ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

Katedra ústavního a evropského práva

DIPLOMOVÁ PRÁCE

Implementace Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 a 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)

Monika Strapková

Plzeň 2020

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Monika STRAPKOVÁ**
Osobní číslo:	**R15M0282P**
Studijní program:	**M6805 Právo a právní věda**
Studijní obor:	**Právo**
Téma práce:	**Implementace Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)**
Zadávající katedra:	**Katedra ústavního a evropského práva**

Zásady pro vypracování

1. Úvod
2. Teoretická část
3. Praktická část
4. Závěr
5. Literatura

Rozsah diplomové práce: **103**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná**

Seznam doporučené literatury:

- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Brusel: Evropský parlament, Rada (EU), 2016.
- Základní příručka k GDPR. Úřad pro ochranu osobních údajů the office for personal data protection [online]. Praha: Úřad pro ochranu osobních údajů, 2013 [cit. 2018-12-29]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744
- NULÍČEK, Michal a Josef DONÁT. GDPR/Obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. ISBN 201797880-7552-765-3.
- NAVRÁTIL, Jiří. GDPR pro praxi. Praha: Čeněk, 2018. ISBN 978-80-7380-689.
- NEZMAR, Luděk. GDPR: Praktický průvodce implementací. Praha: Grada, 2017. ISBN 978-80-271-0668-4.
- ŽŮREK, JUDr. Jiří. Praktický průvodce GDPR. Olomouc: ANAG, 2018. ISBN 978-80-7554-152-9.
- PATTYNOVÁ, Jana a Lenka SUCHÁNKOVÁ. Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě. Komentář. Praha: Leges, 2018. ISBN 978-80-7502-288-2.
- JANEČKOVÁ, Eva. GDPR – Praktická příručka implementace. Praha: Čeněk, 2018. ISBN 978-80-7552-248-1.

Vedoucí diplomové práce: **JUDr. Tomáš Pezl**
Fakulta právnická

Datum zadání diplomové práce: **23. ledna 2019**
Termín odevzdání diplomové práce: **31. března 2020**

L.S.

Doc. JUDr. Jan Pauly, CSc.
děkan

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

V Plzni dne 26. června 2019

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

V Plzni, 14. 4. 2020 ……

Monika Strapková

Poděkování

Ráda bych poděkovala panu JUDr. Tomáši Pezlovi, Ph.D., za jeho cenné rady, trpělivost, ochotu a připomínky, jež mi velice pomohly při vypracování této diplomové práce.

Dále bych ráda poděkovala advokátce Mgr. Martině Slaninové a advokátu Mgr. Ondřeji Vokálovi z advokátní kanceláře Slaninová Vokál za poskytnutí praxe pod tím nejlepším možným vedením, bez které by má diplomová práce v tomto pojetí nemohla vzniknout a advokátnímu koncipientovi Mgr. Davidu Hornovi z téže advokátní kanceláře za úvodní školení a trpělivé rady v průběhu implementací.

Obsah

Úvod

Tématem této diplomové práce je Implementace Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 a o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen jako „*GDPR*“ nebo „*Nařízení*“). Obor ochrany osobních údajů, ale i samotné Nařízení, jsou značně rozsáhlá témata, proto má diplomová práce užší specifikaci a bude směřovat především k praktické stránce tohoto odvětví, a tedy bude se zabývat samotnou implementací Nařízení, samotným procesem, při němž správce nejprve zjišťuje své povinnosti a poté je uvádí do praxe.

Cílem práce je tedy především přinést podrobný a jasný přehled všech činností správce v průběhu implementace Nařízení metodou pozorování a rešerše a zároveň vytvořit přehlednou rešerši k základním teoretickým jevům, jež jsou nezbytné pro praktické navázání.

Pro úplnost a větší přehlednost bude diplomová práce rozdělena do dvou hlavních částí – teoretické a praktické. Ačkoli je tématem práce praktická implementace Nařízení, považuji za nezbytné věnovat se před praxí nejprve alespoň základům teorie, která je k uvedení praxe nepostradatelná.

Teoretická část přitom bude rozčleněna do pěti kapitol. První kapitola se bude věnovat úvodu do tématu, zjištění, s jakými cíli bylo Nařízení přijímáno a jaké změny účinnost Nařízení přinesla, co je v právní úpravě ochrany osobních údajů díky Nařízení úplně nové a co například předchozí úprava znala, ale Nařízením je zpřísněno.

Druhá kapitola představí základní pojmy spojené s ochranou osobních údajů, které Nařízení definuje. Zvláštní pozornost bude věnována stěžejním pojmům jako je osobní údaj, správce, zpracovatel či souhlas, ale také vysvětlení, co znamená pseudonymizace, anonymizace a jaký je mezi těmito dvěma pojmy rozdíl.

Třetí kapitola se bude věnovat právním titulům zpracování osobních údajů, jichž je celkem šest a jejich výčet v Nařízení je taxativní. Nezpracovává-li správce osobní údaje na základě některého z těchto údajů, pak probíhá zpracování

v rozporu s Nařízením. Ve třetí kapitole tedy bude každý z těchto titulů představen s vysvětlením, co takové zpracování znamená, případně kdy k němu dochází.

Nařízení také přináší konkrétní zásady, kterými by se měl správce při zpracování osobních údajů řídit a měl by je dodržovat. Všechny tyto zásady budou představeny v jednotlivých podkapitolách čtvrté kapitoly.

Závěrečná kapitola teoretické části se pak bude zabývat právy, která subjektům údajů stanovuje Nařízení. Uvedu výčet těchto práv, kdy subjektu údajů některé z těchto práv náleží a také jaké povinnosti správce se pojí s právy subjektů údajů.

V druhé – praktické části diplomové práce pak provedu všemi kroky implementace Nařízení z pohledu správce od úplného počátku. Praktická část implementace bude rozčleněna stejně jako teoretická část do pěti kapitol. V první kapitole představím, co se pod spojením implementace Nařízení skrývá.

Druhá kapitola praktické části ponese název Studium, přičemž přinese shrnutí, co vše musí správce nastudovat před započetím implementace a zároveň co vše je pro správce předmětem studia i v průběhu implementace nebo poté, co jeho činnost již v souladu s Nařízením je a dodržuje veškeré zásady. Vysvětlím, proč je studium stále aktuální součástí tématu a jeho aktuálnost nelze vyloučit především z důvodu, že materiály ke studiu budou stále přibývat.

Přípravná část implementace je široké téma, proto bude třetí kapitola rozčleněna do několika podkapitol. Vysvětlím, proč správce začíná vytvořením auditu osobních údajů, k čemu může takový audit sloužit, jakou metodu k jeho vypracování použije, co znamená pojem gap analýza nebo zkratka DPIA. Budu se zabývat i dalšími kroky, které správce směřuje k souladu se stavem požadovaným Nařízením, jimiž jsou například úprava dokumentace či interních předpisů.

Po přípravě následuje realizace všech navrhovaných opatření. Těm se budu věnovat ve čtvrté kapitole. Zaměřím se na školení, které je správce povinen pro sebe a své zaměstnance zajistit, a to nejen pro prvotní seznámení s právní úpravou ochrany osobních údajů, ale takovým způsobem, aby všichni měli průběžně přehled o vývoji celého oboru.

Praktickou část diplomové práce bude uzavírat kapitola, ve které se zaměřím na praxi, tedy na dobu, kdy již správce vykonal všechny potřebné kroky k zajištění souladu své činnosti s Nařízením a nově vytvořený stav neustále udržuje. Vysvětlím také, kdo je to pověřenec pro ochranu osobních údajů, jaké jsou jeho úkoly i jací správci jsou povinni třetí osobu ochranou osobních údajů pověřit.

Teoretická část

1. GDPR

Pod zkratkou GDPR se skrývá anglické spojení *General Data Protection Regulation*, což v překladu znamená Obecné nařízení o ochraně osobních údajů. Že je toto nařízení úzce spojeno s Evropskou unií, poznáme hned z jeho celého názvu, který zní Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Evropská unie tedy upravila ochranu osobních údajů, a stojí tak za vznikem celého nařízení, které jednotně vstoupilo v účinnost dne 25. května 2018 a v České republice nahradilo dosavadní právní úpravu, kterou představovala směrnice 95/46/ES a zákon č. 101/2000 Sb., o ochraně osobních údajů.

1.1 Cíle Nařízení

Jelikož předchozí úprava zabývající se ochranou osobních údajů pochází z roku 1995, mezi cíle Nařízení lze nepochybně zařadit zejména snahu o to, aby právní předpisy v oblasti ochrany osobních údajů odpovídaly současným poměrům, jelikož předchozí úprava již postrádala aktuálnost[1], a to zejména v technologické oblasti, kdy dochází ke sběru dat například prostřednictví internetových nákupů nebo v souvislosti s personalizovanými reklamami[2].

Za přijetím Nařízení ale stála též snaha, aby bylo právo v této oblasti v zemích Evropské unie a v těch zemích, na které dopadá, sjednocené[3], aby se práva subjektů údajů posílila a také aby byla posílena důvěryhodnost samotné Evropské unie, ale i jednotlivých členských států[4].

1.2 Co se účinností Nařízení změnilo

Nařízení tedy přináší řadu změn, mezi ty hlavní například patří princip odpovědnosti správce a přístup založený na riziku. Odpovědnost správce zakládá povinnost správců dbát dodržování zásad zpracování osobních údajů v souladu

[1] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 27-28.
[2] KOČICOVÁ, Věra a HORÁK, Filip. (R)evoluce v ochraně osobních údajů?: General Data Protection Regulation (GDPR). *IT Systems*, 2016, 18(7-8), s. 20-21. ISSN 1802-002X.
[3] MORÁVEK, Jakub. Když dva dělají totéž, není to totéž, aneb, GDPR jako přestupková amnestie?. *Právní rozhledy*. 2018, roč. 26, č. 13-14. s. 487-493. ISSN 1210-6410.
[4] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. s. 30-31.

s Nařízením a současně být schopen soulad s Nařízením doložit[5]. Podle Nařízení je přitom správce povinen k zajištění souladu přijmout vhodná technická a organizační opatření a dodržovat zásadu záměrné a standardní ochrany osobních údajů[6].

Přístup založený na riziku pak představuje povinnost správce přizpůsobovat zabezpečení osobních údajů možným rizikům, která hrozí, s ohledem na rozsah, povahu, kontext a účel zpracování[7], přičemž Nařízení rozlišuje riziko, vysoké riziko a nízké riziko jako tři různé druhy rizika. Riziko je obecný pojem, který správce uplatní při zavádění technických a organizačních opatření, kdy zjišťuje, zda při zpracování osobních údajů hrozí riziko, které představuje újmu pro subjekt údajů, jaká je pravděpodobnost jeho vzniku a jakým způsobem může takovému riziku předcházet. Zjistí-li správce hrozbu vysokého rizika, znamená to pro něj, že má navíc povinnost provést posouzení vlivu na ochranu osobních údajů, předchozí konzultaci s dozorovým úřadem a případně, došlo-li k porušení zabezpečení osobních údajů, uvědomit subjekty údajů. Zjištění nízkého rizika pak pro správce představuje výjimku z ohlašovací povinnosti porušení zabezpečení osobních údajů dozorovému úřadu[8]. Právě za účelem identifikace případných rizik správce vytvoří analýzu rizik všech jednotlivých účelů zpracování osobních údajů. Po dokončení implementace analýzu rizik zopakuje, přičemž jejím výsledkem bude zjištění efektivnosti přijatých opatření[9].

Zároveň na předchozí povinnosti navazuje povinnost správce oznámit případné porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a subjektu údajů. Správce je také nově povinen vyhotovit posouzení dopadu činnosti na ochranu osobních údajů, udržovat kontakt s Úřadem pro ochranu osobních údajů za účelem případných předběžných konzultací, vést záznamy

[5] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 32-33.

[6] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 247.

[7] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 32-33.

[8] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 249-250.

[9] MALÝ, Zbyněk. GDPR je nekonečný příběh... *Sdělovací technika*, 2018, 66(10), s. 32. ISSN 0036-9942.

o činnostech zpracování osobních údajů, neprodleně hlásit případy porušení bezpečnosti osobních údajů, poskytnout subjektu údajů možnost přenést osobní údaje k jinému správci a případně ustanovit pověřence pro ochranu osobních údajů[10].

Obecně lze konstatovat, že Nařízení zvýšilo správcovu informační povinnost, kterou má vůči subjektům údajů, a to především s ohledem na udělování souhlasu se zpracováním osobních údajů, jejichž dosavadní forma ve velké míře neodpovídala požadavkům právní úpravy. Zároveň Nařízení značně posiluje práva subjektů údajů, která mají vůči všem správcům[11].

Nicméně nových povinností pro správce Nařízení nepřináší tolik, že by mělo jejich splnění činit výraznější problémy. Plnil-li si správce řádně své povinnosti podle předchozí právní úpravy, znamenala pro něj účinnost Nařízení pouze dílčí změny a úpravy. Opravdový problém ovšem představovala skutečnost, že teprve s účinností Nařízení začala velká většina správců zjišťovat, že existuje právní úprava v oblasti ochrany osobních údajů, ze které jim také plynou určité povinnosti[12].

2. Základní pojmy

Nařízení přináší řadu důležitých pojmů, jejichž správné a úplné pochopení je zásadní pro úspěšnou implementaci. Jejich význam vysvětluje v čl. 4. Následující odstavce se budou vybraným pojmům věnovat.

2.1 Osobní údaj

U vysvětlování pojmů plynoucích z Nařízení, které se týká ochrany osobních údajů, nelze začít jiným pojem, než je osobní údaj. Tento pojem je zcela zásadní, neboť Nařízení upravuje zpracování pouze takových informací, jež lze tímto pojmem označit[13].

Podle Nařízení je osobní údaj jakákoliv informace, která se týká určeného nebo určitelného subjektu údajů. Jedná se přitom o fyzickou osobu, jíž lze přímo či

[10] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. str. 32-33.
[11] OTEVŘEL, Petr. GDPR od A do Z: díl první: Obecný úvod o nové úpravě nakládání s osobními údaji. 1. Díl. *IT Systems*, 2017, 19(7-8), s. 38-39. ISSN 1802-002X.
[12] MORÁVEK, Jakub. Ochrana dat zaměstnanců: stačí drobně seřídit stroj. *Právní rádce*, 2018, 26(2), s. 46-48. ISSN 1210-4817.
[13] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s.77.

nepřímo identifikovat, a to hlavně pomocí určitých identifikátorů, jimiž jsou např. číslo, kód či určitý prvek fyzické, psychické nebo sociální identity této osoby[14].

Není pochyb, že v praxi představuje osobní údaj například jméno, datum narození, telefonní číslo či adresu[15], a to ať se nachází některé z údajů pohromadě nebo se jen některý z nich vyskytuje samostatně. Důležité kritérium představuje skutečnost, zda lze fyzickou osobu přímo nebo nepřímo identifikovat, je-li to možné, jedná se o identifikovanou fyzickou osobu, pak tedy i údaj, pomocí něhož je osoba identifikovaná, představuje osobní údaj. Tedy například i samotné jméno představuje postačující prostředek k tomu, aby bylo možné fyzickou osobu identifikovat[16]. Nejen tyto informace jsou ovšem osobními údaji a pro správné posouzení je nutné do osobních údajů zahrnout i veškeré další údaje, které se o určené nebo určitelné osobě shromažďují a zpracovávají. Takovými údaji jsou např. údaj o platu, a to i bez označení jménem, výsledky posouzení bonity klienta finančním subjektem či historie prohlížení internetových stránek určenou či určitelnou osobou[17].

Pojem osobní údaj zůstal v porovnání se zákonem č. 101/2000 Sb., zákon o ochraně osobních údajů a o změně některých zákonů, nezměněn[18], neboť říká, že „*osobním údajem je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“*[19].

Nezbývá než zdůraznit, že, jak je patrné již z definice osobního údaje, osobní údaje nejsou údaje týkající se právnických osob, tedy např. obchodní firma či základní kontaktní údaje právnické osoby. O osobní údaje se u právnické osoby jedná v případě údajů o členech statutárních orgánů či společníků, tedy fyzických

[14] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 4 odst. 1.
[15] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 42-43.
[16] Stanovisko generálního advokáta M. Campos Sánchez-Bordony přednesené dne 14. ledna 2020(1), Věc C-78/18
[17] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 42-43.
[18] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 32.
[19] Zákon č. 101/2000 Sb., *zákon o ochraně osobních údajů a o změně některých zákonů*. čl. 4.

osob, a dále je osobním údajem také personalizovaný e-mail[20]. To znamená, že např. adresa ve tvaru obchodni@společnost.cz není osobním údajem, oproti tomu jan.novak@obchodnispolecnost.cz už ano[21].

Osobními údaji jsou i pseudonymizované osobní údaje, neboť pseudonymizace sice slouží jako určitá ochrana osobních údajů, ovšem takovou ochranu nelze považovat za absolutní[22]. Pseudonymizované údaje jsou přitom takové údaje, které již nelze přiřadit ke konkrétnímu subjektu údajů, aniž by k tomu byly použity ještě dodatečné údaje[23]. Zároveň jsou uchovávány odděleně a zabezpečeny organizačními a technickými prostředky[24].

Oproti tomu anonymní údaje nejsou osobními údaji ve smyslu GDPR, neboť je nelze spojit s žádnou identifikovanou či identifikovatelnou osobou. Tedy to znamená, že mezi nimi a subjektem údajů nelze nalézt spojitost, přičemž taková spojitost ani nemůže být nikým obnovena[25].

Rozdíl mezi anonymními a pseudonimizovanými údaji pak spočívá právě v nevratnosti spojení údajů s konkrétní osobou. Tedy například pokud by správce zpracovával jméno, příjmení, věk, dosažené vzdělání a pracovní pozici, jméno a příjmení by ovšem následně trvale nevratně zlikvidoval, zbylé údaje by se staly anonymními, neboť tyto údaje nelze přiřadit k žádné konkrétní osobě ani za pomocí speciálního šifrování. Kdyby ovšem správce jméno a příjmení od ostatních údajů pouze oddělil a nezpracovával současně, přičemž by k těmto dvěma údajům přiřadil jedinečný kód, a právě místo jména a příjmení by společně s údaji zpracovával onen kód, věděl by, který kód patří ke které konkrétní osobě, a mohl by tak osobní údaje snadno spojit. V tomto případě by se jednalo o pseudonimizaci, neboť odstranění určitých údajů není nevratné[26].

---

[20] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 42-43.
[21] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 2.
[22] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. s. 69.
[23] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 4 odst. 5.
[24] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 87.
[25] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 43.
[26] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 43-46.

2.1.1 Kategorie osobních údajů

Veškeré osobní údaje pak můžeme rozdělit do dvou hlavních skupin – obecné osobní údaje a zvláštní, tzv. citlivé osobní údaje. Do skupiny obecných osobních údajů řadíme základní údaje, např. jméno, příjmení, datum narození, rodné číslo, dále fotografie, telefonní číslo či číslo občanského průkazu, ale i dosažené vzdělání, pracovní zkušenosti nebo současnou pracovní pozici.

