Západočeská univerzita v Plzni

Fakulta právnická

Diplomová práce

Vybrané dopady GDPR na subjekty a správce osobních údajů

Eliška Heisenbergerová

Plzeň 2020

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

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

Jméno a příjmení:	**Eliška HEISENBERGEROVÁ**
Osobní číslo:	**R15M0091P**
Studijní program:	**M6805 Právo a právní věda**
Studijní obor:	**Právo**
Téma práce:	**Vybrané dopady GDPR na subjekty a správce osobních údajů**
Zadávající katedra:	**Katedra ústavního a evropského práva**

Zásady pro vypracování

1. Úvod
2. Historický exkurz
3. Rekodifikace a podněty k ní
4. Vybrané změny v právech a povinnostech subjektů osobních údajů
5. Vybrané změny v právech a povinnostech správců osobních údajů
6. Závěr

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

Seznam doporučené literatury:

- Nulíček, M., Donát, J. Nonnemann, F., Lichnovský, B., Tomíšek, J., Kovaříková, K. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR, 2018. 580 s
- Pattynová, J., Suchánková, L., Černý, J. a kolektiv. Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář. Praha: Leges. 488 s
- Paul Voigt, Axel von dem Bussche. The EU General Data Protection Regulation (GDPR): a practical guide. Cham: Springer. 383 s
- Nezmar, L. GDPR : praktický průvodce implementací. Praha: Grada Publishing. 2017. 301 s

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

Datum zadání diplomové práce: **6. března 2019**
Termín odevzdání diplomové práce: **31. března 2020**

Západočeská univerzita v Plzni
L.S.
Fakulta právnická

Doc. JUDr. Jan Pauly, CSc.
děkan

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

V Plzni dne 26. června 2019

Prohlášení

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

V Plzni, duben 2020 _____

Eliška Heisenbergerová

Poděkování

Ráda bych poděkovala JUDr. Tomáši Pezlovi za odborné vedení během zpracování této diplomové práce, mé rodině a přátelům za podporu během studia a mým kolegům za cenné rady a prostor pro vzdělávání se v právu ochrany osobních údajů.

Obsah

Úvod

Dne 25. května 2018 vstoupilo v účinnost 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, jeden z nejdiskutovanějších právních předpisů posledních let. Již přípravy na účinnost tohoto nařízení vyvolávaly bouřlivé reakce, mnohdy spíše negativního charakteru a důvodů k nim bylo hned několik.

Aby mohly být analyzovány změny, které toto nařízení přineslo, bude za tímto účelem jako první nastíněna historie a vývoj pojetí osobních údajů a jejich ochrany.

První velkou změnu představovala forma právního předpisu. Vůbec poprvé byla zvolena forma přímo účinného nařízení, z toho důvodu bude další kapitola zaměřena na důvody a okolnosti, které vedly k vytvoření takového právního předpisu, který jednotně upravuje zacházení s osobními údaji ve všech členských státech Evropské unie.

Příchod nové legislativy na poli ochrany osobních údajů avizoval revoluci v této právní úpravě, a to především z důvodů posílení slabšího postavení subjektu údajů v rozšíření jeho práv a zároveň zatížení správců novými povinnostmi. Než však bude přistoupeno k popisu jednotlivých práv a povinností, bude definována základní terminologii v právu na ochranu osobních údajů. Následovat bude popis práv subjektů, která jim přiznává toto nařízení a následně jaké povinnosti a vyplývající nové nástroje pro jejich dodržování ukládá správcům.

Společnosti v rámci příprav na účinnost nařízení investovaly nemalé peněžní částky do implementace této právní úpravy. Proto cílem této diplomové práce bude zjistit, jaké konkrétní dopady s sebou přinesla účinnost nařízení pro práva a povinnosti subjektů a správců osobních údajů a zhodnotit, zda se jedná o revoluci v právu osobních údajů v takové míře, za jakou byla považována během příprav na ni, zda obavy z účinnosti nařízení byly oprávněné a výše peněžních investic adekvátní.

1 Stručný vývoj ochrany osobních údajů

Pokud má být hovořeno o vývoji ochrany osobních údajů, musí být nejprve vymezen a objasněn vývoj samotných osobních údajů. Osobní údaje existují takřka od prvopočátku lidstva jako jakýsi soubor identifikačních znaků jednotlivce, byť v té době zajisté nebyl tak rozsáhlý a především zpracovatelný. Od dob, kdy identifikátorem mohla být například jistá forma jména a lidstvo nemělo pražádnou potřebu osobní údaje chránit, prošla společnost komplexním rozvojem, během nějž byly osobní údaje čím dál více využívány a zpracovávány.

S ohledem na rozlišování různých druhů osobních údajů nicméně ve společnosti docházelo k uvědomování si odlišností mezi jednotlivci, zejména náboženské, rasové či majetkové rozdíly, které vedly ke vzniku konfliktů nejen mezilidských, nýbrž až ke gradaci ve války světového měřítka. Jejich následkem bylo pocítěno riziko zneužívání osobních údajů a následná potřeba je chránit, což položilo základní kameny úpravy jejich ochrany.

1.1 Historický exkurz světového vývoje ochrany osobních údajů

Za první dokumenty, které se z určitého hlediska zabývají ochranou osobních údajů, lze považovat Deklaraci práv člověka a občana z roku 1789, na kterou posléze navázala Všeobecná deklarace lidských práv z roku 1948, byť nikdy nebyla právně závazná. Oba tyto dokumenty se nezabývají přímo ochranou osobních údajů, nýbrž ochranou soukromí.

Obdobně jako Všeobecná deklarace upravovaly oblast práva na soukromí Evropská úmluva o ochraně lidských práv a základních svobod a Mezinárodní pakt o občanských a politických právech. Tyto však již právně závazné byly.

Prvním samostatným dokumentem, který se komplexně věnoval ochraně osobních údajů, byla až Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (č. 115/2001 Sb. m. s.), známá také jako Úmluva č. 108 z roku 1981 a její Dodatkový protokol z roku 2001[1] (dále jen „Úmluva č. 108“). Ta poprvé stanovila základní zásady zpracování osobních údajů v právním předpisu, které byly doposud pouze nepsanou zvyklostí. Definovala také základní pojmy, kterými jsou například „osobní údaj“, „zpracování“ či „správce“, které jsou po

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

obsahové stránce nezměněné až dodnes. Také není náhodou, že právě den přijetí Úmluvy č. 108, tj. 28. leden, je na její počest Mezinárodním dnem ochrany osobních údajů[2].

S ohledem na vývoj společnosti v 80.-90. letech 20. století musela legislativa adekvátně reagovat především na technologický pokrok, díky němuž se zvyšovala potřeba předávat osobní údaje do třetích zemí a zároveň bylo zavedeno automatizované zpracovávání osobních údajů. S ohledem na základní myšlenku fungování Evropské unie a evropského prostoru vznikla potřeba sjednotit úpravu ochrany osobních údajů vhodným právním nástrojem regulace pro členské státy. Uvedené požadavky naplnila Směrnice Evropského parlamentu a Rady 95/46/ES, ze dne 24. října 1995 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů* (dále jen „Směrnice č. 95/46/ES“).

Tato směrnice vycházela z Úmluvy č. 108, v níž se v mnohých úpravách inspirovala. Řešila problematiku předávání osobních údajů, a to nejen v rámci Evropské unie, ale hlavně i mimo členské státy. Poprvé se zde objevila i práva subjektů údajů, tj. pilíř současné právní úpravy v Evropské unii[3].

Další vývoj ochrany osobních údajů reflektoval stupeň globalizace a rapidní nárůst užívání internetu za vzniku sociálních sítí, pro jejichž problematiku už zastaralá Směrnice č. 95/46/ES a z ní vycházející vnitrostátní zákony nebyly nadále použitelné. To dalo impuls pro reakci vycházející z půdy Evropské unie, tedy vznik 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* (dále jen „Obecné nařízení“). Důvodům a okolnostem jeho vzniku se budu věnovat v dalších kapitolách.

