno.[58]

4.1.8. Právo na přenositelnost

Toto právo uvedené v článku 20 GDPR je zcela nové a při svém zveřejnění vzbudilo řadu emocí. Právo, aby vůbec mohlo vzniknout, je podmíněno řadou dílčích podmínek, jež musí být současně splněny. Jedná se o podmínku zpracování na základě souhlasu či smlouvy a jde-li o automatizované zpracování.

„Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že“[59] zpracování je založeno na souhlasu, smlouvě a zpracování je prováděno automatizovaně. V praxi to znamená opětovné použití „svých“ údajů pro své soukromé účely, a to napříč různými službami. Právo nám usnadňuje možnost přesunu údajů bez zábran mezi různé informační prostředí. Uplatněním tohoto institutu jím nejsou ostatní práva dotčena. Subjekt tak může využívat služby dosavadního správce i v případě provedení této operace.[60] Jedním z cílů tohoto institutu je omezení situací, kdy subjekt údajů zůstává u stávající služby jen z důvodu počáteční velké časové investice, a to například vytvářením vlastního obsahu.[61]

Specifikace formátů poskytovaných správcem údajů má zaručit efektivní žádoucí výsledek. Právě ve stanovení formátu spočívá odlišení od práva na přístup k osobním údajům. Zároveň to však neznamená povinnost správců zachovávat kompatibilní systémy. Vzájemná spolupráce správců spočívá v poskytnutí co největšího množství metadat, a to v co největší míře zachování přesného významu vyměňovaných informací.

[58] NULÍČEK, Michal, 2017, op. cit., str. 216.
[59] Čl. 20 odst. 1 Obecného nařízení GDPR
[60] JANEČKOVÁ, Eva, 2018, op. cit., str. 24, 25.
[61] NULÍČEK, Michal, 2017, op. cit., str. 221.

5. Zpracování osobních údajů

Za zpracování osobních údajů se považuje každá operace, či jejich soustava, které správce nebo jejich zpracovatel soustavně provádí s osobními údaji pomocí automatizovaných či dalších prostředků.

Tímto pojmem rozumíme především shromažďování, ukládání dat na nosiče, zpřístupňování, úpravu či změnu, vyhledávání, používání, předávání, šíření, zveřejnění, uchování, výměnu, třídění, kombinování, blokování a likvidaci. Pojmem shromažďování rozumíme systematické postupy s cílem získat osobní údaje, a to pro jejich další uložení na datový nosič, pro okamžité či pozdější zpracování. Uchování znamená jejich uložení v podobě, která umožní jejich pozdější zpracování.

Operace také může být blokována, což znamená, že je po určitou dobu omezen způsob či prostředek zpracování, s výjimkou nezbytných základů. V neposlední řadě si osvětlíme pojem likvidace, jímž rozumíme faktické zničení datového nosiče, výmaz či jiné trvalé vyloučení z dalšího zpracování.[62]

5.1. Zpracování osobních údajů podle zákona č. 101/2000 Sb.

Základní definice uvedená ve směrnici Evropského parlamentu a Rady 95/46/ES převzatá do vnitrostátní úpravy v zákoně č. 101/2000 Sb. zní: *„Zpracováním osobních údajů je jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.“* Z této definice nám vyplývá, že jakýkoliv úkon nebo operaci označujeme za nakládání s osobními údaji.

Systematičnost je jednou z hlavních charakteristik zpracování, k jejím pravidelným, nikoliv však definičním znakům patří opakovanost nebo jednotný účel.[63] Evropské právo ovšem tento pojem vůbec nezná, a i proto se Úřad

[62] § 4, odst. 1, písm. f - i zákona č. 101/2000 Sb.
[63] Stanovisko č. 4/2013, k pojetí zpracování osobních údajů, říjen 2013, ÚOOÚ, dostupné z www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22256

pro ochranu osobních údajů ve výkladu zákona č. 101/2000 Sb. přiklání k jeho okrajovému významu, a dokonce jej označuje za nadbytečný. Znakem zpracování však není ani účelnost, neboť i neúčelné zpracování se stále považuje za zpracování osobních údajů.

Shromažďování je jedním ze základních způsobů zpracování, jedná se o jakoukoliv operaci nebo úkon, ve kterém se osobní údaje cíleně dostanou ke správci. Jde o záměrnou činnost s cílem získání osobních údajů za účelem jejich dalšího uložení na nosič informací. Uložení na nosič probíhá pro účely okamžitého nebo budoucího zpracování. Typickým příkladem může být zajištění důkazů, vystupují-li při něm osobní údaje. Nahodilé shromáždění se za předpokladu, že nedochází k dalšímu zpracování, za takové zpracování nepovažuje, naproti tomu zpracování výlučně pro osobní potřebu za zpracování osobních údajů považujeme.[64]

Uchovávání osobních údajů znamená jejich udržování v takové podobě, jež umožňuje jejich další zpracování, tradičním typem uchovávání osobních údajů je rejstřík, kterým můžeme rozumět spis, soupis nebo databázi. Rejstřík nebo datový soubor v žádném případě nemusí být jediným výsledkem zpracování, což potvrzuje i rozsudek ESD ve věci C-101/01, Lindqvistová vs. Švédsko, jehož výrok zní: *„Úkon, který spočívá v tom, že se na internetové stránce odkáže na různé osoby, které jsou identifikovány buď svým jménem, nebo jinými prostředky, například telefonním číslem nebo údaji o pracovních poměrech a zálibách, je zcela nebo částečně automatizovaným zpracováním osobních údajů ve smyslu čl. 3 odst. 1 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.“* Jedním z prosazovaných přístupů zpracování je znak hromadnosti, obecně je však za znak považována ordinalita, neboli první osobní údaj. Z normativní definice je však tento přístup zcela neodvoditelný, neboť zde máme definiční rozpor mezi „jakýmkoli úkonem“ a na straně druhé „souborem úkonů“. Tudíž i pokud vezmeme v úvahu, že třídění, srovnání nebo kombinování může být v některých zpracováních údajů vyloučeno, neznamená to, že se nejedná o zpracování osobních údajů v rámci zákonné definice.

[64] § 3,odst. 3 a 4zákona č. 101/2000 Sb.

Za typ zpracování musíme považovat i tzv. blokování, což je operace, která po stanovenou dobu omezí způsob nebo prostředky zpracování osobních údajů. Úřad pro ochranu osobních údajů se přiklání k definici, kterou lze využít jako nápravné a bezpečnostní opatření v případech porušení ochrany osobních údajů. Blokování je jednou z metod, jež umožňuje dočasné znepřístupnění.

Mezi zpracováním a jiným nakládáním s osobními údaji existuje pouze tenká hranice. „*Některé znaky skutkové podstaty pomáhají v její správné kvalifikaci (systematičnost, hromadnost), avšak jejich absence neznamená, že se o zpracování osobních údajů nejedná.“*[65] Správci a zpracovatelé by tak měli výše uvedené brát na zřetel a v případě pochybností následovat názor Úřadu a takové nakládání s osobními údaji spíše za zpracování považovat, v opačném případě se vystavují nebezpečí sankce.

5.1.1. Zásady

Právní princip, také označovaný jako právní zásada, je pojmem, kterým se označují základní pravidla určitého právního institutu, zákona, právního odvětví nebo i právního řádu jako celku. *„Pojem obecných zásad právních má několikerý a vždy více či méně neostrý význam.“*[66] Právní principy jsou vůdčí zásady stojící na právním systému. Stejně jako právní normy mají preskriptivní charakter, ale od těch se ve dvou významných znacích odlišují. Tím prvním rozdílem je vyšší míra abstraktnosti, kdy zásady stanoví nejabstraktnější východiska, kterými se pak jednotlivé právní normy řídí. Z právních principů nám bezprostředně nevyplývají žádná práva ani povinnosti vůči adresátům. Na rozdíl od norem pro zásady neplatí logické vztahy a mohou mít, i nezřídka mají, kontradiktorní charakter.

Právní principy můžeme rozlišovat hned z několika hledisek na principy tradiční a moderní, dále z hlediska jejich obecné či univerzální právní povahy oproti principům platným jen v určitých právních odvětvích a v neposlední řadě na právní normy hmotněprávní a procesněprávní.[67]

---

[65] Stanovisko č. 4/2013, k pojetí zpracování osobních údajů, op. cit.
[66] KNAPP, Viktor. *Teorie práva*. Vyd. 1., 3. dot. Praha: C.H. Beck, 1995. Beckovy právnické učebnice, str. 137.
[67] GERLOCH, Aleš. Teorie práva. 7. aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. Právnické učebnice (Aleš Čeněk), str. 35-36.

Prvotní smysl právních předpisů na ochranu osobních údajů vychází z § 1 zákona č. 101/2000 Sb., z něhož vyplývá, že každý má právo na ochranu před neoprávněným zasahováním do soukromí, a to pomocí stanovení práv a povinností při zpracování. Za základní princip tak můžeme považovat stanovení podmínek zpracování osobních údajů.[68] Podmínky pro zpracování jsou klíčová ustanovení, jež mohou působit jako částečná prevence možné újmy. Principy ochrany osobních údajů mají svůj původ v mezinárodním právu, především pak v Úmluvě č. 108. a jejím Dodatkovém protokolu, kterými došlo k jejich vlastnímu pojmenování a systematickému zpracování. Základní zásady stanovené Úmluvou č. 108 jsou všeobecně používány a každá z nich má svůj určitý „obraz" ve vnitrostátní právní úpravě.

5.1.1.1. Zásada legitimity zpracování

První zásadou ovládající ochranu osobních údajů je zásada legitimity zpracování, která představuje jejich získání a zpracování v souladu se zákonnou právní úpravou a garantovanými základními lidskými právy a svobodami.[69]

Aspekt legality je v ZoOÚ prezentován zejména v § 5 odst. 1 písm. c) věta první a v §5 odst. 3. Doplňující hlediska zákonnosti a poctivosti zpracování shledáváme v jejich způsobu zpracování, přičemž shromažďování osobních údajů je možné pouze otevřeně a je vyloučeno shromažďovat osobní údaje k jiným činnostem a účelům.[70] Z této zásady nám vyplývá přidružený princip, který nám praví, že osobní údaje mohou být zpracovány zejména na základě souhlasu subjektu.

5.1.1.2. Zásada omezení účelem

Jako další zmíníme zásadu omezení účelem, která zakotvuje shromažďování osobních údajů pro specifické a legitimní účely. Podle tohoto principu nelze zpracovávat osobní údaje, jež jsou pouze obecně vymezené, a zároveň tento účel nemůže být v rozporu s právními předpisy.[71]

Ustanovení v § 5 odst. 1 písm. d) ZoOÚ předpokládá, že správce v první řadě splnil svou povinnost, a to určit účel, neboť bez toho by splnění tohoto institutu

[68] MAŠTALKA, Jiří, 2008, op. cit., str. 37.
[69] BARTÍK, Václav a Eva JANEČKOVÁ, 2012, op. cit., str. 9.
[70] § 5, odst. 1 písm. g zákona č. 101/2000 Sb.
[71] MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012. Praktik (Leges), str. 11.

nebylo možné.[72] Prakticky se jedná o vztah účelu a informace, která má být dílčím prostředkem pro jeho dosažení. Tato zásada rovněž vylučuje možnost zpracování údajů v rozporu s původním účelem. Osobní údaje lze shromažďovat pouze v mezích předem určeného účelu a v nezbytném rozsahu pro jeho naplnění. Cílem tedy je, aby pro dosažení zamýšleného účelu došlo k použití, co možná nejužší skupiny osobních údajů.

5.1.1.3. Zásada časového omezení

Zásada časového omezení je reflektována v ustanovení § 5 odst. 1 písm. e) ZoOÚ, kde je stanovena povinnost uchovávat osobní údaje pouze po dobu nezbytnou k účelu jejich zpracování. Po dosažení takového účelu mohou být údaje uchovány pouze pro historické, vědecké či statistické účely. Zde je však potřeba klást důraz na ochranu před neoprávněnými zásahy dostatečným aparátem ochranných a bezpečnostních opatření, např. pomocí anonymizace.[73]

Podle všeobecného předpokladu není „neomezená doba“ pro ochranu osobních údajů naplněním požadavku časového rámce. Spornou otázkou však zůstává délka časového úseku, po který má k uchování osobních údajů docházet. ZoOÚ vyžaduje, aby mezi účelem a dobou uchování osobních údajů existovala úzká souvislost.[74] Doba uchování by měla být posuzována vždy s ohledem na konkrétní okolnost jednotlivého případu zpracování.

5.1.1.4. Zásada proporcionality

Zákonné zakotvení zásady proporcionality nalezneme v §5 odst. 1 písm. d) a f), také označované pojmy přiměřenosti a potřebnosti chápeme jako nezbytnost vyžadující, aby zpracovávané osobní údaje nebyly nadměrné a směřovaly v nezbytném rozsahu k dosažení požadovaného účelu.

Tento princip musíme brát v úvahu po celou dobu zpracování, neboť situace, která platí na počátku, v další fázi zpracování již platit nemusí a některé údaje již nadále nejsou nezbytné, tudíž by měly být odstraněny.[75] Správce by si tak měl

[72] § 5, odst. 1, písm. d zákona č. 101/2000 Sb.
[73] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2003. Beckovy texty zákonů s komentářem, str. 332.
[74] KUČEROVÁ, Alena, 2003, op. cit., str. 72.
[75] MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK, 2012, op. cit., str. 15.

předem stanovit prostředky a způsob, stejně jako rozsah potřebných údajů. Cílem je opět zpracování co nejužšího okruhu osobních údajů.

5.1.1.5. Zásada transparentnosti

Zásada transparentnosti, někdy též označována jako zásada průhlednosti, vyžaduje úplnou informovanost fyzických osob o všem, co se týká zpracování jeho údajů, a to ve srozumitelném formátu.

Úmluva č. 108 ve svém článku 9 uvádí situace, za kterých je možné takovéto poskytování informací omezit. Takové omezení je možné na základě zákona, vyžaduje-li to veřejný zájem, bezpečnost, potírání trestné činnosti, je-li to v zájmu subjektu údajů nebo dalších osob apod.[76] Podle § 11 zákona č. 101/2000 Sb. *„je správce při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy“*. Součástí informace musí být taktéž poučení, zda je poskytnutí údajů povinné nebo dobrovolné a o případných důsledcích při jejich neposkytnutí.

5.1.1.6. Zásada bezpečnosti

Zásadou bezpečnosti je v § 13 ZoOÚ zakotvena potřebnost bezpečnostních opatření chránících osobní údaje v datových souborech, a to pomocí přiměřených, technických, organizačních a personálních opatření.

Přijetí těchto opatření minimalizuje hrozbu zásahu do soukromí, jež je potřeba hodnotit právě prostřednictvím provedených bezpečnostních opatření. Tato opatření musí být zajištěna s ohledem na odbornou úroveň a náklady jejich provedení odpovídající míře rizik a povaze zpracovávaných údajů. Obecně však musí být vyhodnocována zeširoka.[77]

Z tohoto hlediska zákon nepřipouští žádné výjimky. Pokud tedy správce neučiní potřebná opatření, protože nemůže, a to ani částečně s ohledem na provádění jen některých kroků zpracování, případně nenakládá-li s osobními údaji vůbec, přechází tato povinnost na zpracovatele. Samozřejmostí je obecně stanovená

[76] KUČEROVÁ, Alena, 2003, op. cit., str. 332.
[77] MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK, 2012, op. cit, str. 19.

povinnost mlčenlivosti pro všechny, kteří pracují s osobními údaji, a to jak za doby trvání pracovněprávního či obdobného vztahu, tak i po jeho ukončení.

5.1.1.7. Zásada práva přístupu k datům

Přístup dotčeného subjektu k údajům je jednou ze základních zásad a smí být omezen pouze zákonem. V § 12 ZoOÚ jsou vyjádřeny podmínky žádosti správce o předání informací. Správce má povinnost bez zbytečných průtahů této žádosti vyhovět. Možnosti nevyhovění žádosti nastává v případě, že má na tom stát zvláštní zájem a vyžaduje-li to zvláštní právní úprava.

Obsahem informace je sdělení o účelu, rozsahu či kategoriích zpracovávaných údajů, povaze prostředků a také o jejich příjemci. Tato služba může být správcem zpoplatněna, ale jen do výše nákladů na poskytnutí informací.

5.1.1.8. Zásada práva na opravu a výmaz

Ze zásady práva na opravu a výmaz této zásady nám vyplývá povinnost zpracování pouze pravdivých, přesných a aktuálních dat. Výjimku z tohoto pravidla tvoří např. policejní a soudní spisy nebo zdravotnická dokumentace, kde nepravdivá data mohou mít důležitý význam.[78]

Subjekt se může domáhat opravy nepravdivých informací, požadovat vysvětlení a odstranění stavu především blokací, opravou, výmazem či likvidací údajů.[79] V takových situacích by měl subjekt právo učinit prohlášení ohledně pravdivosti údajů nebo dalších požadavků na jejich úpravu.

V případě nečinnosti správce má subjekt právo obrátit se přímo na Úřad s podnětem, který jej přijme a vyhodnotí. Způsob zásahu je však v plné kompetenci Úřadu a subjekt údajů není nadán jakoukoliv možností domoci se konkrétního opatření. Právní úprava nepočítá ani se zahájením správního řízení, jež je plně ovládáno zásadou oficiality a může být tedy zahájeno jen z moci úřední. Podání stěžovatele tak může být považováno pouze za podnět k provedení kontroly a zahájení řízení o nápravných opatření podle § 40 ZoOÚ. Tyto závěry plynou přímo z rozsudku Nejvyššího správního soudu ze dne 16. 3. 2010, č. j. 1 As 93/2009-126.

[78] MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK, 2012, op. cit, str. 23.
[79] § 21 zákona č. 101/2000 Sb.

5.1.1.9. Zásada nezávislého dozoru

Zásada nezávislého dozoru, vyjadřuje povinnost každého státu zajistit dozor nad ochranou a zpracováváním osobních údajů. Stát má pověřit jeden nebo několik orgánů veřejné moci, které na svém území zajistí požadovaný dohled, a to zcela nezávisle. Mezi další pravomoci takového úřadu budou patřit různá šetření, přístup k údajům, shromažďování veškerých informací apod.