Mezi zvláštní osobní údaje pak řadíme ty, které Nařízení výslovně definuje, tedy genetické údaje, biometrické údaje a údaje o zdravotním stavu. Genetickými údaji Nařízení rozumí zděděné nebo geneticky získané znaky fyzické osoby, přičemž jí tyto údaje poskytují jedinečné informace týkající se její fyziologie či zdraví a zároveň vyplývají především z analýzy biologického vzorku[27]. Jako příklad genetického osobního údaje uvedeme DNA nebo krevní skupinu, fakticky se ale jedná i například o vlas s kořínkem. Biometrickými údaji Nařízení rozumí takové údaje, které vyplývají z konkrétního technického zpracování, jež se týká fyzických nebo fyziologických znaků či znaků chování fyzické osoby umožňující nebo potvrzující jedinečnou identifikaci[28]. To znamená například podpis, snímek obličeje či otisk prstu[29]. Nakonec údaje o zdravotním stavu definuje Nařízení jako takové osobní údaje, které se vztahují k tělesnému nebo duševnímu zdraví fyzické osoby, přičemž do této skupiny patří i údaje o poskytnutí zdravotních služeb vypovídající o jejím zdravotním stavu[30]. Pod zvláštní osobní údaje ale můžeme zařadit například i rasový nebo etnický původ, sexuální orientaci, politické názory či náboženské vyznání[31].

Zpracování zvláštních osobních údajů věnuje Nařízení speciální pozornost v čl. 9. V zásadě jejich zpracování zakazuje, uvádí ovšem i zvláštní podmínky, kdy se zákaz nepoužije. Například existuje-li jeden nebo více stanovených účelů, pro jejichž zpracování subjekt údajů udělil výslovný souhlas a nebylo-li stanoveno právem Evropské unie nebo členského státu, že subjekt údajů tento zákaz nemůže

---

[27] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 4 odst. 13.
[28] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 94.
[29] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 3.
[30] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 56.
[31] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 52.

zrušit, je-li zpracování těchto údajů nezbytné pro ochranu životně důležitých zájmů subjektu údajů či jiné fyzické osoby nebo zveřejnil-li zjevně tyto údaje sám subjekt údajů[32]. Další podmínky či omezení si pak mohou stanovit členské státy samy nebo, pokud již nějaké takové před účinností Nařízení měly, mohou zachovat stávající[33].

2.2 Subjekt údajů

Pod pojmem subjekt údajů se skrývá jakákoli fyzická osoba, jejíž osobní údaje jsou zpracovávány, a to správcem, pověřenou osobou nebo zpracovatelem. Skutečnost, že subjektem údajů nikdy nemůžeme označit právnickou osobu, lze logicky dovodit z popisu subjektu údajů v Nařízení, jež říká, že subjekt údajů je identifikovaná nebo identifikovatelná fyzická osoba[34].

2.3 Zpracování

Jakákoliv operace nebo souborná operace, kdy je s osobními údaji nebo soubory osobních údajů nakládáno, a to ať již jde o nakládání s pomocí či bez pomoci automatizovaných postupů, je podle Nařízení zpracováním osobních údajů. Jako automatizované postupy přitom Nařízení označuje 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[35].

Zpracování osobních údajů ovšem neznamená jakékoliv nakládání s osobními údaji. Správce osobních údajů provádí zpracování za nějakým cílem a určitým způsobem systematicky, proto je Nařízení závazné pro všechny, kteří jako správci zpracovávají osobní údaje ve smyslu definice dle Nařízení[36]. Na druhou stranu je potřeba při rozlišování situací, kdy se jedná o zpracování ve smyslu Nařízení či nikoliv, přistupovat s velkou pečlivostí, neboť i situace, u kterých by se

[32] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 9.
[33] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 55.
[34] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 4 odst. 1.
[35] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 3.
[36] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 31.

na první pohled nemuselo zdát, že jsou zde nějakým způsobem využívány osobní údaje, mohou být zpravováním ve smyslu Nařízení[37].

Například provádí-li se zpracování pomocí prostředků informační a komunikační technologie, vždy se bude jednat o zpracování osobních údajů ve smyslu Nařízení. Oproti tomu osobní údaje ve fyzické, listinné formě jsou zpracovávány ve smyslu Nařízení pouze tehdy, je-li cílem takového zpracování určitá evidence osobních údajů a nejedná se o nahodilé shromáždění bez konkrétního cíle[38].

2.4 Evidence

Pod pojmem evidence se ukrývá jakýkoliv strukturovaný soubor osobních údajů, jež jsou přístupny na základě zvláštních kritérií, přičemž nerozhoduje, je-li soubor centralizovaný, decentralizovaný či rozčleněný funkčním nebo zeměpisným hlediskem[39]. Jedná se tedy o jakoukoliv databázi s osobními údaji, jež lze v rámci databáze vyhledat podle určitého znaku, například jména, věku nebo telefonního čísla[40].

Evidenci představují například lékařské kartotéky v listinné formě, v nichž jsou zahrnuty osobní údaje[41].

2.5 Správce

Nařízení definuje správce jako jakoukoliv „*fyzickou nebo právnickou osobu, orgán veřejné moci, agenturu nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů*“[42]. V otázce, kdo je správcem, tedy nerozhoduje právní forma ani status subjektu, ale skutečnost, že právě on určí účely a prostředky zpracování osobních údajů[43]. Správce je tedy

[37] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 85.
[38] NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. První vydání. Praha: Klika, 2018. 141 s. Otevřeno. ISBN 978-80-88298-10-6. s. 26-27.
[39] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 15.
[40] MALIŠ, Petr. GDPR od A do Z: díl druhý: Územní a věcná působnost GDPR. 2. Díl. *IT Systems*, 2017, 19(9), s. 54-56. ISSN 1802-002X.
[41] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 88.
[42] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 4 odst. 7.
[43] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 90.

osoba, která nese odpovědnost za dodržování povinností plynoucích z Nařízení, z nichž klíčovou představuje dodržování zásad zpracování osobních údajů, jež musí být schopen jako správce doložit[44].

Nově má správce možnost rozložit své povinnosti společně s další osobou a vytvořit tak institut tzv. společných správců. Znamená to, že dva či více správců společně jasně a zřetelně ujednají své podíly na odpovědnosti za plnění povinností[45]. Potřebnost definování vzájemné odpovědnosti za plnění Nařízení přitom plyne ze vztahu společných správců, a to především jedná-li se o výkon práv subjektu údajů[46]. Společní správci tak spolu uzavřou smlouvu, kde vzájemná práva, povinnosti a podíly na odpovědnosti definují. Zřídit institut společných správců je vhodné zejména vykonávají-li správci podobnou či stejnou činnost, sdílí jedno sídlo nebo jsou provázáni personálně.

2.6 Zpracovatel

Zpracovatel zpracovává osobní údaje[47], přičemž jeho právní forma není podstatná[48], tedy může to být fyzická i právnická osoba, orgán veřejné moci, agentura či jiný subjekt[49]. Zpracovatel stojí mimo správce, není jeho součástí nebo zaměstnancem a zpracovává osobní údaje, které mu k tomu účelu správce svěřil[50]. Důvodem, proč osobní údaje zpracovává pro správce zpracovatel, může být například skutečnost, že pro správce není zpracování možné z personálních či technických důvodů[51] anebo zkrátka takové zpracování nepředstavuje jeho hlavní činnost a, ač by mohl zpracování provádět sám, chce svůj čas věnovat právě své hlavní činnosti.

---

[44] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 39.
[45] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 39.
[46] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 90-91.
[47] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 4 odst. 8.
[48] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 91.
[49] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 4 odst. 8.
[50] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 4.
[51] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 92.

Aby takové zpracování probíhalo legálně, uzavře správce se zpracovatelem smlouvu o zpracování osobních údajů. I zpracovatelé musí dodržovat vhodná technická a organizační opatření, a tak je správce odpovědný za svou volbu, s jakým zpracovatelem naváže spolupráci[52]. V některých případech ale může správci uložit zpracování prostřednictvím zpracovatele právní předpis. To platí například u systému centrální evidence obyvatel, jelikož správci osobních údajů, jenž s údaji vedenými v systému pracují, jsou územní samosprávné celky, Ministerstvo vnitra a případně další subjekty, které správcem zákon o evidenci obyvatel stanoví. Zpracovatelem je přitom Ministerstvo vnitra[53].

Typickým příkladem správce, místo něhož některé osobní údaje zpracovává zpracovatel, může být správce, který zaměstnává určité množství lidí, ovšem jako relativně malý subjekt jeho zaměstnance tvoří pouze lidé s oborovým zaměřením souhlasícím s hlavní činností správce. I správce se chce věnovat své činnosti, proto k vyřízení účetní agendy vyhledá odborníka, kterého nezaměstná, ale bude s ním spolupracovat externě, tedy v tomto případě se bude jednat o externího zpracovatele účetnictví.

Nebo například správce nedisponuje znalostmi a dovednostmi dostatečnými k tomu, aby si zvládl vytvořit vlastní webové stránky, ani se u něj nenachází IT oddělení, jehož pracovníci by webové stránky byli schopni vytvořit. Správce tak pouze kvůli webovým stránkám nebude IT oddělení zakládat, ale osloví společnost, která se na vytváření webových stránek specializuje a nechá si své stránky vytvořit externě, například na základě smlouvy o dílo. Ovšem pokud správce chce prezentovat na webu své zaměstnance a webové stránky mu budou zmíněnou společností vypracovány kompletně se všemi údaji, musí této společnosti poskytnout i veškeré osobní údaje, které chce na webu zveřejnit. Typicky se jedná o jméno, příjmení, emailovou adresu či telefon a fotografii, případně další. Osobní údaje subjektů údajů, kterými jsou v tomto případě zaměstnanci, tak v tuto chvíli zpracovává kromě správce i zpracovatel. Správce a zpracovatel tedy musejí uzavřít ještě smlouvu o zpracování osobních údajů. Ke zpracování by nedošlo, pokud by si správce nechal zpracovat pouze vzor webových stránek, do kterého by konkrétní

[52] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 99.

[53] MALIŠ, Petr. GDPR od A do Z: díl sedmý: Vztah správce a zpracovatele osobních údajů podle GDPR. 7. Díl. *IT Systems*, 2018, 20(3), s. 46-48. ISSN 1802-002X.

údaje doplnil sám. Pak by společnost, která webové stránky tvoří, nebyla zpracovatelem osobních údajů, a nebylo by tedy potřebné uzavírat zpracovatelskou smlouvu.

Dalšími typickými zpracovateli jsou poskytovatelé různých internetových databází, kteří poskytují správci možnost spravování těch osobních údajů, které do databáze zapíší, ovšem zajišťují-li provoz těchto databází, řadí se právě také mezi zpracovatele osobních údajů.

Příkladnými zpracovateli pak ale mohou být také společnost, jenž pro správce provádí likvidaci nosičů osobních dat, bezpečnostní agentura, která užívá ke střežení objektu kamerový nebo jiný sledovací, případně monitorovací systém nebo externí archiv[54].

2.7 Souhlas

Souhlas subjektu údajů pak 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*“[55].

Souhlas tedy musí být učiněn právním jednáním, o něž se nejedná, pokud nebyla projevena vůle jednající osoby[56], vůle musí být svobodná, to znamená, že při projevu vůle nesmí být na subjekt údajů vyvíjen nátlak a skutečnost, že správci souhlas neudělí, nesmí představovat zásah do jeho základních práv[57].

Konkrétní a jednoznačný projev vůle je určitý, nevyvolává pochybnosti, přičemž právním jednáním nelze označit takové jednání, jehož obsah není možné zjistit pro neurčitost či nesrozumitelnost ani výkladem[58] . Konkrétní souhlas tedy znamená, že ho subjekt údajů učinil pro konkrétní účel zpracování, není možné udělit obecný souhlas například pro všechny potřebné účely a jednoznačnost

[54] NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. První vydání. Praha: Klika, 2018. 141 s. Otevřeno. ISBN 978-80-88298-10-6. s. 29.
[55] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 4 odst. 11.
[56] Zákon č. 89/2012 Sb., *občanský zákoník*. § 551.
[57] NEUWIRT, Karel. GDPR změní některé dosavadní zvyklosti. *Sdělovací technika*, 2017, 65(12), s. 10-11. ISSN 0036-9942.
[58] Zákon č. 89/2012 Sb., *občanský zákoník*. § 553 odst. 1.

vylučuje pochybnosti o záměru subjektu údajů udělit souhlas se zpracováním svých osobních údajů[59].

Informovanost představuje nezbytnou složku projevu vůle, bez níž nelze osobní údaje zpracovávat na základě souhlasu. Znamená to, že správce je povinen subjekt údajů informovat o způsobu zpracování osobních údajů, přičemž na základě informací se subjekt údajů může rozhodnout, zda správci souhlas udělí. Zároveň je správce povinen být schopen informovanost a svobodu souhlasu doložit. Za souhlas přitom nelze považovat předem správcem označené pole v on-line formuláři či oznámení v obchodních podmínkách[60]. Předem správcem označené pole přitom zároveň postrádá i aktivitu subjektu údajů, odporuje tedy nejen informovanosti, ale i svobodnému souhlasu, jenž nepřipouští pasivní jednání subjektu údajů[61], předem zaškrtnuté pole proto jednoznačně nelze považovat za souhlas udělený subjektem údajů dle Nařízení[62]. Pokud se přeci jen v obchodních podmínkách, nebo podobně obsáhlém textu, nachází, nesmí s ostatním textem splynout, správce ho musí jednoznačně odlišit, aby ho mohl subjekt údajů snadno nalézt, porozumět mu a mohl se sám rozhodnout, zda souhlas správci udělí[63]. Správce je tedy povinen subjekt údajů informovat o všech rozhodných skutečnostech týkajících se zpracování osobních údajů ještě před udělením souhlasu, a to především o totožnosti správce, účelech a operacích zpracování a právu subjektu údajů svůj souhlas kdykoli odvolat[64].

3. Právní tituly zpracování

Nařízení přináší šest právních titulů, jenž představují jediné možné zákonné zpracování osobních údajů, přičemž každé zpracování by mělo probíhat na základě pouze jednoho z těchto titulů[65]. Ustanovení týkající se právních titulů zpracování Nařízení uvádí taxativně, správce tedy nemůže zpracovávat osobní údaje na základě

[59] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 147.
[60] NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. První vydání. Praha: Klika, 2018. 141 s. Otevřeno. ISBN 978-80-88298-10-6. s. 128.
[61] Stanovisko generálního advokáta Macieje Szpunara přednesené dne 4. března 2020 (1), věc C-61/19.
[62] Rozsudek Soudního dvora ze dne 1. října 2019, ve věci C-673/17.
[63] NEUWIRT, Karel. GDPR změní některé dosavadní zvyklosti. *Sdělovací technika*, 2017, 65(12), s. 10-11. ISSN 0036-9942.
[64] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 147.
[65] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 29.

žádného jiného titulu, který v Nařízení není uveden, a zároveň nesvědčí-li správci žádný z uvedených titulů, nesmí ke zpracování vůbec docházet[66], a to ani plní-li správce perfektně všechny své ostatní povinnosti[67].

3.1 Souhlas

Pojem souhlasu považujeme z pohledu ochrany osobních údajů za velmi důležitý, neboť je jedním z právních titulů, pouze na jejichž základě může správce zpracovávat osobní údaje subjektů údajů, ovšem je-li možné zpracovávat osobní údaje na základě jiného právního titulu, než je souhlas, má tento právní titul přednost a souhlas se již nevyžaduje. Důvodem je především možnost subjektu údajů souhlas kdykoli odvolat, což může správci způsobit potíže spojené se zpracováním takových údajů, proto údaje, které jsou zpracovávány na základě souhlasu, bývají tedy údaji, jejichž zpracování není nezbytné[68]. Typickým příkladem je zasílání newsletterů, obchodních sdělení, soutěže, či třeba zveřejnění fotografií zaměstnanců na webových stránkách, případně na sociálních sítích, zaměstnavatele[69].

Souhlas musí mít také určitou formu, nelze ho začlenit například do textu obchodních podmínek nebo smlouvy, musí být subjektem údajů určen ke konkrétnímu účelu[70], s čímž souvisí požadavek, dle kterého je správce povinen umět udělený souhlas se zpracováním osobních údajů doložit[71].

Nařízení také nově vyjasňuje otázku možnosti odvolání souhlasu subjektu údajů, kdy dává právo subjektu údajů svůj souhlas kdykoli odvolat. V době účinnosti předchozí úpravy totiž správce tuto svobodu často subjektu údajů neposkytoval, například subjekt údajů musel souhlas správci udělit na dobu předem

---

[66] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0., s. 16.
[67] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9., s. 67.
[68] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 82.
[69] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 86.
[70] *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: DonauMedia, s.r.o., [2018], ©2018. 96 s. ISBN 978-80-8183-049-5. s. 16-17.
[71] LUPIEŃSKÁ, Petra. Rozesílání obchodních sdělení prostřednictvím třetí strany a souhlas dle GDPR. *Epravo.cz* [online]. 2020, 10. 1. 2020 [cit. 2020-04-01]. Dostupné z: https://www.epravo.cz/top/clanky/rozesilani-obchodnich-sdeleni-prostrednictvim-treti-strany-a-souhlas-dle-gdpr-110440.html

určenou správcem či správce stanovoval, že jednou udělený souhlas již subjekt údajů nemůže odvolat[72].

3.2 Plnění smlouvy

Jsou-li správce a subjekt údajů společně ve smluvním vztahu, musí správce plnit určité povinnosti vůči subjektu údajů. K řádnému plnění ovšem správce potřebuje znát některé osobní údaje subjektu údajů, přičemž rozsah zpracovávaných údajů závisí na charakteru smlouvy. Může jít například o pracovní, darovací, zprostředkovatelskou či jinou smlouvu[73].

3.3 Plnění právních povinností správce

V určitých případech může správci stanovit povinnost zpracovávat osobní údaje zákon, případně právní předpis Evropské unie. V takovém případě má správce takovým právním předpisem určen účel zpracování, může mít stanoveny i kategorie osobních údajů ke zpracování určené[74].

3.4 Ochrana životně důležitých zájmů subjektu údajů

Životně důležitým zájmem subjektu údajů je především jeho život a zdraví, proto zpracování jeho údajů v zájmu ochrany jeho životně důležitých zájmů může znamenat například zpracování za účelem monitorování epidemií a přenosných chorob či pro humanitární účely[75].

3.5 Veřejný zájem

Ke zpracování osobních údajů ve veřejném zájmu dochází zejména při činnosti orgánů veřejné moci. Takovými správci jsou pak především obce, kraje či profesní komory. Veřejný zájem představuje právní důvod zpracování, u nějž je subjekt oprávněn vznést námitku proti takovému zpracování podle čl. 21 odst. 1 Nařízení[76].

---

[72] NEUWIRT, Karel. GDPR změní některé dosavadní zvyklosti. *Sdělovací technika*, 2017, **65**(12), s. 10-11. ISSN 0036-9942.
[73] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 28-29.
[74] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0., s. 81-82.
[75] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 29.
[76] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9., s. 82-83.

3.6 Oprávněný zájem správce

Převažují-li pro účely zpracování zájmy správce nad zájmy a základními právy a svobodami subjektu údajů, probíhá zpracování na základě oprávněného zájmu správce. Příkladem takového zájmu může být například instalace a provoz bezpečnostního opatření k zamezení podvodů[77].

4. Zásady zpracování osobních údajů

Základní zásady pro zpracování osobních údajů uvádí a zároveň popisuje přímo samotné Nařízení, a to v čl. 5. Tyto zásady tvoří obecná pravidla napříč veškerým zpracováním osobních údajů, zároveň je mohou správci osobních údajů pojmout za návod v situaci, nestačí-li jim pouze jazykový výklad právních norem[78].

Důležitost dodržování zásad pak podtrhuje 2. odst. čl. 5[79] ve spojení s 1. odst. čl. 24, neboť stanovuje nejenom odpovědnost správce za jejich dodržování, ale i povinnost správce být schopen jejich dodržování doložit[80] a zároveň zavést vhodná technická a organizační opatření k zajištění souladu s Nařízením tak, aby to byl zároveň schopen i doložit[81]. Dokládání souladu se zásadami přitom nepředstavuje jednorázovou povinnost správce, nýbrž nepřetržitý proces[82].