1.2 Historický exkurz vývoje ochrany osobních údajů na území České republiky

Počátky ochrany soukromí na našem území nalezneme již v dobách monarchie, kdy byly poprvé uzákoněny zákonem č. 87/1862 Sb.z.s., *o ochraně svobody osobní* a následně se vznikem Československa ústavním zákonem č. 293/1920 Sb., *o ochraně svobody osobní, domovní a tajemství listovního*. Zatímco zbytek západního světa legislativou reagoval na vzrůstající potřebu chránit si své

[2] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 14.
[3] Tamtéž, str. 15.

soukromí a zvláště pak chránit své osobní údaje, zde nastala situace diametrálně odlišná. Československo se stalo součástí východního bloku a díky komunistickému režimu trvajícímu čtyřicet let zde byl vyloučen jakýkoliv rozvoj práva na ochranu soukromí.

O jakémsi počátku nápravy tohoto stavu můžeme mluvit s přijetím zákona č. 256/1992 Sb., *o ochraně osobních údajů v informačních systémech*, který se dle názvu vztahoval pouze na informační systémy, byť v 90. letech převažovalo zpracovávání v materiálních evidencích. Tento zákon také neobsahoval sankční ustanovení a ani nestanovil dozorčí orgán.

Ochrana osobních údajů byla také promítnuta do Listiny základních práv a svobod, konkrétně do čl. 10 odst. 3, který zní: *„Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“*[4] Nicméně realizace tohoto ustanovení narazila na problém, spočívající v dosud neexistujícím zákoně, který by ho prováděl.

Komplexní zákonnou úpravu ochrany osobních údajů během jejich zpracování jsme získali až účinností zákona č. 101/2000 Sb., *o ochraně osobních údajů a o změně některých zákonů* (dále jen „ZOOÚ“), který nahradil zákon o ochraně osobních údajů v informačních systémech. Tento právní předpis poprvé zřídil nezávislý dozorový orgán, a to Úřad pro ochranu osobních údajů[5].

ZOOÚ byl mnohokrát za svoji účinnost novelizován, z čehož nejvýznamnější novelizace proběhla v roce 2004. Z důvodu vstupu České republiky do Evropské unie muselo i v případě legislativy upravující ochranu osobních údajů dojít k uvedení v soulad s právem unijním, přičemž tehdejší podoba ZOOÚ neodpovídala Směrnici č. 95/46/ES a bylo nutné její transponování do vnitrostátní právní úpravy.

S účinností Obecného nařízení, tj. 25. května 2018, přešla role hmotněprávní úpravy ochrany osobních údajů na nařízení, přičemž ZOOÚ měl být zrušen a zároveň měl být zhotoven adaptační zákon, jehož funkcí je prakticky vytvořit jistý „můstek“ mezi obecnou právní úpravou unijní a právní úpravou vnitrostátní. Pro

[4] Čl. 10 odst. 3 usnesení č. 2/1993 Sb., usnesení předsednictva České národní rady *o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky*.
[5] Pro účely této práce bude pro tento úřad používána zkratka ÚOOÚ či pojmenování dozorový úřad, pokud kontext nebude potřebovat konkretizaci.

příklad lze uvést problematiku ustanovení dozorového úřadu – nařízení říká následující: *„Každý členský stát stanoví, že jeden nebo více nezávislých orgánů veřejné moci jsou pověřeny monitorováním uplatňování tohoto nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie.“*[6] ÚOOÚ byl ustanoven dozorovým úřadem nad zpracováním osobních údajů v § 50 odst. 1 zákona č. 110/2019 Sb., *o zpracování osobních údajů*, který je adaptačním zákonem k nařízení.

Nutno však podotknout, že přes adekvátně dlouhou *vacatio legis* k uvedení v soulad s Obecným nařízením tento stav v den účinnosti nařízení nenastal. Jak bylo zmiňováno výše, přestože Obecné nařízení převzalo hmotněprávní roli ZOOÚ[7], tento právní předpis byl účinný až do 23. 4. 2019, než prošel legislativním procesem adaptační zákon.

[6] Čl. 51 odst. 1 Obecného nařízení.
[7] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 19.

2 Okolnosti a důvody rekodifikace právní úpravy ochrany osobních údajů

Jak již bylo nastíněno v předchozí kapitole, změna právní úpravy je reakcí na vývoj společnosti, a to především na přesun notné části každodenního života lidí do virtuální oblasti – internetu. Směrnice č. 95/46/ES reflektovala stav 90. let 20. století, tedy dobu, kdy existoval velmi malý počet webových stránek a co se elektronické komunikace týká, pouze omezené množství osob používalo e-mail.

S nástupem digitalizace a kybernetizace našeho prostoru vyvstala teprve reálná hodnota osobních údajů, resp. jak cennou komoditou ve skutečnosti jsou.[8] Vlivem internetového obchodování, bankovnictví a rozmachem sociálních sítí docházelo k automatizování osobních údajů v mnohem větší míře než doposud. Zároveň vyvstala taková rizika zneužívání a krádeže osobních údajů, na které již nebylo možné reagovat dalšími novelami zmíněné směrnice.[9]

Debaty o potřebě modernizace pravidel pro ochranu osobních údajů započaly již v roce 2009, kdy Evropská komise zahájila veřejné diskuze týkající se budoucího právního rámce ochrany osobních údajů. O tři roky později byl Evropskou komisí předložen první návrh právního předpisu, jenž spustil zdlouhavý legislativní proces.[10] Nicméně již při předkládání onoho prvního návrhu se jednalo o nařízení jakožto druhu právního předpisu, nikoliv o směrnici.

2.1 Aspekty vedoucí ke změně druhu právního předpisu

Použití směrnice jako právního aktu Evropské unie znamenalo počátek harmonizace právní úpravy členských států. Tento právní akt nepřímo stanovuje, čeho mají státy dosáhnout.[11] Nicméně směrnici je nezbytné transponovat do vnitrostátní právní úpravy. Tato transpozice však umožňovala, byť nikterak cíleně, různorodou interpretaci norem užitých ve směrnici jednotlivými státy. Důsledkem toho došlo k odlišnému obsahu právních předpisů, které členské státy přijímaly do svých vnitrostátních právních řádů. Žůrek ve své publikaci uvádí následující příklad

[8] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi, str. 14.
[9] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi, str. 29.
[10] European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2018. ISBN 978-92-871-9849-5, str. 30.
[11] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 15.

této odlišnosti: *„V některých státech byli povinní tzv. pověřenci pro ochranu osobních údajů, v jiných státech byli fakultativní a v ostatních nebyli právně zakotveni.“*[12]

Uvedená diferenciace byla během dalších let ještě umocněna prováděním novelizací těchto právních předpisů, a způsobila tak opak oproti žádoucí harmonizaci jednotné úpravy.

Použití nařízení Evropské unie se jeví jako zcela logický krok vzhledem k předešlým zkušenostem se směrnicí. Nařízení je na rozdíl od směrnice obecně závazné a bezprostředně použitelné[13], tedy stanovuje práva a povinnosti adresátům přímo, bez nutnosti jakékoliv formy recepce do vnitrostátního práva.

2.2 Cíle revize právní úpravy ochrany osobních údajů

Účel přijetí nového právního rámce ochrany osobních údajů lze rozdělit do tří hlavních myšlenek.