Právní postavení našeho Úřadu pro ochranu osobních údajů nalezneme v § 28 ZoOÚ, jenž je téměř doslovnou adaptací Směrnice 95/46/ES: *„(1) Úřad je nezávislý orgán. Ve své činnosti postupuje nezávisle a řídí se pouze zákony a jinými právními předpisy. (2) Do činnosti Úřadu lze zasahovat jen na základě zákona. (3) Činnost Úřadu je hrazena ze samostatné kapitoly státního rozpočtu České republiky.“*

5.1.2. Správce

„Správcem je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.“[80] Jeho práva a povinnosti vyplývají ze základních zásad, jimiž je celý proces ovládán. Správce je v první řadě povinen stanovit účel, prostředky a způsob zpracování. Zpracovávat a shromažďovat lze pouze konkrétní údaje, a to v rozsahu nezbytném k předem stanovenému účelu.

Základní určení správce je dále doplněno ustanovením § 3 odst. 1 ZoOÚ, podle něhož se zákon *„vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.“* Toto ustanovení nám tedy přímo vymezuje okruh adresátů právní normy z hlediska osobní a věcné působnosti. Z výčtu je patrné, že zákon dopadá na každý subjekt, jenž osobní údaj zpracovává, neboť vzhledem k rozsahu vymezení budeme těžko hledat subjekt, který by byl ze základního vymezení působnosti vyňat.[81]

Definice tudíž nelze omezovat pouze na tzv. velké správce, jakými jsou orgány státní správy a samosprávy, soudy, obchodní společnosti apod. Za správce považujeme kohokoliv, kdo v rámci své podnikatelské činnosti, profese, živnosti

[80] § 4, písm. j zákona č. 101/2000 Sb.
[81] BARTÍK, Václav. Zákon o ochraně osobních údajů s komentářem. Olomouc: ANAG, 2010. Právo (ANAG), str. 55.

zpracovává osobní údaje, tedy systematicky spravuje databázi svých obchodních partnerů, klientů, pacientů, zákazníků atd. Konkrétním příkladem může být každý lékař vykonávající zdravotní péči, jenž v této souvislosti vede zdravotní dokumentaci pacientů.

5.1.2.1. Práva a povinnosti správce

Správce je při zpracování vázán taktéž pravidly legality, která máme zakotvena v §10 ZoOÚ. Má dbát, aby subjekt údajů neutrpěl újmu na svých právech, a to především na zachování lidské důstojnosti. Dále má na starost ochranu před neoprávněnými zásahy do soukromého života.

Při shromažďování osobních údajů musí správce informovat o jeho rozsahu a účelu zpracování a také komu budou zpřístupněny. Subjekt údajů musí být poučen o tom, zda se jedná o dobrovolné nebo povinné, jakož i o následcích odmítnutí poskytnutí osobních údajů. Poučení není třeba, dochází-li ke zpracování pouze pro vědecké, statistické a historické účely. Dochází ke zpracování pouze legálně zveřejněných dat, a to na základě souhlasu či bez něj. Rozhodnutí, jehož důsledkem je zásah do právního postavení subjektu, nelze bez ověření vydat pouze automatizovaným zpracováním. Toto neplatí, pokud rozhodnutí působí ve prospěch subjektů či na jeho žádost. V automatizovaném zpracování osobních údajů je správce a zpracovatel povinen dbát na použití těchto systémů pouze oprávněnými osobami, přístupu pouze k vymezenému oprávnění, zamezení neoprávněného přístupu k datovým nosičům.[82] Správce i zpracovatel musí přijmout opatření k zamezení neoprávněného či nahodilého přístupu k osobním údajům. Tato povinnost zůstává v platnosti i po ukončení zpracování.[83]

Správce musí přijmout opatření dostačující pro naplnění legitimního účelu zpracování. Dbá na zajištění ochrany běžných a rozumně předpokládaných rizik. Povinnost tedy není absolutní, neboť nelze poskytnout garanci ochrany dat při výjimečných událostech, např. teroristický útok, živelní pohroma. Zde se musí zkoumat míra opatření, která by mohla tyto situace alespoň zmírnit.[84]

[82] § 11 zákona č. 101/2000 Sb.
[83] § 13 odst.1zákona č. 101/2000 Sb.
[84] MAŠTALKA, Jiří, 2008, op. cit., str. 103.

Mezi další významnou povinnost správce patří oznamovací povinnost, která zní: *„Ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle tohoto zákona, s výjimkou zpracování uvedených v § 18, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováváním osobních údajů.“*[85]

Povinné obsahové náležitosti oznámení jsou identifikační údaje správce, fyzické osoby, účel a kategorie zpracovávaných údajů, popis způsobu, jejich místo a příjemce, popis bezpečnostních opatření a předpoklad předání jiným státům.[86]

Tato povinnost podle výše citovaného § 16 ZoOÚ se nevztahuje na zpracování osobních údajů veřejně přístupných podle zvláštního zákona, které správci přímo ukládá zvláštní právní úprava, jedná-li se o skupinu údajů, k jejichž zpracování byl dán souhlas a sledují-li politické, filozofické, náboženské či odborové cíle, za předpokladu, že se týká pouze jejich členů, případně osob, s nimiž je v opakovaném kontaktu.[87]

Mezi neopominutelnou povinnost správce patří provedení likvidace osobních údajů, a to ihned, jakmile pomine účel, či na základě žádosti samotného subjektu. Výjimkou zachování údajů zůstávají pro účely archivnictví a uplatnění práv v občanském soudním řízení, trestním a správním řízení.[88] Likvidace osobních údajů představuje takovou operaci, jejímž důsledkem je nenávratné zničení takových informací. K takovému kroku může dojít jak přímým jednáním správce či zpracovatele, tak jednáním jiného oprávněného subjektu.[89] V zásadě se jedná o fyzickou likvidaci, *„u papírových nosičů se nabízí skartace, u elektronických nosičů jejich vymazání způsobem, který vyloučí zpětnou obnovu dat.“*[90]

[85] § 16 odst. 1zákona č. 101/2000 Sb.
[86] § 16odst. 2zákona č. 101/2000 Sb.
[87] § 18zákona č. 101/2000 Sb.
[88] § 20 zákona č. 101/2000 Sb.
[89] KUČEROVÁ, Alena, 2003, op. cit., str. 57.
[90] BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012. Olomouc: ANAG, 2012. Právo (ANAG), str. 27.

5.1.3. Zpracovatel

„Zpracovatelem je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.“[91] Zpracovatel na rozdíl od správce „pouze“ provádí zpracování osobních údajů. Neurčuje účel ani prostředky zpracování, zároveň nemusí provádět ani všechny operace, může plnit jen některé povinnosti nebo činnosti související se zpracováním. Zpracovatel tedy nemusí být vždy tím subjektem, jenž osobní údaje shromáždil.[92]

„Z pohledu odpovědnosti za zpracování osobních údajů nelze být zároveň v postavení správce a zpracovatele.“[93] Pokud si tedy vezmeme za příklad třeba podnikatelský subjekt, který bude správcem osobních údajů, ani jeho některá organizační složka nemůže být současně zpracovatelem téhož zpracování týchž osobních údajů. V případě nesprávného užití terminologie správce a zpracovatele se v postavení podnikatelského subjektu nic nemění. Pokud subjekt plní povinnosti správce a je nevhodně označen pojmem zpracovatel, nepovažujeme to za porušení ZoOÚ.

Činnost zpracovatele může být řízena dvěma způsoby, zaprvé výslovným zákonným zmocněním nebo zadruhé na základě smluvního ujednání, je-li k tomu správcem zmocněn. Z běžné praxe vyplývá, že vztah správce a zpracovatele je ve valné většině ovládán jejich smluvním vztahem.[94] V některých případech je zákonem přímo stanoveno, že zpracování provádí odlišný subjekt od správce, tedy zpracovatel. Takovéto zákonné zmocnění se ve většině případů týká pouze některých způsobů zpracování, především shromažďování, a správce má potom na starost provedení dalších způsobů, jakými je uchování údajů a jejich předávání.

Ustanovení § 14 ZoOÚ předpokládá, že se na zpracování údajů budou podílet rovněž zaměstnanci správce nebo zpracovatele, případně další osoby, které jsou vůči nim ve smluvním vztahu. Z této formulace nám plyne závěr, že správce může zpracováním pověřit i další osoby, resp. zpracovatel může uzavřít smlouvu o zpracování s jiným subjektem.[95] Smyslem tohoto ustanovení je však zejména

[91] § 4, písm. k zákona č. 101/2000 Sb.
[92] Důvodová zpráva k zákonu č. 101/2000 Sb.
[93] BARTÍK a JANEČKOVÁ, z pohledu zvláštních právních úprav k 1.8.2012, op. cit., str. 20.
[94] BARTÍK, Václav, 2010, op. cit., str. 58.
[95] MATES, Pavel. Ochrana soukromí ve správním právu. Praha: Linde, 2004, str. 192.

zajištění bezpečnosti osobních údajů, tím, že zpracovávat mohou jen pověřené osoby. Zpravidla se jedná o zaměstnance či osoby v jiném poměru než pracovněprávním, např. členský vztah k družstvu. Platnou zásadou ale je, že správce smí zpracováním pověřit i více zpracovatelů, avšak samotný zpracovatel nemůže uzavřít smlouvu o zpracování s dalším subjektem.[96]

Všechny tyto osoby jsou taktéž povinny zachovávat mlčenlivost o osobních údajích a bezpečnostních opatřeních, pakliže by jejich zveřejnění znamenalo ohrožení zabezpečení takových údajů. Tato povinnost mlčenlivosti zůstává zachována i po ukončení zaměstnání nebo obdobného poměru.

5.1.4. Souhlas

Jeden z nejdůležitějších pojmů provázející oblast zpracování máme definovaný v § 4 písm. n) ZoOÚ: *„Souhlasem subjektu údajů svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.“* Svoboda vůle představuje její dobrovolné vytvoření, bez fyzického či psychického donucení. Vědomost souhlasu při poskytování souhlasu znamená uvědomění důsledků svého konání.

Poskytnutí souhlasu je obecně chápáno jako jednostranný právní úkon, nejedná se tedy o dohodu mezi správcem nebo zpracovatelem na straně jedné a subjektem údajů na straně druhé. Pro posouzení jeho platnosti musíme brát v úvahu i úpravu právního jednání v obecném právním předpisu, zejména ustanovení § 545 zákona č. 89/2012 Sb., občanský zákoník, jež uvádí, že *„právní jednání vyvolává právní následky, které jsou v něm vyjádřeny, jakož i právní následky plynoucí ze zákona, dobrých mravů, zvyklostí a zavedené praxe stran“* a ustanovení § 547 zákona č. 89/2012 Sb., občanský zákoník, jež zní: *„Právní jednání musí obsahem a účelem odpovídat dobrým mravům i zákonu.“* Takový souhlas musí rovněž splňovat obecné náležitosti vůle čili být svobodný a vážný a projev by měl být určitý a srozumitelný.

Obecné pravidlo stanoví, že zpracování osobních údajů se může dít zásadně na základě souhlasu. Bez udělení tohoto souhlasu je zpracování možné pouze ve vymezených případech, a to je-li to nezbytné pro dodržení právní povinnosti

[96] MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI), str. 216

správce, vyžaduje-li to plnění smlouvy, jejímž předmětem budou jistá práva a povinnosti. Nakládání s údaji bude tak spojeno s existencí konkrétní smlouvy. Dále pokud se jedná o neodkladný úkon či je-li to nezbytné k ochraně životně důležitých zájmů. Jde-li o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem nebo je-li to nezbytné k ochraně zájmů správce, příjemce či jiné dotčené osoby.[97] Zpracování však nemůže být v rozporu s právy na ochranu soukromého a osobního života subjektu údajů. Souhlas není třeba ani v případě uvádění informací o veřejně činné osobě, zaměstnanci veřejné správy, údajů týkajících se jeho veřejné či úřední činnosti a také jde-li výlučně o zpracování pro historické účely.

Při udělování souhlasu musí být subjekt informován o účelu zpracování, rozsahu, příjemci a období, po které bude souhlas poskytnut. *„Jestliže má být souhlas v tomto smyslu informovaný, pak uvedené skutečnosti musejí být subjektu údajů sděleny před tím, než souhlas poskytne.“*[98]

Zákon o ochraně osobních údajů pro souhlas nestanoví povinnou formu, ale správce musí být schopen po celou dobu zpracování existenci souhlasu prokázat. Pro případy zpracování citlivých údajů však musí být učiněn výslovně. V rámci své správcovské činnosti pro účely nabídky obchodu či služeb smí použít údaje získané z veřejného seznamu. Takto použité údaje ovšem nelze dále zpracovávat, vyslovil-li k tomu subjekt svůj nesouhlas. Nesouhlas musí být v písemné formě a správce má povinnost o tom vyrozumět všechny správce, kterým již předal osobní údaje. K dosažení cíle, že již tyto údaje, jako je jméno, příjmení a adresa, nebudou dále používány, je smí správce pro tuto vlastní potřebu zpracovávat. V případě konfliktu, kdy subjekt údajů tvrdí, že správce provádí zpracování bez souhlasu, je důkazní břemeno na straně správce.

Souhlas se zpracováním je potřeba chápat jako návrh nepojmenovaného kontraktu. Rozhodně se pro nejedná o izolovaný jednostranný úkon. V současném znění zákona není blíže specifikována forma souhlasu. Dřívější verze zákona znala institut zákona odvolání souhlasu kdykoliv v průběhu jeho zpracování, v praxi to však způsobovalo nemalé komplikace, a proto se s tímto institutem již nesetkáme.[99]

---

[97] § 5 odst. 2 zákona č. 101/2000 Sb.
[98] Stanovisko č. 2/2008, souhlas se zpracováním osobních údajů, ÚOOÚ, září 2008, dostupné z www.uoou.cz/files/stanovisko_2008_2.pdf
[99] MAŠTALKA, Jiří, 2008, op. cit., str. 51.

5.1.5. Zpracování citlivých údajů

Citlivé údaje je možné zpracovávat, jen pokud: *„Subjekt údajů dal ke zpracování výslovný souhlas. Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Existenci souhlasu subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování. Správce je povinen předem subjekt údajů poučit o jeho právech podle § 12 a 21.“*[100]

Zpracování citlivých údajů je upraveno zvláštní postupem, pokud je to nezbytné v zájmu zachování života či zdraví, odvrácení bezprostředního nebezpečí. Ve výjimečných případech lze tuto kategorii osobních údajů zpracovávat i bez souhlasu, a to v případě, že souhlas nelze získat v důsledku fyzické, duševní nebo právní nezpůsobilosti, je-li nezvěstný či z jiných obdobných důvodů.

Pod tuto kategorii řadíme zpracování údajů týkajících se zdravotního stavu, služeb, ochrany veřejného zdraví, pojištění a výkonu státní správy ve zdravotnictví stanovených zvláštním zákonem. Dalším případem může být nezbytnost pro dodržení práv a povinností správce. Dále jde-li o zpracování údajů sledujících politické, filozofické, náboženské či odborové cíle v rámci oprávněné činnosti, týkajících se pouze jejich členů či osob, s nimiž jsou v opakovaném kontaktu. Mezi zpracování těchto údajů řadíme i informace nezbytné pro provedení nemocenského a důchodového pojištění, státní sociální podpory a také dalších sociálních dávek. Ve zvláštních případech lze zpracovávat, týká-li se to zveřejněných údajů, jejich zpracování je nedílnou součástí pro uplatnění jejich nároků či jsou použity výlučně pro archivnictví a v neposlední řadě se jedná postup dle zvláštního právního předpisu v případech předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách.[101]

[100] § 9 písm. a) zákona č. 101/2000 Sb.
[101] § 9 zákona č. 101/2000 Sb.

5.2. Zpracování podle GDPR

Pojem zpracování osobních údajů má prakticky stejný význam, jako měl v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, jemuž je věnována kapitola 5.1. Ovšem je potřeba vypíchnout několik patrných rozdílů.

Obecné nařízení definuje zpracování v čl. 4 bodě 2 jako: *„Jakoukoliv operaci nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“* Z definice nařízení nám tak zmizel prvek systematičnosti, jenž však byl čistě českou specialitou a neměl podklad v definici Směrnice 95/46/ES. *„Zpracování ve smyslu Obecného nařízení však nelze chápat jako jakékoli nakládání s osobním údajem.“*[102] Nakládání s osobními údaji, kterým nebude zpracování, je poskytována ochrana např. zákonem č. 89/2012 Sb., občanský zákoník. Zpracování musíme považovat za sofistikovanější činnost, již správce osobních údajů provádí za určitým účelem.

Obecné nařízení se vztahuje na zcela nebo částečně automatizované zpracování a na neautomatizované zpracování osobních údajů, které jsou obsaženy v evidenci nebo mají-li být do ní zařazeny. Pojem automatizace není v GDRP přímo definován, ale představu si můžeme udělat z pojmu „automatizovaných postupů“. Evidencí se podle čl. 4 bodu 6 Obecného nařízení rozumí: *„Jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.“* Recitál 15 dále výslovně uvádí, že údaje, jež nejsou uspořádány podle určitých hledisek, by z působnosti Obecného nařízení měly být vyňaty.

Hlavním atributem zpracování by měla být kategorie subjektu údajů. Zpracování by se tak mělo týkat určité skupiny fyzických osob. Jako podpůrný

[102] Praktický manuál GDPR pro každého: vše, co potřebujete vědět o novém nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně osobních údajů v praktickém kompletu s webem, e-bookem a aktualizačním servisem. Bratislava: Donau Media, 2018, str. 12.

argument lze použít ustanovení čl. 30 odst. 1 písm. c), které v rámci záznamů o činnostech uvádí jako jednu z náležitostí i popis kategorií subjektu údajů.