4.1 Zákonnost, korektnost a transparentnost

Zásada zákonnosti zpracování není uvedena na prvním místě náhodou, její význam je zásadní, neboť bez jejího dodržení vůbec nemůže ke zpracování dojít[83]. Znamená to, že správce musí mít vždy alespoň jeden právní důvod – titul k tomu, aby údaje subjektu údajů mohl zpracovávat a pakliže tato zásada není dodržena, správce zpracovává údaje nelegálně. Byla-li zásada zákonnosti nejprve dodržena,

---

[77] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 30.
[78] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 5.
[79] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 5.
[80] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). čl. 5 odst. 2.
[81] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). čl. 24 odst. 1.
[82] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 60.
[83] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0., s. 5.

pak ale správce právní důvod zpracování pozbyl a nemůže zároveň uplatnit důvod jiný, má povinnost zpracovávané údaje zlikvidovat[84].

Transparentnost pak představuje zákonný požadavek, aby vše se zpracováním osobních údajů související bylo snadno přístupné, srozumitelné a formulované jasně a jednoduše. Transparentnost zpracování zejména vyžaduje, aby subjekty údajů byly poučeny o totožnosti správce a účelech, jakými jsou zpracovávány jejich údaje[85]. Zároveň je potřebné, aby správce usnadnil subjektu údajů uplatnění výkonu jeho práv[86].

4.2 Účelové omezení

Zásada omezení účelu představuje závazek správce zpracovávat osobní údaje pouze pro určité, výslovně vyjádřené legitimní účely a zároveň nezpracovávat osobní údaje způsobem neslučitelným s takovými účely[87].

Pod pojmem účel zpracování se přitom skrývá důvod, pro něž správce osobní údaje zpracovává. Účel tak lze považovat za určitou limitaci správce osobních údajů při zpracování takovým způsobem, aby zpracovával osobní údaje pouze v jeho rámci.

Například zpracovává-li správce čísla bankovních účtů svých zaměstnanců, je to z důvodu plnění právní povinnosti zaměstnavatele, jenž vyplývá z pracovní smlouvy, kterou spolu uzavřeli. Konkrétním účelem je pak zasílání mzdy zaměstnanci. Číslo bankovního účtu pak lze zpracovat pouze za tímto účelem[88].

4.3 Minimalizace údajů

Zásada minimalizace údajů znamená povinnost zpracovávat pouze přiměřené a relevantní osobní údaje, a především zpracovávat je v omezeném rozsahu tak, aby nedocházelo ke zpracování více údajů, než je nezbytně nutné[89]. Správce je tedy povinný dbát účelu zpracování a nezpracovávat větší rozsah

[84] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 60-61.
[85] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 43.
[86] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0., s. 8.
[87] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9., s. 62.
[88] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0., s. 6-7.
[89] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9., s. 62-63.

osobních údajů, než jaký je přiměřený a odůvodněný ve vztahů k účelu zpracování[90].

4.4 Přesnost

Zásada přesnosti zahrnuje požadavek zpracovávat osobní údaje v přesné podobě a, je-li to potřeba, aktualizované. Nejsou-li totiž osobní údaje aktuální, jejich zpracování postrádá smysl. Správce nemusí aktivně pátrat po nepřesných údajích, nýbrž tato zásada mu ukládá povinnost opravit nebo vymazat nesprávný, nepřesný či neaktuální osobní údaj, požádá-li o to subjekt údajů nebo zjistí-li takovou nepřesnost správce sám[91].

4.5 Omezení uložení

Stejně tak jako rozsah zpracovávaných osobních údajů nesmí být neomezený, ani doba, po kterou budou osobní údaje zpracovávány, nesmí být neomezená.

Stanovení doby, po kterou smí správce osobní údaje zpracovávat pak může plynout ze smlouvy uzavřené mezi správcem a subjektem údajů, přičemž údaje smí být zpracovány pouze po dobu trvaní smluvního vztahu, nebo z právního předpisu[92].

Dokumenty obsahující osobní údaje určené k likvidaci ovšem není nezbytně nutné nevratně likvidovat, je-li to možné, lze je převést do anonymizované podoby. Výhodu této formy likvidace lze spatřovat ve skutečnosti, že anonymizované údaje smí správce dále využívat, má-li to pro něj nějaký význam[93]. Osobní údaje nelze uchovávat déle, než je nezbytně nutné a v takové formě, díky níž by bylo možné subjekt údajů identifikovat, na anonymizované údaje ovšem není pohlíženo jako na osobní údaje, ochrana údajů se tak ne ně neuplatní, a tedy anonymizací správce dospěje k podobnému výsledku jako jejich vymazáním[94].

---

[90] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 10.
[91] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 63-64.
[92] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 12.
[93] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 65.
[94] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 115.

4.6 Integrita a důvěrnost

Správce je povinen zajistit, aby se k osobním údajům dostaly pouze osoby k tomu oprávněné a současně aby byly osobní údaje zpracovávány pouze v přesné a správné podobě[95].

Zároveň ze zásady integrity a důvěrnosti plyne správci povinnost přijetí takových technických a organizačních opatření, aby bylo zabráněno neoprávněnému či protiprávnímu zpracování osobních údajů, jejich náhodné ztrátě, zničení a poškození[96]. Musí být tedy zajištěna důvěrnost a integrita systému, v němž správce osobní údaje zpracovává. Zároveň je správce při zabezpečování povinen zohlednit povahu, rozsah, kontext a účel zpracování[97].

V integritě a důvěrnosti je pak přímo promítnuta povinnost správce osobní údaje náležitě zabezpečit, a tedy také princip přístupu založeném na riziku. To znamená, že správce je povinen přijmout taková opatření, aby řádně zabezpečil osobní údaje, které zpracovává, s ohledem na charakter své činnosti, rozsah a účel zpracování osobních údajů[98].

4.7 Odpovědnost

Zásada odpovědnosti pak ukládá správci povinnost zpracovávat osobní údaje v souladu s Nařízením, za své zpracování nést odpovědnost a zákonnost zpracování umět též doložit[99].

5. Práva subjektů údajů

Nařízení přináší výčet práv, která má každý subjekt údajů v souvislosti se zpracováním jeho osobních údajů. Správce má povinnost se vždy zabývat, uplatní-li subjekt údajů některé ze svých práv, a také vyrozumět subjekt údajů o výsledku, přičemž uplatnění i vyřízení práva subjektu údajů je bezplatné[100].

---

[95] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 11.
[96] NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. První vydání. Praha: Klika, 2018. 141 s. Otevřeno. ISBN 978-80-88298-10-6. s. 130.
[97] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 65.
[98] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 11.
[99] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 15.
[100] NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. První vydání. Praha: Klika, 2018. 141 s. Otevřeno. ISBN 978-80-88298-10-6. s. 131.

Ovšem smí také žádost o uplatnění práva odmítnout, případně požadovat od subjektu údajů uhrazení nákladů se žádostí spojených, a to například v situaci, kdy impuls subjektu údajů postrádá přiměřenost, důvodnost nebo lze-li ji považovat za šikanózní[101].

5.1 Právo na přístup k osobním údajům

Subjekt údajů má právo podat správci žádost, jejímž předmětem může být dotaz, zda a případně jaké jeho údaje správce zpracovává, za jakými účely, jací příjemci mají přístup ke kterým jeho osobním údajům, po jak dlouhou dobu bude dané osobní údaje správce zpracovávat, případně jak dlouho budou u něj uloženy a smí-li požadovat opravu či výmaz. Žádá-li o to subjekt údajů, musí ho také správce informovat, zda smí podat stížnost u dozorového úřadu, pokud správce zpracovává některé údaje subjektu údajů, které získal od někoho jiného, než je subjekt údajů, musí subjektu osobních údajů sdělit veškeré dostupné informace o tomto zdroji údajů. Správce musí subjekt údajů také na žádost informovat, probíhá-li automatizované rozhodování, a to i včetně profilování[102].

5.2 Právo na opravu

Právo subjektu údajů na opravu a výmaz se odráží v zásadě přesnosti, jelikož správce musí zpracovávat osobní údaje subjektu údajů přesné a, je-li to potřeba, aktualizované. Zjistí-li subjekt údajů, že jeho osobní údaje správce zpracovává v neúplné, nepřesné, nesprávné či neaktuální podobě, má právo požádat správce o opravu či doplnění[103]. Správce pak musí žádost subjektu údajů zpracovat a informovat subjekt údajů o výsledku nejpozději do jednoho měsíce, přičemž má možnost lhůtu prodloužit[104].

[101] MATYSOVÁ, Monika a NONNEMANN, František. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, 26(12), s. 424-433. ISSN 1210-6410.
[102] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 118.
[103] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 138.
[104] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 100.

5.3 Právo na výmaz – „právo být zapomenut“

Nechce-li již subjekt údajů, aby správce nadále zpracovával jeho osobní údaje, má právo obrátit se na správce se žádostí o výmaz svých údajů. Je-li splněna jedna z podmínek, správce osobní údaje bez zbytečného odkladu vymaže[105].

Osobní údaje mohou být smazány, pokud již pro správce nejsou potřebné s ohledem na účel, pro který je zpracovává, pokud je právním titulem zpracování osobních údajů souhlas a subjekt údajů se rozhodl tento souhlas odvolat nebo pokud subjekt údajů uplatní právo vznést námitku a následně je shledán vyšší zájem subjektu údajů nad zájmem správce na zpracování osobních údajů subjektu údajů. Osobní údaje také musí správce smazat, pokud jejich zpracování probíhalo protiprávně, pokud povinnost vymazat osobní údaje správci ukládá právo Evropské unie nebo právo členského státu nebo pokud správce získal osobní údaje dětí v souvislosti s nabídkou služby informační společnosti[106].

Ovšem obdrží-li správce žádost subjektu údajů o výmaz osobních údajů, kromě posouzení, zda jsou splněny podmínky k výmazu, správce vždy posoudí uplatnitelnost výjimky. To znamená, že nařízení přináší ještě výčet situací, kdy správce není povinen osobní údaje vymazat, neboť se uplatní výjimka dle čl. 17 odst. 3 Nařízení[107]. Takovou situací je například výkon práva na svobodu projevu a informace nebo zpracování osobních údajů z důvodu veřejného zájmu v oblasti veřejného zdraví[108].

Nicméně výjimku nepředstavuje skutečnost, že osobní údaje jsou zpracovávány správcem prostřednictvím provozovny na území některého členského státu Evropské unie, zatímco správce se nachází mimo Evropskou unii. Požádá-li subjekt údajů o výmaz, správce musí smazat jeho osobní údaje nejen z databáze vedené na území Evropské unie, ale i z jakékoliv jiné databáze mimo Evropskou unii[109].

---

[105] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 33.
[106] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3., s. 210-211.
[107] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3., s. 212.
[108] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 33-34.
[109] Rozsudek Soudního dvora ze dne 24. září 2019, ve věci C-507/17

5.4 Právo na omezení zpracování

Kromě práva na výmaz též náleží subjektu údajů právo na omezení zpracování jeho osobních údajů. Rozdíl mezi těmito dvěma právy spočívá především v dočasnosti omezení, jelikož výmaz je oproti tomu trvalý. Subjekt údajů může žádat omezení zpracování, má-li za to, že jeho správcem zpracovávané údaje jsou nepřesné, a to právě na dobu, jíž je pro správce nezbytná k ověření přesnosti údajů, nebo také pokud zpracování neprobíhá legálně, ale subjekt údajů se rozhodl upřednostnit omezení zpracování před výmazem svých údajů. Také nastane-li situace, že subjekt údajů žádá správce o své osobní údaje z důvodu určení, výkonu nebo obhajoby právních nároku, ačkoli osobní údaje již správce nepotřebuje zpracovávat, nebo subjekt údajů uplatnil své právo vznést námitku proti zpracování a prozatím není rozhodnuto, zda převažují oprávněné zájmy správce či subjektu údajů, i tehdy smí subjekt uplatnit své právo omezení zpracování osobních údajů[110].

Po omezení zpracování osobních údajů smí správce zpracovávat tyto osobní údaje, pouze souhlasil-li subjekt údajů s takovým zpracováním. Ovšem výjimku, za které správce smí tyto údaje zpracovávat i bez souhlasu subjektu údajů, tvoří případy, kdy zpracování probíhá za účelem určení, výkonu nebo obhajoby právních nároků, ochrany práv jiné fyzické či právnické osoby nebo je-li zde důležitý veřejný zájem Evropské unie nebo některého z členských států[111].

5.5 Právo na přenositelnost osobních údajů

Nařízení poskytuje subjektu údajů právo, při jehož uplatnění obdrží své osobní údaje, které správce zpracovává, a to ať už tyto údaje poskytl správci sám, nebo správce zpracovává osobní údaje, které se týkají subjektu údajů, i když mu byly poskytnuty třetí osobou. Přenositelnost údajů také znamená, že subjekt údajů smí po správci požadovat, aby jeho osobní údaje předal jinému správci[112]. Subjekt údajů má právo na přenositelnost, dochází-li ke zpracování na základě právního titulu souhlasu nebo probíhá zpracování automatizovaně[113].

---

[110] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 141.
[111] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 34
[112] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 104-105.
[113] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 220-221.

5.6 Právo vznést námitku

Právo vznést námitku poskytuje subjektu údajů možnost kdykoli se obrátit na správce a vznést námitku proti zpracování jeho osobních údajů, a to zpracovává-li správce osobní údaje na základě veřejného zájmu nebo oprávněných zájmů správce. Pakliže správce nedokáže doložit skutečnost, že ke zpracování ho vedou oprávněné závažné důvody, které převyšují zájmy subjektu údajů, osobní údaje již nadále nesmí zpracovávat[114].

Zpracovává-li správce osobní údaje subjektu údajů se záměrem přímého marketingu, dává Nařízení subjektu údajů právo vznést námitku proti zpracování osobních údajů kdykoliv a bezplatně, zároveň by měl o tomto právu být správcem informován[115].

5.7 Právo nebýt předmětem automatizovaného individuálního rozhodování

Na právo vznést námitku pak navazuje právo nebýt předmětem automatizovaného individuálního rozhodování, jež by pro subjekt údajů představovalo právní nebo obdobné účinky, přičemž toto právo se vztahuje i na profilování[116].

Automatizované individuální rozhodování znamená, že zpracování probíhá podle dopředu určeného algoritmu. Cílem ustanovení, které automatizované individuální rozhodování upravuje, pak je regulace automatizovaných postupů tak, aby zpracování probíhalo transparentně a subjekt údajů získal šanci bránit se proti případnému nezákonnému zásahu do jeho práv[117].

„*Profilování je podle článku 4 odst. 4 Nařízení GDPR jakákoliv forma automatizovaného zpracování osobních údajů spočívajících v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektu týkajících se jejích pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování,*

[114] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 147-148.
[115] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. s. 76.
[116] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 148.
[117] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3., s. 232.

místa pohybu nebo pobytu.“[118] Profilováním je například sběr informací z rozlišných veřejných nebo soukromých zdrojů pro rozlišování subjektů údajů do kategorií dělících se podle volnočasových zájmů za účelem cílené reklamy[119].

5.8 Právo podat stížnost u dozorového úřadu

Má-li subjekt údajů za to, že správce zpracovává jeho osobní údaje v rozporu s Nařízením, má právo podat stížnost u dozorového úřadu, kterým je v České republice Úřad pro ochranu osobních údajů. Ten má povinnost subjektu údajů sdělit, k jakému výsledku v průběhu šetření stížnosti došel a zda se smí za účelem své ochrany obrátit na soud[120].

5.9 Právo na účinnou soudní ochranu

Právo na účinnou soudní ochranu subjektu údajů se vztahuje jak vůči dozorovému úřadu, tak také vůči správci či zpracovateli.

Nařízení přináší právo bránit se proti právně závaznému rozhodnutí, které vydal dozorový úřad a týká se bránícího se subjektu údajů, zároveň ale také proti dozorovému úřadu, který nečiní žádné kroky k vyřešení stížnosti subjektu údajů nebo subjekt údajů do tří měsíců nepoučí, v jakém stavu se nachází řešení jeho podané stížnosti.

Zároveň má subjekt údajů právo na účinnou soudní ochranu v situaci, kdy podle něho došlo k porušení jeho práv vyplývajících z Nařízení v souvislosti se zpracováním jeho osobních údajů[121].

5.10 Právo na zastupování subjektů údajů

Nařízení dává subjektu údajů právo nechat se zastupovat při podání stížnosti u dozorového úřadu, při uplatnění práva na účinnou soudní ochranu vůči dozorovému úřadu, správci nebo zpracovateli či práva na náhradu újmy, uplatnil-li

[118] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 37.
[119] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 37.
[120] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 107.
[121] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 40.

právo na odškodnění. Subjekt údajů může pověřit zastupováním neziskový subjekt, organizaci nebo sdružení[122].

5.11 Právo na náhradu újmy a odpovědnost

Subjekt údajů má právo na náhradu újmy, pokud jednání správce nebo zpracovatele v rozporu s Nařízením způsobilo jeho majetkovou nebo nemajetkovou újmu. Odpovědnost správce zakládá zpracování, které správce provádí a není v souladu s Nařízením, zatímco odpovědnost zpracovatele nastává pouze v situaci, kdy zpracovatel nedodržel povinnosti, které mu ukládá Nařízení, nebo pokud jeho jednání přesahovalo zákonné instrukce správce[123].

5.12 Právo odvolat souhlas

Nařízení rovněž poskytuje subjektu údajů kdykoli odvolat souhlas, který správci udělil za účelem zpracování jeho osobních údajů. Účinky, které takové odvolání vyvolá, představují pro správce ztrátu právního titulu ke zpracování osobních údajů subjektu údajů, musí tedy osobní údaje zlikvidovat[124].

[122] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 473.
[123] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 40-41.
[124] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 151.

Praktická část

1. Proces implementace GDPR

1.1 Uvedení do implementace

Tato část diplomové práce se již bude zaměřovat přímo na samotný proces implementace GDPR, který se skládá z několika na sebe navazujících částí, přičemž každá část bude podrobně rozepsána a vždy bude uvedeno, co všechno každá z částí obnáší. Budou zde tedy popsány jednotlivé kroky procesu zavádění Nařízení do praxe, činnosti správce.

Implementace GDPR znamená zavedení všech pravidel a postupů, které Nařízení přináší, do praxe a jejich následné udržování, úprava a případně také doplnění dokumentace do takové podoby, aby byla v souladu s Nařízením, seznámení sebe i svých zaměstnanců s Nařízením a povinnostmi, ale i právy s ním spojenými, znamená to uvedení skutečného stavu do naprostého souladu s Nařízením, tedy realizace Nařízení a následné dlouhodobé udržování zavedených opatření.

Samotné uvedení Nařízení do praxe představuje vždy to stejné, tedy koncový stav po každé implementaci by měl být vždy stejný, to znamená, že na konci procesu by měly být všechny dokumenty upravené v souladu s Nařízením, případně dokumenty, které chyběly a Nařízení je vyžaduje, by měly být doplněné a personál dostatečně vyškolený, každý by měl znát, jaké povinnosti mu Nařízení přináší, tyto povinnosti by měli všichni dodržovat a také by měli všichni vědět, jakých práv se smí na základě Nařízení dožadovat.