Jako první lze uvést již zmiňovaný technologický rozvoj. S ohledem na digitalizaci dochází k nebývalému rozsahu poskytování a sdílení osobních údajů samotnými subjekty. Dále z důvodu globalizace technologický pokrok značně usnadňuje volný pohyb osobních údajů nejen v rámci členských států Evropské unie, ale také častěji dochází k jejich předávání do třetích zemí. Cílem přijetí Obecného nařízení je pružně reagovat na tento rozvoj, ať už v jeho pozitivech či negativech, která představuje.[14]

Druhým bodem je bezesporu sjednocení právní úpravy v rámci Evropské unie. Cílem nařízení je napravit roztříštěnost právní úpravy, která byla způsobena rozdílnou interpretací a aplikací Směrnice č. 95/46/ES, zároveň zajistit jednotnou a soudržnou ochranu osobních údajů a usnadnit tak jejich volný pohyb v rámci unie.[15]

Třetí bod vychází z předcházejících dvou a je jím posílení práv subjektů údajů. Dynamický rozvoj technologií podstatně změnil rizika týkající se zneužívání osobních údajů. Obecné nařízení tak přichází s nástroji, které rozšiřují jak práva

[12] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 15.
[13] KRÁL, R. Nařízení v ES. In: HENDRYCH, D. a kol. Právnický slovník. In: Beck-online.cz [online databáze]. 3. vydání. Praha: C. H. Beck, 2009. [cit. 2019-02-09]. Dostupné z: https://www-beck-online.cz
[14] Recitál č. 6 Obecného nařízení.
[15] Recitál č. 9 a 10 Obecného nařízení.

subjektů osobních údajů, tak povinnosti správců, kteří údaje zpracovávají. Nařízení tak umožňuje subjektům větší kontrolu nad zpracováním jejich osobních údajů, zároveň zvyšuje právní jistotu a důvěru s ohledem na účinné nástroje důsledného vymáhání práv.[16]

Konkrétní vybrané změny práv a povinností budou podrobně popsány v dalších částech této práce.

2.3 Změny v pojetí přístupu založeném na riziku a principu odpovědnosti správce

Velmi významnou změnou, kterou se Obecné nařízení liší od Směrnice č. 95/46/ES, jsou změny ve dvou základních přístupech, a to přístupu založeném na riziku a principu odpovědnosti správce. Aby nedošlo k omylu, tyto principy nejsou novinkou ve svém slova smyslu, v určité míře je obsahovala již zmiňovaná směrnice. Avšak v případě Obecného nařízení uvedené přístupy prostupují právním předpisem jako celkem a dle Žůrka *„…představují jednu z nejvýraznějších kvalitativních změn oproti Směrnici 95/46/ES“*.[17]

2.3.1 Přístup založený na riziku

Pojetí tohoto přístupu tak, jak je stanoveno v Obecném nařízení, je mnohem důmyslněji zpracovanou verzí jejího předchůdce, který byl použit ve Směrnici č. 95/46/ES.

Dle názoru ÚOOÚ přístup založený na riziku obecně znamená, že *„správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů.“*[18]

Zpracování osobních údajů vždy představuje určité riziko pro jejich subjekty, nelze však určit jednotnou míru tohoto rizika, ani stanovit nástroje k zabezpečení. Touto logikou se již zabývala Směrnice č. 95/46/ES. Obecné nařízení však pokročilo ještě dál a stanovilo správcům různé povinnosti dle stupně

[16] Recitál č. 7 a 8 Obecného nařízení.
[17] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 25.
[18] *Nové přístupy a povinnosti*. [online] In: *Uoou.cz*. [cit. 3. 3. 2020]. Dostupné z: https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=4744.

rizika, které zpracování představuje. Lze hovořit o jednoduché přímce – se stoupajícím rizikem stoupá i množství povinností.[19]

Pro splnění těchto povinností stanovuje Obecné nařízení nástroje, kterými jsou záznamy o činnostech zpracování, jmenování pověřence pro ochranu osobních údajů, posouzení vlivu na ochranu osobních údajů a předchozí konzultace s dozorovým úřadem. [20] Vzhledem ke skutečnosti, že poslední tři uvedené instituty jsou zcela novými povinnostmi správce osobních údajů, budou později detailně rozpracovány v následujících částech práce.

2.3.2 Princip odpovědnosti správce

Jak už napovídá samotný název, jedná se o princip, jenž stanovuje, že správce je odpovědný za prováděné zpracování osobních údajů. Stejně jako v případě přístupu založeném na riziku i tento institut již znala Směrnice č. 95/46/ES. Obecné nařízení však přináší změnu v povinnosti z odpovědnosti vycházející, a tedy že správce musí být schopen doložit soulad se zásadami zpracování. Tuto povinnost stanovuje čl. 5 v odst. 2[21] a 24 odst. 1[22] Obecného nařízení.

I zde Obecné nařízení přichází se zcela novými instituty, díky nimž lze doložit soulad. Jedná se zejména o kodexy chování, osvědčení, pokyny Evropského sboru pro ochranu osobních údajů či také záznamy o činnostech zpracování.[23] Nejedná se však o povinnost tyto nástroje užít, například použití kodexů a osvědčení je založeno na čistě dobrovolné bázi.

Zpracovávání osobních údajů v souladu s tímto principem, tedy zajišťování a následné dokládání souladu, není záležitostí jednorázového aktu. Naopak se jedná o průběžnou činnost, během níž správce pravidelně přezkoumává, zda během

[19] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 28.
[20] *Nové přístupy a povinnosti*. [online] In: *Uoou.cz*. [cit. 3. 3. 2020]. Dostupné z: https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=4744
[21] Správce odpovídá za dodržení odstavce 1 a musí být schopen toto dodržení souladu doložit („odpovědnost“).
[22] S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením
[23] Recitál č. 77 Obecného nařízení.

zpracování nenastala nová rizika, kontroluje adekvátnost zabezpečení a odstraňuje případné nesoulady.[24]

[24] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 27.

3 Působnost Obecného nařízení

Tato kapitola bude zaměřena na osobní, věcnou a místní působnost, jejich negativní i pozitivní pojetí a extrateritorialitu.

3.1 Osobní působnost

Osobní působnost Obecné nařízení explicitně nikterak neupravuje, jako je tomu u věcné a místní působnosti, kterým jsou věnovány samostatné články. Nicméně i tak ji lze určit, neboť vychází z celého právního předpisu.

Adresáty jsou bezesporu zejména správci, zpracovatelé, subjekty osobních údajů a dozorový úřad. Obecné nařízení vymezuje ještě další adresáty, mezi než lze zařadit také akreditované monitorovací orgány dozorující nad dodržováním kodexů chování či orgány akreditované k udělování osvědčení. V neposlední řadě jsou jimi i samotné členské státy, jimž Obecné nařízení také uděluje určité povinnosti.[25]

3.2 Věcná působnost

Obecné nařízení v čl. 2[26] vymezuje, na jaký okruh případů se vztahuje, a to jak pozitivně, tak negativně.

Pozitivní vymezení věcné působnosti se nikterak neliší od ustanovení, které obsahovala Směrnice č. 95/46/ES. Případy, na které se působnost Obecného nařízení bude vztahovat, mohou být dvojího typu - zcela nebo z části automatizované zpracovávání osobních údajů např. webovým skriptem a osobní údaje zpracovávané v evidenci, tedy takové zpracování, kdy jsou osobní údaje např. uloženy v kartotéce.[27]

Negativnímu vymezení se věnuje článek 2 odst. 2 Obecného nařízení, přičemž uvádí čtyři výjimky.

[25] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 36.
[26] Čl. 2 odst. 1: *Toto nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.*
[27] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 65.

První výjimka je dle písm. a) výše uvedeného odstavce zpracování při výkonu činnosti, která nespadá do oblasti působnosti práva Unie. Dle Nulíčka a spol. k této situaci může dojít v souvislosti se zajišťováním národní bezpečnosti.[28]

Druhou výjimkou dle písm. b) stejného odstavce je zpracování členskými státy při výkonu činností, které spadají do působnosti hlavy V kapitoly 2 Smlouvy o EU.

Třetí výjimku dle písm. c) téhož odstavce tvoří fyzickou osobou v průběhu výlučně osobních či domácích činností. Tuto výjimku obsahoval již zákon č. 101/2000 Sb., *o ochraně osobních údajů a o změně některých zákonů* v § 3 odst. 3.[29] Podle Žůrka sem lze zařadit i užívání jakýchkoliv sociálních sítí, pokud nejde o profesní či obchodní činnosti.[30] Nutno však podotknout, že k této problematice uvádí recitál 18 Obecného nařízení, že se tato výjimka nevztahuje na poskytovatele těchto prostředků jako např. sociálních sítí.