Ke zpracování v pravém významu dochází tedy v případech, kdy si podnik sám rozhodne o účelech a prostředcích zpracování, tzn., když se zpracovatel řídí stanovenými pokyny. Typickými příklady mohou být personální a mzdové agendy, zpracování reklamních adres v adresáři, zákaznické systémy, evidence obyvatel, veřejné rejstříky obsahující osobní údaje, externí zajišťování části vlastního provozu telekomunikačních zařízení apod. Naopak o zpracování se nejedná v souvislosti s využíváním externích odborných služeb, např. nábor pracovníků, péče o smluvní zákazníky, finanční a daňové poradenství, audity, inkasní činnost atd.[103]

Pracovní skupina WP29 rozšiřuje definici Obecného nařízení o pojem rozsáhlé zpracování, které bere v úvahu zejména následující faktory: počet dotčených subjektu údajů, objem zpracovávaných dat, doba trvání nebo nepřetržitost zpracovatelské činnosti. Konkrétními příklady pak může být: *„zpracování údajů o pacientech v rámci běžné činnosti nemocnice, zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu, zpracování údajů o aktuální zeměpisné poloze zákazníků mezinárodních řetězců rychlého občerstvení pro statistické účely zpracovatelem zaměřeným na tuto činnost, zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky, zpracování osobních údajů vyhledávačem pro behaviorální reklamy, zpracování dat poskytovatelem telefonních a internetových služeb.“*[104]

5.2.1. Zásady

Obecnou úpravu zásad, neboli právních principů, jsme si přiblížili již v kapitole 5.1.1. a bezpochyby na ní můžeme stavět i v této kapitole týkající se zásad Obecného nařízení.

Jak již bylo zmíněno v předchozí kapitole, zásady v evropském právním rámci nejsou žádnou novinkou. Prvotní mechanismy pocházejí již ze směrnice OESD, následně byly v pozměněném stavu včleněny do Úmluvy č. 108 a poté do Směrnice

[103] GDPR v kostce: praktický průvodce povinnostmi pro podniky a spolky. Praha 2018, str. 21.
[104] Praktický manuál GDPR pro každého, 2018, op. cit., str. 14.

94/46/ES.[105] Naše vnitrostátní úprava v zákoně pro ochranu osobních údajů sice neobsahuje jejich přesný výčet, ale jsou vloženy do úpravy povinností správce v jeho § 5. Nařízení však stejně jako směrnice vyčlenilo pro zásady samostatný článek 5. Ve srovnání těchto dvou úprav nalezneme materiální úpravy a jejich zpřesnění téměř u všech, snad pouze s výjimkou zásady integrity a důvěrnosti a zásady přesnosti. Z pohledu nových povinností pro správce a zpracovatele bude nejvíc patrný dopad na změnu zásady odpovědnosti.

Těmito zásadami se řídí celé Obecné nařízení a všechna jeho ustanovení musí být vykládána tak, aby s nimi byla v souladu. Základní zásady považujeme samy o sobě za nejvýznamnější povinnosti, které určují, jak má správce zpracovávat osobní údaje. Tyto principy můžeme do jisté míry označit rovněž za obecné klauzule, pod něž můžeme rozřadit většinu povinností plynoucích z Obecného nařízení.

5.2.1.1. Zásada zákonnosti, korektnosti a transparentnosti

Osobní údaje musí být „*ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem",*[106] Zákonností rozumíme zpracování, jež probíhá v souladu s právními předpisy. Zde to tedy znamená zpracování na základě souhlasu, a to předvídatelným způsobem.[107]

Korektnost znamená především poctivé zpracování osobních údajů. Případ se musí posuzovat individuálně se zohledněním všech okolností. Obecně můžeme tuto zásadu chápat jako princip ohleduplnosti, který znamená i zpřesnění zásad přiměřenosti. V praxi se jedná např. o vyloučení skrytých osobních údajů a jejich zpracování. Transparentnost je potom zárukou informační povinnosti při sběru osobních údajů. Předpokladem je jednoduchá přípustnost, srozumitelnost a jejich vyhotovení v jasné a jednoduché řeči.[108] Musí být dodrženo poučení o rizicích, právních předpisech, právech atd. Rozhodně však musí být předem stanovený účel, jehož má být dosaženo přiměřeným způsobem.

[105] NULÍČEK, Michal, 2017, op. cit., str. 105.
[106] Čl. 5 odst. 1 písm. a Obecného nařízení GDPR
[107] Rozsudek ESD Rechnungshof (C-465/00) proti Österreichischer Rundfunk a dalším a Christa Neukomm (C-138/01) a Joseph Lauermann (C-139/01) proti Österreichischer Rundfunk ze dne 20. 5. 2003
[108] NAVRÁTIL, Jiří, 2018, op. cit., str. 40-41.

V současné době je ve Směrnici 95/46/ES výslovně uvedena pouze zásada korektnosti, ale vzhledem k tomu, že zásady korektnosti a transparentnosti mají téměř totožný obsah, je takové doplnění pouze deklaratorního účelu. Stejně tak v zákoně pro ochranu osobních údajů doposud nenajdeme explicitní vyjádření zásady zákonnosti.

5.2.1.2. Zásada účelového omezení

Účelové omezení můžeme považovat za hlavní zásadu zpracování osobních údajů, které je pro nás nejvýznamnějším určovatelem pro nakládání s osobními údaji, jež jsou *„shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely.“*[109]

Tato zásada se objevuje v obou právních úpravách a je doplněním zásady transparentnosti. Znamená, že účel zpracování musí být znám již při sběru dat.[110] Takový účel musí být určitý, výslovně vyjádřený a legitimní. Určitost má představovat jasný základ pro zpracování, a to tak, aby mohl být posouzen soulad s Obecným nařízením.[111] Na druhou stranu však není vhodné účel specifikovat příliš úzce, jelikož by se sám správce omezil ve svých operacích. Účel musí být rovněž výslovně vyjádřen, z čehož plyne závěr, že jej správce musí až na výjimky sdělit subjektu údajů. Pro splnění tohoto předpokladu je podstatné, aby jej všichni dotčení chápali stejně. Legitimita účelu znamená soulad účelu s právním řádem, nikoliv tedy pouze s GDPR, ale i s dalšími předpisy jak zákonnými, tak podzákonnými.[112]

Pozdější úprava účelu či jeho rozšíření je možná, pokud pro to existuje zákonný podklad a není-li to neslučitelné s účelem prvotního sběru. Důležitou roli hraje taktéž celkový kontext, za nějž byla data sesbírána a očekávání dotčených osob. V případě absence účelu se jedná o nelegální zpracování osobních údajů.

---

[109] Čl. 5 odst. 1 písm. b Obecného nařízení GDPR
[110] Recitál č. 39 Obecného nařízení GDPR
[111] Stanovisko WP29 č. 3/2013 ze dne 2. 5. 2013 k účelovému omezení, WP 203, dostupné z https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf, str. 16
[112] NULÍČEK, Michal, 2017, op. cit., str. 108.

5.2.1.3. Zásada minimalizace údajů

Princip minimalizace údajů je vyjádřen tak, že údaje musí být *„přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány“.*[113]

Zásada je ovládána třemi podstatnými prvky. Informace musí být podstatná, a to vzhledem ke sledovanému účelu, má se tak redukovat zpracování pouze na relevantní data opět ve vztahu k účelu zpracování a omezit se pouze na nutnou míru údajů, a to přiměřeným způsobem. Ve chvíli, kdy správce jednou stanoví účel zpracování, musí při každé další operaci pečlivě vážit, zda využívá pouze relevantní a přiměřené osobní údaje.

Oproti stávající úpravě ve Směrnici 95/46/ES Obecné nařízení tuto zásadu lehce zpřísňuje, a to právě stanovením omezeného nezbytného rozsahu zpracovávaných údajů ve vztahu k účelu.[114] Ovšem vzhledem k interpretaci této zásady do § 5 odst. 1 písm. d) v zákoně č. 101/2000 Sb. tato změna nebude mít na praxi v ČR prakticky žádný dopad.

5.2.1.4. Zásada přesnosti

Zásada přesnosti je vyjádřením požadavků na údaje *„přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.“*[115]

Předmětná data musí být věcně správná a dle potřeby aktuální. Nepřesné údaje musí být vymazány, což má na starost odpovědná osoba, jež získává informace a zpochybňuje správnost nebo přesnost údajů.[116] Tento požadavek však není absolutní, neboť např. údaje určené ke zpracování pro účely archivace rozhodně nebudeme aktualizovat, neboť by došlo ke zmaření původního účelu.

To, že máme požadavek na přesnost údajů, ovšem neznamená, že musí být vždy pravdivé. Zásada přesnosti je odrazem v právu subjektu údajů na opravu či doplnění údajů.

---

[113] Čl. 5 odst. 1 písm. c Obecného nařízení GDPR
[114] NULÍČEK, Michal, 2017, op. cit., str. 110.
[115] Čl. 5 odst. 1 písm. d) Obecného nařízení GDPR
[116] NAVRÁTIL, Jiří, 2018, op. cit., str. 42.

5.2.1.5. Zásada omezení uložení

Osobní údaje musí být *„uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány.“*[117] Pokud již uchování není potřebné, musí dojít ke smazání takových údajů, mimo stanovenou výjimku ve veřejném zájmu pro archivaci, vědecké a statistické účely. V případě, že zpracování nebude nezbytné pro nějaký zbývající účel, musí dojít k jejich výmazu nebo anonymizování.

Patrným rozdílem oproti stávající úpravě je zpřesnění formulace v Obecném nařízení, a to konkrétně pasáž „ve formě umožňující identifikaci“. Zavedení této formulace má význam především z důvodu, že Obecné nařízení deklaruje anonymizaci jako další zpracování. *„Pokud totiž správce osobní údaje anonymizuje, docílí podobného efektu, jako by je vymazal.“*[118] Takové údaje totiž nejsou vůbec považovány za osobní údaje a ochrana Obecného nařízení se na ně nevztahuje.

5.2.1.6. Integrita a důvěrnost

Integrita a důvěrnost znamená, že údaje jsou *„zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.“*[119]

Integrita vymezuje ochranu nedotknutelnosti údajů pomocí jednotlivých prostředků a opatření zejména jejich vhodností k individuálnímu případu.[120] Na rozdíl od současné úpravy zařadilo Obecné nařízení tuto povinnost mezi základní zásady a deklaruje tak zabezpečení osobních údajů jako klíčovou povinnost. Konkrétní požadavky zabezpečení jsou uvedeny v ustanovení čl. 32 GDPR.

[117] Čl. 5 odst. 1 písm. e Obecného nařízení GDPR
[118] NULÍČEK, Michal, 2017, op. cit., str. 115.
[119] Čl. 5 odst. 1 písm. f) Obecného nařízení GDPR
[120] NAVRÁTIL, Jiří, 2018, op. cit., str. 43.

5.2.1.7. Zásada odpovědnosti

Zásada je složena ze dvou významných povinností správce, který má v první řadě odpovídat za dodržení všech povinností a zajištění dodržování zásad vyplývajících z Obecného nařízení. Nově musí správce dodržení tohoto souladu doložit.[121]

Správce nově musí zavádět vhodné systémy ochrany a mít vše řádně zdokumentováno. Odpovědná osoba odpovídá za přijetí technických a organizačních opatření, ale nikoliv za výsledek. Dozorové úřady provádí kontrolu a dohlíží na dodržování stanovených postupů. Správce však odpovídá za přiměřenou míru rizika, které si musí vyhodnotit a vzít do úvahy náklady, stav techniky či povahu, rozsah a účely zpracování.

5.2.2. Souhlas

Obecné nařízení institut udělení souhlasu v zásadě nemění, ale doplňuje jeho nové požadavky. Podstatným rozdílem je, že Obecné nařízení nestanoví výlučné postavení souhlasu, jako praví naše stávající právní úprava. Nařízení staví souhlas na stejnou úroveň s ostatními podmínkami pro zpracování osobních údajů. Máme zde zakotveno doporučení nejprve najít některý zákonný důvod, a až pokud tu žádný není, máme žádat souhlas, neboť zpracování podle souhlasu je jeden z nejsložitějších způsobů.

Definice souhlasu je zakotvena v čl. 4 odst. 11 GDPR, který říká, že souhlasem *„subjektu údajů je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.“* Základním a nejpodstatnějším atributem souhlasu je jeho dobrovolnost. *„Subjekt údajů není povinen souhlas udělit a nesmí být za jeho neudělení ze strany správce nijak trestán.“*[122] Toto platí především ve vztazích nadřízenosti a podřízenosti, kde by souhlas neměl nacházet využití, neboť zde nelze moc dobře hovořit o svobodném udílení souhlasu. S těmito případy se nejčastěji setkáváme v pracovněprávních vztazích, kde velmi často dochází ke koncipování souhlasu subjektu údajů i na zpracování, jehož účelem je pokrýt právním důvodem plnění smlouvy či zákonem stanovené povinnosti.

[121] NULÍČEK, Michal, 2017, op. cit., str. 118.
[122] ŽŮREK, Jiří, 2018, op. cit., str. 73.

Takový souhlas je však neplatný a zbytečně mate zaměstnance o možnosti odvolání. Do budoucna je tak vhodné tento souhlas vypustit a nahradit písemnou informací ve smyslu čl. 13 Obecného nařízení.

První změnu v definici souhlasu představuje požadavek udělení souhlasu prohlášením nebo zjevným potvrzením, ale ani zde nemáme zakotven požadavek písemnosti souhlasu, pouze to, že souhlas musí být konkrétní a jednoznačný. V praxi se může jednat např. o zaškrtnutí políčka na internetové stránce, volba technického nastavení, další prohlášení nebo jednání, z čehož nám jasně vyplývá souhlas. Nařízení také zdůrazňuje, že se bude muset jednat o aktivní udělení souhlasu, kdy mlčení neznamená souhlas a předem zaškrtnutá políčka nebo nečinnost by neměly být považovány za souhlas.[123] Změna nastane i v oblasti získávání a zpracování identifikátorů cookies. Nově již nebude stačit dovození souhlasu z pouhého užívání webové stránky bez aktivního vyjádření souhlasu.

Souhlas by se měl týkat veškeré činnosti vztahující se k účelu. Pokud zde existuje účelů více, souhlas by měl být udělen ke každému jednotlivě. GDPR, stejně tak jako zákon o ochraně osobních údajů. vyžaduje schopnost správce kdykoliv v průběhu prokázat jeho existenci.

Obecně vzato se jedná o jednostranný právní úkon. Svoboda udělení souhlasu bude mít především dopad u souhlasů získávaných v rámci tzv. formulářových smluv, u nichž má subjekt údajů negociační šance, protože se jedná o smlouvy uzavírané s bankami, telefonními operátory či poskytovateli energií.[124] Dříve jsme se však poměrně často shledávali se situací, kdy byl souhlas včleňován do smlouvy, všeobecných podmínek nebo dalších dvoustranných právních úkonů. V praxi souhlas často sloužil jako „doplňkový“ právní důvod, kdy nešlo odmítnout souhlas se zpracováním osobních údajů na straně jedné a zároveň podepsat smlouvu, jednalo se tedy o smlouvy typu „ber, nebo nech být“. Tyto transakce byly často velmi nesrozumitelné a právně složité, či umístěné tak, aby byly snadno přehlédnutelné.

Nařízení se na tento nešvar snaží reagovat novým požadavkem, a to, aby písemné prohlášení souhlasu bylo od dalších skutečností jednoznačně a srozumitelně odlišeno a zejména vyjádřeno použitím jednoduchých jazykových

[123] Recitál č. 32 Obecného nařízení GDPR
[124] ŽŮREK, Jiří, 2018, op. cit., str. 74.

prostředků, a to pod hrozbou v případě nedodržení zrušení její závaznosti.[125] Toto kritérium odlišitelnosti značí především jeho snadné oddělení od ostatního textu a posílení autonomie rozhodování subjektu údajů.

Další změnou, kterou v GDPR nalezneme, je explicitní úprava odvolatelnosti souhlasu, jež byla v naší právní úpravě pouze dovozována ze Směrnice 95/46/ES. Tato výslovná úprava je zakotvena v článku čl. 7 odst. 3, který stanoví, že *„subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.“* Novotou je zde i znění odst. 4, jež stanoví, že „*při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.* Tento stav je považován za vysoce nežádoucí, a pokud je za těchto podmínek poskytnut, má se za to, že nebyl svobodný. Odst. 4 čl. 7 má zaručit, aby nedocházelo k maskování účelu zpracování, nebo být vázán na plnění kontraktu či poskytnutí služby.

Toto přímé zakotvení souhlasu v čl. 7 Obecného nařízení posiluje právní jistotu subjektů údajů, ale také správců, pro které výslovné definice znamenají příznivější právní prostředí, než kdyby si některé aspekty musely nadále odvozovat.[126]

Nařízení má za cíl umožnit správci pokračovat ve stávajícím zpracování i po začátku účinnosti nové úpravy, je-li toto zpracování založeno na souhlasu podle Směrnice 95/46/ES, respektive zákona č. 101/2000 Sb. Není nutné, aby subjekt údajů znovu udělil svůj souhlas, „p*okud je způsob udělení daného souhlasu v souladu s podmínkami tohoto nařízení, s cílem umožnit správci pokračovat v tomto zpracování i po dni použitelnosti tohoto nařízení“.*[127] Jestliže však dříve udělený souhlas nenaplňuje například znak odlišitelnosti souhlasu od ostatních skutečností nebo nebyl informovaný apod., bude neplatný a správce si musí sjednat nový souhlas, který bude odpovídat nově zavedeným podmínkám.[128] Do budoucna však bude potřeba zvážit potřebnost souhlasů

[125] JANEČKOVÁ, Eva, 2018, op. cit., str. 14.
[126] ŽŮREK, Jiří, 2018, op. cit., str. 72.
[127] Recitál č. 171 Obecného nařízení GDPR
[128] ŽŮREK, Jiří, 2018, op. cit., str. 75.

a odstranit ty nadbytečné v situacích, kdy existuje zákonný důvod pro zpracování a zrevidovat stávající znění souhlasů.