Celý proces zahrnuje několik dílčích částí, přičemž přesné hranice jednotlivých fází implementace GDPR nejsou oficiálně stanoveny, proto je každý správce, který implementaci provádí, může vidět lehce odlišně. V této práci bude rozčleněna na celkem čtyři, a to na studium, tedy před samotnou implementací je nejprve důležité se s Nařízením řádně seznámit, přípravnou část, která zahrnuje sestavení auditu nakládání s osobními údaji společně s analýzou a hodnocením rizik, revizi dokumentace a smluv, návrhy opatření potřebných k zajištění souladu s Nařízením a vypracování směrnice pro zpracování a ochranu osobních údajů, případně úpravu dalších interních předpisů, realizační část, ve které už pak dochází k zavedení navržených opatření do praxe a školení personálu a nakonec praxi, jelikož splněním předchozích bodů povinnosti správce nekončí a je potřeba vše dlouhodobě

udržovat. Při praxi se dohlíží na dodržování všech principů a povinností a neustále se vzdělává personál.

2. Studium

2.1 Studium právních předpisů

Nařízení přináší řadu nových pojmů, práv, povinností i principů spojených s ochranou osobních údajů, proto před započetím implementace je nutné nejprve se s jeho zněním řádně seznámit. Tato fáze je nepochybně velice důležitá, neboť bez ní by nebylo možné s implementací vůbec započít, nicméně po jejím provedení zpravidla není nutné ji při udržování žádoucího stavu opakovat v plném rozsahu, získané vědomosti zůstávají a na místě je pouze občasné, ale přesto pravidelné, doškolování a informování se o nejnovějším vývoji celého oboru.

O to důležitější je ale tuto fázi nepodcenit. Čím důkladněji je provedena tato fáze před implementací, o to snáze se bude dále Nařízení implementovat a žádoucí stav udržovat a tím méně bude nutné se k různým pojmům nebo principům vracet.

Při studiu samozřejmě nejlépe poslouží samotné plné znění Nařízení a zákon č. 110/2019 Sb., o zpracování osobních údajů. Tento zákon byl přijat jako adaptační zákon, jehož úkolem je blíže upřesnit či rozvinout ustanovení Nařízení, také se ale v určitých oblastech od Nařízení odklání a aplikuje tak možnost vymezit určité výjimky[125], a to například v oblasti způsobilosti dítěte k udělení souhlasu se zpracováním osobních údajů, kdy stanovil hranici pro udělení souhlasu na 15 let věku[126], což znamená, že Nařízením stanovenou hranici snížil o jeden rok[127]. Dále pak správci pomůže upřesnit nejasnosti Komentář, ale užitečné budou i odborné publikace zabývající se teoretickým vysvětlením Nařízení i prakticky zaměření průvodci implementací Nařízení, kterých je na trhu v současné době již velké množství.

[125] CETKOVSKÁ, Barbora a Jakub MÁLEK. Adaptační zákon k GDPR byl konečně přijat. *Epravo.cz* [online]. Praha: epravo.cz, 2019, 3. 4. 2019 [cit. 2020-03-22]. Dostupné z: https://www.epravo.cz/top/clanky/adaptacni-zakon-k-gdpr-byl-konecne-prijat-109122.html

[126] Zákon č. 110/2019 Sb., *zákon o zpracování osobních údajů*. § 7

[127] CETKOVSKÁ, Barbora a Jakub MÁLEK. Adaptační zákon k GDPR byl konečně přijat. *Epravo.cz* [online]. Praha: epravo.cz, 2019, 3. 4. 2019 [cit. 2020-03-22]. Dostupné z: https://www.epravo.cz/top/clanky/adaptacni-zakon-k-gdpr-byl-konecne-prijat-109122.html

V současné době, kdy je nařízení již účinné a všichni správci by jej měli znát, měli by se jím řídit a svoji činnost provozovat v souladu s ním, by se mohlo zdát, že je již tato fáze implementace neaktuální. Ovšem není vyloučeno, naopak je velice pravděpodobné, že budou stále vznikat noví a noví správci nových organizací, kteří sice nebudou původní zpracování přizpůsobovat požadavkům Nařízení, jak byli povinni učinit správci před účinností Nařízení, protože se zpracováním teprve začnou, a žádné původní zpracování se jich tak netýká, ale před spuštěním své činnosti se s Nařízením budou muset důkladně seznámit, aby od počátku probíhalo zpracování jakýchkoli osobních údajů v naprostém souladu s Nařízením. Z tohoto pohledu se tedy část implementace zvaná studium Nařízení nestane neaktuální nikdy po celou dobu účinnosti Nařízení.

2.2 Vývoj oboru ochrany osobních údajů

Nelze vést pochybnosti o tom, že právní úprava a celý obor ochrany osobních údajů se stále vyvíjí, a i nadále se bude neustále vyvíjet. Už jen doposud prošel vývoj několika etapami, kdy nejprve v roce 2016 vstoupilo Nařízení v platnost, v roce 2018 pak v účinnost a dále v roce 2019 byl na národní úrovni v České republice přijat adaptační zákon č. 110/2019 Sb., o zpracování osobních údajů.

Úřad pro ochranu osobních údajů provádí a bude provádět dozorovou činnost v souladu se zákonem č. 255/2012 Sb., o kontrole, č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich a č. 500/2004 Sb., správní řád, což je jeho klíčovým úkolem[128]. Ideální, ovšem ne příliš pravděpodobnou situací by bylo, pokud by Úřad pro ochranu osobních údajů při dozorové činnosti žádná pochybení neodhalil, protože všichni správci dbají svých povinností. Ovšem na to se nelze spoléhat, a tak se i Úřad pro ochranu osobních údajů bude dozorovou činností podílet na vývoji oboru ochrany osobních údajů, jelikož nejen že sám provádí kontrolu v rámci zjišťování souladu s Nařízením a případně soulad vymáhá, ale také se zabývá stížnostmi subjektů údajů[129].

[128] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Dozorová a rozhodovací činnost* [online]. [cit. 2020-03-30]. Dostupné z: https://www.uoou.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277

[129] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Dozorová a rozhodovací činnost* [online]. [cit. 2020-03-30]. Dostupné z: https://www.uoou.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277

Lze předpokládat ale i vývoj judikatury v oblasti ochrany osobních údajů, jelikož pokud subjekt údajů nebude spokojen s výsledkem řízení před Úřadem pro ochranu osobních údajů, smí se dále bránit ve správním soudnictví, neboť vysoký počet takových rozhodnutí lze soudně přezkoumat[130].

Jelikož je ovšem Nařízení předpisem Evropské unie, promítne se zde i evropský prvek. Nastane-li situace, kdy si soud členského státu nebude jistý s aplikací Nařízení tak, aby nevybočil z jednotnosti jeho výkladu, smí podat předběžnou otázku k Soudnímu dvoru Evropské unie[131]. Právo podat předběžnou otázku je již využíváno, a tak tyto i případné další předběžné otázky pak budou předmětem studia, neboť mohou správci pomoci objasnit situace, kdy mu není výklad Nařízení jasný.

Zároveň ovšem dohlíží na dodržování všech požadavků Nařízení Evropský sbor pro ochranu osobních údajů, nyní zvaný již pouze sbor. Ten představuje nejvyšší dozorový orgán v oblasti ochrany osobních údajů, jehož činnost se soustředí na správnou aplikaci Nařízení u všech členských států Evropské unie, která má probíhat především jednotně[132].

Sbor dále například poskytuje součinnost Komisi v podobě poradenství v oblastech týkajících se ochrany osobních údajů v Evropské unii[133], pomáhá se společnými školícími programy, výměnou vědomostí a listin. Je také provozovatelem elektronického registru rozhodnutí, jež byla přijata dozorovými úřady a soudy v oblasti soustavy jednotnosti, a jenž je veřejně dostupný[134].

3. Příprava implementace

Přípravná část implementace představuje proces, jenž zahrnuje detailní zmapování současné situace zpracování osobních údajů, její vyhodnocení, návrhy eliminace případných rizik a následnou úpravu veškeré dokumentace, a to do

[130] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 151.
[131] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 181.
[132] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 160.
[133] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 161.
[134] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 166.

takové podoby, aby byla v souladu s Nařízením, a zároveň odstranění nežádoucích a zavedení správných postupů v souladu s Nařízením.

V této fázi také správce dokončí vnitřní směrnici pro zpracování a ochranu osobních údajů, seznámí s ní své zaměstnance a dohlédne, aby všichni řádně rozuměli svým povinnostem, jež jim z Nařízení vyplývají. Může také případně zvážit vytvoření protokolu o seznámení se směrnicí. Upraví také další své užívané vnitřní předpisy do podoby souhlasící s Nařízením.

3.1 Audit osobních údajů

Audit osobních údajů je prvním krokem ke zjištění současné situace týkající se ochrany, sběru, uchovávání osobních údajů a osobních údajů vůbec v dané organizaci, ve které se implementace provádí.

Audit lze přitom provádět různými metodami. Jelikož je audit dokument sloužící pouze správci k další práci, přizpůsobení se Nařízení a úpravě nevhodných postupů a dokumentů, záleží pouze na správci, jaký postup v hodnocení současné situace zvolí. Může použít například SWOT nebo gap analýzu.

3.1.1 SWOT analýza

Termín SWOT představuje zkratku z počátečních písmen slov strenghts, weaknesses, opportunities a threats, jež představují předmět zájmu této analýzy. SWOT analýza se tedy zabývá silnými a slabými stránkami, příležitostmi a hrozbami zkoumané organizace. Patří mezi základní postupy analýzy, když při jejím tvoření jsou srovnávány silné a slabé stránky zkoumané organizace společně s možnými příležitostmi a hrozbami vyhodnocenými za daných okolností[135]. „*Analýza spočívá v rozboru a hodnocení současného stavu organizace (vnitřní prostředí) a současné situace okolí organizace (vnější prostředí).*“[136]

3.1.2 Gap analýza

Gap analýza oproti tomu zkoumá mezery a rozdíly mezi aktuálním stavem a plánovanou situací. Metoda používaná v rámci gap analýzy tedy spočívá

[135] GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. Brno: Computer Press, 2010. ISBN 978-80-251-2621-9. s. 295-296.
[136] GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. Brno: Computer Press, 2010. ISBN 978-80-251-2621-9. s. 297.

v představení si pravděpodobného vývoje a s ním spojenými možnými hrozbami pro organizaci, přičemž možné hrozby plynou z porovnání aktuální a plánované situace, cílů a možného dosažení dalších cílů v delším časovém úseku. Zaměření se na možná negativa a nedostatky pak pomůže přizpůsobit situaci a využít znalost možných hrozeb k snazšímu dosažení svých cílů[137].

Gap analýza pak stojí na pěti postupných krocích, které vytváří konečný celek. Nejprve se jedná o kontrolní část, kdy správce posoudí aktuální systém práce se všemi součástmi, které ho tvoří. Poté si určí, jakého cíle chce dosáhnout a následně srovná současnou a plánovanou situaci. V dalším kroku se zamyslí nad možnými riziky spojenými s přechodem k cílovému stavu, a nakonec vyhledá vhodná opatření k eliminaci zjištěných rizik[138]. V průběhu provádění analýzy přitom správce vyhledává, na jakých místech jsou u něj osobní údaje shromažďovány, kdo se může k osobním údajům dostat, jakým způsobem jsou osobní údaje ukládány či jakým způsobem správce získal od subjektu údajů souhlas se zpracováním jeho osobních údajů[139].

V konečném výsledku pak vytvoření gap analýzy znamená podrobné zmapování současného stavu všech operací či uložišť správce s přihlédnutím k mezerám, jež vyplynuly z porovnání s budoucím plánovaným stavem[140].

3.1.3 Vytvoření auditu metodou gap analýzy

Ačkoli je rozhodnutí zcela na správci, metoda gap analýzy se v případě implementace Nařízení a přechodu k požadovanému stavu jeví jako vhodnější a účelnější než zmiňovaná SWOT analýza, neboť gap analýza se přímo soustředí na mezery, možné chyby, rizika a hrozby a slouží k jejich předejití. Naopak metodika SWOT analýzy se kromě hrozeb zabývá i silnými a slabými stránkami a případnými příležitostmi, což pro správce v průběhu implementace Nařízení nepředstavuje rozhodující informace. Pro správce je důležité mít podrobný přehled o současné situaci, jasnou vizi o budoucím stavu, který nastane po dokončení

[137] GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. Brno: Computer Press, 2010. ISBN 978-80-251-2621-9. s. 232-233.
[138] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. str. 141.
[139] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 96
[140] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. s. 170.

implementace[141] a zároveň potřebuje odhalit, jaká rizika mohou z jakékoliv jeho činnosti s ohledem na současnou a budoucí situaci plynout, aby jim mohl snáze předcházet. Popis splnění takového účelu pak lépe vystihuje právě spíše metodika gap analýzy, proto bude praktický popis vytvoření auditu správcem užívat právě metodu gap analýzy.

K tomu, aby mohl být audit proveden co nejpřesněji, potřebuje si správce shromáždit veškeré dokumenty, ve kterých se mohou vyskytovat jakékoliv osobní údaje fyzických osob. Obvykle to ovšem nebývají pouze dokumenty, kde se osobní údaje vyskytují, proto si správce dále potřebuje vytvořit přehled všech možných uložišť společně s výčtem osobních údajů, které se v nich nacházejí a informací, jakým způsobem tyto údaje získal. Takovými uložišti zpravidla bývají telefony, počítače, listinné diáře a kalendáře či různé elektronické databáze. Nesmí zapomenout ale ani na webové stránky, případně facebookové a instagramové profily nebo profily na jiných sociálních sítích, neboť i tam se zpravidla určité osobní údaje nacházejí.

Veškeré takto sesbírané údaje si správce systematicky poznamená a dále k nim uvede, kde se které konkrétní údaje nacházejí – tedy zda v počítači, telefonu, internetovém uložišti nebo diáři, kdo je subjektem těchto údajů, do jaké kategorie osobních údajů konkrétní údaj patří – tedy zda se jedná o údaj obecný či zvláštní, jaký je účel zpracování tohoto údaje – například poskytování služeb, plnění smlouvy, zajištění komunikace nebo třeba zajištění financování. Zapíše také, na základě jakého právního titulu je tento údaj zpracováván – tedy uvede jeden z právních titulů zpracování dle Nařízení a dospěje-li ke zjištění, že konkrétní osobní údaj nezpracovává na základě žádného z uvedených titulů, jedná se o nezákonné zpracování a tento údaj dále nesmí zpracovávat a musí ho zlikvidovat. Dále uvede, kde je uložen – v archivu nebo internetové databázi, ve skříni nebo v polici, na pracovním stole nebo například v paměti telefonu, a jací příjemci k němu mohou mít přístup – například externí zpracovatel účetnictví či poskytovatel webhostingových služeb.

Správce si také vytvoří přehled všech operací, které u něho v souvislosti se zpracováním osobních údajů probíhají. To znamená, že další bod auditu bude znázorňovat shrnutí postupů, které zahrnují jakoukoliv práci s osobními údaji, ať

[141] JIRÁKOVÁ, Gabriela a KALAŠOVÁ, Lucie. Praktický pohled na GDPR. *Právní rádce*. 2018, roč. 26, č. 4, s. 38-40. ISSN 1210-4817.

už se jedná o jejich shromáždění, uložení, evidenci, použití, přenos, šíření či publikaci nebo zpřístupnění zpracovateli. Takto označené zpracování pak správce ještě blíže popíše, resp. uvede, co konkrétně znamená daná operace u jednotlivého zpracování osobního údaje.

Výsledkem popsané práce pak bude podrobný rozbor, který bude tvořit základ každého dalšího postupu v procesu implementace a k němuž se bude správce v průběhu implementace vracet. Bude tvořit tzv. zrcadlo současného stavu, od kterého se správce odrazí a do kterého vždy nahlédne, aby zjistil, co vše je potřeba zajistit a co podmínkám Nařízení vyhovuje. Audit se tedy nesestavuje do takové podoby, jak by mělo zpracování správně vypadat a probíhat, ale jak skutečně aktuálně vypadá a probíhá, aby se mohlo do požadovaného stavu přeměnit.

Rozsah auditu přitom nezávisí na velikosti organizace, ale spíš na její činnosti a na tom, jaké údaje ke své činnosti potřebuje sbírat. I malá organizace s pouze pár zaměstnanci se může zaměřovat na činnost, k níž potřebuje velké množství osobních údajů, stejně tak velké organizaci může stačit naprosté minimum údajů. Například významná společnost s velkým množstvím zaměstnanců podniká v oblasti, při jejíž činnosti nepřichází do kontaktu s fyzickými, ale pouze právnickými osobami. Jejími klienty, smluvními partnery, objednateli či zadavateli jsou pouze právnické osoby. Pak jediné osobní údaje, které tato společnost zpracovává, jsou údaje zaměstnanců. Jedná se tedy o poměrně malé množství osobních údajů nezbytných k plnění pracovních smluv, případně prezentaci zaměstnanců na webových stránkách a sociálních sítích.

Provádí-li implementaci Nařízení v dané organizaci někdo jiný než správce, to znamená, nechal-li si správce implementaci Nařízení někým zpracovat, zkonzultuje ten, kdo implementaci provádí, obsah auditu se správcem po jeho sestavení ještě před tím, než se pustí do dalších kroků. Zejména správce musí zkontrolovat, zda obsah souhlasí se skutečností a žádná informace nechybí, a může se z něj tak vycházet pro další práci. Chybějící nebo nesprávný údaj by mohl způsobit nepřesnosti v dalších krocích, proto je úplnost, správnost a přesnost všech údajů v auditu zásadní.

3.1.4 Příklady výskytu osobních údajů

Shromáždění osobních údajů, které se u správce vyskytují v dokumentech, a to ať se jedná o listinnou nebo elektronickou dokumentaci převedenou do

elektronické podoby například pomocí konverze či skenu, by pro správce nemělo představovat výrazné komplikace. Hlavní podíl bude představovat pravděpodobně smluvní dokumentace a dále případně souhlasy se zpracováním osobních údajů a osobní údaje se zde budou vyskytovat většinou hned v hlavičce a bude se jednat především o jméno, příjmení, datum narození či rodné číslo a adresu.

Telefonní, e-mailové či listinné diáře jsou k ukládání osobních údajů přímo určené a obsahují nejčastěji jméno, příjmení, telefonní číslo a e-mailovou adresu.

Na webových stránkách se většinou osobní údaje objevují v medailoncích zaměstnanců, kde nalezneme osobní údaje v různém rozsahu, informující o jejich pracovním zaměření nebo pozici, případně vzdělání, společně s fotografií a kontaktem. Další zdroj osobních údajů pocházející z webu také představují kontaktní formuláře, do nichž zájemce uvádí své jméno a kontaktní údaje, nejčastěji e-mail nebo telefon. U sociálních sítí se pak jedná převážně o fotografie, případně jméno a příjmení, mohou se objevit ale i údaje o zaměstnancích či klientech nebo smluvních partnerech, a dále pak případně údaje, které zájemce sdělí při kontaktování organizace do soukromé zprávy.

3.1.5 Příklady postupů zpracování osobních údajů

Zpracování osobních údajů zahrnuje například jejich uložení nebo zaevidování, což v praxi znamená, že správce uložil dokumenty, které obsahují osobní údaje, do archivu, trezoru, skříně, police či je zapsal do elektronické databáze, která představuje jeho evidenci.

Vyhledání a použití osobních údajů může představovat různé činnosti vždy s ohledem na to, kde se dané osobní údaje, které zrovna správce používá, nacházejí. Například jedná-li se o osobní údaje z životopisu subjektu údajů, použití znamená přípravu na pohovor, vedení výběrového řízení a výběr vhodného kandidáta na vypsanou pozici. Jsou-li používanými osobními údaji osobní údaje získané z již uzavřené smlouvy, představuje vyhledání nalezení konkrétních údajů, které správce potřebuje a použití pak splnění jeho povinností, které mu vyplývají ze smlouvy. Například správce si vyhledá číslo účtu zaměstnance, aby mohl splnit svou povinnost uhrazení mzdy zaměstnanci vyplývající z pracovní smlouvy. Nebo správce provozující internetový obchod si vyhledá adresu subjektu údajů, aby mohl splnit svou povinnost odeslání objednaného zboží vyplývající z kupní smlouvy.