Čtvrtou výjimkou dle písm. d) onoho odstavce je zpracování příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Tuto oblast upravuje zvláštní směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV*, která byla přijata současně s Obecným nařízením.

3.3 Místní působnost

Při stanovení místní působnosti Obecného nařízení došlo k významným změnám oproti právní úpravě Směrnice č. 95/46/ES. Místní působnosti se věnuje článek 3 Obecného nařízení a určuje, na jaké území se vztahuje působnost Obecného nařízení, přičemž tak vymezuje tři situace.

[28] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 66.
[29] Tento zákon se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.
[30] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 37.

První situace dle čl. 3 odst. 1 nastává, pokud dojde ke zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii bez ohledu na to, zda na území Unie k samotnému zpracování dochází. Zde můžeme jednoznačně spatřovat rozšíření oproti ustanovení užitému ve směrnici. Nejen že se vztahuje jak na činnost správce, tak i zpracovatele, navíc je zde užit pojem provozovny. Lze tak soudit, že pokud společnost se sídlem v Japonsku, jejíž zástupce zpracovávající osobní údaje bude mít provozovnu např. na Slovensku, podléhá Obecnému nařízení.

Druhá situace obsažená v čl. 3 odst. 2 hovoří o extrateritoriální působnosti nařízení, neboť vymezuje, za jakých okolností se Obecné nařízení vztahuje na správce či zpracovatele, kteří nemají sídlo ani provozovnu na území Evropské unie. Prvním případem je nabízí-li správce zboží či služby subjektům údajů v Evropské unii. Nicméně o něco obtížněji prokazatelné je právě úmyslné zacílení na občany Unie. S vyřešením této problematiky napomáhá recitál č. 23 Obecného nařízení uvedením několika faktorů, které by toto zacílení mohly dokládat: *„…používání jazyka nebo měny obecně používaných v jednom nebo více členských státech, spolu s možností objednat zboží a služby v tomto jiném jazyce nebo zmínky o zákaznících či uživatelích nacházejících se v Unii.“*[31] Druhý případ nastává, pokud dochází k monitorování chování subjektů údajů na území Evropské unie. Typicky tato situace nastává při sledování chování uživatelů na internetu např. za použití tzv. cookies či sledování IP adresy.[32] Tyto údaje lze považovat za osobní, neboť vypovídají o tom, co konkrétní subjekt údajů vyhledával ve spojitosti s údajem o čase a místě.

Třetí situace se dle čl. 3 odst. 3 vztahuje na zpracování osobních údajů správcem, který není usazen v členském státu Evropské unie, zároveň je ale splněna podmínka, že se na tomto místě uplatňuje právo některého členského státu v souladu s mezinárodním právem veřejným. Typicky tak půjde o zastoupení členského státu Unie během vykonávání diplomatických či konzulárních misí.[33]

[31] Recitál č. 23 Obecného nařízení.
[32] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 72.
[33] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 39.

4 Definování základních terminologických pojmů

Pojmům používaným v právu na ochranu osobních údajů se věnuje čl. 4 Obecného nařízení čítající 26 odstavců neboli 26 pojmů. V této kapitole budou charakterizovány pojmy nejvíce užívané, a to nejen v této práci, ale především v praxi a také pojmy, jejichž definování se jeví jako značně problematické.

4.1 Osobní údaj

Definice tohoto pojmu je naprosto zásadní pro celou oblast úpravy osobních údajů. Obecné nařízení uvádí následující znění: „*Osobními údaji (se rozumí) veškeré informace o identifikované nebo identifikovatelné fyzické osobě…* “[34] Tato definice je obsahově shodná s tou, jež byla použita ve Směrnici č. 95/46/ES a rovněž i v ZOOÚ.

Základní informací je, že Obecné nařízení se vztahuje pouze na osobní údaje fyzických osob. Do působnosti nařízení tedy nespadají osoby právnické. Rovněž je podmínkou fyzická existence dané osoby, nelze tedy hovořit o osobách zemřelých. Na ochranu jejich osobnostních práv se užijí ustanovení soukromého práva, resp. občanského.[35]

K problematice vazby mezi informací a subjektem údajů lze použít výkladové stanovisko pracovní skupiny WP 29 (orig. *Article 29 Data Protection Working Party*, dále jen „WP 29“), byť bylo vytvořeno k výkladu ustanovení užitého v předešlém právním předpisu. V uvedeném stanovisku stojí za zmínku zejména část věnující se spojitosti informace s osobou tak, aby mohla být osobním údajem. Stanovisko uvádí, že zde musí být posouzeny tři složky – složka obsahová, složka účelová a složka výsledku. Jinými slovy údaj musí obsahovat informaci o subjektu, která je zpracovávána za určitým účelem a její zpracování má určitý dopad na práva a zájmy subjektu údajů.[36]

Ustanovení definující osobní údaj v Obecném nařízení nicméně pokračuje následovně: „*…identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze*

[34] Čl. 4 odst. 1 Obecného nařízení.
[35] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 81.
[36] Opinion (WP 136) 4/2007 on the concept of personal data adopted on 20th June. In: *Ec.europa.eu* [online]. s. 10 [cit. 2020-03-09]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“[37] Byť se zdá, že Obecné nařízení rozšiřuje demonstrativní výčet identifikátorů, uvedené však byly považovány za možné identifikátory již za účinnosti Směrnice č. 95/46/ES. Přesto však v explicitním zakotvení zejména lokačních údajů či síťového identifikátoru lze spatřovat reflektování kybernetizace společnosti.

4.1.1 Anonymní a anonymizované údaje

V souvislosti s pojmem osobní údaj je možné charakterizovat dva snadno zaměnitelné termíny, a to anonymní a anonymizované údaje.

Anonymní údaj byl definován v předchozí právní úpravě v § 4 písm. c) ZOOÚ[38]. Jedná se o údaj, který nikdy nebyl osobním údajem, a tedy neexistuje žádná vazba mezi ním a subjektem údajů.[39]

Oproti tomu anonymizovaný údaj dříve byl osobním údajem, posléze však došlo k takové úpravě, že nadále není spojitelný se subjektem údajů, a to ani takovou osobou, která anonymizaci provedla. Technikám, jak provádět anonymizaci, bylo věnováno stanovisko WP 29 Opinion (WP216) 05/2014 *on Anonymisation Techniques*. Byť tedy původně dochází ke zpracování osobních údajů, na anonymizované údaje se nadále nepohlíží jako na osobní údaje, tudíž se na ně po takové úpravě Obecné nařízení nevztahuje.

4.1.2 Pseudonymizované údaje

Pseudonymizaci údajů je nezbytné odlišit od anonymizace. Pod pseudonymizací si lze v praxi představit jakési šifrování osobních údajů takovým způsobem, kdy určitý údaj (např. jméno) je nahrazen zdánlivě náhodně generovaným kódem a takto je evidován v určité databázi. V odlišné databázi je pak zaznamenáno, že k onomu konkrétnímu jménu byl přiřazen uvedený kód.

Při spojení těchto dvou databází je tedy možné údaj rozšifrovat a získat kompletní osobní údaj. Proto se na takovou úpravu stále Obecné nařízení vztahuje

[37] Čl. 4 odst. 1 Obecného nařízení.
[38] § 4 písm. c) ZOOÚ *„Anonymním údajem (je) takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů.“*
[39] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 43.

a zároveň je kladen důraz na splnění technických a bezpečnostních opatření, aby bylo zamezeno přístupu neoprávněných osob.