5.2.3. Zpracování zvláštních kategorií

Tato kategorie je upravena ve speciálním ustanovení čl. 9 odst. 1 nařízení, jež jejich zpracování a priori zakazuje. *„Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.“*

Zároveň zde máme ale odst. 2 čl. 9, jenž nám stanoví případy, které nám předchozí pravidlo vyruší. Takovéto prolomení zákazu zpracování musí zároveň splňovat podmínku zákonnosti. Zpracování citlivých údajů je tak možné především na základě výslovného souhlasu subjektu údajů, nezbytnosti pro účely plnění povinností a výkon plynoucí ze zvláštních práv správce či subjektu v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany nebo pro zpracování pro ochranu životně důležitých zájmů. Týká-li se zpracování v rámci svých oprávněných činností sledujících politické, filozofické, náboženské nebo odborové cíle či zjevně zveřejněných informací. K prolomení samozřejmě dochází, vyžaduje-li to určení, výkonu či obhajovacích nároků, veřejný zájem EU a jejího členského státu. Výjimka se tradičně vztahuje na údaje výlučně zpracovávané pouze pro účely historické, vědecké a statistické. Jedná-li se o údaje podle zvláštního zákona potřebné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytnutí zdravotní, sociální péče nebo léčby. Existence veřejného zájmu v oblasti veřejného zdraví, zejména ochrana před vážnými přeshraničním zdravotními hrozbami, zajištění přísných norem kvality, bezpečnosti zdravotní péče, léčivých přípravků dle unijního právo nebo jeho člena.

Co se týká komparace zpracování zvláštních kategorií osobních údajů ve stávající právní úpravě, jež jsme si přiblížili v kapitole 5.1.5, můžeme zde opět vidět její rozšíření a zpřesnění, a jak již bylo avizováno, vyčlenění samostatného článku 10 pojednávajícího o zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

5.2.4. Správce

Subjektem, bez kterého se žádné zpracování osobních údajů neobejde je správce osobních údajů. Existence správce je nezbytným předpokladem každého procesu zpracování, neboť právě on určuje jeho účel a prostředky. Jen správce smí rozhodovat o účelech zpracování a je tak nadán odpovědností za soulad zpracování s Obecným nařízením, kdy správce musí být schopen tento soulad prokázat. Správce je tedy hlavním adresátem povinností vyplývajících z nařízení.

Správce je definován v Obecném nařízení v čl. 4 bodě 7, jenž stanoví, že správcem je *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů“*.

„Každého správce se Obecné nařízení dotkne jiným způsobem, a to v závislosti na aspektech zpracování, které provádí.“[129] Správci jsou určitými způsoby diferencovány dopady, jež na ně plynou z GDPR, a to vzhledem k rizikům, která jednotlivá zpracování představují. Každý správce tak musí Obecné nařízení pokaždé vykládat s jinou mírou intenzity a být si vědom skutečnosti, že za zpracování má odpovědnost.[130] Správce by si měl v první řadě udělat vlastní analýzu zpracování, jíž zjistí, jaké eventuální povinnosti se na něj vztahují. Pokud však správce řádně plní dosavadní povinnosti stanovené ze zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, nemělo by pro něj Obecné nařízení představovat výraznější problém.

Společní správci, tedy ustanovení dvou či více správců zároveň je zcela novým institutem zavedeným novou právní úpravou. Pro společné správce je charakteristické, že účely a prostředky stanovují mezi sebou.[131] V praxi se může jednat o případ, kdy se několik nezávislých subjektů dohodne na společné platformě provozování zpracování osobních údajů, a to i konkurujících si subjektů. Z tohoto vztahu je nezbytné vzájemně si vymezit rozsah odpovědnosti, a to zejména pokud se jedná o výkon práv subjektů údajů. Subjekt zde může bez ohledu na jejich vzájemné ujednání spolupracovat s každým z nich. Pakliže však za zpracování

[129] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: GradaPublishing, 2017. Právo pro praxi, str. 39.
[130] ŽŮREK, Jiří, 2018, op. cit., str. 89 – 90.
[131] Čl. 26, odst. 1 Obecného nařízení GDPR

odpovídá více než jeden správce, platí, že za způsobenou újmu odpovídá v plné míře každý správce, a to tak, aby byla zajištěna účinná náhrada újmy subjektu údajů.[132]

5.2.5. Zpracovatel

Správce ke zpracování může využít i jiný subjekt, zpracovatele, jímž může být *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce“.*[133] Zpracovatel na rozdíl od správce není obligatorním prvkem zpracování, jelikož jeho ustanovení záleží čistě na vůli správce. V praxi se můžeme setkat s hraničními případy, kdy je těžké určit, zda se jedná o správce nebo zpracovatele. V tomto případě je na místě prvotně zkoumat, kdo stanovil účel zpracování.

Zpracovatel plní jak povinnosti jemu stanovené GDPR, tak povinnosti uložené správcem, od kterých se nemůže z vlastní libovůle odchýlit. Zpracovatel rovněž nemůže zpracovávat údaje pro vlastní účely, neboť by začal vystupovat jako druhý správce, jenž by v tomto případě nedisponoval splněním zákonných podmínek a jednal by tak protiprávně. Správce smí zpracovatele přizvat prakticky kdykoliv bez nutnosti souhlasu dotčeného subjektu údajů nebo jiného právního důvodu. Nejčastěji dochází k ustanovení správce v případech, kdy správce nemá dostatečné personální či technické prostředky nebo je-li to pro něj ekonomicky výhodné.[134]

Článek 28 Obecného nařízení zpřesňuje podmínky vztahu správce a zpracovatele. Správce může využít zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technický a organizačních opatření, a to tak, aby byla zajištěna ochrana práv subjektu údajů v souladu s GDPR. Jakékoliv zpracování může klást různé požadavky na kvalitu zpracovatele, a to v důsledku rozsahu a kategorií zpracovávaných údajů. Pokud dojde k ustanovení zpracovatele, musíme znovu připomenout a zdůraznit, že správce je stále primárním odpovědným subjektem, jeho odpovědnost se při využití zpracovatele nikdy v plném rozsahu nepřenáší a nezaniká. To ovšem neplatí, jestli došlo k pochybení výlučně na straně

[132] Čl. 82odst.4Obecného nařízení GDPR
[133] Čl. 4 bod 8 Obecného nařízení GDPR
[134] ŽŮREK, Jiří, 2018, op. cit., str. 91 - 92.

zpracovatele. Správce by však v tomto případě mohl být konfrontován, že v dostatečné míře neprověřil jím zvoleného zpracovatele.

Jak již bylo zmíněno, zpracovatel musí poskytovat dostatečné záruky zavedením vhodných opatření, aby došlo ke splnění požadavků Obecného nařízení. Skupina WP29 se ve svém stanovisku zabývala právě těmito opatřeními, která jsou vhodná a čím jsou definovaná. Závěry z tohoto stanoviska mohou být inspirací i pro jiné oblasti. Stanovisko mezi technická a organizační opatření zařazuje integritu osobních údajů, která zaručuje pravost osobních údajů, dále důvěrnost pomocí šifrování nebo pseudonymizace, jež přispívají ke zvyšování zabezpečení osobních údajů. Stejně tak k zajištění důvěrnosti patří vymáhání povinnosti mlčenlivosti. Transparentnost je dalším opatřením, které má zajistit přezkoumatelnost a vhodnost zpracovatele, izolovanost je potom opatřením, jež má zajistit, že při zpracování údajů od více správců nedojde k záměně nebo sloučení osobních údajů. Do opatřeních skupina WP29 řadí samozřejmě i součinnost, která vede k řádnému výkonu práv subjektů údajů, a dále odpovědnost, jež je reflektována efektivním dodržováním zásad ochrany osobních údajů.[135]

Základním nástrojem, který upravuje vztah správce a zpracovatele, je smlouva o zpracování osobních údajů či další obdobný právní akt. Hlavním cílem má být nastolení právně vyváženého a pro osobní údaje bezpečného vztahu mezi těmito subjekty. Obligatorními náležitosti smlouvy je předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů, kategorie subjektu údajů, práva a povinnosti správce.

Mimo rámec obligatorních náležitostí smlouvy zde máme řadu dalších znaků, jež by měly ze zpracovatelské smlouvy vyplývat. V první řadě jsou to informace, že dochází ke zpracování osobních údajů pouze na základě pokynů správce. Zpracovatel má zajistit, aby se osoby podílející na činnosti zavázaly k mlčenlivosti a přijaly nařízením požadovaná bezpečnostní opatření. Dále zde musí být zahrnut dohled nad dodržením podmínek pro řetězení zpracovatelů, zohlednění povahu zpracování. Zpracovatel má být správci přiměřeně nápomocen při plnění jeho povinností podle článků 32 až 36 nařízení. Smlouva stanoví, že zpracovatel v souladu s rozhodnutím správce po ukončení zpracování osobní údaje vymaže,

[135] Stanovisko WP29 č. 5/2012 ze dne 1. 7. 2012 *ke cloudcomputingu*, WP 196, dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, str. 14.

vrátí správci, případně uloží, požaduje-li to některé právo Evropské unie nebo členského státu. V neposlední řadě smlouva upravuje poskytnutí správci veškerých informací k prokázání splnění uložených povinností, umožnění auditu a inspekcí prováděných přímo správcem nebo jím pověřeným auditorem.[136]

Dalším novým institutem, který Obecné nařízení zavádí, je vznik standardních smluvních doložek pro úpravu vztahu mezi správcem a zpracovatelem, jež mohou vyřešit problémy menších správců využívajících služeb zpracovatele, kteří si mnohdy nevědí rady se všemi náležitostmi smlouvy.[137]

V souvislosti s velkým rozšířením tohoto institutu je po účinnosti nové právní úpravy zakotvena povinná revize stávajících smluv uzavřených na základě podmínek stanovených zákonem č. 101/2000 Sb., kdy nevyhovující smlouvy je potřeba nahradit novými.[138]

„Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá.“[139] Tyto záznamy obsahují informace o jméně a kontaktních údajích správce, o účelu zpracování, popisu kategorií subjektů a osobních údajů. Rovněž zahrnují informace o případném předávání do třetí země nebo mezinárodní organizaci. Pokud je to možné, záznamy obsahují i plánované lhůty pro výmaz osobních údajů či obecný popis technických a organizačních bezpečnostních opatření. Obdobné povinnosti stanovené v odst. 1 se podle odst. 2 v menším rozsahu vztahují i na zpracovatele osobních údajů. Tyto záznamy se primárně vyhotovují v písemné formě, na požádání mohou být poskytnuty dozorovému úřadu.[140]

5.2.6. Pověřenec

Pověřenec pro ochranu osobních údajů neboli DPO (anglicky Data Protection Officer), je v České republice novým institutem, neboť k jeho zakotvení do účinnosti GDPR naše platná právní úprava nikdy nepřistoupila.

Povinnost jmenovat správce je zakotvena v čl. 37 odst. 1 v případech, kdy: „*a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů*

[136] Čl. 28, odst. 3 Obecného nařízení GDPR
[137] Čl. 28, odst. 7 Obecného nařízení GDPR
[138] ŽŮREK, Jiří, 2018, op. cit., str. 94.
[139] Čl. 30, odst. 1 Obecného nařízení GDPR
[140] Čl. 31 Obecného nařízení GDPR

jednajících v rámci svých soudních pravomocí; k písm. a) je nutno podotknout, že stále žádný evropský pramen nedefinuje pojem orgánu veřejné moci. V současné době se tedy přikláníme k významu, jejž mu přiznává právní řád ČR, ale za vědomí, že nemusí být stejný jako konečná definice SDEU. Podle teoretického pojetí, které uznává i náš Ústavní soud, lze orgán veřejné moci definovat jako druh právnické osoby, jež je zřízena k trvalému a opakujícímu se výkonu činnosti, který spočívá v autoritativním rozhodování o právech a povinnostech jiných subjektů, a to přímém nebo zprostředkovaném.[141] *b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;* za hlavní činnost považujeme primární aktivitu správce či zpracovatele, jež je primární aktivitou správce či zpracovatele. Zařazujeme sem aktivity, které od hlavní činnosti nejdou oddělit, na druhou stranu sem však nebudou patřit běžné aktivity organizací.[142] Monitorování je dalším pojmem, který není Obecným nařízením definován, obecně je však považujeme za aktivitu spočívající ve sledování subjektů údajů či jejich chování. K takovému jednání bude pravděpodobně docházet např. při provozu telekomunikační sítě a poskytování telekomunikačních služeb, profilování, sledování polohy na základě lokalizačních údajů, zpracování osobních údajů v rámci věrnostních programů, monitorování prostoru pomocí kamer apod.[143] *nebo c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.“*

Institut pověřence a povinnost jeho jmenování je odvislá od větší míry rizika, jak je patrno z výše vyjmenovaných důvodů. Riziko pro práva a svobody fyzických osob, jež vyplývá přímo z jeho, dá se říct, vrchnostenského statusu, vyžaduje dohled a zajištění souladu zpracování kvalifikovanou osobou. Přestože se jmenování pověřence vztahuje pouze k výše jmenovaným subjektům, případně druhům zpracování, ustanovený pověřenec nadále plní tuto funkci pro všechny následující operace daného správce či zpracovatele.

[141] Nález Ústavního soudu I. ÚS 229/98 ze dne 10. 11. 1998
[142] Návrh výkladového pokynu WP29 ze dne 13. 12. 2016 k pověřenci pro ochranu osobních údajů, WP 243, str. 6.
[143] Návrh výkladového pokynu WP29 ze dne 13. 12. 2016 k pověřenci pro ochranu osobních údajů, WP 243, str. 7.

Pověřencem smí být ustanovena fyzická osoba, a to přímo zaměstnaná u zaměstnavatele, ale i osoba externí na základě smlouvy o poskytování služeb. Není vyloučena ani možnost, že funkci bude vykonávat právnická osoba, zde se však vyžaduje zastoupení konkrétní fyzickou osobou, jež bude funkci vykonávat. Tento důvod plyne i z funkce, že pověřenec zároveň slouží jako kontaktní místo pro dozorové orgány a subjekty údajů. Vlastními pověřenci budou disponovat především velcí správci a zpracovatelé, kteří budou takové soby potřebovat zaměstnávat na plný úvazek, kdežto tzv. externí pověřence nalezneme spíše u menších správců a zpracovatelů. V těchto případech je třeba brát zvýšený ohled na zjištění informací o tom, jakým subjektům zvolený pověřenec dále poskytuje služby, a to, aby se předešlo situacím, kdy by pověřenec vykonával svou činnost např. pro konkurující si subjekty. Uvedené podmínky hlavní činnosti, rozsáhlosti a pravidelnosti vyplývající z čl. 37 odst. 1 písm. b) a c) musí být vždy splněny kumulativně. [144]

Podle čl. 37 odst. 5 Obecného nařízení musí být pověřenec jmenován na základě svých profesních kvalit. Úroveň odbornosti by měla odpovídat citlivosti zpracovávaných údajů a komplexnosti procesů zpracování. Pověřenec by měl mít dostatečné schopnosti k plnění svých úkolů. Neznamená to, že musí být odborníkem na IT, bezpečnost, právo a lidské zdroje, ale stačí, když bude mít dostatečné povědomí. Podle názoru WP29 by měl mít pověřenec taktéž určitý standard morální integrity a etiky. Požadavky jednotlivých správců a zpracovatelů na kvality pověřence se však budou lišit. Podpůrný charakter doložení odborné způsobilosti může být certifikát, tedy doklad potvrzující absolvování specializovaného kurzu pro pověřence.

5.2.6.1. Úkoly pověřence

Úkoly pověřence korespondují s jeho rolí a účelem, pro který byl v nové právní úpravě zakotven. Má být zejména k dispozici správci a dosáhnout tak co největšího souladu se zpracováním osobních údajů a chránit tím práva a svobody subjektu údajů v rizikovějších situacích.[145] Jednou z hlavních rolí pověřence je odborná podpora příslušného správce osobních údajů, a to na jeho žádost. Tato poradní činnost spočívá především v poskytnutí rady, informace, zvolení metodiky, použití

[144] NULÍČEK, Michal, 2017, op. cit., str. 340.
[145] ŽŮREK, Jiří, 2018, op. cit., str. 107.

vlastních nebo externích sil, přijmutí dostatečných opatření pro zmírnění rizik a podobně.[146] Odpovědnost však na pověřence nepřechází a zůstává ležet na správci.

Pověřenec má tedy neustále monitorovat soulad zpracování s GDPR a dalšími relevantními předpisy, zvyšovat povědomí a pečovat o odbornou přípravu zaměstnanců a dalších pracovníků zapojených do činností zpracování a poskytování služeb. Může provádět školení, případně jednorázově upozornit na určitou změnu právní úpravy. WP29 pověřenci doporučuje sbírat informace o zpracování a identifikovat jednotlivé procesy, které má následně analyzovat a ověřovat jejich soulad, v neposlední řadě o všem informovat správce nebo zpracovatele.

Výše uvedené úkoly považujeme za základní činnosti pověřence, zároveň může vykonávat i jiné nesouvisející činnosti za předpokladu, že nejsou ve střetu zájmů. Plnění úkolů musí být prováděno s ohledem na rizika zpracování v kontextu povahy, rozsahu a účelů zpracování.[147] Pověřenec je nadán i řadou dalších úkolů za účelem kontroly, a to informováním, sledováním dodržování předpisů, spoluprací s dozorovým orgánem, prověřováním stížností a dalším.

Pro někoho tento institut může představovat byrokratickou zátěž, v praxi je však tento institut v podstatě nedocenitelný, neboť řeší a odpovídá na otázky a problémy v roli odborníka, tedy bez ohledu na jakékoliv přání či představy.[148]

Aby pověřenec mohl dostát řádnému plnění svých úkolů, „*správce a zpracovatel zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů*“.[149] Pověřenec tak dostává poměrně široká oprávnění, jež zahrnují seznámení se s vnitřním chodem organizace. Mimo informování o všech podstatných okolnostech má být pravidelně účasten na schůzích vysokého a středního managementu, týká-li se ochrany osobních údajů. Stanovisku pověřence musí být vždy věnována značná pozornost, pokud dojde k nějakému incidentu majícímu vliv

[146] Pokyn WP29 ze dne 13. 12. 2016 k pověřenci pro ochranu osobních údajů, WP 243, dostupné z https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/gdpr-dokumenty/2018/1/Preklad-Metodiky-poverence-WP29.pdf, str. 16-17.
[147] ŽŮREK, Jiří, 2018, op. cit., str. 116-117.
[148] GDPR v kostce: praktický průvodce povinnostmi pro podniky a spolky, 2018, str. 29.
[149] Čl. 38 odst. 1Obecného nařízení GDPR

na osobní data, je povinností pověřence o tom okamžitě informovat.[150] Pro řádné plnění své funkce mu musí být rovněž poskytnuty zdroje a podpora jeho dalšího vzdělávání.