Typický příklad šíření a publikace může znázorňovat uvádění informací na webových stránkách či profilech na sociálních sítích. Správce zveřejní fotografii se svým týmem zaměstnanců se snahou o šíření povědomí o jeho organizaci či zveřejní kontaktní údaje na své zaměstnance za účelem publikace kontaktů, které mohou případní zákazníci, klienti či subjekty údajů použít, chtějí-li se na správce obrátit s dotazem, žádostí, snahou o navázání spolupráce nebo například objednávkou. Správce zveřejní kontaktní údaje na různé zaměstnance s popisem, kteří zaměstnanci provádějí kterou konkrétní agendu. Urychlí tak čas potřebný k vyřízení požadavku, neboť předejde situaci, kdy si zaměstnanci budou nejprve předávat informace a rozdělovat úkoly a celý proces se tak právě o tyto úkony prodlouží, zatímco kontaktuje-li subjekt údajů konkrétního pracovníka rovnou, sdělí přímo jemu veškeré potřebné informace a vyřizování požadavku může začít ihned.

Zpřístupní-li správce osobní údaje zpracovateli, znamená to, že se jedná o zpracovatele, se kterým spolupracuje a měli by mít společně uzavřenou zpracovatelskou smlouvu. Správce například zpřístupní osobní údaje v rozsahu jméno, příjmení a adresa za účelem vystavení faktury externím zpracovatelem účetnictví.

O poskytnutí osobních údajů zpracovateli se nejedná, prodá-li správce jinému správci databázi osob za účelem rozšíření klientely správce, který databázi kupuje. Takové zpracování již většinou nebude možné[142].

3.2 Posouzení vlivu na ochranu osobních údajů

Anglické spojení Data Protection Impact Assessment v češtině znamená posouzení vlivu na ochranu osobních údajů, někdy též znázorňované pouze pod zkratkou DPIA, která vychází právě z prvních písmen slov v anglickém názvu a představuje povinnost opírající se o zodpovědnost správce[143].

Povinnost provést před zpracováním posouzení vlivu na ochranu osobních údajů přináší Nařízení správcům ve svém čl. 35. Ovšem plyne pouze těm správcům, kteří vyhodnotí pravděpodobnost vysokého rizika pro subjekty osobních údajů

[142] HLADÍK, Martin, HRUŠKA, Jan a KRAMER, Jaroslav, ed. Osobní údaje 2018. *Právní rádce*, 2018, 26(4), s. 16-18. ISSN 1210-4817.
[143] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 98-99.

a jejich práva a svobody s ohledem na využívání pokrokových technologií, charakter, rozsah, účel a souvislosti zpracování[144].

K takovému zpracování by mohlo docházet zejména ve třech případech. Zpracovává-li správce obsáhle a uspořádaně za účelem vyhodnocování osobních hledisek, které se týkají subjektů údajů, zároveň probíhá zpracování automatizovaně, a to i pomocí profilování. Takové zpracování pak vede k rozhodnutí, které by mohlo subjektu údajů způsobit závažný dopad, například v podobě právních účinků. Dále je posouzení vlivu na ochranu osobních údajů nezbytné učinit v případě, že správce zpracovává citlivé osobní údaje v širokém rozsahu nebo zpracovává-li osobní údaje, které se vztahují k trestním věcem nebo trestným činům jmenovaným v čl. 10 Nařízení. Nakonec také musí správce posoudit vliv na ochranu osobních údajů tehdy, monitoruje-li obsáhle a uspořádaně veřejné prostory[145].

3.2.1 Analýza rizik

Ovšem neodpovídá-li charakter správcovy činnosti ani jedné z popsaných možností, které zakládají povinnost vytvoření posouzení vlivu na ochranu osobních údajů, je i tehdy vhodné, aby se správce zamyslel nad možnými hrozbami, které by mohly vyvstat osobním údajům a právům či svobodám subjektů údajů v souvislosti s jeho zpracováním.

Další krok při implementaci Nařízení by tak měl vést k analýze a hodnocení rizik, jenž přehledně shrnuje systematicky uspořádané skupiny osobních údajů společně s hodnocením, zda hrozí těmto údajům nějaká rizika, případně jaká a co je jejich zdrojem, se zdůvodněním, proč by taková rizika mohla nastat a s doporučeními, jak jim lze zabránit či rovnou předejít a zároveň bezprostředně navazuje na právě vytvořený audit.

Při zpracování analýzy se správce snaží představit si všechna možná rizika, která by eventuálně mohla nastat, klidně až v absurdních rozměrech. Rozdělí si je do kategorií podle toho, zda by v případě, že by k nim došlo, znamenala zničení, ztrátu, pozměnění či neoprávněné zpřístupnění a zároveň co by každou z těchto

[144] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 127.
[145] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 101-102.

kategorií rizik mohlo způsobit. Tedy zda by takové riziko mohl způsobit nesprávný přístup či chování zaměstnanců, špatné zabezpečení pracovního prostředí, zda by hrozbu mohl představovat nedostatek financí, chyba na straně technických prostředků či nesprávný přístup externích zpracovatelů. Takovéto rozdělení pomůže správci lépe od sebe oddělit případná možná rizika a tím pádem i přiřadit ke každému z nich individuální postup pro předejití či snížení rizika. Účinkem bude bezpečnější zpracování osobních údajů, neboť čím individuálněji bude označeno každé riziko, tím pravděpodobnější je skutečnost, že postup pro jeho eliminaci bude funkční a efektivní.

V dalším kroku analýzy rizik pak správce určí, jak vysoká je pravděpodobnost, že takové riziko skutečně nastane a jaký by měl dopad jeho důsledek. Ke každému riziku pak doporučí vhodná opatření, kterými jim lze předejít nebo je alespoň eliminovat.

3.2.2 Příklady možných rizik a hrozeb a jejich eliminace

U listinných dokumentů s osobními údaji by například mohlo dojít k jejich zničení v důsledku požáru či povodní, což by mohlo být způsobeno nedostatečným zabezpečením pracovního prostředí. Takové situace lze eliminovat například vhodnými protipožárními opatřeními, jako je přítomnost hasícího přístroje v prostorách sídla správce, vypojování rychlovarné konvice po použití z elektřiny nebo zákaz kouření v prostorách sídla správce.

Dále by mohlo dojít k jejich ztrátě, a to nechtěným vyhozením do odpadků bez dostatečné likvidace údajů například skartací. Takovou situaci by způsobilo nesprávné zacházení zaměstnanců a v důsledku by mohlo nastat kromě ztráty také neoprávněné zpřístupnění, neboť by se osobní údaje mohly snadno dostat ke třetím osobám. Riziko ztráty lze v takovém případě eliminovat zákazem vynášení listin z prostor sídla správce, pokud to není nezbytně nutné, neoprávněné zpřístupnění zase povinností likvidovat listiny vždy po určité době například v souladu se skartačním řádem. Nemá-li správce skartační a archivační řád, lze doporučit jeho vyhotovení. Ten by stanovoval evidenci, uchovávání, ukládání a následnou likvidaci všech dokumentů s osobními údaji.

Listinné dokumenty by také mohl klient, smluvní partner či jiná osoba, která není správcem ani zaměstnancem správce a vyskytuje se v prostorách, kde se osobní údaje nacházejí, odcizit. Tento stav by mohl být způsoben nedostatečným

zabezpečením pracovního prostředí, selháním lidského faktoru, který na dokumenty dostatečně nedohlíží, ale i nedostatkem financí, v jehož důsledku si správce nemůže dovolit dostatečné zabezpečovací prostředky. V případě, že by nastalo toto riziko, mohlo by dojít k neoprávněnému zpřístupnění či ztrátě, ale i zničení osobních údajů.

Dále by mohlo dojít k odcizení či ztrátě mobilního telefonu, počítače nebo listinného diáře obsahujícího osobní údaje nedostatečným zabezpečením či nesprávným přístupem na straně zaměstnance správce či přímo správce, čímž by mohly být osobní údaje opět ztraceny, zničeny nebo neoprávněně zpřístupněny třetím osobám.

Pokud by byly osobní údaje vyzrazeny při běžném hovoru zaměstnance správce s přáteli, a to ať už úmyslně či neúmyslně, kdy chce zaměstnanec správce v zápalu konverzace přispět nějakou drobnou příhodou z práce a neuvědomí si důsledky, pak by byly osobní údaje neoprávněně zpřístupněny vinou nesprávného chování zaměstnance. K vyzrazení může dojít i rozhovorem mezi zaměstnanci správce na nevhodných místech, například v hromadné dopravě, v restauraci nebo na jiných místech, kde by hovor mohly zaslechnout třetí osoby. Takovému riziku by mělo být zamezeno povinností mlčenlivosti, jíž by měli dodržovat kromě správce i všichni jeho zaměstnanci.

Nejčastějším problémem bývá především právě nedostatečné zabezpečení osobních údajů, k nimž se tak snadno mohou dostat třetí osoby, tedy může nastat neoprávněné zpřístupnění. Například listinné dokumenty obsahující osobní údaje jsou uloženy v otevřených policích kanceláře správce, do které má přístup většina zaměstnanců, případně ve volně přístupných skříních, v lepším případě jsou ve skříních uzamčeny, ovšem každý ví, kde se nachází klíč a není těžké se k němu dostat. Na počítačích či telefonech se nevyužívá bezpečnostní kód nebo heslo, případně pokud se na počítači používá, je napsáno na lepícím štítku a přilepeno k obrazovce počítače. Pro dostatečné zabezpečení listinných dokumentů lze doporučit bezpečnostní trezor, případně samostatnou uzamykatelnou místnost fungující jako archiv, ovšem klíče by měly podléhat pečlivému dozoru, například měla by k nim mít přístup pouze určitá osoba nebo by správce mohl vést evidenci osob, jež s klíči manipulují.

3.2.3 Zpráva o posouzení vlivu na zpracování osobních údajů

Je-li správce povinen vypracovat posouzení vlivu na zpracování osobních údajů, vytvoří na základě zjištěných výsledků zprávu, kde zjištěné vlivy rozebere, upřesní a shrne, jaká je pravděpodobnost, že by mohlo ke konkrétnímu riziku skutečně dojít a jak mu lze předejít.

Nevztahuje-li se na správce povinnost vytvoření posouzení vlivu na zpracování osobních údajů, ten si ale i přesto vytvořil analýzu rizik a posoudil případná rizika, po dokončení analýzy rizik si může vytvořit pro větší přehlednost dokument, který lze nazvat výstup z analýzy rizik a představuje to stejné, jako zpráva o posouzení vlivu na zpracování osobních údajů. Jelikož analýza rizik byla pro tohoto správce opět pouze informativním dokumentem, není další rozpracovávání nezbytné, ovšem přenesení zjištěných informací do samostatného dokumentu může pomoci správci s lepší orientací a efektivnějším vyhledáváním pro další práci.

Pokud Nařízení neimplementuje sám správce a vše si nechává zpracovat, takový dokument od osoby, která implementaci provádí, pravděpodobně obdrží, a to právě proto, aby správce seznámila srozumitelně a přehledně s výsledkem analýzy.

Jelikož výstup z analýzy rizik také není předepsaným dokumentem, který by Nařízení vyžadovalo, jeho podoba může být různá. Například zde mohou být uvedena místa, kde u správce dochází ke zpracování osobních údajů, nebo související skupiny osobních údajů, tedy například listinná složka se smluvní dokumentací, elektronické vedení provozních dokumentů, prezentace na webu a sociálních sítích a další. Ke každé skupině pak bude uvedeno, zda v souvislosti s jejím zpracováním dochází, může nebo by mohlo za určitých okolností docházet k nějakým rizikům, případně pak k jakým rizikům, za jakých okolností a jak vysoké je toto riziko. Nakonec se uvede doporučení, jakým způsobem lze konkrétním rizikům předcházet, snížit je či je úplně eliminovat.

Stejně tak ovšem nemusí být tento dokument vůbec vytvářen, vystačí-li si správce s vytvořením analýzy rizik a jsou-li pro něj závěry, které z analýzy vyplývají, dostatečně srozumitelné a přehledné.

3.3 Záznamy o činnostech zpracování

Povinnost vést záznamy o činnostech zpracování plyne každému správci z čl. 30 Nařízení. Správce je povinen do záznamů zahrnout své, a případně společného správce, zástupce správce či pověřence pro ochranu osobních údajů, jméno a kontaktní údaje, účely zpracování, dále musí uvést popis kategorií subjektů údajů, kategorií osobních údajů a kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, a to i s příjemci ze třetích zemí nebo mezinárodních organizací. Záznamy musí obsahovat také informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, přičemž u této třetí země či mezinárodní organizace nesmí chybět její identifikace[146]. Nesmí totiž vyvstat pochybnosti o tom, že tato třetí země poskytuje pro osobní údaje stejně vysoký stupeň ochrany[147]. Pokud to lze určit, uvede také plánované lhůty pro výmaz jednotlivých kategorií údajů a obecný popis technických a organizačních bezpečnostních opatření specifikovaných v čl. 32 odst. 1 GDPR. Takovými opatřeními jsou například šifrování osobních údajů či schopnost obnovit dostupnost osobních údajů a přistup k nim včas v případě fyzických či technických incidentů[148]. Obsahem záznamů o činnostech zpracování je tedy zpravidla individuální popis prováděných postupů, při nichž správce či zpracovatel zpracovává osobní údaje. Nejedná se tím pádem o výčet všech prací s osobními údaji, nýbrž o přehled aktuálního zpracování osobních údajů[149].

Záznamy o činnostech zpracování do určité míry nahrazují oznamovací povinnost, jež správcům s účinností Nařízení odpadla. Záznamy o činnostech zpracování tak musí vést správce a zpracovatel, nevztahuje-li se na něj výjimka z této povinnosti[150].

Správce takový dokument vytvoří na základě všech dokumentů, databází a informací zjištěných pomocí auditu. Není-li správce zpracovatelem základního

---

[146] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 30.

[147] Stanovisko generálního advokáta H. Saugmandsgaard Øe přednesené dne 19. prosince 2019(1), Věc C-311/18

[148] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. čl. 30.

[149] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 111.

[150] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 31.

zavedení Nařízení do činnosti organizace, tedy nechává si správce tuto dokumentaci zpracovat, budou mu zpracovány záznamy pravděpodobně pouze dle aktuální činnosti a dále je po prvotním zpracování na správci, aby si již záznamy poté neustále doplňoval a průběžně aktualizoval.

Záznamy o činnostech zpracování pak plní dvojí účel. Předně správce, který tvoří záznamy a dále je doplňuje a aktualizuje, zvyšuje svou orientaci ve svých procesech zpracování a tím pádem i šanci na případné včasné zjištění možného porušení Nařízení, které tak může okamžitě začít řešit. Dále slouží záznamy o činnostech zpracování jako doklad souladu činnosti správce s Nařízením, který by v případě kontroly vyžadoval Úřad pro ochranu osobních údajů[151]. Záznamy o činnostech zpracování tedy představují dokument, který už neslouží na rozdíl od auditu osobních údajů pouze ke zmapování a posouzení současné situace, odrazení se pro další postup a potřeby správce, naopak tento dokument musí organizace řádně vést a v případě kontroly předložit.

Nicméně není to jen správce, koho se dotýká povinnost vést záznamy o činnostech zpracování. Tato povinnost dopadá rovněž na zpracovatele, a to v rozsahu jména a kontaktních údajů zpracovatele, případně zpracovatelů, všech správců, se kterými zpracovatel spolupracuje, a také případně zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů. Další položku v záznamech představuje rozlišení kategorií osobních údajů, které zpracovatel zpracovává pro jednotlivé správce. Předává-li zpracovatel osobní údaje do třetí země, i o tom musí záznamy o činnostech zpracování informovat společně s identifikací třetí země nebo mezinárodní organizace, do které předávané osobní údaje putují[152].

3.3.1 Výjimka z povinnosti vést záznamy o činnostech zpracování

Nařízení však předpokládá z povinnosti vést záznamy o činnostech zpracování též výjimku, a to za situace, že má daný podnik nebo organizace méně než 250 zaměstnanců, přičemž se nejedná pouze o zaměstnance, jež pracují na základě pracovněprávního poměru, ale i na základě dohod konaných mimo pracovní poměr a těch, jejichž práci zprostředkovala agentura. Aby mohla být výjimka uplatněna,

[151] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 22-23.
[152] TOMEK, Roman. Soulad s GDPR a dokumentace potřebná k jeho dosažení. Část I. *Soukromé právo*, 2019, 7(2), s. 9-17. ISSN 2533-4239.

nesmí takové zpracování představovat zjevné riziko právům a svobodám pro subjekty údajů, zpracování probíhá občasně a správce nezpracovává citlivé osobní údaje a osobní údaje, jenž se vztahují k trestním věcem nebo trestným činům jmenovaným v čl. 10 Nařízení[153].

Nekompromisní podmínky ovšem způsobují téměř nedosažitelnost možnosti využití výjimky, neboť ač správce nemá 250 zaměstnanců, může mít například pouhé dva zaměstnance, i tehdy probíhá zpracování pravidelně, a tedy podmínky výjimky nesplňuje a měl by vytvořit záznamy o činnosti zpracování alespoň v rozsahu účetních, mzdových a daňových záležitostí[154].

3.4 Revize dokumentace

Dalším nezbytným krokem je pak revize veškeré dokumentace organizace a vyhodnocení a zajištění souladu s Nařízením.

3.4.1 Smluvní dokumentace

Typicky mezi revidované dokumenty patří zejména smluvní dokumentace, tedy pracovní smlouvy či dohody o provedení práce a pracovní činnosti a další smlouvy v závislosti na charakteru činnosti organizace, např. dodavatelské smlouvy, smlouvy o spolupráci, o poskytování služeb nebo třeba nájemní smlouvy. Smlouvy by měly obsahovat ustanovení týkající se ochrany osobních údajů, zejména by měla organizace jakožto správce osobních údajů upozornit na způsob jejich zpracování, naproti tomu subjekt osobních údajů svým podpisem potvrdí, že byl se zpracováním seznámen.

Takto upravené smlouvy pak správce používá pro případ dalšího uzavírání, uzavřel-li ale v minulosti nějaké smlouvy, jejichž účinnost stále běží, není nutné smluvní vztah ukončovat a vzápětí uzavírat novou smlouvu, jeví se ovšem jako vhodné stávající smluvní stranu o způsobu zpracování informovat, a to např. dodatkem ke smlouvě.

3.4.2 Další revidované dokumenty

Ve výčtu revidovaných dokumentů se ovšem nejedná pouze o smluvní dokumentaci. V případě, že organizace zpracovává některé osobní údaje na základě

[153] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 111

[154] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 112.

souhlasu, je nezbytné zjišťovat, zda takový souhlas skutečně má a pokud ano, zda jeho forma vyhovuje Nařízení. V situaci, že souhlas nesplňuje požadavky Nařízení, je nutná úprava tak, aby byl v souladu s Nařízením. Zejména musí být jasný a srozumitelný[155]. Pokud souhlas vůbec nemá, je potřebné vypracovat dokument, pomocí kterého souhlas získá.

Nejčastěji je potřeba získat souhlas k uveřejnění fotografií na webu či sociálních sítích nebo ke zpracování osobních údajů pro účely zasílání obchodních a reklamních sdělení.