Pokud porovnáme úpravu anonymizace a pseudonymizace, můžeme s trochou nadsázky hovořit o rozdílu v nevratnosti tohoto procesu, tedy jestliže již nadále není možné subjekt s údajem spojit, jedná se o anonymizaci, v opačném případě jde o pseudonymizaci.[40]

4.1.3 Zpracování osobních údajů

Definice zpracování osobních údajů se v zásadě neliší od úpravy užité ve Směrnici č. 95/46/ES, potažmo ZOOÚ. Zpracováním se dle Obecného nařízení rozumí *„operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů,...“* [41]

Obecné nařízení rovněž uvádí demonstrativní výčet operací s osobními údaji. Jsou jimi např. *„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.“*[42]

Z uvedeného vyplývá, že nezáleží na užitém způsobu zpracování, tedy zda k tomu dochází elektronickým způsobem či manuálně, ani zda s nimi správce nakládá aktivně, např. shromažďováním, či pasivně, např. pouhým uchováváním.

Zpracováním osobních údajů však není jakákoliv činnost s osobními údaji, jak se bohužel dostalo do podvědomí laické veřejnosti. Zejména se nejedná o nahodilé a jednorázové zpracování. Naopak se jedná o činnost soustavnou systematickou činnost vykonávanou za určitým účelem či cílem.[43]

K rozlišení, co je zpracování a co není, slouží stanovení účelů dané činnosti.[44] Jako příklad lze uvést vedení personální evidence zaměstnanců pro účely

[40] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 88.
[41] Čl. 4 odst. 2 Obecného nařízení.
[42] Tamtéž.
[43] *Nejdůležitější pojmy*. [online] In: *Uoou.cz*. [cit. 11. 3. 2020]. Dostupné z: https://www.uoou.cz/3-nejd-lezit-jsi-pojmy/d-27293.
[44] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 86.

plnění pracovněprávních smluv a povinností dle zákoníku práce nebo sebepropagace správce údajů na webových stránkách.

4.2 Zvláštní kategorie osobních údajů

Do zvláštní kategorie osobních údajů patří údaje, z jejichž podstaty vyplývá nutnost zvýšeného režimu ochrany, neboť mohou subjekt údajů poškodit ve společenské či profesní sféře nebo i mít za následek diskriminaci. Tuto kategorii nenajdeme mezi výkladovými ustanoveními v čl. 4, nýbrž se jí věnuje speciální čl. 9. V něm nalezneme taxativní výčet údajů řazených do zvláštní kategorie. Dle Obecného nařízení jsou jimi: „…*osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.*“[45]

Nejen že oproti předchozí právní úpravě došlo ke změně v rámci terminologie, neboť dříve se místo pojmu „zvláštní kategorie osobních údajů“ používal pojem „citlivý údaj“, došlo také k rozšíření výčtu o biometrické a genetické údaje.

Z výčtu údajů v čl. 9 nalezneme v Obecném nařízení výklad pouze u tří z nich. Jsou jimi právě biometrické údaje, genetické údaje a také údaje o zdravotním stavu. Jejich definice nalezneme v čl. 4. V případě genetických údajů a údajů o zdravotním stavu je výklad poměrně jednoznačný, naopak interpretace biometrických údajů tak jednoduchá není.

Důležitým rozdílem mezi čl. 4 a čl. 9 je účel zpracování biometrických údajů. Zatímco v čl. 4 se hovoří jak autentizaci a identifikaci osobních údajů tak, aby biometrické údaje byly považovány za zvláštní kategorii osobních údajů v souladu s čl. 9, musí být zpracovávány pouze účelem jedinečné identifikace subjektu údajů.[46] Následkem této legislativní změny došlo i ke změně v rámci výkladové praxe ÚOOÚ. Dozorový úřad totiž ve svém stanovisku č. 3/2009 *k biometrické identifikaci* uvedl dva rozdílné druhy zpracování biometriky.

[45] Čl. 9 odst. 1 Obecného nařízení.
[46] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 53.

Podstatou tohoto rozlišení bylo rozdělení na systémy, které zpracovávají běžné osobní údaje a na systémy, které zpracovávají citlivé údaje.[47]

V prvním případě docházelo k postupu, kdy po získání biometrických údajů byly matematicky převedeny na kód a následně byly porovnávány tyto kódy k identifikaci subjektu za neexistence žádná evidence biometrických údajů. Ve druhém případě naopak taková databáze existovala a k identifikaci či autentizaci osob docházelo za porovnávání právě těchto údajů z databáze.

ÚOOÚ zveřejnil poměrně stručnou informaci, ve které uvádí, že výše uvedené dělení s ohledem na novou právní úpravu už nadále nebude využívat, neboť i systémy, které ukládaly pouze šablony vytvořené z biometrických údajů a následné přiřazení číselného kódu, zpracovávají zvláštní kategorii osobních údajů.[48]

4.2.1 Zpracování zvláštní kategorie osobních údajů

Zpracování zvláštní kategorie osobních údajů lze pouze na základě splnění podmínek alternativního charakteru uvedených v čl. 9 odst. 2 písm. a) až j). Jedná se o následující podmínky:

- výslovný souhlas subjektu údajů;
- za účelem plnění povinností a výkon zvláštních práv v oblasti pracovního práva a práva sociálního zabezpečení;
- ochrana životně důležitých zájmů;
- oprávněné činnosti nadací, sdružení nebo jiných neziskových subjektů, které sledují politické, filozofické, náboženské nebo odborové cíle;
- údaje zjevně zveřejněné subjektem údajů;
- určení, výkon nebo obhajoba právních nároků nebo zpracování soudy v rámci jejich pravomocí;
- z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu;

[47] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 172.

[48] *Upozornění na změnu v posuzování systémů využívajících biometrické údaje (dříve "Stanovisko č. 1/2017 - Biometrická identifikace nebo autentizace zaměstnanců")*. In: *Uoou.cz* [online].[cit. 2020-03-11]. Dostupné z: https://www.uoou.cz/upozorneni-na-zmenu-v-nbsp-posuzovani-systemu-vyuzivajicich-biometricke-udaje-drive-quot-stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu-quot/d-29048/p1=3069.

- pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby a řízení systémů;
- z důvodu veřejného zájmu v oblasti veřejného zdraví;
- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.[49]

4.3 Subjekt osobních údajů

Obecné nařízení neobsahuje samostatnou definici subjektu údajů. V čl. 4 odst. 1 je však užit jako legislativní zkratka. Jak již bylo uvedeno v kap. 4 č. 1 této práce, subjektem může být pouze fyzická osoba, k níž se osobní údaje vztahují. Z působnosti jsou vyloučeny právnické osoby a osoby zemřelé.

Určitým problémem jsou pak fyzické osoby podnikající. V souvislosti s jejich činností jsou zpracovávány nejen údaje profesního charakteru, ale také jejich osobní údaje. Byť se Ústavní soud České republiky v nálezu Pl. ÚS 38/02 vyjádřil tak, že do působnosti ZOOÚ podnikající fyzické osoby nespadají, vzhledem k rozhodovací praxi Soudního dvora Evropské unie (dále jen „SDEU“) je považován uvedený nález za překonaný.[50] Shodně s rozhodnutími SDEU stanovil působnost ZOOÚ nad osobními údaji fyzických osob podnikajících také ÚOOÚ ve svém stanovisku 3/2011 o*chrana osobních údajů podnikajících fyzických osob.*

Lze tak usuzovat, že vzhledem k uvedenému a principům Obecného nařízení do jeho působnosti podnikající fyzické osoby rovněž náleží.

4.4 Správce

Vedle subjektu osobních údajů je správce dalším obligatorním subjektem při zpracování osobních údajů. Správce je definován v čl. 4 odst. 7 Obecného nařízení. Vzhledem k poměrně širokému vymezení užitému v nařízení je zjevné, že zákonodárci nezamýšleli vyloučení žádné osoby pro formu či povahu. Správcem

[49] Čl. 9 odst. 2 písm. a) až j) Obecného nařízení.
[50] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 81.

tak může být fyzická i právnická osoba, orgán veřejné moci, agentura či jakýkoliv další subjekt.[51]

Správcem je osoba vykonávající činnost, během které dochází ke zpracování osobních údajů, přičemž určuje účel a prostředky jejich zpracování. Právě stanovení účelu a prostředků je naprosto klíčové k určení, zda jde o správce osobních údajů. Naopak naprosto irelevantním aspektem je skutečnost, zda je tím, kdo osobní údaje fakticky zpracovává. Správce může prováděním zpracování pověřit zcela jinou osobu, tzv. zpracovatele, přičemž tato možnost je Obecným nařízením nejen povolena, nýbrž v určitých případech zákonem přímo stanovena.