Pověřenec je přímo podřízen vrcholovým pracovníkům správce či zpracovatele. Jeho role je do jisté míry značně nezávislá, neboť správce a zpracovatel má zajistit, že pověřenec nebude dostávat žádné pokyny týkající se plnění jeho úkolů. Tento zákaz se však nevztahuje na prostou komunikaci s pověřencem o jeho činnosti. V souvislosti s plněním své funkce nemůže být propuštěn ani jinak sankcionován. Ale ani zde to neplatí absolutně, pokud se pověřenec neosvědčí řádným plněním úkolů, nebo tvrzenou odborností, může dojít k jeho propuštění.[151]

[150] NEZMAR, Luděk, 2017, op. cit., str. 173.
[151] ŽŮREK, Jiří, 2018, op. cit., str. 117-119.

6. Zabezpečení osobních údajů

„Bezpečnost osobních údajů se v posledních letech stala v souvislosti s množícími se masivními úniky dat velkým tématem.“[152] Problémem zde nebyla jen nedostatečná úroveň zabezpečení, ale také zejména nedostatečná právní úprava, která nenutila správce v případě úniků k žádnému nahlašování, a to orgánům veřejné moci, ale ani dotčeným subjektům údajů. V důsledku této chybějící právní regulace docházelo k tomu, že se dotčené fyzické osoby o poruše zabezpečení dozvěděli až ex post a s výrazným zpožděním.

6.1. Z pohledu zákona č. 101/2000 Sb.

Výše uvedený nedostatek právní úpravy si můžeme demonstrovat i na naší vnitrostátní úpravě v zákoně o ochraně osobních údajů, který se povinnosti zabezpečení osobních údajů věnuje v § 13 odst. 1: *„Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.“*

Ochranná a bezpečnostní opatření musí být danému zpracování individualizovaná a přiměřená. Zákon tak neuvádí konkrétní prostředky ochrany a zabezpečení, ale stanovil pouze obecné vodítko, kterým by se správce měl řídit a vyhodnocovat rizika.[153] Nejvyšší správní soud v tomto směru apeluje alespoň na dodržování základních principů ochrany. Soud se ve svém rozsudku vyslovil, že při ochraně osobních údajů je zapotřebí automaticky aplikovat dnes již běžné standardy ochrany v tomto směru, a to tak, že bližší specifikace přímo v zákoně není podle něj nezbytností.[154] V praxi je tak soubor vyžadovaných opatření pro zabezpečení určován zejména prostředky a způsobem zpracování, které až na výjimky určuje správce.

[152] NULÍČEK, Michal, 2017, op. cit., str. 290
[153] MELOTÍKOVÁ, Petra. Ochrana osobních údajů v rámci veřejné správy. Praha: Leges, 2018, str. 105
[154] Rozsudek Nejvyššího správního soudu čj. As 21/2005-105 ze dne 10.5.2006

V následujícím odstavci pak už Zákon jen zmiňuje povinnost *„Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.“* Tato obecná formulace však nezakotvuje žádnou formu ani obsah požadovaného dokumentu.

V oblasti automatizovaného zpracování osobních údajů má správce nebo zpracovatel další stanovené povinnosti. Mezi tyto povinnosti patří zpracování údajů pouze oprávněnými osobami, přístup k takovým systémům mají mít opět pouze osoby na základě a v rozsahu jejich oprávnění. Pořizování elektronických záznamů je omezeno určením a ověřením, kdy, kým a za jakého důvodu byly osobní údaje zaznamenány, anebo jinak zpracovány. Dále má být zabráněno neoprávněnému přístupu k datovým nosičům, zde je zdůrazněna povinnost ochrany nejen pro samotné zpracování probíhající pomocí prostředků výpočetní techniky, ale rovněž individuálních datových nosičů, jež mohou obsahovat např. zálohové soubory.

Zákon se dále zabývá zaměstnanci nebo jinými osobami, které zpracovávají osobní údaje. Tyto osoby *„mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném“.*[155] Podmínkami můžeme rozumět především interní a organizační pokyny zaměstnavatele, které *„spočívají zejména ve stanovení vedoucích pracovníků a určení odpovědnosti konkrétních osob za jednotlivé kroky v rámci zpracování.“*[156] Rovněž sem můžeme řadit pokyny ohledně využití konkrétních prostředků a způsobu práce s nimi nebo konkrétní pokyny ohledně používání přístupových hesel, zamykání kanceláří apod.

S ochranou osobních údajů úzce souvisí problematika jejího technického zabezpečení. Na druhou stranu si však musíme uvědomit, že i v tomto ohledu zde důležitou roli hraje lidský faktor, který nelze podceňovat. I přes sebelepší technické zabezpečení může dojít k excesům spočívajícím v trestné činnosti zaměstnance nebo v zásahu vyšší moci. Tato rizika se však musí aktivní snahou eliminovat, a to řádným proškolováním, seznámením s vnitřními pokyny nebo adekvátním systémem kontrolní činnosti.[157]

[155] §14zákona č. 101/2000 Sb.
[156] MELOTÍKOVÁ, Petra, 2018, op. cit., str. 110
[157] MELOTÍKOVÁ, Petra, 2018, op. cit., str. 113

6.2. Z pohledu GDPR

Nařízení se proto rozhodlo na tento nedostatek reagovat a na zabezpečení klade daleko větší důraz, a to tím, že některá opatření přímo výslovně specifikuje, a dále v souladu se zásadou odpovědnosti musí být takto přijatá opatření prokazatelná. Dále je zavedena ohlašovací povinnost dozorovému úřadu a někdy i přímo dotčeným subjektům údajů. Tato povinnost však pro značnou skupinu správců není úplnou novinkou, neboť obdobná povinnost vyplývá ze zákona o kybernetické bezpečnosti nebo zákona o elektronických komunikacích.

Každý správce je povinen přijmout adekvátní bezpečnostní opatření, a to: *„s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.“*[158] Opatření mohou být jak technická, tak organizační, správce má být schopen vždy doložit splnění této povinnosti. Příkladem takového zabezpečení může být pseudonymizace nebo šifrování osobních údajů.

Dále také schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování. Tato skupina v sobě zahrnuje velkou množinu jednotlivých bezpečnostních opatření. Do skupiny opatření pro zajištění důvěrnosti přispívají již zmíněné psedonymizace nebo šifrování, rovněž zde však můžeme využít i různých metod autentizace a autorizace. Do kategorie opatření k zajištění integrity je potřeba zařadit konzistentnost, přesnost a důvěryhodnost osobních údajů, a to v celém průběhu zpracování, nejčastěji za použití monitorování přístupů konkrétních osob k osobním údajům. Zajištěním dostupnosti pak Obecné nařízení rozumí zejména to, aby v případě výpadku systému byly k dispozici záložní zdroje. Příkladem takového opatření může být rozprostření síťové služby a dat mezi větší počet serverů, a to s cílem snížit riziko nedostupnosti. Odolností systému pak rozumíme schopnost jednotlivých prvků zpracování zachovávat funkcionalitu a bezpečnost celku v případě excesu.[159] Dalším příkladem technicko-organizačních opatření je schopnost obnovit dostupnost osobních údajů, a to v případě fyzických i technických incidentů. Zabezpečení je

[158] Čl. 32 odst. 1 Obecného nařízení GDPR
[159] NULÍČEK, Michal, 2017, op. cit., str. 293 - 294

provázeno procesy pravidelného testování, posuzování a hodnocení účinnosti zavedených opatření.

Výše uvedené prvky jsou však nepovinné a rozhodně nejsou vyčerpávajícím popisem konkrétních opatření. Současně je nelze aplikovat na každé zpracování, minimálně ne bez ohledu na jeho specifika. *„Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.“*[160] Tuto povinnost známe již z úpravy v ZoOÚ, v praxi znamená povinnost pro správce a zpracovatele zavázat své zaměstnance a další dotčené osoby jasnými a jednoznačnými pokyny v rámci pracovní smlouvy nebo interního předpisu, jak s osobními údaji nakládat. Rovněž musí být zajištěna vhodnými instrumenty důvěryhodnost třetí strany, jež má k údajům přístup, např. správa IT systému.

Pokud dojde k jakémukoliv porušení zabezpečení osobních údajů, správce by to měl v ideálním případě od okamžiku, kdy se o něm dozví, do 72 hodin ohlásit dozorovému úřadu. Pokud není ohlášeno do 72 hodin, musí být současně uveden důvod zpoždění. Takové ohlášení musí obligatorně obsahovat popis porušení. Pokud je to možné, tak zároveň kategorie a přibližný počet dotčených subjektů a přibližné množství dotčených záznamů osobních údajů. Dále také jméno a kontaktní údaje pověřence nebo jiného kontaktního místa, jež smí poskytnout bližší informace. Ohlášení by mělo rovněž obsahovat popis pravděpodobných důsledků a popis opatření, která správce navrhl nebo přijal k vyřešení poruchy zabezpečení.

Další článek 34 Obecného nařízení je věnován případům, ve kterých je pravděpodobnost, že porušení zabezpečení bude mít za následek vysoké riziko pro subjekty údajů, v těchto případech by měl správce reagovat neprodleným oznámením dotčeným fyzickým osobám.

[160] Čl. 32 odst. 2 Obecného nařízení GDPR

7. Posouzení vlivu na ochranu osobních údajů a předchozí konzultace

Další novou povinností, které přináší pro správce Obecné nařízení, je povinnost provádět v některých případech tzv. posouzení vlivu na ochranu osobních údajů. *„Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.“*[161] Podle čl. 35 odst. 2 GDPR má správce povinnost vyžádat si posudek pověřence pro ochranu osobních údajů, samozřejmě za předpokladu, že byl jmenován. Výsledkem takového posouzení by měla být dokumentace, jež správci umožní přijmout opatření ke zmírnění očekávaných rizik.

V rámci obecného posouzení rizika je potřeba přihlédnout k povaze, rozsahu, kontextu a účelům zpracování a zhodnotit, jestli zpracování představuje vysokou pravděpodobnost rizika pro práva a svobody fyzických osob. Takové riziko pramení zejména z využívání nových technologií a v situacích, kdy je složitější uplatnění práv subjektů údajů.[162] Správce by při posuzování rizik měl zohlednit, zda jím zamýšlená operace neobsahuje některé faktory s vysokým rizikem, především: profilování subjektu údajů, automatizované rozhodování s právními nebo obdobnými účinky, systematické monitorování subjektu údajů, zpracování citlivých údajů, zpracování osobních údajů ve velkém rozsahu, kombinování osobních údajů z různých datových sad, zpracování osobních údajů týkající se zvlášť zranitelných osob, inovativní užití či aplikace technologických nebo organizačních řešení, předávání údajů mimo EU, bránění subjektům údajů v uplatňování svých práv v používání některé služby či v uzavření smlouvy. WP29 uvádí, že pokud správce vyhodnotí, že zamýšlená operace zpracování obsahuje minimálně dva z výše uvedených faktorů, měl by provést posouzení vlivu na ochranu osobních údajů.[163] Dozorový úřad může v souladu s čl. 34 odst. 4 sestavit seznam a zveřejnit druhy operací zpracování, jež budou podléhat posouzení vlivu.

[161] Čl. 35 odst. 1 Obecného nařízení GDPR
[162] Recitál 91 Obecného nařízení GDPR
[163] Výkladový pokyn WP29 ze dne 4.4.2016 k posouzení vlivu na ochranu osobních údajů (DPIA) a určování, zda je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro potřeby nařízení 2016/679, WP 248, dostupné z https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, str. 7-9

Posouzení vlivu na ochranu osobních údajů je povinné zejména v následujících případech: *„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; rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10 nebo rozsáhlé systematické monitorování veřejně přístupných prostorů.“*[164]

Samotné posouzení vlivu je komplexní proces, který musí obsahovat alespoň systematický popis zamýšlených operací, posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů, posouzení rizik pro práva a svobody subjektu údajů a také plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů.[165]

Obecné nařízení výslovně nestanoví, zda se povinnost posouzení vlivu vztahuje pro zpracování započatá až po účinnosti tohoto nařízení, nebo zdali je potřeba dodatečné posouzení pro zpracování již započatá. WP29 však v tomto ohledu zastává názor, že se tato povinnost vztahuje až na zpracování započatá po účinnosti Obecného nařízení, zároveň však důrazně správcům doporučuje, aby posouzení aplikovali i na již započatá zpracování. Bez ohledu na počátek zpracování má správce minimálně povinnost, v případě, kdy dojde ke změně rizika, provést přezkum, zda je zpracování stále v souladu s předchozím posouzením, nebo je potřeba jeho aktualizace. WP29 proto doporučuje správci provádět pravidelnou revizi minimálně každé tři roky.[166]

Pro případy zpracování, které by mohlo mít za následek velké riziko v případě neprovedení potřebných opatření, může správce tyto činnosti konzultovat s dozorovým úřadem. Pokud se úřad domnívá, že by zamýšlené zpracování porušovalo Obecné nařízení, upozorní správce, a to ve lhůtě osmi týdnů od obdržení žádosti správce o konzultaci. Správce při konzultaci poskytuje dozorovému úřadu

[164] Čl. 35, odst. 3Obecného nařízení GDPR
[165] Čl. 35, odst. 7Obecného nařízení GDPR
[166] Výkladový pokyn WP29 ze dne 4. 4. 2016 k posouzení vlivu na ochranu osobních údajů (DPIA) a určování, zda je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro potřeby nařízení 2016/679, WP 248, dostupné z https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, str. 11

náležitou součinnost, zejména informace o rozdělení odpovědnosti správce a zpracovatelů, účelech a způsobech zpracování, opatřeních a zárukách, kontaktních údajích případného pověřence, posouzení vlivu a veškerých dalších informací, o něž dozorový úřad požádá. Případy zpracování, které se týkají veřejného zájmu, sociální ochrany nebo veřejného zdraví podléhají nejen povinné konzultaci, ale taktéž povinnosti předchozího povolení dozorového úřadu. Další situace, jež povinně podléhají konzultaci, jsou návrhy legislativních opatření. V těchto případech však dozorový úřad nemá pravomoc autoritativně zasahovat do legislativního procesu státu a o přijetí legislativního opatření bude ve finále rozhodovat parlament.[167]

[167] Čl. 36 Obecného nařízení GDPR

8. Dozorová činnost

Kontrolní a dozorčí činnosti veřejné správy se rozdělují především na ty, které jsou vykonávány vůči nepodřízeným adresátům, a na ty, jež jsou prováděny v rámci interní činnosti veřejné správy vůči jí podřízeným adresátům, a řadíme k nim zejména správní dozor, instanční dozor, služební dozor, dozor nad veřejnoprávními korporacemi, finanční kontrolu nebo přezkoumávání hospodaření územních samosprávných celků a dobrovolných obcí.[168]

Správní dozor je vrchnostenská činnost, kdy vykonavatel veřejné správy, v tomto případě dozorčí orgán, sleduje chování nepodřízených adresátů a porovnává je se stavem žádoucím a s požadavky právních norem. Tento institut probíhá v rámci vnějších vztahů veřejné správy, tedy vůči subjektům občanské společnosti mimo rámec vnitřních vztahů ve veřejné správě. Dozorčím orgánem je vykonavatel veřejné správy, kterému zákon svěřuje takovou působnost.[169] *„Při výkonu správního dozoru se hodnotí soulad dozorované činnosti nebo stavu s právem, ne tedy s jinými kritérii, jako např. vhodnost, efektivnost prováděných činností.“*[170] Povinnosti provedení výkonu správního dozoru mohou vyplývat ze zákona či jiného právního předpisu, z opatření obecné povahy, ze správního aktu, z veřejnoprávní smlouvy.

Správní dozor je rozdělen do dvou základních fází. První fází je fáze zajišťovací a hodnocení, jejím cílem je zjištění skutkového stavu a jeho porovnávání se stavem žádoucím. Jeho poznatky jsou zaznamenávány do kontrolního protokolu. Druhou fází správního dozoru je fáze nápravná, kdy po shledání negativních odchylek přichází náprava charakteru správního řízení a udělení nápravných opatření a udělení případných sankcí. Dozor je vykonáván různými způsoby, a to jako dozor průběžný, následný nebo předběžný. Druhé hledisko dělení dozoru je podle délky jeho trvání, a to na dozor soustavný a jednorázový. Soustavný je vykonán zejména vůči předem stanovenému okruhu subjektu údajů, naproti tomu dozor jednorázový může vyplývat z úkolu založeného na úředním podnětu nebo stížnosti zvenčí. Za zvláštní druhy správního dozoru můžeme považovat dozor technický, vrchní nebo pořádkový.

---

[168] KOPECKÝ, Martin. *Správní právo: obecná část*. V Praze: C.H. Beck, 2019. Beckovy právnické učebnice, str. 203
[169] HENDRYCH, Dušan. Správní právo: obecná část. 9. vydání. V Praze: C.H. Beck, 2016. Academia iuris (C.H. Beck), str. 201
[170] KOPECKÝ, Martin, 2019, op. cit., str. 204

Správní dozor je relativně samostatná správní činnost, jež není součástí jiných institutů správního práva, a jeho základní postupy a pravidla kontrolní činnosti se řídí zákonem č. 255/2012 Sb., o kontrole. Některé typy kontrol, např. daňová kontrola, celní dozor, mohou mít svou vlastní zvláštní právní úpravu, zde se potom kontrolní řád použije pouze subsidiárně.[171] *„V našem současném správním právu je správní dozor koncipován jako věcně specializovaný, zaměřený na určitý úsek ochrany veřejného zájmu.“*[172] Výkon správního dozoru je prováděn pomocí dozorčích orgánů, jimiž jsou buď orgány veřejné správy, kterým přímo zákon svěřuje výkon dozorčí činnosti, nebo na straně druhé soukromé fyzické nebo právnické osoby, na něž stát deleguje pravomoci.