Může se také stát, že v současné době organizace žádné údaje na základě souhlasu nezpracovává, ovšem očekává se, že do budoucna by mohla nebo pravděpodobně nastane situace, kdy bude takové údaje zpracovávat a bude tedy potřeba souhlas získat. V takové situaci tedy dokument přinášející souhlas se zpracováním osobních údajů není nutné mít dopředu hotový, pokud neví, kdy k takové situaci dojde, nicméně je dobré mít ho připravený, protože až nastane situace, kdy bude organizace zpracovávat údaje na základě souhlasu, pouze předloží dokument k podpisu subjektu údajů, a jeho veškerá činnost tak bude probíhat v souladu s Nařízením a nebude si muset hlídat jeho zajištění, až nastane jeho potřebnost.

S ohledem na konkrétní činnost může správce využívat i další dokumenty obsahující osobní údaje subjektů údajů, potřebu jejich revize ovšem musí správce určit jednotlivě. Některé dokumenty nebudou vyžadovat s ohledem na Nařízení žádný zásah, ovšem i tak musí jejich zpracování probíhat v souladu s Nařízením, tady správce musí posoudit potřebnost jejich zpracování a zvážit, zda zpracování probíhá vhodným způsobem. Takovými dokumenty mohou být různá jednostranná prohlášení od smluvních partnerů, klientů či jiných osob nebo například potvrzení o studiu.

3.5 Obecné informování subjektů údajů správcem

V průběhu implementace a dále i po tom, co správce veškerou svou činnost uvedl do souladu s Nařízením, a soulad tak už jen dále udržuje, hlídá si správce správné postupy a dodržuje určité zásady.

[155] VEJVODOVÁ, Alžběta. GDPR očima expertů: Žádný strašák, ale příležitost. *Právní rádce*, 2017, 25(4), s. 24-25. ISSN 1210-4817.

Vzhledem k tomu, že ovšem zpracovává údaje někoho jiného než své, tedy údaje subjektu údajů, je vhodné, aby tedy i subjekt údajů měl přehled o tom, jakými zásadami se správce při zpracování jeho údajů řídí, jaká má v souvislosti se zpracováním jeho údajů práva či na koho se může obrátit v případě, že podle něj například správce zpracovává jeho údaje, které by zpracovávat neměl.

V ideálním případě správce zpracuje dokument, kde veškeré tyto informace shrne a zveřejní ho pak na svých webových stránkách, kde si je subjekt údajů může kdykoliv vyhledat a seznámit se s nimi, případně ho bude mít vytisknutý u sebe pro případ, že se se subjekty údajů například pravidelně osobně setkává a ti do něj budou chtít nahlédnout. Takový dokument může správce pojmenovat jako zásady ochrany osobních údajů.

3.5.1 Obsah zásad ochrany osobních údajů

Takové zásady pak obsahují několik hlavních bodů. V první části se zpravidla správce údajů představí, zveřejní své identifikační a kontaktní údaje a uvede obecně, z jakého důvodu osobní údaje subjektů zpracovává. Pokud je správce poskytovatelem nějakých služeb, bývá to proto, aby mohl právě jako poskytovatel služeb poskytovat své služby co nejkvalitněji, jelikož v některých případech může širší znalost určitých osobních údajů pomoct poskytnout službu vhodnější, více uzpůsobenou „na míru“ klientovi. Je-li správce zaměstnavatel, pak jsou některé osobní údaje nezbytné ke splnění povinností zaměstnavatele.

V další části pak mohou být uvedeny modelové příklady, kdy dochází ke zpracovávání osobních údajů s vysvětlením, jaký účel k tomuto zpracovávání správce údajů vede a v jakém rozsahu zpracovávání probíhá. Vždy záleží na konkrétním charakteru činnosti správce, podle toho i zpracovává různé osobní údaje za různými účely, i když určité modelové příklady se budou u více různých správců často opakovat nebo podobat.

Například správce osobních údajů, který je poskytovatelem určitých služeb, typicky uvede jako jeden z modelových příkladů situaci, kdy se na něj potenciální klient-subjekt údajů obrátí se žádostí o poskytování či poskytnutí služeb či s objednávkou. To může proběhnout telefonicky, přes e-mail, sociální sítě či třeba kontaktní formuláře. Rozsah zpracovávaných údajů by pak záležel na konkrétní formě – při kontaktování přes e-mail by správce zpracovával e-mailovou adresu a všechny další údaje, které mu v e-mailu subjekt údajů sdělí, především jméno

a příjmení a další údaje v závislosti na charakteru poskytované služby. Vždy by to ale měly být pouze takové údaje, které jsou k naplnění konkrétního účelu nezbytně nutné. Při telefonickém kontaktování pak správce zpracovává telefonní číslo, jméno a opět další údaje, které – pokud vůbec nějaké – mu klient do telefonu sdělí. Sociální sítě či kontaktní formuláře pak většinou prozrazují minimálně jméno a příjmení.

Dalším modelovým příkladem může být výběrové řízení, kdy subjekt údajů se u správce uchází o práci. Potom budou zpracovávanými údaji zpravidla jméno, příjmení, adresa, nějaký kontaktní údaj – tedy telefonní číslo či e-mailová adresa, dosažené vzdělání a dosavadní pracovní zkušenosti, případně fotografie, je-li součástí životopisu. Kontaktní údaj správce potřebuje, aby mohl kandidátovi-subjektu údajů sdělit výsledek výběrového řízení, vzdělání může představovat ukazatel, na jakou pracovní pozici by měl být kandidát-subjekt údajů zařazen a pracovní zkušenosti dodají správci určitou představu o tom, jak vysoké nároky lze na kandidáta-subjekt údajů klást. Fotografie většinou nebývá povinnou součástí životopisu, někteří kandidáti ji ovšem připojují dobrovolně, z vlastní iniciativy.

Na což pak logicky navazuje situace, kdy se subjekt údajů stane zaměstnancem správce. V tu chvíli se rozsah zpracovávaných údajů rozšíří o, stále pouze nezbytně nutné, další údaje, jakými budou například údaj o mzdě, číslo účtu, pracovní pozice či den nástupu do práce. Neuspěl-li uchazeč o práci ve výběrovém řízení, povinností správce je jeho údaje poskytnuté v rámci výběrového řízení zlikvidovat.

Správci zpracovávají určité údaje také v situaci, kdy si subjekt údajů prohlíží správcovy webové stránky. V tomto případě se ovšem jedná o údaje o tom, jakým způsobem jsou webové stránky využívány nebo co je na nich vyhledáváno nejčastěji, ne o údaje o samotném subjektu údajů, který si webové stránky prohlíží. Takové zpracování funguje na principu tzv. cookies, což jsou krátké textové soubory, které tvoří webový server a ukládá je v používaném zařízení pomocí prohlížeče. Funkce cookies spočívá ve skutečnosti, že pomocí nich lze jednotlivé uživatele vzájemně odlišit a uložit údaje o nich. Cookies pak lze rozlišit na několik druhů podle různých kritérií, například podle doby uložení na krátkodobé, které se po zavření internetového prohlížeče vymažou a dlouhodobé, které zůstávají v prohlížeči uloženy až do doby smazání, případně kratší dobu v závislosti na nastavení konkrétního prohlížeče a cookies.[156] Zásady ochrany osobních údajů

[156] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 219.

ovšem nepředstavují jediné místo, kde musí správce pamatovat na cookies. O jejich sběru by měl informovat ihned při otevření webové stránky, což v praxi vypadá většinou tak, že po otevření stránky se automaticky objeví informující okno spolu s políčkem, ve kterém subjekt údajů označí, že byl správcem informován o sběru cookies a rozumí tomu[157].

Ke zpracování určitých osobních údajů dochází též v situaci, zasílá-li správce subjektu osobních údajů různá obchodní či reklamní sdělení. Zpracovávanými údaji v tomto případě jsou především kontaktní údaje, kam jsou tato sdělení zasílána, tedy zejména e-mailová adresa nebo adresa trvalého či přechodného bydliště a většinou také jméno a příjmení.

Zpracování vždy musí probíhat na základě nějakého právního důvodu, proto i subjekt údajů by měl být seznámen se všemi právními důvody, na základě kterých je s jeho údaji nakládáno. Tedy další částí zásad ochrany osobních údajů bývá výčet a seznámení s těmito právními tituly.

Například zveřejňuje-li správce na webových stránkách či sociálních sítích fotografie svých zaměstnanců nebo třeba klientů, potřebuje k tomu nezbytně souhlas subjektu údajů, jehož fotografie zveřejňuje. Ani zasílání newsletteru či obchodních sdělení nelze podřadit pod jiný právní titul, než je souhlas subjektu údajů.

Uzavře-li subjekt údajů a správce smlouvu, k jejímu řádnému plnění potřebuje správce znát určité osobní údaje subjektu údajů. Jejich rozsah pak závisí vždy na konkrétním smluvním vztahu. Subjekt údajů jako zaměstnanec musí sdělit správci číslo svého účtu, aby správce jako zaměstnavatel věděl, kam má být zaměstnanci zasílána mzda. Správce jako dodavatel zboží se zase neobejde bez adresy subjektu údajů zákazníka, aby mu objednané zboží mohl řádně doručit. Takové zpracování tedy probíhá na základě právního titulu plnění smlouvy.

Povinnost zpracovávat některé údaje mohou správci uložit i právní předpisy. Například vystavuje-li správce subjektu údajů fakturu, má povinnost určité údaje zpracovávat podle daňových či účetních předpisů.

Probíhá-li zpracování některých údajů s cílem ochrany životně důležitých zájmů subjektu údajů nebo je prováděno ve veřejném zájmu, pak musí správce

[157] VEJVODOVÁ, Alžběta. Neznámá pro byznys: nová pravidla pro práci s citlivými daty. *Právní rádce*, 2017, 25(3), s. 24-26. ISSN 1210-4817.

uvést v zásadách i tyto právní tituly a přiblížit, jaké údaje na jejich základě zpracovává.

Nakonec může zpracování probíhat i z důvodu oprávněného zájmu správce nebo třetí osoby, a to například snaží-li se správce v roli zaměstnavatele vybrat co nejvhodnějšího kandidáta na určitou pozici ve výběrovém řízení nebo shromažďuje-li údaje o návštěvnosti webových stránek s cílem zkvalitnění přizpůsobení online prostředí více uživatelům. Advokát zase zpracovává osobní údaje protistrany svého klienta, kterého zastupuje v určitém sporu, za účelem oprávněných zájmů třetí osoby – klienta.

Dalším důležitým bodem zásad ochrany osobních údajů je seznámení s právy subjektu osobních údajů a způsobem, jakým lze tato práva uplatnit. Práva by měla být nejprve vyjmenovaná a blíže popsaná a dále by mělo být uvedeno, na koho se může subjekt údajů obrátit v případě, že je chce uplatnit. Správce subjekty údajů nejprve směřuje na svůj e-mail, kde by mu měl subjekt údajů vysvětlit, jaká práva chce uplatnit a z jakého důvodu. Správce vše pečlivě posoudí a k žádosti subjektu údajů se vyjádří. Subjekt údajů má ale rovněž právo obrátit se na Úřad pro ochranu osobních údajů. Rychlejší zjednání nápravy se dá pravděpodobně očekávat, obrátí-li se subjekt údajů rovnou na správce, který situaci může začít okamžitě řešit, ovšem i na právo domoci se svých práv u Úřadu pro ochranu osobních údajů by měl být subjekt údajů upozorněn. Zároveň může subjekt údajů Úřad pro ochranu osobních údajů požádat o pomoc v situaci, kdy správce plně nevyhověl jeho představám, a i přesto má za to, že mu právo, jehož se domáhá, náleží.

Každý subjekt údajů má právo na přístup ke svým osobním údajům. Například pokud neví, jaké jeho údaje správce zpracovává, může se vždy na správce obrátit s dotazem. Povinností správce je rozsah zpracovávaných údajů subjektu údajů sdělit.

Také zpracovává-li správce nepřesné, nesprávné nebo neúplné údaje a subjekt údajů se o tom dozví, má právo na opravu nebo doplnění osobních údajů. Zpracovávané údaje mohou být přitom od začátku u správce evidovány nesprávně nebo mohlo dojít k jejich změně v průběhu určité doby. Může se například stát, že došlo k překlepu při zveřejňování jména či kontaktních údajů zaměstnance správce na webových stránkách, subjekt údajů je žena, která se vdala či rozvedla a změnila

si své příjmení nebo subjekt údajů sdělil správci omylem nesprávný údaj – například staré telefonní číslo.

V případě, že subjekt údajů již nechce, aby správce zpracovával jeho osobní údaje, má právo na výmaz osobních údajů – tzv. právo „být zapomenut“. Požádá-li subjekt o výmaz svých údajů, správce nejprve zkontroluje, jestli jsou k němu splněny podmínky. Například nelze vymazat údaje subjektu údajů, jehož smluvní vztah se správcem osobních údajů stále trvá či jsou mu stále poskytovány služby, jeho údaje tak správce stále potřebuje.

Subjekt údajů může také požadovat, aby správce omezil zpracování, a to například z důvodu, že osobní údaje zpracovávané správcem jsou podle subjektu údajů nepřesné. Správce pak omezí zpracování na dobu nezbytnou k tomu, aby zjistil, zda označené údaje skutečně nepřesné jsou.

Subjekt údajů má také právo na přenositelnost osobních údajů, což znamená, že správce předá zpracovávané osobní údaje jinému správci, požádá-li o to subjekt údajů a provedením nebudou dotčena práva třetích osob. Například pokud byl správce poskytovatelem služeb subjektu údajů a subjekt údajů se rozhodl k daným službám využít jiného poskytovatele a ukončit spolupráci se správcem, původní správce předá osobní údaje novému poskytovateli.

Pokud má subjekt údajů za to, že osobní údaje, které jsou označeny jako údaje zpracovávané na základě oprávněných zájmů správce, by správce zpracovávat vůbec neměl nebo třeba ne v takovém rozsahu, v jakém jsou současně zpracovávány, má právo vznést námitku proti zpracování osobních údajů. Takovou námitkou má správce povinnost se zbývat.

Subjekt údajů má také právo kdykoliv odvolat souhlas se zpracováním jakýchkoliv osobních údajů, které jsou na základě souhlasu zpracovávány.

Vzhledem ke skutečnosti, že ne všechny osobní údaje zpracovává správce sám, ale některé údaje jsou také zpracovávány prostřednictvím zpracovatele, měl by subjekt údajů informovat, kdo tito zpracovatelé jsou a proč se k nim jeho údaje dostávají. Zpravidla jimi bývají externí poskytovatelé účetních služeb, externí správci webových stránek či profilů na sociálních sítích, provozovatelé sociálních sítí či poskytovatelé internetových databází.

Na konci zásad ještě může správce vysvětlit, proč a jakým způsobem jsou ukládány cookies a co pro jejich ovlivnění může udělat sám subjekt údajů – tedy může nastavit, změnit nebo zakázat jejich ukládání na každém svém zařízení sám.

Dál uvede jen způsob, jakým můžou být zásady měněny a odkdy nabývají platnosti.

3.6 Směrnice pro zpracování a ochranu osobních údajů

Směrnice pro zpracování a ochranu osobních údajů představuje vnitřní předpis pro správce a zaměstnance správce, který, stejně jako zásady ochrany osobních údajů, upravuje postupy a pravidla správce a jeho zaměstnanců při práci s osobními údaji, ovšem na rozdíl od zásad ochrany osobních údajů nesměřuje vně, ale dovnitř, tedy jeho adresáti jsou zaměstnanci správce, jelikož se i oni, ne pouze správce, dostanou do kontaktu s osobními údaji subjektů údajů, a musí tedy dodržovat stejná pravidla jako správce. Proto se její obsah také od zásad ochrany osobních údajů liší, neboť nepřináší představení způsobů zpracování a práv, ale spíše povinností. Závaznost všech osob by také měla mít ve směrnici své místo a měla by být ve směrnici jasně vymezena. O všech, kteří osobní údaje zpracovávají jménem správce, pak směrnice hovoří jako o pověřených osobách. Vnitřní směrnice tedy představuje jakýsi manuál správce a pověřených osob ke správnému zacházení se zpracovávanými osobními údaji.

Povinností správce je zaměstnance se směrnicí řádně seznámit, umístit ji někam, kde k ní budou mít všichni zaměstnanci snadný přístup, například na společnou nástěnku či sdílené uložiště. Povinností zaměstnance je oproti tomu řídit se všemi pokyny směrnice a dodržovat jí stanovená pravidla a postupy. S ohledem na skutečnost, že se jedná o interní předpis, zavazuje pouze všechny, kdo se podílejí na činnosti správce v pracovněprávním vztahu.

3.6.1 Obsah směrnice pro zpracování a ochranu osobních údajů

Aby každý, kdo se s ní má seznámit a řídit se jí, směrnici dobře a správně porozuměl, může správce zvážit, zda by nebylo vhodné do směrnice zařadit článek, jenž by definoval klíčové pojmy. Lze-li důvodně předpokládat, že vysvětlování pojmů by bylo pro zaměstnance nadbytečné, může správce takový článek vynechat. Například pokud zaměstnává osoby vzdělané v oboru právo, od nichž lze bez pochybností předpokládat znalost výkladu těchto pojmů. V ostatních případech je vhodné základní pojmy alespoň stručně představit.

Stejně jako správce, i jeho zaměstnanci jsou při zpracovávání osobních údajů vázáni Nařízením. Vztahuje se tím pádem samozřejmě i na ně povinnost dodržování všech zásad zpracování osobních údajů v souladu s Nařízením, tedy zásady zákonnosti, korektnosti a transparentnosti, zásady účelového omezení zpracování, zásady minimalizace údajů, zásady přesnosti, zásady omezení uložení a zásady integrity a důvěrnosti blíže specifikované v kapitole Zásady ochrany osobních údajů v Teoretické části této práce.

Subjekt údajů má v souvislosti se svými zpracovávanými osobními údaji určitá práva, na něž a na možnost a způsob jejich uplatnění je upozorněn v zásadách ochrany osobních údajů. Oproti tomu má správce povinnost se jakýmkoliv případným uplatněním zabývat. Proto ve vnitřní směrnici zakotví, jakým způsobem bude on i pověřené osoby postupovat v případě, že některý subjekt údajů uplatní některé ze svých práv.

Vést záznamy o činnostech zpracování je pro správce velice důležitou povinností, která by měla být ve směrnici zmíněna společně s rozsahem záznamů a stručným postupem, jak záznamy o činnostech zpracování vést.

Stejně jako zásady ochrany osobních údajů vyjmenovávají práva subjektů údajů a postupy, jakými je lze uplatnit, vyjmenovává tato práva i směrnice pro zpracování osobních údajů, ovšem společně s postupy nikoli pro subjekty osobních údajů, ale pro pověřené osoby v případě, že subjekt údajů hodlá svá práva uplatnit. Část práva subjektů údajů je tedy ve vnitřní směrnici rozsáhlejší než v zásadách ochrany osobních údajů, neboť musí vymezit všechny kroky pověřených osob při uplatňování práv, počínaje přijetím a potvrzením přijetí žádosti a její následné evidence. Dále správce posoudí, zda je žádost oprávněná. Poté ji může správce vyřídit sám, stejně tak ji mohou vyřídit i správcem pověřené osoby, a to v co nejkratším možném čase bez zbytečných průtahů. Určité kroky v postupu jsou závislé na tom, jaké právo subjekt údajů uplatňuje, například uplatňuje-li právo na přístup k osobním údajům, správce či pověřená osoba informuje subjekt údajů o rozsahu zpracovávaných kategorií údajů a pokud tím nebudou ohrožena práva a svobody třetích osob a nebude tím porušena zákonná povinnost mlčenlivosti, předá správce či pověřená osoba subjektu údajů kopii zpracovávaných údajů. Uplatňuje-li subjekt údajů právo na výmaz osobních údajů, po ověření identity žadatele posoudí správce oprávněnost a v případě, že shledá žádost důvodnou, tedy že mu povinnost zpracování osobních údajů například neukládají právní předpisy,

osobní údaje zlikviduje, uvědomí subjekt údajů a zapíše způsob vyřízení do evidence.