Správce je adresátem povinností, které mu ukládá Obecné nařízení, je odpovědný za jejich plnění, a to i v případě, že zpracováním osobních údajů pověří zpracovatele.[52] Vzhledem k principu nařízení, kterým je přístup založený na riziku (viz kapitola 2.3.1), se rozsah povinností diferencuje dle míry rizika, které zpracování představuje.[53]

4.4.1 Společní správci

Obecné nařízení explicitně stanovuje úpravu tzv. společných správců. Předchozí právní úprava neupravovala společné správce samostatně, nicméně v ustanovení definujícím správce možnost většího počtu správců nalezneme. To se ovšem netýká ZOOÚ, který takovou úpravu nepřejal vůbec.

Tato situace nastane, pokud se na určení účelů a prostředků podílí dva a více správců.[54] V takovém případě je nezbytné, aby si správci stanovili rozsah povinností ve smluvním závazku, a to tak, aby byla dodržena ochrana práv a svobod subjektů údajů.[55]

Subjektu údajů musí být umožněno uplatňování svých práv u jakéhokoli ze společných správců. Pokud nastane situace, kdy dojde k újmě na právech subjektu údajů, odpovídají správci společně a nerozdílně, přičemž správce, který nahradí

[51] Čl. 4 odst. 7 Obecného nařízení.
[52] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 90.
[53] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 90.
[54] Čl. 26 odst. 1 Obecného nařízení.
[55] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 286.

újmu, má právo požadovat po ostatních správcích náhradu ve výši odpovídající jejich podílu, tzv. regresní nárok.[56]

4.5 Zpracovatel

Zpracovatel je fakultativním subjektem v rámci zpracování osobních údajů. Zpracovatel může být pověřen správcem, aby prováděl zpracování části nebo celku osobních údajů namísto něj. Vzhledem k definici v čl. 4 Obecného nařízení nedochází k jinému vymezení, než v případě správce. Zpracovatelem tak může být: *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.“*[57]

K ustanovení zpracovatele dochází nejčastěji v rámci služeb poskytovaných externími mzdovými účetními, správci cloudových úložišť, bezpečnostních agentur aj. Vždy se jedná o subjekt s odlišnou právní identitou od správce. Pokud např. správci zpracovává mzdy účetní oddělení, nepůjde zde o vztah správce – zpracovatel.

Obecné nařízení neupravuje odlišně, pokud se jedná o zpracovatele zákonem zmocněného či zpracovatele pověřeného správce. Pokud se jedná o druhou z uvedených možností, správce má povinnost uzavřít se zpracovatelem smlouvu či jiný právní akt v souladu s čl. 28 Obecného nařízení, přičemž její náležitosti jsou stanoveny zejména v odst. 3. Jsou jimi: *„předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce.“*[58] Stejný odstavec také vymezuje požadavky na zpracovatele osobních údajů, a to v písm. a) až h). Jedná se především o podmínku dodržení technických a bezpečnostních opatření zpracovatelem, postupování dle pokynů správce či dodržování mlčenlivosti. Vyloučeno je také řetězení zpracovatelů, tedy zapojení dalšího zpracovatele, bez předchozího souhlasu správce.

Institut zpracovatele a rovněž i zpracovatelské smlouvy není novum v právu na ochranu osobních údajů. Obecné nařízení však značně rozšiřuje náležitosti právního aktu. Proto bylo do skončení legisvakanční doby důležité stávající

[56] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 512.
[57] Čl. 4 odst. 8 Obecného nařízení.
[58] Čl. 28 odst. 3 Obecného nařízení.

smlouvy uvést do souladu s nařízením, a to tak, že již existující zpracovatelské smlouvy budou revidovány dle nové právní úpravy. Tento soulad s nařízením bylo možné provést změnou právního aktu, jejím dodatkem či akt nahradit novým.

Avšak nerevidování zpracovatelských smluv či vůbec neexistující smlouvy byly častým problémem i po účinnosti Obecného nařízení mnoha správců, jak vychází z mnohých zhodnocení stavu implementace nařízení po určité době po uplynutí účinnosti.[59] I já jsem se v praxi s tímto nedostatkem setkala téměř u každého subjektu, u kterého byla prováděna implementace a paradoxně velké subjekty byly v toto ohledu často mnohem více nedbalé než některé malé společnosti.

[59] DEMETEROVÁ, L., HAKROVÁ, K. *A zase to GDPR! Tentokrát poznatky z praxe a auditů aneb nejčastější chyby a jak jim předejít - část II.* In: *Pravniprostor.cz* [online].[cit. 2020-03-15]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/ht-a-zase-to-gdpr-tentokrat-poznatky-z-praxe-a-auditu-aneb-nejcastejsi-chyby-a-jak-jim-predejit-cast-ii.

5 Práva subjektů údajů

S příchodem Obecného nařízení došlo k velmi významné změně v právech subjektů údajů. Tato změna byla jedním z klíčových aspektů rekodifikace. Rozšíření práv a zároveň zpřísnění sankcí reflektuje potřebu zvýšené ochrany vlivem vývoje společnosti a změnu rizik, která mohou nastat.

Právům subjektu údajů je věnována celá kapitola č. 3 Obecného nařízení čítající 9 článků. Obsahuje nejen rozšířenou právní úpravu práv, která jsou již známá ze Směrnice č. 95/46/ES, potažmo ZOOÚ, ale také řadu práv, s nimiž se setkáváme poprvé. V tomto postupu lze spatřovat záměr zákonodárce vyvážit nerovný vztah mezi správcem a subjektem osobních údajů.[60]

Zajištění výkonu práv subjektů je často podceňovanou povinností ze strany správců. Možná právě proto je jejich porušování sankcionováno Obecným nařízením pokutou s vyšší částkou než jiná porušení povinností.[61]

5.1 Právo na transparentní informace, sdělení a postupy

Kapitolu práv subjektu údajů uvozuje čl. 12 obsahující požadavky na způsob komunikace mezi správcem a subjektem údajů. Jedná se o zásadu transparentnosti, která se promítá jak do práv subjektů, tak i do povinností správců. V případě subjektů lze hovořit o skupině pasivních práv.

Definice užitá v nařízení obsahuje klíčové aspekty pro správný postup, který musí být uplatňován v rámci jakékoliv komunikace se subjektem údajů. Jsou jimi:

- stručný, transparentní, srozumitelný a snadno přístupný způsob;
- jasné a jednoduché jazykové prostředky;
- předchozí bod je zvláště důležitý při poskytování informací dětem;
- písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě;
- na žádost subjektu mohou být poskytnuty ústně;
- bezplatnost.[62]

[60] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 130.
[61] Tamtéž.
[62] Guidelines on transparency under Regulation 2016/679 (WP260 rev.01) adopted on 29 November 2017. In: *Ec.europa.eu* [online]. str. 6 [cit. 2020-03-22]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Z uvedeného vyplývá, že správce by měl pracovat se skutečností, jakou cílovou skupinu tvoří subjekty, jejichž údaje zpracovává a způsob sdělování informací o zpracování tomu přizpůsobit. Tedy pokud se bude jednat o komunitu odborníků, k čemuž dochází například během oborových konferencí, není na škodu užít odbornější terminologii. Pokud je však okruh subjektů smíšený i s laickou veřejností, správce musí užít takové jazykové prostředky, aby subjekt mohl předpokládat rozsah a důsledky zpracování.[63]

Stejně tak musí pečlivě zvážit, jakou formou bude sdělování probíhat. V převážné většině správců tomu dochází prostřednictvím internetových stránek. Nicméně z praktického hlediska se často nedá hovořit o „snadném přístupu“, neboť umístění informací je mnohdy uživatelsky nepřívětivě skryto pod množstvím záložek. Zároveň také dochází k přehlcování informacemi (mnohdy i záměrně), což má za následek, že u subjektu nastane tzv. syndrom únavy informacemi.