8.1. Úřad pro ochranu osobních údajů

Úřad byl zřízen 1. června 2000 jako nezávislý správní orgán v oblasti ochrany osobních údajů, který ve své činnosti postupuje pouze v souladu se zákony a jinými právními předpisy.[173] Jeho činnost je vymezena zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. „*Úřad je ústředním správním úřadem pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem, zvláštními právními předpisy, mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropské unie.“*[174]

Správní úřad je chápán jako zákonem stanovený okruh záležitostí, jež jsou přiřazeny organizační jednotce. Legální vymezení termínu správní orgán obsahuje § 1 odst. 1 zákona č. 500/2004 Sb., správní řád: *„Tento zákon upravuje postup orgánů moci výkonné, orgánů územních samosprávných celků a jiných orgánů, právnických a fyzických osob, pokud vykonávají působnost v oblasti veřejné správy.“* Správní úřad je*de lege lata* v souladu s Ústavou, tedy jako státní orgán institucionální součásti moci výkonné, kdy Ústava výslovně rozlišuje: „*Ministerstva a jiné správní úřady lze zřídit a jejich působnost stanovit pouze zákonem.“*[175] Aby tedy instituce mohla existovat jako správní úřad, musí za něj být označena a tím pádem zařazena do moci výkonné a podřízena vládě.

---

[171] HORZINKOVÁ, Eva a Zdeněk FIALA. Správní právo hmotné: obecná část. 2., aktualizované vydání. Praha: Leges, 2015. Student (Leges), str.122
[172] HENDRYCH, Dušan, 2016, op. cit., str. 203
[173] Historie Úřadu pro ochranu osobních údajů, dostupné z www.uoou.cz/historie-uradu-pro-ochranu-osobnich-udaju/ds-1061/archiv=0&p1=1059
[174] § 2 odst. 2 zákona č. 101/2000 Sb.
[175] Čl. 79 odst. 1 ústavního zákona č. 1/1993 Sb., Ústava České republiky

Nezávislost správního orgánu je chápána jako vrchnostenská regulace určitého sektoru, přičemž je nezávislý na vrcholném orgánu a tvůrci politiky, tedy vládě. Jedná se o státní úřady, které stojí mimo organizační soustavu státní správy řízené vládou. Regulace není primárně založena je jednorázových či nesouvisejících rozhodnutí, ale jedná se o soustavnou činnost, pro niž je stěžejní její konzistentnost. Nezávislý orgán má řešit problém politické nejistoty a prohlubovat prvky kontinuity. Tyto orgány se vyznačují relativně úzce vymezeným okruhem společenských vztahů, který vyžaduje vysoce odborné znalosti. Mezi pojmové znaky tak můžeme řadit specializovanou věcnou působnost, jež je úzce vymezená, a expertnost jejich členů.[176] Otázka ústavní opory zřízených na vládě nezávislých správních orgánů vyvstává zejména s ohledem na ustanovení § 21 kompetenčního zákona: *„Ministerstva se ve veškeré své činnosti řídí ústavními a ostatními zákony a usneseními vlády.“*[177] Odpověď je však poměrně snadná, neboť takové nezávislé správní úřady jsou zřízeny zákonnými úpravami, které jsou ve vztahu ke kompetenčnímu zákonu úpravou pozdější, a zjevně také zákony zvláštními, problém zde tedy vyřešíme pomocí standardních aplikačních pravidel. Mezi nezávislé správní úřady řadíme Radu pro rozhlasové a televizní vysílání, Úřad pro ochranu osobních údajů, Úřad pro ochranu hospodářské soutěže, Český statistický úřad, Energetický regulační úřad, Český telekomunikační úřad.

Vymezení působnosti úřadu nalezneme v § 2 odst. 3 ZoOÚ: *„Úřad vykonává působnost dozorového úřadu pro oblast ochrany osobních údajů vyplývající z mezinárodních smluv, které jsou součástí právního řádu.“* A dále v § 29 zákona č. 101/2000 Sb. V některých zvláštních agendách je jeho působnost vymezena ve zvláštních předpisech, jako např. výkon správních činností z procesního hlediska je ovládán zákonem č. 500/2004 Sb., správní řád. Výkon dozorové činnosti je řízen zákonem č. 255/2012 Sb., o kontrole, spravování informačních systémů spadá pod působnost zákona č. 365/2000Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, poskytování informací se vztahuje k působnosti podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a mnoho dalších.[178]

[176] Pouperová Olga, Nezávislé správní úřady, dostupné z www.mvcr.cz/clanek/nezavisle-spravni-urady.aspx
[177] § 21 zákona č. 2/1969 Sb., zákon České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky (kompetenční zákon)
[178] Působnost Úřadu, dostupné z www.uoou.cz/pusobnost-uradu/ds-1269/archiv=0&p1=1059

Úřad primárně provádí dozor nad dodržováním povinností stanovených pro zpracování osobních údajů, vede registr zpracování osobních údajů, přijímá podněty a stížnosti na porušení povinnosti, zpracovává a zpřístupňuje výroční zprávu o své činnosti, projednává přestupky a ukládá případné sankce. Jako nezávislý orgán zajišťuje plnění požadavků plynoucích z mezinárodních smluv a přímo použitelných předpisů EU. Do působnosti úřadu spadá mezinárodní spolupráce s obdobnými úřady jiných států, orgány EU a jiných mezinárodních organizací. V neposlední řadě poskytuje konzultace v oblasti ochrany osobních údajů.[179]

Pro řádný výkon *„Ministerstvo vnitra nebo Policie České republiky poskytuje Úřadu pro výkon působnosti stanovené tímto zákonem a dalšími právními předpisy referenční údaje ze základního registru obyvatel, údaje z agendového informačního systému evidence obyvatel, údaje z agendového informačního systému cizinců“*.[180] Z poskytnutých údajů však lze v konkrétním případě použít vždy jen ty nezbytné ke splnění daného úkolu.

V čele úřadu stojí předseda a jeho zaměstnanci jsou inspektoři, kteří provádí kontrolní činnost, a další pověření zaměstnanci. Předseda je jmenován prezidentem republiky, a to na pětileté období maximálně dvakrát po sobě. Předseda je považován za služební orgán, jenž je oprávněn vydávat příkazy státním zaměstnancům podle zákona o státní službě. Inspektoři jsou taktéž jmenováni prezidentem republiky na desetileté období, které může být opakované. Inspektor řídí samotnou kontrolu a provádí další úkony spadající do působnosti úřadu.[181]

8.1.1. Činnost

První významnou činností úřadu je vedení registru zpracování osobních údajů, kde se uvádí informace o správci a datu jeho provedení, případně zrušení. Dalším výsledkem činnosti úřadu je každoroční výroční zpráva o provedené kontrolní činnosti a jejím zhodnocení. Tato zpráva je předkládána předsedovi Úřadu pro informaci, Poslanecké sněmovně a Senátu Parlamentu České republiky, a to do dvou měsíců po skončení rozpočtového roku.

[179] § 29 zákona č. 101/2000 Sb.
[180] § 29a zákona č. 101/2000 Sb.
[181] hlava V. zákona č. 101/2000 Sb.

Úřad, jak už bylo řečeno, je kontrolním orgánem a má právo seznámit se všemi nezbytnými informacemi pro dosažení účelu kontroly. Kontrolující je povinen se prokázat průkazem, jeho forma je stanovena nařízením vlády. Kontrolní činnost je vykonána na základě kontrolního plánu.

Dojde-li k porušení uložené povinnosti, je v kompetenci inspektora uložit opatření k odstranění zjištěných nedostatků. Pokud jsou tyto nedostatky odstraněny bezprostředně po upozornění, lze upustit od uložení pokuty.[182]

8.2. Dozorové úřady

Součástí ochrany osobních údajů při jejich zpracování jsou dozorové úřady jednotlivých členských států, jimž jsou svěřeny úkoly a pravomoci. Jeho definiční vymezení nalezneme již v úvodním článku 4, bodě 21, který dozorovým úřadem rozumí *„nezávislý orgán veřejné moci zřízený členským státem podle článku 51“*.

„Každý členský stát stanoví, že jeden nebo více nezávislých orgánů veřejné moci jsou pověřeny monitorováním uplatňování Obecného nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie.“[183] Každý úřad přispívá k jednotnému uplatňování GDPR, a to za přispění spolupráce jednotlivých úřadů a Komise. Podmínkou úřadu je jeho nezávislost na vnějších vlivech přímých či nepřímých. Členové dozorového úřadu se musí zdržet jakéhokoli jednání neslučitelného s jejich funkcí, což spočívá v zákazu jiné výdělečné i nevýdělečné pracovní činnosti v průběhu svého funkčního období. Každý členský stát má zajistit, aby každý dozorový úřad byl vybaven lidskými, technickými a finančními zdroji, prostorami a infrastrukturou, jež budou potřeba pro splnění úkolů a výkon pravomocí.

Obecná příslušnost dozorového úřadu k plnění úkolů a svěřených pravomocí je na území svého státu. Tyto úřady nejsou příslušné ke zpracování operací prováděných soudy v rámci svých soudních pravomocí.[184]

[182] hlava VI. zákona č. 101/2000 Sb.
[183] Čl. 51 odst. 1 Obecného nařízení GDPR
[184] Čl. 55 Obecného nařízení GDPR

Roli dozorového úřadu na našem území vykonává Úřad pro ochranu osobních údajů, který dosud působí v původním postavení, a to do doby přijetí adaptačního zákona, jenž by měl zakotvit nový status a organizaci.

8.2.1. Úkoly

Výčet jednotlivých úkolů dozorového úřadu nám poměrně obsáhle stanovuje čl. 57 odst. 1 Obecného nařízení. Mezi povinnosti každého dozorového úřadu patří monitorování a vymáhání obecného nařízení, jeho úkolem je zvyšování povědomí širší veřejnosti o všech nástrahách, rizicích, právech a povinnostech. Úřad rovněž vystupuje v roli poradce parlamentu, správcům a zpracovatelům, jakož i v roli plnění informační povinnosti vůči subjektům údajů, kteří o to požádají.

Úřadu náleží rozhodování o stížnostech subjektů, dále má za cíl zajistit jednotné uplatňování a prosazování tohoto nařízení, stejně tak jako prověřovat pomocí šetření jeho uplatňování. Do kompetence úřadu náleží monitorování vývoje v relevantních oblastech, přijímání standardních smluvních doložek a mnoho dalšího.

Provádění úkolů úřadu je pro subjekty údajů a pověřence bezplatné, pouze ve výjimečných situacích lze uložit přiměřený poplatek, a to např. v situacích zjevně nedůvodných, nepřiměřených nebo opakujících se požadavků.

8.2.2. Pravomoc

Pravomoci k plnění jednotlivých úkolů rozděluje nařízení do tří skupin: vyšetřovací, nápravná, povolovací a poradní. Tyto pravomoci musí úřad vhodně využívat, a to i jejich kombinace.

Do skupiny vyšetřovacích pravomocí řadíme pravomoc nařídit správci a zpracovateli poskytnutí všech potřebných informací, provedení vyšetřování pomocí auditů, přezkum osvědčení. Jako další sem řadíme ohlášení porušení nařízení příslušnému správci či zpracovateli, vyžádání si přístupu ke všem osobním údajům potřebným k výkonu svěřených úkolů, stejně tak jako přístup do prostor těchto osob.[185]

[185] Čl. 58 odst. 1 Obecného nařízení GDPR

Nápravné pravomoci vypovídají o své funkci již v samotném názvu. Patří sem upozornění nebo napomenutí správce či zpracovatele o porušení Obecného nařízení, dále také nařízení správci a zpracovateli uvedení operací do souladu s GDPR a oznámení subjektům údajů o případném porušení zabezpečení osobních údajů.

Dozorový úřad může uložit dočasné nebo trvalé omezení zpracování, nařídit opravu či výmaz osobních údajů. Úřad může taktéž odebrat osvědčení, uložit správní pokutu či přerušit tok údajů příjemci ve třetí zemi.[186]

Do poslední skupiny povolovacích a poradních pravomocí spadá pravomoc poskytování poradenství správci, vydávání stanovisek a schvalování návrhů kodexů chování. Dále sem řadíme vydávání osvědčení, přijímání standardních doložek, povolování smluvních doložek a správních ujednání či schválení závazných podnikových pravidel.[187]

8.2.3. Spolupráce a jednotnost

Spolupráce dozorových úřadů je předpokládána z důvodu efektivnějšího uplatňování Obecného nařízení, a to především pomocí poskytování relevantních informací, žádostí o informace a opatření v oblasti dozoru.

Každý dozorový úřad se může v rámci spolupráce obrátit s jakoukoliv žádostí na jiný dozorový úřad. Dožádaný orgán je povinen ve lhůtě jednoho měsíce přijmout vhodná opatření týkající se obdržené žádosti. Úřad nesmí žádost odmítnout, ledaže by k projednání byl nepříslušný. Dožádaný orgán má informační povinnost k žádajícímu orgánu ohledně výsledků, pokroku, opatřeních, kterých bylo ve věci dosaženo, případně sdělení důvodů, proč nebylo žádosti vyhověno.[188]

V nařízení je zakotvena možnost přímé společné spolupráce dozorových úřadů, zejména týká-li se to správce či zpracovatele, jenž má své provozovny v několika členských zemích. Další možností je pravděpodobnost, že provedenými operacemi bude dotčen značný počet subjektů údajů ve více členských státech, potom má každý dotčený úřad právo účasti na společných postupech. Dozorový úřad může své pravomoci svěřit členům či pracovníkům vysílajícího dozorového orgánu.

[186] Čl. 58 odst. 2 Obecného nařízení GDPR
[187] Čl. 58 odst. 3 Obecného nařízení GDPR
[188] Čl. 61 Obecného nařízení GDPR

Tento institut najde své opodstatnění hlavně při plnění úkolů a uplatňování pravomocí ze strany tzv. vedoucího dozorového úřadu.

Vedoucí dozorový úřad má smysl v přeshraničním zpracování osobních údajů, a to, aby byly vůči správci nebo zpracovateli efektivně využity pravomoci jednoho dozorového úřadu a došlo k efektivnímu postihnutí za přeshraniční zpracování pouze jedním dozorovým úřadem. Do působnosti tohoto institutu nespadají místní zpracovávané údaje, jakými jsou např. vedení personální agendy nebo kamerový systém.[189] Pro určení takového úřadu je podstatné místo hlavní provozovny.

Mechanismus jednotnosti je Obecným nařízením ustanoven z důvodu hrozby odlišného výkladu některých institutů či povinností v jednotlivých členských státech. Tento mechanismus spočívá ve vzájemné spolupráci dozorových úřadů, Evropské komise a Sboru, který má dbát na jednotnou aplikaci nařízení bez nezdůvodněných rozdílů.[190]

Aby se mohlo předejít odlišným opatřením, je v působnosti Sboru vydávání stanovisek, a to ve lhůtě osmi týdnů, jež lze případně prodloužit o dalších šest týdnů. Dozorový úřad má následně stanovisko v co největší míře zohlednit a do dvou týdnů sdělit Sboru, zda svůj postoj zachová, nebo naopak změní. Díky snaze o zachování co největší míry jednotnosti disponuje Sbor nadáním řešit spory mezi jednotlivými dozorovými úřady. Jednotnost je dotvářena postupem pro naléhavé případy, kdy se dozorový úřad může odchýlit od jednotného výkladu a přijmout předběžná opatření.[191]

[189] ŽŮREK, Jiří, 2018, op. cit., str. 179 - 180.
[190] Čl. 63Obecného nařízení GDPR
[191] Čl. 64Obecného nařízení GDPR

9. Předávání informací a mezinárodní spolupráce

Nezbytnost tohoto institutu vyplývá z rozvoje mezinárodního obchodu a mezinárodní spolupráce, kdy jsou toky informací do zemí mimo Evropskou unii a mezinárodních organizací nezbytné. V budoucnu je plánován vznik seznamů tzv. bezpečných zemí, kde jejich úroveň bude odpovídat běžným standardům v EU. V praxi by to pak znamenalo možnost předávání informací bez jakéhokoliv povolení.[192]

9.1. Podle zákona č. 101/2000 Sb.

Právní rámec předávání osobních údajů nalezneme zakotvený v § 27 zákona č. 101/2000 Sb., jehož odst. 1 zní: „*Volný pohyb osobních údajů nemůže být omezován, pokud jsou údaje předány do členského státu Evropské unie.“* K předání údajů do třetích zemí může dojít na základě ratifikované mezinárodní smlouvy nebo rozhodnutí orgánu Evropské unie. Tato rozhodnutí najdeme ve věstníku Úřadu pro ochranu osobních údajů.[193]

Odst. 3 téhož paragrafu stanoví výjimku z výše stanovených základních pravidel. Předání údajů tak může proběhnout, pokud správce prokáže souhlas nebo přímo pokyn subjektu údajů. Dále pokud prokáže ve třetích zemí existenci dostatečného ochranného aparátu a záruk prostřednictvím právních, profesních nebo bezpečnostních předpisů. Tyto záruky jsou často upřesněny smlouvou mezi správce a příjemcem. Dalším případem je situace, kdy se jedná o údaje, které jsou podle zvláštního zákona součástí veřejně přístupného datového souboru, nebo alespoň přístupnému každému, kdo prokáže právní zájem. Základní pravidla jsou taktéž prolomena, jedná-li správce v naléhavém veřejném zájmu či pro ochranu životně důležitých zájmů fyzické osoby, a to pro záchranu života nebo poskytnutí zdravotních služeb. Platí i v případě, je-li předání nezbytné pro jednání o uzavření smlouvy či její změny, a to z podnětu samotného subjektu údajů nebo jejího plnění.

Před takovým postupem předání do zemí třetího světa podle odst. 3 je správce povinen podat Úřadu pro ochranu osobních údajů žádost o povolení k předání. Úřad má posoudit žádost ze všech možných okolností a jemu dostupných informací.

[192] NAVRÁTIL, Jiří, 2018, op. cit., str. 84.
[193] § 27, odst. 2 zákona č. 101/2000 Sb.