Ovšem přestože je zaměstnanec pověřenou osobou, pracuje s osobními údaji subjektu údajů, a musí znát postup při uplatnění některého práva subjektem údajů, i on je subjektem údajů se stejnými právy, která může uplatnit úplně stejně jako kterýkoliv jiný subjekt údajů, a to tím, že se se svou žádostí obrátí na správce, neboť správce zpracovává jeho údaje v rámci pracovněprávního vztahu.

Další povinnost správce představuje dostatečné zabezpečení osobních údajů, což znamená, že správce musí dohlédnout na to, aby bylo zamezeno neoprávněnému a nahodilému přístupu k osobním údajům, aby osobní údaje nebyly zničeny či ztraceny, aby se nedostaly do neoprávněných rukou či nebyly zneužity.

K vymezení faktorů, které by mohly osobní údaje ohrozit, správci pomůže vytvoření analýzy rizik s návrhy opatření eliminující rizika. Závěry, které v analýze zjistí, pak dále využije ve vnitřní směrnici, kde blíže specifikuje opatření k eliminaci rizik, jež budou muset zaměstnanci dodržovat. Opatření správce rozdělí do kategorií podle toho, kde se rizika mohou objevit, na organizační a technická opatření.

Organizační opatření sledují fyzickou bezpečnost osobních údajů, kdy je důležité uchovávat osobní údaje mimo dosah třetích osob, například listinné dokumenty v uzamčených trezorech, místnostech, případně skříních, ke klíčům nesmí být snadný přístup, v prostorách správce se nesmějí pohybovat třetí osoby bez dozoru či doprovodu pověřené osoby, zaměstnanci jsou povinni dodržovat povinnost mlčenlivosti, která by měla trvat i po skončení pracovního poměru. K osobním údajům by měli mít vždy přístup pouze ti zaměstnanci, pro které je nezbytný ke splnění svých pracovních povinností a pouze na pokyn správce nebo vyplývá-li potřebnost z právních předpisů.

Technická opatření pak vyžadují, aby veškeré prostředky výpočetní techniky využívané k práci s osobními údaji byly dostatečně zabezpečeny před neoprávněným přístupem třetích osob. To znamená, že pověřené osoby jsou povinny využívat v počítačích, telefonech, tabletech či ostatních využívaných zařízeních zabezpečovací kódy, gesta, hesla, antivirové programy, dvoufázová ověření či možnost zablokování zařízení při jeho ztrátě. Osobní údaje musí být zabezpečeny také před ztrátou či zničením, k čemuž by mohlo dojít například

smazáním souboru z počítače. Takové ztrátě lze předejít například automatickým zálohováním. Také pokud pověřená osoba využívá k práci s osobními údaji systémy či aplikace, které fungují na principu přihlašování ke konkrétnímu účtu, a ukončí se správcem pracovní poměr, předá správci všechny přihlašovací údaje, které k práci využívala a zároveň správce v co nejkratší době tyto nepotřebné účty trvale zruší.

I přes veškerá opatření ovšem může dojít k situaci, při níž bude zabezpečení osobních údajů porušeno. V takovém případě musí porušení pověřená osoba okamžitě nahlásit správci a zároveň zajistit, aby se osobní údaje nedostaly ke třetím osobám, případně zamezit dalšímu úniku. Správce pak musí porušení zabezpečení osobních údajů neprodleně nahlásit dozorovému úřadu. Výjimka z této správcovy povinnosti nastává pouze v případě, že nelze předpokládat pravděpodobnost, že by takové porušení mělo za následek riziko pro práva a svobody fyzických osob. V ohlášení pro dozorový úřad musí správce uvést, v čem spočívá dané porušení zabezpečení osobních údajů, kategorie a přibližný počet dotčených záznamů osobních údajů, jaké důsledky porušení zabezpečení správce pravděpodobně očekává a výpis opatření, která správce přijal za účelem vyřešení porušení zabezpečení osobních údajů.

Eviduje-li správce vysoký počet pověřených osob, je vhodné úkoly spojené s ochranou osobních údajů systematicky rozdělit, a to například tak, že vybere určité pracovní pozice a k těmto pozicím přidělí konkrétní úkoly. Ve směrnici pak tyto pracovní pozice uvede společně s přesným popisem jejich přidělených úkolů.

Směrnice by také měla informovat o způsobu uchovávání osobních údajů a jejich likvidaci. Že musí být osobní údaje uchovávány takovým způsobem, aby byly dostatečně zabezpečeny, směrnice zmiňuje již v předchozích částech, měla by ale také obsahovat jasné oznámení o době archivace. Většinou to bývá v závislosti na příslušných ustanoveních právních předpisů České republiky, jinou dobu zpracování musí případně správce ve směrnici uvést. Likvidace většinou probíhá prostřednictvím skartace.

Protokol o seznámení se směrnicí

Aby si byl správce jistý, že se všichni jeho zaměstnanci se směrnicí seznámí a budou znát její obsah, může vytvořit protokol, jenž bude obsahovat prohlášení zaměstnanců o tom, že se s interní směrnicí seznámili, že rozumí jejímu obsahu,

znají svá práva i povinnosti ze směrnice vyplývající a nemají ke směrnici žádné výhrady, což potvrzují svým podpisem.

Protokol pak správci slouží jako ujištění, že si zaměstnanci uvědomují vážnost směrnice a důležitost Nařízení a práv a povinností z něho plynoucích. Vypracování protokolu lze doporučit spíše organizacím s vyšším počtem zaměstnanců, naopak u menších organizací, kde lze na seznámení se směrnicí dohlédnout individuálně, protokol není nezbytný.

3.7 Další interní předpisy

Směrnice pro zpracování a ochranu osobních údajů ovšem nereprezentují jediný interní předpis. Vnitřní předpis je mnohem širší pojem, nevztahuje se pouze na ochranu osobních údajů a splnění povinností vyplývajících z Nařízení. To znamená, že nehledě na ochranu osobních údajů, správce již pravděpodobně nějaký jiný vnitřní předpisy používá. Tím můžou být například provozní řády, bezpečnostní předpisy, spisové, archivační a skartační řády, ale například i zakladatelské smlouvy či stanovy. Všechny takové interní předpisy, vyžaduje-li to jejich povaha, by měly reflektovat bezpečnostní opatření, která správce přijímá na základě hrozeb zjištěných analýzou rizik a za účelem ochrany osobních údajů.

Správce se tedy musí zamyslet, jaké užívané interní předpisy je vhodné upravit a jak, aby byly v souladu s Nařízením. Například zákon o archivnictví a spisové službě a změně některých zákonů přináší taxativní výčet všech subjektů, kteří jsou povinni uchovávat dokumenty a poskytnout výběr archiválií. Mezi nimi jsou například státní podniky, zdravotní pojišťovny, vysoké školy či územní samosprávné celky[158]. Takové subjekty pak mají zároveň jako správci osobních údajů povinnost postarat se o ochranu osobních údajů. Ovšem nejen těmto subjektům lze vytvoření archivačního a skartačního řádu doporučit, neboť může vhodně posloužit pro případné doložení, že správce dodržuje zásadu omezení uložení, má přehled o době zpracování osobních údajů a je si vědom povinnosti po uplynulé stanovené době osobní údaje vymazat[159]. Jelikož tedy práce se spisy, archivem, ale i skartace dokumentů představuje práci s určitými údaji, přičemž se může jednat i o osobní údaje, měl by na to správce myslet a spisový nebo archivační a skartační řád by se měl zmiňovat o vhodných opatřeních k bezpečné práci

[158] Zákon č. 499/2004 Sb., *o archivnictví a spisové službě a změně některých zákonů*. § 3 odst. 1.
[159] TOMEK, Roman. Soulad s GDPR a dokumentace potřebná k jeho dosažení. Část II. *Soukromé právo*, 2019, 7(3), s. 25-27. ISSN 2533-4239.

s osobními údaji. Měl by obsahovat například ustanovení o tom, že k práci s osobními údaji jsou oprávněny pouze osoby, pro něž je to nezbytné ke splnění pracovních úkolů.

Provozní řády by zase měly myslet na to, že v místech, kde se vyskytují osobní údaje, by se neměly pohybovat třetí osoby, nebo alespoň ne bez dozoru, že personál osobní údaje nesmí sdělovat třetím osobám či že personál má dbát na to, aby uzamykatelné prostory skutečně řádně zamykal nebo nesděloval přístupová hesla či kódy k počítačům a jiné elektronice obsahující osobní údaje.

3.8 Vztah správce a zpracovatele

Vzhledem ke skutečnosti, že správce a zpracovatel jsou dvě odlišné osoby, nespolupracují v rámci pracovněprávních vztahů a subjekt údajů, který své osobní údaje svěřil správci, nejedná se zpracovatelem, nikdy se s ním nemusí setkat ani mu přímo své osobní údaje poskytnout, a přesto je zpřístupnění osobních údajů subjektu údajů zpracovateli pro správce nezbytné, musí správce spolu se zpracovatelem uzavřít smlouvu o zpracování osobních údajů, v níž vymezí zpracovávané kategorie osobních údajů, účel zpracování i všechna práva a povinnosti správce i zpracovatele tak, aby byl zajištěn soulad činnosti s Nařízením a nebylo porušeno zabezpečení osobních údajů.

Poměrně často se stává, že správce spolupracuje s více různými zpracovateli, jelikož každý z nich svou činnost zaměřuje na něco jiného. Například jeden z nich se specializuje na zpracovávání účetnictví, druhý na poskytování internetových databází a třetí na služby v oblasti informačních technologií. Nezáleží však na počtu, s kolika různými zpracovateli správce spolupracuje, zpracovatelskou smlouvu musí uzavřít vždy s každým zpracovatelem zvlášť, neboť v každé jednotlivé smlouvě musí definovat, v čem konkrétně spočívá jejich smluvní vztah, co je účel právě toho konkrétního zpracování. Neboť každý ze zpracovatelů zpracovává osobní údaje svěřené správcem z jiného důvodu a za jiným účelem.

3.8.1 Zpracovatelská smlouva

Kromě obecných náležitostí obsahuje zpracovatelská smlouva také rozdělení kategorií spolu s rozsahem zpracovávaných údajů v jednotlivých kategoriích, pomocí čehož správce stanoví jasný rámec zpracovávaných údajů. Kategorie správce uspořádá tak, aby spolu údaje logicky souvisely v závislosti na charakteru činnosti správce.

Například je-li správce poskytovatelem nějakých služeb a zároveň zaměstnavatelem, může členění zobrazovat standardní kategorii osobních údajů, které správce získal v rámci poskytování služeb, standardní kategorii osobních údajů, které správce získal v rámci zaměstnávání svých zaměstnanců a standardní kategorii osobních údajů, které správce získal v rámci výkonu své činnosti a chodu organizace.

Ke každé kategorii pak doplní, které osobní údaje a jak dlouho jsou prostřednictvím této kategorie zpracovávány. Společné všem kategoriím budou většinou zejména jméno, příjmení, adresa a telefonní číslo, v určitých údajích se budou jednotlivé kategorie lišit i v závislosti na charakteru činnosti správce. Například číslo bankovního účtu či pracovní zařazení se budou zpracovávat společně s údaji získanými v souvislosti se zaměstnáváním, zatímco datum narození či přechodná adresa mohou být zpracovávány společně s údaji získanými za účelem poskytování služeb.

Smlouva by dále měla definovat povinnosti zpracovatele, například zpracovávat osobní údaje v souladu se zpracovatelskou smlouvou a pokyny správce[160], ale samozřejmě obecně v souladu s Nařízením, a že stejný způsob zpracování zajistí i u pověřených osob, tedy svých zaměstnanců, že budou zpracovávané osobní údaje vhodně technicky i organizačně zabezpečeny, bude zachovávat mlčenlivost a nebude zpracovávané osobní údaje šířit, předávat či jinak sdělovat třetím osobám, poskytne správci součinnost při plnění jeho povinností nebo že musí správci neprodleně ohlašovat jakákoli případná porušení zabezpečení osobních údajů.

Mlčenlivost představuje v oblasti ochrany osobních údajů klíčovou povinnost, proto by jí měla být ve zpracovatelské smlouvě věnována speciální pozornost. Zpracovatel ani jím pověřené osoby nesmějí porušit povinnost mlčenlivosti[161], leda by k tomu dal správce předem povolení. Povinnost mlčenlivosti trvá i po ukončení spolupráce mezi správcem a zpracovatelem. Správce může ve smlouvě o zpracování osobních údajů stanovit, že za porušení mlčenlivosti je zpracovatel povinen uhradit správci smluvní pokutu. V takovém

[160] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0. s. 30.
[161] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 101.

případě by ovšem měl uvést ještě bližší informace, jako je výše pokuty, doba, dokdy má být smluvní pokuta uhrazena a způsob, jakým má být uhrazena.

Nejen zpracovateli plynou ze smlouvy o zpracování osobních údajů povinnosti, ale i správce je povinen přijmout vhodná organizační a technická opatření s cílem co nejvyššího možného zabezpečení osobních údajů a předcházení možným rizikům a ohlašovat zpracovateli případná porušení zabezpečení. Správce i zpracovatel jsou také povinni navzájem se včas informovat o jakýchkoliv okolnostech, které by mohly mít vliv na plnění zpracovatelské smlouvy.

3.9 Společní správci

Článek 26 Nařízení umožňuje rozložení povinností správce mezi dvě či více osob stanovením společných správců. Pokud spolu dva či více subjektů spolupracují, aniž by tvořili jednu obchodní společnost, například mají společné zaměstnance či sdílejí stejné sídlo, mohou při své činnosti sdílet osobní údaje, pak je vhodné si ujasnit, zda je možné, aby osobní údaje zpracovával jen jeden z nich, který by se stal správcem osobních údajů za oba nebo zda by nebylo vhodnější zpracovávat osobní údaje společně jako takzvaní společní správci, a svůj vztah a vzájemná práva a povinnosti tak upravit písemnou smlouvou o společných správcích.

Jednoduchý příklad může představovat například koncern, jelikož se jedná o jednu či více osob podléhající řízení jiné osoby[162], může tak snadno docházet ke sdílení osobních údajů mezi těmito osobami. Nebo jiný příklad: „*výrobce automobilů může s dealery vozů domluvit společný projekt za účelem podpory prodeje (např. soutěž), kdy všechny zainteresované strany určí účel a prostředky zpracování a prostřednictvím internetové stránky, ale i prostřednictvím jednotlivých dealerů, budou zpracovávat osobní údaje soutěžících za účelem soutěže. Tím se stanou společnými správci.“*[163] Zároveň se mohou dohodnout dva či více subjektů, že budou sdílet společnou kancelář, a to s jakýmkoliv zaměřením, například účetní či advokátní. Pro zajištění chodu kanceláře pak mohou mít některé společné zaměstnance, a současně sdílejí stejné prostory sídla.

[162] Zákon č. 90/2012 Sb., *zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích)*. § 79 odst. 1.
[163] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9. s. 90-91.

3.9.1 Smlouva o společných správcích

Smlouva o společných správcích pak nejprve definuje činnost, pro kterou se smluvní strany rozhodly spolupracovat, tedy například pořádání soutěže či provoz kanceláře.

Dále si musejí společní správci ujednat, k předání či zpřístupnění jakých osobních údajů mezi nimi dochází. Může se jednat o subjekty údajů, jimiž jsou například zaměstnanci, případně uchazeči o zaměstnání, klienti, smluvní partneři či jiné subjekty údajů. Také uvedou, za jakým účelem dochází k předávání osobních údajů a o jaké konkrétní kategorie osobních údajů se jedná.

Společní správci si také stanoví vzájemná práva a povinnosti, přičemž jejich rozsah závisí na konkrétních preferencích společných správců, většinou ovšem nebude chybět povinnost poskytovat součinnost, zachovávat mlčenlivost, vzájemné informování se o nezbytných skutečnostech či zpracování osobních údajů jen v rozsahu a za účelem, za kterým byly přijaty.

Společní správci dodržují za účelem dostatečného zabezpečení osobních údajů vhodná organizační a technická opatření. Spravují-li ovšem osobní údaje společně dva či více správců, je vhodné ve smlouvě ujednat konkrétní práva, povinnosti či úkoly spojené se zabezpečením osobních údajů. Například společní správci mohou ve smlouvě přijatá technická a organizační opatření uvést společně s ustanovením, že se zavazují je dodržovat, nebo si mohou úkoly týkající se dodržování těchto opatření rozdělit a uvést, který ze správců má na starosti dohlížení nad dodržováním kterého opatření.

4. Realizační část implementace

Jakmile správce dokončí přípravnou část, nachystá veškeré dokumenty, odhalí všechna rizika a hrozby a připraví vhodná opatření k jejich eliminaci, může se pustit do realizační fáze, v čemž mu právě připravené dokumenty pomohou a svou další činnost o ně bude moci opřít. Realizace představuje přechod od chystání dokumentů a vhodného prostředí pro bezpečné zpracovávání osobních údajů, zjišťování, studium, zkoumání a mapování současného stavu a přípravy návrhů opatření k přeměně v požadovaný stav a realizaci navrhovaných opatření.

Správce zajistí školení pro své zaměstnance k seznámení se všemi povinnostmi z Nařízení vyplývajícími. Školení nepředstavuje pouze část realizační

fáze implementaci Nařízení, v realizační fázi se se školením pouze začíná a je vhodné jej v určitých intervalech pravidelně opakovat. Prolíná se tedy i dále do fáze zvané praxe. Zejména pak správce v realizační části implementace zavede do praxe veškerá opatření, jejichž potřebnost odhalil v přípravné části.

4.1 Školení

Správce i pověřené osoby musejí mít od počátku účinnosti Nařízení, případně od počátku činnosti, vznikla-li organizace správce až po účinnosti Nařízení, přehled o všech důležitých informacích týkajících se ochrany osobních údajů. Prvním krokem správce je seznámení se s Nařízením v rámci studia, dále musí proškolit pověřené osoby, případně školení zajistit, o celkovém obsahu Nařízení, o právech a povinnostech z něho vyplývajících, o zabezpečení zpracovávaných osobních údajů i o postupech napomáhajících k dostatečnému zabezpečení.

Jednorázové školení ovšem nezajistí dostatečný přehled o rozsáhlém odvětví ochrany osobních údajů, obzvlášť lze-li důvodně předpokládat vývoj tohoto odvětví, proto je vhodné v určitých intervalech školení opakovat, ačkoli rozsah a četnost školení nelze jednotně stanovit, vše závisí na konkrétních profesích a pozicích zaměstnanců, kterým je školení určeno, jejich pracovní náplni[164], ale i charakteru činnosti správce.

Důležité je ovšem školení uzpůsobit tak, aby mu konkrétní zaměstnanci porozuměli, aby porozuměli, co pro ně z Nařízení vyplývá a co se stane, poruší-li některou svou povinnost založenou Nařízením, ale také aby byl obsah školení vždy přizpůsoben jednotlivým posluchačům[165], tedy například koná-li se školení u jednoho správce již poněkolikáté, klesá potřebnost vysvětlování základních pojmů, práv či povinností, jelikož to by již měli všichni znát, školení by tedy mělo být zaměřeno hlouběji a praktičtěji s ohledem na konkrétní činnost správce a jeho zaměstnanců.