Byť by se mohlo zdát, že není chybou správce, že si subjekt v takovém případě nepřečte informace o zpracování osobních údajů, přestože mu je poskytl, pokud to však dělá záměrně složitým a rozsáhlým způsobem, nesplňuje tak podmínky práva na transparentnost.

5.2 Právo na informace

Právo na informace rovněž spadá do kategorie práv pasivních. Jsou mu věnovány hned dva články Obecného nařízení, a to čl. 13 a 14. Důvod rozdělení je dán způsobem, jakým správce osobní údaje získal – zda byly získány od subjektu, či nikoliv. Následující tabulka reflektuje rozdíl v poskytování informací dle způsobu získání osobních údajů.

Poskytované informace	**Čl. 13 – získáno od subjektů**	**Čl. 14 – nezískáno od subjektů**
Totožnost správce	ANO	ANO

[63] Guidelines on transparency under Regulation 2016/679 (WP260 rev.01) adopted on 29 November 2017. In: *Ec.europa.eu* [online]. str. 7 [cit. 2020-03-22]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Kontaktní údaje pověřence	ANO	ANO
Účely a právní základ zpracování	ANO	ANO
Kategorie osobních údajů	NE	ANO
Příjemce nebo kategorie příjemců osobních údajů	ANO	ANO
Úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci	ANO	ANO
Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f)	ANO	NE

Mimo výše uvedené má subjekt právo být informován o dalších informacích *„jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování.“*[64] Podmínky zakládající tuto povinnost vychází nejen z povahy zpracování správce, ale i z povahy osoby subjektu. Na straně správce se může jednat o zpracování s vysokým rizikem či pokud dochází k automatizovanému rozhodování a na straně subjektu to může být skutečnost, že je jím dítě.[65] V praxi toto rozlišení bývá pro správce velmi problematické, proto se zpravidla doporučuje uvádět raději více informací.

[64] Čl. 13 odst. 2/ čl. 14 odst. 2 Obecného nařízení.
[65] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 208.

Níže uvedená tabulka rovněž ukazuje rozdíl ve způsobu získání osobních údajů.

Poskytované informace	**Čl. 13 – získáno od subjektů**	**Čl. 14 – nezískáno od subjektů**
Doba, po kterou budou údaje zpracovávány	ANO	ANO
Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f)	Poskytováno vždy	ANO – v tomto případě až za splnění podmínek v odst. 2
Existence dalších práv subjektů	ANO	ANO
Možnost odvolat souhlas, pokud je právním základem	ANO	ANO
Právo podat stížnost	ANO	ANO
Zdroj osobních údajů	-	ANO
Zda jsou je zde dána povinnost poskytnout údaje ze zákonných či smluvních důvodů	ANO	NE
Zda dochází k automatizovanému	ANO	ANO

rozhodování, včetně profilování		

Je zřejmé, že dochází ke značnému rozšíření poskytovaných informací, což vedlo k nezbytné revizi dokumentů, které obsahovaly informace dle ZOOÚ. V praxi však tato úprava byla správci často opomíjena.

5.2.1 Lhůty pro poskytnutí informací

Rovněž v případě lhůt pro poskytování informací jsou rozdíly dle způsobu získání údajů.

Pokud jsou získány přímo od subjektu údajů, jsou zpravidla poskytovány hned v tomto okamžiku. Uvedeným časovým údajem se však myslí okamžik, kdy je subjekt správci předává, nikoliv kdy správci dojdou.[66] Nejčastěji tomu tak dochází v případě vyplňování internetových formulářů, které obsahují interaktivní odkaz na příslušnou stránku, jež informace obsahuje.

V případě, že správce osobní údaje nezískal přímo od subjektu, Obecné nařízení obsahuje tři možnosti, kdy jsou informace poskytovány:

- *„a) v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;*
- *b) nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo*
- *c) nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.“*[67]

5.3 Právo na přístup

Právo na přístup k osobním údajům patří mezi první aktivní práva subjektů z tohoto výčtu. Jedná se o jakési potvrzení ze strany správce, zda osobní údaje subjektů jím jsou zpracovávány a v jakém rozsahu. Pokud ke zpracování dochází,

[66] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 205.
[67] Čl. 14 odst. 3 Obecného nařízení.

správce musí poskytnout subjektu údajů informace, kterými je například účel zpracování, příjemce či doba, po kterou budou osobní údaje uloženy.[68]

Toto právo se stalo pomyslným ukazatelem přípravy správců na soulad s GDPR. Především u větších správců není jednoznačný přehled o všech subjektech, jejich osobních údajích a v jakém systému jsou zpracovávány. Proto musí správce stanovit postupy k vyřizování žádostí subjektů. Bez nich totiž dochází ke zdržení, časovým prodlevám, porušování lhůt při poskytování odpovědí, soudním sporům a následným náhradám nákladů.[69]

Ideálním pomocným prostředkem ke zmapování všech účelů zpracování jsou záznamy o činnostech zpracování, neboť obsahují všechny informace, které by správce subjektu v případě žádosti měl poskytnout.[70]

Dalším aspektem tohoto práva, který Obecné nařízení zavádí, je bezplatnost. Správce je povinen poskytnout subjektu informace o zpracování osobních údajů bezplatně. To je rozdíl oproti předchozí právní úpravě, kdy mohl správce za poskytnutí požadovat přiměřenou úhradu. Výjimkou jsou opakované žádosti totožného subjektu, v takovém případě lze požadovat náhradu administrativních nákladů.

5.4 Právo na opravu

Toto právo reflektuje zásadu přesnosti. Subjekt osobních údajů má právo, aby byly zpracovávány přesné a aktuální osobní údaje. Za tímto účelem může podat žádost na jejich opravu. Správce pak v takovém případě má povinnost přezkoumat, zda se na jím zpracovávané údaje žádost vztahuje. Do doby, než tak učiní a dojde k nápravě, omezí dispozice s údaji. Pokud byla žádost důvodná, správce údaje opraví a informuje o tomto postupu žadatele. [71]

Stejně se postupuje rovněž v případě požadavku na doplnění neúplných informací. Dochází k tomu v případě, že se subjekt rozhodne správci poskytnout

[68] Čl. 15 odst. 1 písm. a) - h) Obecného nařízení.
[69] ŠKORNIČKOVÁ, Eva. *Právo na přístup k osobním údajům prověří připravenost na GDPR.* [online]. gdpr.cz [cit. 2020-03-27]. Dostupné na: https://www.gdpr.cz/blog/pravo-na-pristup-k-osobnim-udajum-proveri-pripravenost-na-gdpr/.
[70] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 137.
[71] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 226.

více svých osobních údajů, nicméně stále musí platit zásada minimalizace a správce by tak neměl zpracovávat údaje nad rámec potřebných.

Toto právo opět představuje aktivní právo subjektu, nikoliv aktivní povinnost správce. Není tedy nutné, aby správce v určitých časových intervalech kontaktoval všechny subjekty, jejichž osobní údaje zpracovává, aby si ověřil jejich správnost.

V praxi však bývá často uplatňován postup, kdy může správce požádat subjekt o kontrolu svých osobních údajů a potvrzení jejich aktuálnosti např. během osobního kontaktu se subjektem.