V povolení Úřad zpravidla uvádí zejména dobu, po kterou může správce předání provádět. Pokud však dojde ke změně podmínek, za kterých bylo povolení vydáno, především na základě rozhodnutí orgánu EU, Úřad takové povolení změní, případně zruší.

9.2. Podle GDPR

Současná právní úprava v zákoně č. 101/2000 Sb. se této problematice věnuje pouze v jediném paragrafu. Nově účinná úprava v podobě nařízení tento institut náležitě rozšířila, a to zejména co se týká oblasti předávání osobních údajů do třetích zemí nebo mezinárodních organizací.

Předávání osobních údajů do jiných zemí může představovat značné riziko pro subjekty údajů, neboť musíme brát zřetel, že míra právní ochrany bude často hodně různorodá. Samostatná dílčí úprava má tak za hlavní cíl zajistit předávaným údajům co nejvyšší úroveň možné ochrany. Forma předání může být různorodá, za předávání nepovažujeme pouze fyzické předání od jednoho subjektu ke druhému, ale i jejich zpřístupnění na dálku, např. přes internet.

Mezinárodní spolupráce v zájmu ochrany osobních údajů spočívá v rozvoji mechanismů pro snadné a účinné prosazování předpisů na ochranu osobních údajů, v poskytování vzájemné pomoci na mezinárodní úrovni. Řadíme sem i zapojení zúčastněných stran do diskusí o prohlubování mezinárodní spolupráce a podpoře výměny a dokumentace v souvislosti s právními předpisy a praxí v oblasti ochrany osobních údajů.[194]

9.2.1. Předávání v rámci Evropské unie

Již z čl. 1 odst. 3 Obecného nařízení nám vyplývá neomezenost pohybu osobních údajů, a to z důvodu ochrany fyzických osob. Možnost takového předávání je založena na institucionálním zabezpečení, což je vyjádřeno stejně vysokým standardem právního rámce zabezpečení ochrany osobních v údajů napříč celou EU.[195] K samotnému předání však platí povinnost správce prokázat právní důvod, stejně jako tomu je i v jiných případech.

[194] Čl. 50 Obecného nařízení GDPR
[195] NEZMAR, Luděk, 2017, op. cit., str. 42.

Obdobný režim se uplatňuje v rámci Evropského hospodářského prostoru i pro nečlenské státy, konkrétně pro Norsko, Island a Lichtenštejnsko.[196]

9.2.2. Předávání mimo Evropskou unii

Složitost předávání do mimoevropských zemích bude podstatně ovládána tím, o jaký stát se jedná, a to zejména z pohledu institucionální zajištění úrovně ochrany osobních údajů. Obecné nařízení podstatně upravuje tento institut a definuje následující možnosti předávání: *„předání založené na rozhodnutí o odpovídající ochraně, předání založené na vhodných zárukách, závazná podniková pravidla, standardní smluvní doložky, výjimky pro specifické situace, kdy nelze aplikovat jeden ze tří shora uvedených bodů“.*[197]

V čl. 45 Obecného nařízení máme upravený režim předávání založený na rozhodnutí o odpovídající ochraně. Rozhodnutí Evropské komise tak může způsobit uplatnění obdobného režimu jako v rámci EU, neboť je osvědčena jejich odpovídající úroveň ochrany. Výčet takovýchto států nalezneme ve Věstníku EU, který v současné době zahrnuje tyto země: Andora, Argentina, Faerské ostrovy, Guernsey, Izrael, Jersey, Kanada, Nový Zéland, Ostrov Man, Švýcarsko, Uruguay.

Spojené státy americké, ačkoliv jsou taktéž zahrnuty do seznamu Evropské komise, zaujímají specifické postavení. Jejich postavení se neuplatňuje v rámci území jako takového, ale záleží na účastenství v tzv. Štítu soukromí. USA, jak už bylo v úvodních kapitolách zmíněno, jsou nadány odlišnou filozofií v oblasti ochrany osobních údajů a nelze je tak považovat za zemi odpovídající úrovní ochrany. Štít soukromí je tak nástroj vytvořený Evropskou komisí v rámci nezbytnosti spolupráce mezi Evropskou unií a USA.

Druhým režimem máme předání založené na vhodných zárukách poskytnutých příjímacím subjektem a za podmínky vymahatelnosti práv subjektu údajů. Vhodné záruky mohou být stanoveny pomocí právně závazného a vykonatelného nástroje mezi orgány veřejné moci nebo veřejnými subjekty, stanovením závazných vnitropodnikových pravidel, standardních smluvních doložek přijatých dozorovým úřadem a následně Evropskou komisí. Za další záruky považujeme schválené kodexy chování či mechanismy pro vydávání osvědčení. Nad rámec shora

[196] ŽŮREK, Jiří, 2018, op. cit., str. 152.
[197] NEZMAR, Luděk, 2017, op. cit., str. 43.

uvedených nástrojů můžeme za záruku za splnění podmínky povolení dozorového úřadu považovat smluvní doložky mezi správcem a zpracovatelem nebo vložená ustanovení do správních ujednání mezi orgány veřejné moci a veřejnými subjekty.[198] Smluvní doložka je instrumentem, jenž obsahuje standardizovaný text, kterým se příjemce osobních údajů zavazuje k dodržování odpovídajících pravidel platných v Evropské unii.

Závazná podniková pravidla jsou koncepcí ochrany osobních údajů, jež jsou interními pravidly správců. Jedná se o činnost *„správce nebo zpracovatele usazeného na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost.“*[199]

Pokud předání osobních údajů nelze zařadit pod žádnou z výše uvedených možností, máme zde velmi obsáhlý čl. 49, jenž se zabývá právě specifickými situacemi a podle kterého se předání může uskutečnit za splnění alespoň jedné podmínky uvedené v odst. 1 Obecného nařízení. Subjekt údajů je informován o rizicích a k takovému předání dal výslovný souhlas, předání je nezbytné pro splnění smlouvy, existuje-li veřejný zájem nebo je nezbytné pro určení, výkon nebo obhajobu právních nároků. Dalšími podmínkami je ochrana životně důležitých zájmů subjektu údajů nebo jiných osob, anebo pokud k předání dochází z rejstříku, jenž je určen a zpřístupněn pro informování veřejnosti nebo jakékoliv osobě, která prokáže oprávněný zájem.

Článek 48 GDPR se věnuje i situacím, kdy by byl správce nucen k předání či zpřístupnění údajů, přičemž by nemělo dostatečnou oporu plynoucí z mezinárodních závazků. V takovém případě je proces předání osobních údajů správcem nebo zpracovatelem zakázán.

[198] Čl. 46 Obecného nařízení GDPR
[199] ŽŮREK, Jiří, 2018, op. cit., str. 43.

10. Správní tresty

Součástí každé právní úpravy bývá vyhrazená část správním trestům a sankcím, která má mít vůči adresátům preventivní a donucující účinek. Za správní delikt považujeme protiprávní jednání odpovědné osoby, jehož znaky jsou uvedeny v zákoně a zákon s ním spojuje hrozbu trestu a sankce. Za jeho pojmové znaky můžeme označit protiprávnost, škodlivost, znaky skutkové podstaty, trestnost a zákonné zmocnění k uplatnění odpovědnosti v rámci veřejné správy.[200] V současné době ve správním právu rozlišujeme správní delikty na přestupky, správní disciplinární delikty a tzv. pořádkové správní delikty.

Pro účely této práce si však vystačíme pouze s přestupkem, který k datu 1. 7. 2017 zaznamenal svou rozsáhlou úpravu. *„Přestupky představují jediný ze správních deliktů, o němž lze říci, že jeho úprava je v určitém rozsahu kodifikována.“*[201] Jeho definice je v § 5 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, a zní: *„Přestupkem je společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.“* Skutkové podstaty jednotlivých přestupků jsou obsaženy ve zvláštních zákonech, kdy některé připouští i dílčí odchylky od obecné úpravy, pro procesní ustanovení však platí subsidiární použití správního řádu.

Sankce je právním následkem přestupku, jež může být uložena na základě zákona pachateli za jím spáchaný přestupek. Ze základní zásady *nulla poena sine lege* plyne požadavek zákonné formy, druhu, výše, podmínek a způsobu ukládání, jakož i hlediska pro výměry sankce v každém jednotlivém případě. Systém sankcí musí odpovídat společenské škodlivosti a závažnosti přestupku, a to, aby sankce byla efektivní a naplnila svůj účel.[202] *„Za přestupek lze uložit správní trest napomenutí, pokuty, zákazu činnosti, propadnutí věci nebo náhradní hodnoty, zveřejnění rozhodnutí o přestupku.“*[203]

[200] MATES, Pavel. *Základy správního práva trestního*. 7., přepracované vydání. V Praze: C.H. Beck, 2017, str. 33.
[201] MATES, Pavel, 2017, op. cit., str. 53.
[202] HENDRYCH, Dušan. Správní právo: obecná část. 9. vydání. V Praze: C.H. Beck, 2016. Academia iuris (C.H. Beck), str. 306
[203] § 35 zákon č. 250/2016 Sb.

Nejčastěji ukládanými tresty jsou především napomenutí a pokuty. Napomenutí je pro svou povahu nejmírnější správní trest, který lze uložit za jakýkoliv přestupek, a to i spolu s jiným trestem, pokud to není vyloučeno. Svým charakterem je určen pro méně závažné přestupky a jedná se o prostředek morálního donucení, jenž má působit zejména výchovně a zahrnovat upozornění pachatele na důsledky protiprávního jednání, které by hrozilo v případě dalšího obdobného jednání v budoucnu.[204] *„Pokuta je nejtypičtějším a nejvíce frekventovaným správním trestem v celé oblasti přestupkového práva a lze ji uložit za každý přestupek.“*[205] Obecná hranice je 1000 Kč, pokud zvláštní zákon nestanoví jinak.[206] Toto ustanovení lze chápat jako pojistku v případě, že by stanovení výše bylo opomenuto. Zákonodárce má však spíše trvalou tendenci ke zvyšování hranic pokut a mnohdy nečiní ani rozdíl, zda je pachatelem fyzická nebo právnická osoba. Při ukládání pokut je ale potřeba brát ohled na jejich reálnost vymáhání. Hranice stanovené pokuty by měla odpovídat osobním a majetkovým poměrům dotčené osoby, její hospodářské situaci a v neposlední řadě závažnosti správního deliktu.

Rozhodování a řízení o přestupcích je v působnosti správního orgánu, v tomto případě Úřadu, který rovněž vybírá pokuty. Uložené pokuty nejsou příjmy Úřadu, je pověřen jen jejich vybíráním, ale jsou příjmem státního rozpočtu. Pokud není pravomocně uložená pokuta uhrazena dobrovolně, předává Úřad pokutu k vymáhání celnímu úřadu.[207]

10.1. Podle zákona č. 101/2000 Sb.

Hlava VII zákona o ochraně osobních údajů je věnována přestupkům. Zákon upravuje pouze jednotlivé skutkové podstaty přestupků, proto je potřeba současně posuzovat jednání fyzické osoby podle obecné právní úpravy zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, které mimo jiné upravují otázky zavinění, okolností vylučujících protiprávnost, obecná ustanovení o sankcích. Zákon rozlišuje skutkové podstaty přestupků do dvou skupin přestupků podle subjektů, jež se jich dopustily, tedy na přestupky fyzických a právnických osob.

[204] MATES, Pavel, 2017, op. cit., str. 113.
[205] MATES, Pavel, 2017, op. cit., str. 114.
[206] § 46, odst. 1 zákon č. 250/2016 Sb.
[207] Porušení povinností při zpracování osobních údajů, dostupné z www.uoou.cz/poruseni-povinnosti-pri-zpracovani-osobnich-udaju/ds-1487/archiv=0&p1=1483

Fyzická osoba se může dopustit přestupku porušení povinnosti mlčenlivosti, a to, pokud je ke správci či zpracovateli v pracovním nebo obdobném poměru, vykonává-li činnost pro správce nebo zpracovatele na základě dohody nebo pokud v rámci plnění uložených oprávnění přichází do styku s osobními údaji. Za tento přestupek zákon umožňuje uložit pokutu ve výši 100 000 Kč.[208]

Dalšími přestupky, kterých se fyzická osoba může dopustit jsou ty, jež zákon hodnotí jako závaznější, a to podle uložení vyšší sazby pokuty až do výše 1 000 000 Kč. Do této skupiny řadíme přestupky, jichž se fyzická osoba dopustí tím, že při zpracování není stanoven jeho účel, prostředky či způsob zpracování. Dochází ke zpracování nepřesných osobních údajů, shromažďování či zpracovávání neodpovídá předem vymezenému účelu nebo trvá delší dobu než nezbytnou. Dále pokud zpracování probíhá bez souhlasu subjektu údajů či bez jeho náležité informovanosti a s tím související porušení informační a oznamovací povinnosti nebo pokud nedojde k provedení stanovených opatření.[209] Poslední skupinou přestupků fyzických osob je přestupek, kterým dojde k ohrožení většího počtu osob svým neoprávněným zasahováním do soukromého a osobního života, nebo jde-li o porušení povinnosti pro zpracování citlivých údajů. Tato skupina spadá do nejzávažnější kategorie porušení, za něž lze uložit pokutu až do výše 5 000 000 Kč.[210]

Zvláštním typem přestupku fyzické osoby může být porušení zákazu zveřejnění osobních údajů, za které lze uložit pokutu ve výši 1 000 000 Kč. Jestliže k takovému zveřejnění dojde v tisku, filmu, rozhlasu, televizi, veřejně přístupnou počítačovou sítí nebo obdobným způsobem, může být sankcionováno pokutou až do výše 5 000 000 Kč.[211]

V případě přestupků právnické nebo podnikající fyzické osoba působící jako správce nebo zpracovatele jsou ukládány vyšší pokuty, v první kategorii do výše 5 000 000 Kč a za přestupky ohrožující větší skupinu neoprávněnými zásahy do soukromého a osobního života a porušení povinnosti pro zpracování citlivých údajů může být uložena pokuta až do výše 10 000 000 Kč.[212]

[208] § 44 odst. 1, 4 zákona č. 101/2000 Sb.
[209] § 44 odst. 2, 5 zákona č. 101/2000 Sb.
[210] § 44 odst. 3, 6 zákona č. 101/2000 Sb.
[211] § 44a zákona č. 101/2000 Sb.
[212] § 45a zákona č. 101/2000 Sb.

10.2. Podle GDPR

Obecné nařízení není výjimkou a stejně tak jako většina právních norem obsahuje i sankční část, jež stanovuje podmínky pro ukládání pokut ve svém článku 83. Dá se říct, že první informací po publikaci GDPR, kterou správci zaznamenali, byla výše maximální pokuty 20 000 000 EUR, v případě podniku do výše 4 % celkového ročního obratu za porušení. Z pohledu českého občana se jedná o nepředstavitelně vysoké částky, ale musíme si uvědomit, že se jedná o celoevropský právní předpis s mezinárodním přesahem.

Obecné nařízení se vztahuje i na některé subjekty sídlící mimo EU, a to, pokud zpracovávají osobní údaje subjektu údajů sídlícího na území Evropské unie. Konkrétně se může jednat o společnosti typu Facebook nebo Google. V těchto případech je možnost udělení takto vysokých pokut zcela na místě, těžko by je odradila maximální pokuta 10 000 000 EUR, kterou připouští zákon o ochraně osobních údajů. Možnosti ukládání pokut vyjádřené v procentech z obratu jsou v současné době velkým trendem, zejména u velikých subjektů, pro něž striktní rozpětí pokut přestávala platit. Zavedení takto vyčíslených pokut má zajistit plnění jejich preventivní a odstrašující funkce, Obecné nařízení se zde tak vyrovnává s dobou i na poli ukládání pokut.[213]

10.2.1. Podmínky ukládání pokut

Čl. 83 GDPR, jak již bylo zmíněno, obsahuje obecné podmínky pro ukládání správních pokut a rovněž mechanismy, které mají zajistit jejich spravedlivé ukládání a v některých případech možnost od udělení pokuty zcela ustoupit. Dozorový úřad má zajistit, aby pokuty byly v první řadě účinné, přiměřené a odrazující, a to s přihlédnutím k jednotlivému případu.

Dozorový úřad musí zohlednit povahu, závažnost a délku trvání porušení, zda došlo k jednání úmyslně nebo z nedbalosti a zda byly podniknuty nějaké kroky ke zmírnění škodlivých následků. Úřad má zohlednit míru odpovědnosti správce a zpracovatele a jejich předchozí relevantní porušení, jakož i míru spolupráce s úřadem pro účely nápravy porušení. Úřad rovněž přihlédne ke kategoriím údajů,

[213] ŽŮREK, Jiří, 2018, op. cit., str. 185.

jež byly porušeny, způsobu, jakým se o porušení dozvěděl, dodržování schválených kodexů a k jakékoliv přitěžující nebo polehčující okolnosti.[214]

V případech, kdy nedojde k uložení pokuty, může dojít pouze k uložení nápravných opatření dozorovým úřadem. Tímto institutem je tak vyvrácen mýtus o likvidačních pokutách Obecného nařízení.

Mezi tyto opatření řadíme upozornění a napomenutí správce či zpracovatele. Dále nařízení povinnosti správci nebo zpracovateli o vyhovění žádosti subjektu údajů, o uvedení operace do souladu s GDPR, oznámení subjektu údajů o porušení zabezpečení údajů. Tato opatření mohou obsahovat povinnost dočasného nebo trvalého omezení zpracování, nařízení opravy, výmazu, případně odebrat osvědčení. V neposlední řadě je zde možnost uložení správní pokuty podle čl. 83. Opatřením rovněž může být přerušení mezinárodní spolupráce.[215]

„V případě, že půjde o bagatelní případ, tedy formální porušení Obecného nařízení, ale s minimální společenskou škodlivostí, nebude pokuta muset být vůbec udělena.“[216] Je možné, že bude postačovat některé nápravné opatření nebo pouze informování správce s očekáváním uvedení stavu do souladu s Obecným nařízením. Tento postup je tak v souladu i se zákonem č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, který upravuje tzv. materiálně-formální pojetí definice přestupku, u které musí dojít i k naplnění materiální stránky, tedy společenské škodlivosti protiprávního činu.