5. Praxe

Ani ve chvíli, kdy už je původní situace zanalyzovaná a pomocí jejích výsledků přizpůsobená a upravená do souladu s Nařízením, je připravená veškerá

[164] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. s.142.
[165] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 180-181.

dokumentace a nové postupy jsou zavedeny do praxe, nekončí povinnosti správce ani aktuálnost tématu Nařízení a ochrany osobních údajů jako takové. Nyní je totiž důležité veškeré předchozí kroky zužitkovat, veškeré postupy a povinnosti dodržovat a na jejich dodržování rovněž dohlížet.

5.1 Pověřenec pro ochranu osobních údajů

V České republice představuje pověřenec pro ochranu osobních údajů nový institut, jelikož zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, pojem pověřence pro ochranu osobních údajů neznal, ačkoli Směrnice 95/46/ES poskytovala členským státům možnost volby správce určit osobu pověřenou ochranou osobních údajů[166]. Některé státy, mezi nimiž je například Německo, ovšem pověřence pro ochranu osobních údajů do své právní úpravy začlenily. Jejich pozitivní zkušenosti pak zavdali příčinu zařazení tohoto institutu přímo do Nařízení[167].

5.1.1 Jací správci musejí mít svého pověřence pro ochranu osobních údajů

Pověřit konkrétní osobu ochranou osobních údajů je povinnost, která ovšem z Nařízení neplyne všem správcům a zpracovatelům. Tato povinnost se týká pouze orgánů veřejné moci, veřejných subjektů a správců, kteří rozsáhle, pravidelně a systematicky monitorují subjekty údajů v rámci své hlavní činnosti nebo jenž se v rámci hlavní činnosti zabývají rozsáhlým zpracováním citlivých osobních údajů[168].

Uvedené znaky naplňují například profesní komory, konkrétně se tedy může jednat o advokátní či lékařskou komoru, jelikož vykonávají zákonem určené úkoly ve veřejném zájmu[169], nebo nemocnice, které potřebují zpracovávat citlivé osobní údaje, aby mohli provádět účinně a spolehlivě svou hlavní činnost, jíž je poskytování zdravotnické péče[170]. Dále plyne povinnost jmenovat pověřence pro ochranu osobních údajů také pro obce. Nařízení ovšem připouští situaci, kdy více

[166] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9., s. 107.
[167] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0., s. 33.
[168] NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. První vydání. Praha: Klika, 2018. 141 s. Otevřeno. ISBN 978-80-88298-10-6. s. 139.
[169] OTEVŘEL, Petr. GDPR od A do Z: díl čtvrtý: Jste povinni jmenovat pověřence pro ochranu osobních údajů?. 4. Díl. *IT Systems*, 2017, 19(11), s. 14-15. ISSN 1802-002X.
[170] NULÍČEK, Michal. První výkladové pokyny k GDPR: Co přináší a jaký budou mít praktický dopad?. *Právní rádce*, 2017, 25(1), s. 58-59. ISSN 1210-4817.

správců svěří ochranu osobních údajů pouze jednomu pověřenci, který bude dohlížet na ochranu osobních údajů těchto správců společně. K tomu ovšem Nařízení klade jednu podmínku, a tedy že správci, kteří společně jmenují jednoho pověřence pro ochranu osobních údajů, musejí být veřejným subjektem či orgánem veřejné moci[171].

Skutečnost, že správce není povinen jmenovat pověřence pro ochranu osobních údajů, ovšem nepředstavuje překážku tak učinit, pokud má správce o pověřence pro ochranu osobních údajů i přesto zájem. V takovém případě mu Nařízení nebrání jmenovat ho dobrovolně[172].

5.1.2 Kdo je pověřenec pro ochranu osobních údajů

Záleží pouze na rozhodnutí správce, zda pověřencem pro ochranu osobních údajů jmenuje svého zaměstnance či externí osobu, přičemž každá z možností přináší svá pro i proti. Například pověřenec pro ochranu osobních údajů coby zaměstnanec nevyžaduje dlouhé seznamování se správcovou činností, jelikož je s ní, jakožto i chodem celé organizace, jako zaměstnanec již dostatečně obeznámen. Oproti tomu externí pracovník například u správce nečerpá dovolenou, tím pádem správci nevzniká složité rozhodování, kdo ho bude zastupovat v plnění jeho úkolů v době nepřítomnosti[173].

Nařízení pak výběr nijak nekonkretizuje, pouze požaduje, aby úkoly pověřence pro ochranu osobních údajů vykonávala osoba, jejíž znalosti, zkušenosti a schopnosti dosahují v oblasti ochrany osobních údajů na národní i evropské úrovni dostatečných kvalit[174].

5.1.3 Činnost pověřence pro ochranu osobních údajů

Úkolem pověřence pro ochranu osobních údajů je pak zejména zajištění souladu správcovy činnosti s Nařízením nebo realizace posouzení vlivu na ochranu

[171] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4. s. 41.
[172] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8. s. 117.
[173] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. s. 258-260.
[174] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3. s. 339-340.

osobních údajů[175], poskytování odborného poradenství,[176] a podpora a školení zaměstnanců správce, jež participují na zpracování osobních údajů subjektů údajů[177]. Pověřenec také poskytuje součinnost Úřadu pro ochranu osobních údajů[178].

To v praktickém dopadu může vypadat například tak, že pověřenec se správcem spolu udržují pravidelný kontakt, správce poskytuje pověřenci ke kontrole veškerou dokumentaci, a to i průběžně, objeví-li se některé nové dokumenty, které se chystá správce používat, správce konzultuje s pověřencem veškeré skutečnosti týkající se jeho činnosti a osobních údajů, se kterými si správce neví rady nebo si jimi není jistý. Pověřenec také pravidelně navštěvuje správce, případně správce navštěvuje pověřence, a to za účelem pořádání školení pro správce a správcovy zaměstnance, a to pravidelně vždy v určitém smluveném intervalu.

[175] KALÍŠEK, Jindřich a Petra VĚŽNÍKOVÁ. Pověřenec pro ochranu osobních údajů dle nařízení GDPR - Nové pokyny WP29 k výkonu funkce. *Epravo.cz* [online]. 2017, 24. 1. 2017 [cit. 2020-04-01]. Dostupné z: https://www.epravo.cz/top/clanky/poverenec-pro-ochranu-osobnich-udaju-dle-narizeni-gdpr-nove-pokyny-wp29-k-vykonu-funkce-104829.html

[176] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7. s. 241.

[177] NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. První vydání. Praha: Klika, 2018. 141 s. Otevřeno. ISBN 978-80-88298-10-6. s. 139.

[178] *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: DonauMedia, s.r.o., [2018], ©2018. 96 s. ISBN 978-80-8183-049-5. s. 31.

Závěr

Cílem této diplomové práce bylo provést čtenáře praktickou implementací Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 a 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), přičemž ke správné implementaci je potřeba nejprve znát výklad určitých pojmů, zásad a práv z teoretické stránky, jež jsou předmětem první části, proto se na samotnou praktickou implementaci zaměřuje až druhá část diplomové práce.

Jelikož praktická část diplomové práce provádí implementací Nařízení, které se zabývá ochranou osobních údajů, bylo nezbytné nejprve vyjasnit, co přesně pojem osobní údaj znamená. Osobní údaje nejsou údaje týkající se právnických osob či anonymizované údaje, oproti tomu pseudonymizované údaje osobními údaji jsou. Osobní údaj přitom náleží subjektu údajů a je zpracováván správcem či zpracovatelem. Je tedy nezbytné dále označit, kdo je subjekt údajů, kdo správce a kdo zpracovatel, jaký mezi nimi panuje vztah a jakou činnost lze považovat za zpracování.

Dále se teoretická část zabývala zásadami, kterými by se měl správce dle Nařízení řídit a právy, kterých se subjekty údajů mohou dožadovat. Uvádím také právní tituly, na jejichž základě smí správce osobní údaje zpracovávat.

Druhá část diplomové práce už se pak zaměřovala právě na praktickou stránku, kdy jsem se snažila přinést čtenáři popis celého procesu implementace z pohledu správce od úplného počátku, kdy se správce nejprve seznamuje se svými povinnostmi, přes jednotlivé kroky přípravy až po uvedení do praxe a udržování zavedených postupů.

Samotná implementace se skládá z několika postupných částí, přičemž nejprve správce sestaví audit osobních údajů, který bude představovat základ pro další práci. Rozhodne, zda má povinnost vypracovat posouzení vlivu na ochranu osobních údajů a pokud nemá, zváží alespoň vypracování analýzy rizik. To jsou přípravné dokumenty, které mu usnadní další práci a pomohou se snadnější orientací ve vlastním zpracování.

Dále už správce postupuje do fáze, kdy přípravné dokumenty slouží k pomoci pro vytvoření dalších dokumentů. Musí vytvořit záznamy o činnostech zpracování, které slouží jako doklad souladu s Nařízením v případě kontroly. Správce také zreviduje veškerou dokumentaci, která není v souladu s Nařízením a zkontroluje, zda mu nechybí formulář pro získávání souhlasu se zpracováním osobních údajů.

Zpracovává-li správce osobní údaje na základě souhlasu subjektu údajů, musí vynaložit vysokou péči při kontrole, jakým způsobem souhlas od subjektů údajů získává. Problematika získávání souhlasu se zpracováním osobních údajů je samo o sobě dostatečně obsáhlé téma. S ohledem na skutečnost, že účinností Nařízení došlo ke zpřísnění požadavků, které musí být splněny, aby se mohlo skutečně jednat o souhlas, je žádoucí, aby se správce při kontrole, zda současná forma vyhovuje Nařízení, zabýval každou jednotlivou položkou, kterou Nařízení klade za podmínku.

Ačkoli už od účinnosti Nařízení uplynula dostatečně dlouhá doba na to, aby i tzv. opozdilci dali všechny své povinnosti do pořádku, stále se lze v každodenním životě běžně dostat do situace, kdy správce hodlá zpracovávat více našich osobních údajů, než je nezbytné a souhlas, který nám předkládá, neplní všechny podmínky. Vzpomeňme například na situaci, kdy jsme naposledy nakupovali v internetovém obchodě a při procházení jednotlivých kroků objednávky jsme se dostali ke kroku, kde nám správce nabízel pravidelné informování o nejnovějších produktech, akcích či soutěžích. A nyní se zamysleme, zda jsme takovou nabídku sami přijali, protože jsme chtěli být informování o novinkách, nebo, pokud jsme o takovou nabídku nestáli, jsme museli souhlas předem již připravený a označený správcem zrušit.

Dále jsem se zabývala, jakým způsobem by měl správce informovat subjekt údajů o zásadách, které dodržuje při zpracování, o právech subjektů údajů a způsobech jejich uplatnění, a také jakým způsobem by se měl vypořádat s pravidly souvisejícími s ochranou osobních údajů uvnitř organizace.

Teoretická část přináší vysvětlení pojmů správce a zpracovatel, praktická část vymezuje jejich vztah, vzájemné povinnosti, nutnost sepsání písemné smlouvy a její náležitosti, také jsem ale zmínila institut společných správců, zamyslela se nad tím, kdy je pro správce vhodné spojit se dohromady s jiným správcem a rozebrala náležitosti smlouvy mezi společnými správci.

V následujících kapitolách přináší diplomová práce zamyšlení nad tím, co po vytvoření přípravných dokumentů musí správce pro správnou implementaci udělat dále. Uvádí, kdy, jak často a o čem je vhodné pořádat školení a praktická část se uzavírá podkapitolou, která se zabývá institutem zvaným pověřenec pro ochranu osobních údajů.

Vzhledem k rozsáhlosti zvoleného tématu se diplomová práce zaměřuje pouze na nejzásadnější teoretické body, a především pak na jejich praktické naplňování, jenž je doplněné příklady a poznatky z praxe.

Resumé

The aim of this diploma thesis is to describe the implementation of the Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as well as certain terms and principles.

The thesis is divided into two main parts, the first of which is theoretical and defines certain terms (e.g., personal data, controller, processor), principles of GDPR and rights of the data subjects. I paid more attention to specific terms, as for example personal data. Personal data include data of natural persons and exclude data of legal persons. Personal data also cover pseudonymous data, however omit anonymous data. I have also dealt with the difference between pseudonymous and anonymous data. Anonymous data cannot be connected with a specific person, on the contrary pseudonymous data can be connected with a specific person with the use of special encryption. The theoretical part also focuses on the situations, when the processing is lawful.

The second - practical - part describes the whole process of the implementation from the controller´s perspective. In summary, the controller has to first acknowledge their obligations, chart the current situation according to the arranged informative documents, create records of processing activities and check or, in case of need, add the documentation required. At last, all the well-established methods are put into practice. The controller has to be especially attentive and inspect the form of consent. The regulation puts strict requirements on the form of the consent. The consent must be specific, informed, unambiguous and must be given freely. All of these requirements must be satisfied in order to process personal data on the basis of consent and for the processing to be lawful. The consent can be given by the data subject themselves only.

Due to the extensiveness of the selected topic, the diploma thesis focuses on the most fundamental theoretical articles and mainly the practical execution and maintenance of the theoretical methods, which are complemented by examples and pieces of knowledge of practice.

Literatura

Seznam použité literatury

- NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 s. Pro praxi. ISBN 978-80-7380-689-7.
- NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. První vydání. Praha: Klika, 2018. 141 s. Otevřeno. ISBN 978-80-88298-10-6.
- NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Vydání první. Praha: Wolters Kluwer, 2017. 525 s. Praktický komentář. ISBN 978-80-7552-765-3.
- ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 343 s. Právo. ISBN 978-80-7554-152-9.
- NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. 301 s. Právo pro praxi. ISBN 978-80-271-0668-4.
- *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: DonauMedia, s.r.o., [2018], ©2018. 96 s. ISBN 978-80-8183-049-5.
- FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR Hmotné a procesní aspekty prakticky*. Praha: C. H. Beck, 2019. ISBN 978-80-7400-762-0.
- STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. První vydání. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8.
- GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. Brno: Computer Press, 2010. ISBN 978-80-251-2621-9.

Seznam použitých časopiseckých zdrojů

- KOČICOVÁ, Věra a HORÁK, Filip. (R)evoluce v ochraně osobních údajů?: General Data Protection Regulation (GDPR). *IT Systems*, 2016, 18(7-8), s. 20-21. ISSN 1802-002X.
- MORÁVEK, Jakub. Když dva dělají totéž, není to totéž, aneb, GDPR jako přestupková amnestie?. *Právní rozhledy*. 2018, roč. 26, č. 13-14, s. 487-493. ISSN 1210-6410.
- MALÝ, Zbyněk. GDPR je nekonečný příběh... *Sdělovací technika*, 2018, 66(10), s. 32. ISSN 0036-9942.
- OTEVŘEL, Petr. GDPR od A do Z: díl první: Obecný úvod o nové úpravě nakládání s osobními údaji. 1. Díl. *IT Systems*, 2017, 19(7-8), s. 38-39. ISSN 1802-002X.
- MORÁVEK, Jakub. Ochrana dat zaměstnanců: stačí drobně seřídit stroj. *Právní rádce*, 2018, 26(2), s. 46-48. ISSN 1210-4817.
- MALIŠ, Petr. GDPR od A do Z: díl druhý: Územní a věcná působnost GDPR. 2. Díl. *IT Systems*, 2017, 19(9), s. 54-56. ISSN 1802-002X.
- MALIŠ, Petr. GDPR od A do Z: díl sedmý: Vztah správce a zpracovatele osobních údajů podle GDPR. 7. Díl. *IT Systems*, 2018, 20(3), s. 46-48. ISSN 1802-002X.
- NEUWIRT, Karel. GDPR změní některé dosavadní zvyklosti. *Sdělovací technika*, 2017, 65(12), s. 10-11. ISSN 0036-9942.
- MATYSOVÁ, Monika a NONNEMANN, František. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, 26(12), s. 424-433. ISSN 1210-6410.
- HLADÍK, Martin, HRUŠKA, Jan a KRAMER, Jaroslav, ed. Osobní údaje 2018. *Právní rádce*, 2018, 26(4), s. 16-18. ISSN 1210-4817.
- TOMEK, Roman. Soulad s GDPR a dokumentace potřebná k jeho dosažení. Část I. *Soukromé právo*, 2019, 7(2), s. 9-17. ISSN 2533-4239.
- VEJVODOVÁ, Alžběta. GDPR očima expertů: Žádný strašák, ale příležitost. *Právní rádce*, 2017, 25(4), s. 24-25. ISSN 1210-4817.

- TOMEK, Roman. Soulad s GDPR a dokumentace potřebná k jeho dosažení. Část II. *Soukromé právo,* 2019, 7(3), s. 25-27. ISSN 2533-4239.
- OTEVŘEL, Petr. GDPR od A do Z: díl čtvrtý: Jste povinni jmenovat pověřence pro ochranu osobních údajů?. 4. Díl. *IT Systems,* 2017, 19(11), s. 14-15. ISSN 1802-002X.
- NULÍČEK, Michal. První výkladové pokyny k GDPR: Co přináší a jaký budou mít praktický dopad?. *Právní rádce*, 2017, 25(1), s. 58-59. ISSN 1210-4817.
- JIRÁKOVÁ, Gabriela a KALAŠOVÁ, Lucie. Praktický pohled na GDPR. *Právní rádce*. 2018, roč. 26, č. 4, s. 38-40. ISSN 1210-4817.

Seznam použité judikatury

- Stanovisko generálního advokáta M. Campos Sánchez-Bordony přednesené dne 14. ledna 2020(1), Věc C-78/18
- Stanovisko generálního advokáta Macieje Szpunara přednesené dne 4. března 2020 (1), Věc C-61/19
- Rozsudek Soudního dvora ze dne 1. října 2019, ve věci C-673/17
- Rozsudek Soudního dvora ze dne 24. září 2019, ve věci C-507/17
- Stanovisko generálního advokáta H. Saugmandsgaard Øe přednesené dne 19. prosince 2019(1), Věc C-311/18

Seznam použitých právních předpisů

- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- Zákon č. 101/2000 Sb., zákon o ochraně osobních údajů a o změně některých zákonů
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 90/2012 Sb., zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích)

- Zákon č. 110/2019 Sb., zákon o zpracování osobních údajů
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a změně některých zákonů

Seznam použitých internetových zdrojů

- LUPIEŃSKÁ, Petra. Rozesílání obchodních sdělení prostřednictvím třetí strany a souhlas dle GDPR. *Epravo.cz* [online]. 2020, 10. 1. 2020 [cit. 2020-04-01]. Dostupné z: https://www.epravo.cz/top/clanky/rozesilani-obchodnich-sdeleni-prostrednictvim-treti-strany-a-souhlas-dle-gdpr-110440.html
- ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Dozorová a rozhodovací činnost* [online]. [cit. 2020-03-30]. Dostupné z: https://www.uoou.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277
- CETKOVSKÁ, Barbora a Jakub MÁLEK. Adaptační zákon k GDPR byl konečně přijat. *Epravo.cz* [online]. Praha: epravo.cz, 2019, 3. 4. 2019 [cit. 2020-03-22]. Dostupné z: https://www.epravo.cz/top/clanky/adaptacni-zakon-k-gdpr-byl-konecne-prijat-109122.html
- KALÍŠEK, Jindřich a Petra VĚŽNÍKOVÁ. Pověřenec pro ochranu osobních údajů dle nařízení GDPR - Nové pokyny WP29 k výkonu funkce. *Epravo.cz* [online]. 2017, 24. 1. 2017 [cit. 2020-04-01]. Dostupné z: https://www.epravo.cz/top/clanky/poverenec-pro-ochranu-osobnich-udaju-dle-narizeni-gdpr-nove-pokyny-wp29-k-vykonu-funkce-104829.html