Adaptační zákon by měl obsahovat i institut odložení, aniž by došlo k zahájení řízení o přestupku, a to, pokud vzhledem k významu a míře porušení či ohrožení chráněného zájmu, způsobu provedení činu, jeho následku, okolnostem, za nichž byl čin spáchán, bylo účelu, kterého by bylo možné dosáhnout řízením o přestupku, již dosaženo nebo jej lze dosáhnout jinak.

10.2.2. Výše pokut

Obecné nařízení rozlišuje dva druhy pokut, a to pomocí různé výše sankce a možného dopadu na chráněný zájem. Jednotlivé skutkové podstaty jsou definovány poměrně zeširoka, a to podle porušení povinností plynoucích z daných

[214] Čl. 83 odst. 2 Obecného nařízení GDPR
[215] Čl. 58 odst. 2 Obecného nařízení GDPR
[216] ŽŮREK, Jiří, 2018, op. cit., str. 187.

článků. Sankce tak může být udělena nejen za porušení hlavní povinnosti, ale zároveň i za nesplnění povinností souvisejících. Pro obě kategorie zůstává v platnosti, že pokud dojde k porušení několika ustanovení Obecného nařízení, celková výše správní pokuty nesmí překročit stanovenou horní hranici pro nejzávažnější porušení.

Pokuty ukládané orgánům veřejné moci a veřejným subjektům smí členský stát v mezích GDPR upravit sám. Podle adaptačního zákona by měla být maximální výše stanovena na 10 000 000 Kč, neboť tyto pokuty plynou především z veřejných rozpočtů a vyšší pokuta by byla zcela jistě neúčelná.

První kategorie porušení Obecného nařízení umožňuje uložit pokutu do výše 10 000 000 EUR, případně jde-li o podnik, tak do výše 2 % celkového ročního obratu celosvětově, a to podle toho, která hodnota je vyšší. Do této kategorie řadíme porušení povinností plynoucích z čl. 8, 11, 25 až 39, 42 a 43 GDPR.[217] Konkrétně jde o případy porušení povinností při zabezpečení ochrany osobních údajů, podmínek přibrání zpracovatele. Dále porušení povinností vyhotovení záznamů o činnostech zpracování, spolupráce s dozorovým úřadem, ohlašování, posouzení vlivu na ochranu osobních údajů týkajících se jmenování a podmínek pověřence, povinností ustanovení zástupce pro zpracování mimo EU či činností týkajících se získávání osvědčení.

Do druhé kategorie řadíme závažnější porušení, za které lze udělit pokutu až do výše 20 000 000 EUR, případně, jde-li o podnik, tak do výše 4 % celkového ročního obratu celosvětově, zase podle toho, která hodnota je vyšší.[218] Do této kategorie náleží zejména porušení základních zásad pro zpracování, podmínek souhlasu a zpracování zvláštních kategorií údajů, práv subjektů a podmínek pro předávání osobních údajů do třetích zemí. Dále také porušení povinností plynoucích z právních předpisů členského státu týkajících se zvláštních situací, jež jsou v jeho působnosti, stejně jako porušení povinnosti splnit příkaz, dočasné nebo trvalé omezení či přerušení toků údajů. V neposlední řadě sem spadá nesplnění příkazu dozorového úřadu nebo neposkytnutí přístupu při uplatnění dozorové pravomoci.[219]

[217] Čl. 83 odst. 4 Obecného nařízení GDPR
[218] Čl. 83 odst. 5 Obecného nařízení GDPR
[219] ŽŮREK, Jiří, 2018, op. cit., str. 191.

11. Závěr

Jak již bylo řečeno v úvodu, zamýšleným cílem práce bylo podat komplexní přehled oblasti ochrany osobních údajů, zejména ve světle srovnání naší právní úpravy, zákona o ochraně osobních údajů, s evropskou právní úpravou, tedy Obecným nařízením GDPR.

Ve své práci jsem se snažila vyzdvihnout ty nejdůležitější pojmy, které tuto problematiku provází. Zároveň jsem se zaměřila na instituty, jež s sebou tato nová právní úprava přináší. Úvodní kapitola věnovaná základnímu pojmosloví byla uvedením do problematiky, kdy jsem se snažila především vystihnout ty nejdůležitější osobní údaje. Ve srovnání obou právních úprav jsem zde zaznamenala pouze méně významné rozdíly týkající se zařazení nebo naopak vynětí určitých pojmů z kategorií citlivých údajů. Pro mě v této kapitole bylo podstatné upozornit zejména na pojmy biometrických a genetických údajů, jejichž definice Obecné nařízení poměrně detailně upravilo.

Další částí věnovanou vývoji právní regulace osobních údajů jsem se snažila stručně zaměřit na všechny relevantní právní úpravy, které dosavadní vývoj ovládaly. V této kapitole se tak osvětlila potřeba takto rozsáhlé právní regulace, a to v podobě Obecného nařízení. Zároveň došlo i na upozornění, kdy si můžeme všimnout, že naši zákonodárci rozhodně nejsou natolik flexibilní, jak by asi bylo žádoucí, neboť adaptační zákon, který měl být přijat již v průběhu legisvakanční lhůty, ke dni odevzdání práce stále prochází legislativním procesem.

Subjekt údajů, se díky nové úpravě v GDPR stal jedním ze stěžejních pojmů nové právní regulace. Fyzické osobě byla přiznána v celku rozsáhlá práva na ochranu svých osobních údajů. Jednotlivá práva jsem se v této kapitole snažila poměrně detailně popsat, neboť, jak již bylo řečeno, takto podrobně popsaná a definovaná práva jsou v naší právní úpravě novinkou.

V hlavní části mé práce věnované zpracování osobních údajů jsem nejprve definovala samotný pojem zpracování. Ve světle srovnání práv a povinností v postavení správce a zpracovatele osobních údajů jsem upozornila na rozsáhlejší úpravu zejména nových povinností. Významnou novinkou v postavení správce je zavedení institutu společných správců, GDPR se rovněž zaměřilo na úpravu vzájemného vztahu správce a zpracovatele, a to především pomocí zavedení

standardních smluvních doložek. Institut souhlasu osobních údajů byl Obecným nařízením taktéž rozšířen a konkretizován o nové požadavky. Největší novinkou v této části je však institut pověřence pro ochranu osobních údajů, jenž vyvolal řadu diskuzí a pro některé byrokratickou zátěž. Pověřenec má být odborným elementem pro správce a správci poskytovat zejména odborné rady a rovněž sledovat soulad zpracování s Obecným nařízením.

Další části práce byly věnovány zabezpečení osobních údajů a novému institutu posouzení vlivu na ochranu osobních údajů. Obecné nařízení pro oblast zabezpečení osobních údajů nově upravuje demonstrativní výčet konkrétních technicko-organizačních opatření, jejichž pomocí má být zmiňovaná bezpečnost osobních údajů zajišťována.

Kontrolní a dozorčí činnost veřejné správy je neopominutelnou částí, ve které jsem se věnovala hlavně pravomoci a působnosti dozorových úřadů. Následující část práce se věnuje přeshraničnímu předávání osobních údajů, kdy Obecné nařízení oproti naší dosavadní právní úpravě obsahuje rozsáhlou úpravu věnovanou předávání informací do třetích zemí.

Poslední část práce se týká správních trestů za porušení ochrany osobních údajů. Hrozba vysokých pokut stanovených GDPR vyvolala nemalou řadu diskusí. Zde je však potřeba si znovu připomenout a uvědomit, že hrozba takto vysokých sankcí platí zejména pro velké obchodní korporace, pro něž by sankce i na samé horní hranici nemusela představovat větší problém a sankce by tak nenaplnila svůj účel.

A co se týká zhodnocení po necelém roce účinnosti Obecného nařízení? S ohledem na stávající právní stav tuto regulaci musím hodnotit vcelku kladně. Spousta nejasných pojmů, která se předtím pouze dovozovala, je nyní přesně vymezená, což si myslím, že je v jistých ohledech pro správce, zpracovatele a další osoby rozhodně přehlednější a usnadňující situace. Díky jednoznačnému definování některých pojmů by mělo i dojít k částečnému sjednocení činnosti jednotlivých správců.

Na druhou stranu však Obecné nařízení pro mnohé představuje byrokratickou zátěž a revizi stávajících souhlasů zpracování a zhodnocení množství zpracovávaných údajů. Zde si ale opět nemyslím, že by se jednalo až o takový zásah a novou povinnost. Pokud totiž správce dodržoval stávající právní úpravu, neměly

by pro něj být tyto novinky příliš zatěžující. Z mého pohledu představuje Obecné nařízení velkého „strašáka“ a běžní adresáti se s ním setkali zejména prostřednictvím zahlcené e-mailové schránky plné žádostí o poskytnutí nových souhlasů se zpracováním osobních údajů. Je však otázkou, na kolik tento boom získávání nových souhlasů byl potřeba, nebo zda se většina spíše zalekla hrozby vysokých pokut a raději udělala revizi těch stávajících, byť jen z preventivního hlediska.

Adaptační zákon je stále v legislativním procesu a problematické situace, které měl vyřešit, se zatím řeší provizorně nebo prostou improvizací. Jedním z takových řešení je třeba postavení Úřadu pro ochranu osobních údajů, jehož existence ve stávajícím postavení je zatím plánovaná minimálně do konce roku 2019.

12. Zdroje

12.1. Zákony

1) Nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů
2) Všeobecná deklarace lidských práv
3) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
4) Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
5) Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich
6) Zákon č. 255/2012 Sb., o kontrole
7) Zákon č. 89/2012 Sb., občanský zákoník
8) Zákona č. 262/2006 Sb., zákoník práce
9) Zákon č. 2/1969 Sb., zákon České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky (kompetenční zákon)
10) Ústavní zákon č. 1/1993 Sb., Ústava České republiky
11) Usnesení č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky

12.2. Literatura

1) BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012. Olomouc: ANAG, 2012. Právo (ANAG). ISBN 978-80-7263-749-2.
2) BARTÍK, Václav. *Zákon o ochraně osobních údajů s komentářem*. Olomouc: ANAG, 2010. Právo (ANAG). ISBN 978-80-7263-613-6.
3) GDPR v kostce: praktický průvodce povinnostmi pro podniky a spolky. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-704-0.
4) GERLOCH, Aleš. Teorie práva. 7. aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. Právnické učebnice (Aleš Čeněk). ISBN 978-80-7380-652-1.
5) HENDRYCH, Dušan. *Správní právo: obecná část*. 9. vydání. V Praze: C.H. Beck, 2016. Academia iuris (C.H. Beck). ISBN 978-80-7400-624-1.

6) HORZINKOVÁ, Eva a Zdeněk FIALA. *Správní právo hmotné: obecná část*. 2., aktualizované vydání. Praha: Leges, 2015. Student (Leges). ISBN 978-80-7502-092-5.
7) JANEČKOVÁ, Eva. GDPR: praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.
8) KNAPP, Viktor. Teorie práva. Vyd. 1., 3. dot. Praha: C.H. Beck, 1995. Beckovy právnické učebnice. ISBN isbn80-7179-028-1
9) KOPECKÝ, Martin. *Správní právo: obecná část*. V Praze: C.H. Beck, 2019. Beckovy právnické učebnice. ISBN 978-80-7400-727-9.
10) KUČEROVÁ, Alena. Zákon o ochraně osobních údajů: komentář. Praha: C.H. Beck, 2003. Beckovy texty zákonů s komentářem. ISBN 80-7179-762-6.
11) MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008. Beckova edice ABC. ISBN 978-80-7400-033-1
12) MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012. Praktik (Leges). ISBN 978-80-87576-12-0.
13) MATES, Pavel. Ochrana soukromí ve správním právu. Praha: Linde, 2004. ISBN 80-7201-458-7.
14) MATES, Pavel. *Základy správního práva trestního*. 7., přepracované vydání. V Praze: C.H. Beck, 2017. ISBN 978-80-7400-680-7.
15) MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 978-80-7357-322-5.
16) MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 978-80-7357-322-5.
17) MELOTÍKOVÁ, Petra. Ochrana osobních údajů v rámci veřejné správy. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2.
18) NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.
19) NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.
20) NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.
21) Praktický manuál GDPR pro každého: vše, co potřebujete vědět o novém nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně osobních

údajů v praktickém kompletu s webem, e-bookem a aktualizačním servisem. Bratislava: Donau Media, 2018. ISBN 978-80-8183-049-5.
22) ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

12.3. Judikatura

1) Nález Ústavního soudu I. ÚS 229/98 ze dne 10. 11. 1998
2) Rozsudek ESD C 131/12 GoogleSpain SL a Google Inc. v. AgenciaEspañola de Protección de Datos (AEPD) a Mario CostejaGonzález ze dne 13. 5. 2014
3) Rozsudek ESD Rechnungshof (C-465/00) proti Österreichischer Rundfunk a dalším a Christa Neukomm (C-138/01) a Joseph Lauermann (C-139/01) proti Österreichischer Rundfunk ze dne 20. 5. 2003
4) Rozsudek ESD ve věci C-101/01, Lindqvistová vs. Švédsko ze dne 6. 11. 2003
5) Rozsudek Nejvyššího správního soudu čj. As 21/2005-105 ze dne 10. 5. 2006

12.4. Ostatní

1) Historie Úřadu pro ochranu osobních údajů, dostupné z www.uoou.cz/historie-uradu-pro-ochranu-osobnich-udaju/ds-1061/archiv=0&p1=1059
2) Kohútová Zuzana, Anonymizace, pseudonymizace a šifrování osobních údajů jako bezpečnostní opatření dle GDPR, dostupné z fly-eye.cz/blog-detail-1.html
3) Nonnemann František, Skácelová Michaela, Zpracování biometrických údajů ve světle obecného nařízení osobních údajů (GDPR), dostupné z www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-ve-svetle-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-106028.html
4) Obecné nařízení o ochraně osobních údajů prakticky, dostupné z www.gdpr.cz/blog/
5) Porušení povinností při zpracování osobních údajů, dostupné z www.uoou.cz/poruseni-povinnosti-pri-zpracovani-osobnich-udaju/ds-1487/archiv=0&p1=1483
6) Pouperová Olga, Nezávislé správní úřady, dostupné z www.mvcr.cz/clanek/nezavisle-spravni-urady.aspx
7) Pracovní skupina 29, dostupné z www.gdpr.cz/gdpr/heslo/pracovni-skupina-29/

8) Působnost Úřadu, dostupné z www.uoou.cz/pusobnost-uradu/ds-1269/archiv=0&p1=1059
9) Stanovisko č. 1/2017, biometrická identifikace nebo autentizace zaměstnanců, červen 2017, dostupné z www.uoou.cz/assets/File.ashx?id_org =200144& id_dokumenty=29089
10) Stanovisko č. 2/2008, souhlas se zpracováním osobních údajů, září 2008, dostupné z www.uoou.cz/files/stanovisko_2008_2.pdf
11) Stanovisko č. 3/2009, biometrická identifikace nebo autentizace zaměstnanců, červen 2017, dostupné z www.uoou.cz/assets/File.ashx?id_org=200144&id_ dokumenty=23858
12) Stanovisko č. 3/2012, k pojmu osobní údaj, březen 2012, dostupné z www.uoou.cz/stanovisko-c-3-2012-k-pojmu-osobni-udaj/d-1535/p1=1863
13) Stanovisko č. 4/2013, k pojetí zpracování osobních údajů, říjen 2013, dostupné z www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22256
14) Stanovisko č.12/2012, k použití fotografie, obrazového a zvukového záznamu fyzické osoby, únor 2014, dostupné z www.uoou.cz/assets/ File.ashx?id_org= 200144&id_dokumenty=22538
15) Usnesení Poslanecké sněmovny z 27. schůze ze dne 12. března 2019, dostupné z www.psp.cz/sqw/text/tiskt.sqw?o=8&v=US&ct=561
16) Stanovisko WP29 č. 3/2013 ze dne 2. 5. 2013 *k účelovému omezení*, WP 203, dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
17) Stanovisko WP29 č. 5/2012 ze dne 1. 7. 2012 *ke cloudcomputingu*, WP 196, dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
18) Pokyn WP29 ze dne 13. 12. 2016 k pověřenci pro ochranu osobních údajů, WP 243, dostupné z https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/gdpr-dokumenty/2018/1/Preklad-Metodiky-poverence-WP29.pdf
19) Výkladový pokyn WP29 ze dne 4. 4. 2016 k posouzení vlivu na ochranu osobních údajů (DPIA) a určování, zda je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro potřeby nařízení 2016/679, WP 248, dostupné z https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Resume

My thesis deals with protection of personal data. It is a current and living issue thanks to the massive development of social networks. We can increasingly experience massive misuse of personal data on the social media, both when processing and preserving it. So to respond to this problem there was a need for new legal regulation.

In my thesis I am concentrating on comparison of Law on Protection of Personal Data n. 101/2000 with General Data Protection Regulation n. 679/2016. In particular, I highlight the areas where the biggest changes have occurred and those that are brand new. It is a very comprehensive topic that includes a number of concepts and institutes that deserve more attention than scope of this thesis allows. But for my purposes I want to point out these terms in particular and to highlight the most important or common.

In the introductory chapter I am focusing on describing definitions of basic terminology, especially the term "personal data". I outline the concepts of special categories of personal data, also referred to as sensitive data. I only mention the ones directly defined by the regulation, such as genetic, biometric and health data. From other data I only choose the most commonly discussed ones. Then I am introducing concepts of anonymous data and pseudonymization.

The next part of the work is focused on the origin of personal data protection, its historical development, both worldwide and nationwide. The subject of data has certainly leading role in this chapter. I am defining its position and the extensive rights granted to it by the General Regulation.

Main chapter of the thesis deals with the process of personal data processing. First from the point of view of Czech legislation also known as the Personal Data Protection Act. The second part is devoted to processing from the perspective of the General Regulation, with the all newly introduced institutes. The following chapters are devoted to personal data protection and the new impact assessment institute. The next part is devoted to the supervisory activity in the protection of personal data. This includes the powers of supervisory authorities. Part of the work is devoted to cross-border transfer of personal data. The last part of this thesis deals with administrative penalties for violations of personal data protection.