5.5 Právo na výmaz

Obecné nařízení přináší v čl. 17 úplnou novinku ve formě práva subjektu na výmaz osobních údajů. Do návrhu Obecného nařízení se dostal po značně zmedializovaném sporu mezi společností Google Inc. a panem Costeja Gonzálezem.[72] Španělský občan p. González požadoval skrytí či vymazání svých osobních údajů společností Google Spain, které souvisely se zajištěním jeho dluhu dražbou nemovitosti. Přestože byl dluh již uhrazen, stále dohledatelný odkaz zhoršoval jeho pověst. SDEU zde rozhodl o uplatnění práva na výmaz, které se do podvědomí dostalo pod názvem „právo být zapomenut“.[73]

Dle čl. 17 Obecného nařízení má subjekt právo, aby bez zbytečného odkladu došlo k výmazu jeho osobních údajů správcem, který je zpracovává. První odstavec obsahuje alternativní výčet důvodů, za nichž je právo na výmaz aplikovatelné. Jsou jimi:

- nadále již neexistuje původní účel zpracování, v tomto případě by k výmazu měl přistoupit sám správce, ale i tak může subjekt podat žádost;
- subjekt odvolal souhlas a žádný jiný právní titul neopravňuje správce ke zpracování;

[72] Soudní dvůr: Rozsudek ze dne 13. května 2014, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, bod 14, 15.
[73] SLANINA, Jan. *Právo být zapomenut a další dopady rozsudku SDEU C-131/12 Google Spain.* [online]. In: *Epravo.cz* [cit. 2020-03-29]. Dostupné na: https://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-sdeu-c-13112-google-spain-94498.html.

- subjekt vznese námitky proti zpracování dle čl. 21 odst. 1 nebo 2, tedy ke zpracování dochází na základě oprávněného zájmu správce či veřejného zájmu, v takovém případě musí správce přezkoumat, zda zájem subjektu nepřevažuje a není tak zpracování neoprávněné;
- protiprávní zpracování;
- výmaz musí být proveden ke splnění právní povinnosti;
- pokud byly osobní údaje nezletilé osoby shromážděny v souvislosti s nabídkou služeb informační společnosti a subjekt požádal o výmaz, musí vždy dojít k likvidaci údajů.[74]

Z uvedených důvodů existují výjimky, které správci umožňují další zpracování i v případě, že subjekt údajů podal žádost na výmaz. Patří mezi ně zpracování údajů na základě práva na svobodu projevu např. v žurnalistice anebo na základě práva na informace, kdy jsou osobní údaje zpracovávány ve veřejných rejstřících.[75] Další výjimkou je zpracování podmíněné právní povinností, „*jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen*.“[76] V praxi se jedná většinou o povinnost uchovávat osobní údaje subjektu za účelem účetnictví, nicméně právě tato výjimka bývá ze strany laického subjektu často nepochopena a považována za nedodržení jeho práv. Dalšími výjimkami jsou zpracování z důvodu veřejného zájmu ve věci veřejného zdraví, ve věci archivace, vědeckého či historického výzkumu, za statistickými účely. Poslední výjimku tvoří určení, výkon či obhajoba právních nároků, pokud tak nelze učinit bez zpracování konkrétních osobních údajů.

Vzhledem k uvedenému lze usoudit, že právo na výmaz rozhodně není absolutním právem subjektu osobních údajů, neboť Obecné nařízení umožňuje správcům dispozice se širokou škálou výjimek.

Jednoznačným posílením práv subjektů se však jeví povinnost správce informovat další správce, kteří rovněž zpracovávají tytéž osobní údaje, aby došlo k výmazu i v jejich případě. O posílení jde především v internetovém prostředí, kdy

[74] Čl. 17 odst. 1 písm. a) - f) Obecného nařízení.
[75] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 232.
[76] Čl. 17 odst. 2 písm. b) Obecného nařízení.

dožádaný správce osobní údaje zveřejnil a další správci je na základě toho zpracovávají. V takové situaci musí být zajištěno, aby byly odstraněny veškeré odkazy a kopie.[77]

5.6 Právo na omezení zpracování

Právo na omezení zpracování je dalším zcela novým institutem, který obecné nařízení zavádí v čl. 18. Toto právo umožňuje subjektu požadovat omezení procesu zpracování svých osobních údajů správcem za splnění některé z následujících podmínek:

- subjekt namítá nepřesnost osobních údajů, jejichž zpracování je pak pozastaveno na takovou dobu, než správce tuto skutečnost ověří;
- zpracování osobních údajů není v souladu s právními předpisy, avšak subjekt nepožaduje jejich výmaz;
- pokud je subjekt potřebuje pro účely určení, výkonu či obhajoby právního nároku, byť pro správce již nejsou nezbytné pro další zpracování;
- pokud subjekt vznesl námitku dle čl. 21 proti zpracování založenému na oprávněném zájmu správce či veřejném zájmu, a to do doby, než správce přezkoumá oprávněnost námitky.[78]

V případě, že nastanou odpovídající podmínky pro omezení zpracování, existuje jediný způsob zpracování, který může správce s údaji vykonávat, a to je jejich uchovávání. Mimo uložení může správce vybrané osobní údaje zpracovávat pouze se souhlasem subjektu osobních údajů, za účelem určení, výkonu nebo obhajoby právních nároků, ochrany práv další fyzické nebo právnické osoby nebo v případě podstatného veřejného zájmu.[79]

Zásadním rozdílem mezi právem na výmaz a právem na omezení zpracování je jeho dočasnost, přičemž správce je povinen informovat subjekt o skutečnosti, že

[77] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi, str. 76.
[78] Čl. 18 odst. 1 písm. a) - d) Obecného nařízení.
[79] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 236.

dojde ke zrušení omezení zpracování ve chvíli, kdy odpadne důvod, pro který omezení nastalo.[80]

Pro správce je důležité mít nastavené adekvátní postupy, aby mohl zajistit výkon tohoto práva. Recitál č. 67 Obecného nařízení obsahuje řadu možností, jak by správce mohl postupovat. V případě, že jsou údaje předmětem automatizovaného zpracování, musí být do systému implementovány takové technické prostředky, které údaje vyřadí z určitých operací zpracování. V ostatních případech musí být osobní údaje jasně označeny. Efektivním nástrojem je dočasné přesunutí do jiného systému, aby nedocházelo ke zpracování, zamezení přístupu nebo dočasné odstranění z veřejně přístupných zdrojů, kterými jsou například internetové stránky.

5.7 Právo na přenositelnost údajů

Jinak také jako právo na portabilitu je dalším ze zcela nových práv, která vznikla subjektům údajů s účinností Obecného nařízení a dá se považovat za jednu z významných změn.

Právo na přenositelnost představuje možnost subjektu získat osobní údaje, které správci poskytl a předat je jinému správci za splnění kumulativních podmínek, a to, že zpracování musí probíhat automatizovaným způsobem a na základě právního titulu souhlasu subjektu či na základě smlouvy. Obecné nařízení také vymezuje, v jakém formátu mají být údaje předávány, a to ve *„strukturovaném, běžně používaném a strojově čitelném formátu“* [81].

Odst. 2 článku upravujícímu právo na přenositelnost obsahuje také možnost předání údajů jinému správci původním správcem bez mezikroku zahrnujícím součinnost samotného subjektu. Podmínkou je technická proveditelnost tohoto postupu. Vzhledem k dosud neznámému institutu práva na portabilitu vydala WP 29 stanovisko, které osvětluje i problematiku významu technické proveditelnosti. Dle tohoto stanoviska by tak mělo být možné přímé předání mezi správci, pokud je možná vzájemná komunikace zašifrovaným či obdobně zabezpečeným

[80] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi, str. 120.
[81] Čl. 20 odst. 1 Obecného nařízení.

způsobem.[82] Tento postup má umožnit subjektům přechod mezi uživateli, a zvýšit tak schopnost konkurence.[83]

Původní správce nesmí bránit předání osobních údajů – WP 29 ve svém stanovisku tento pojem popisuje jako úmyslné kladení překážek právního, technického nebo finančního charakteru za účelem zdržet, zabránit či znemožnit předání osobních údajů. Zde je promítnut především základní prvek tohoto práva, a to že musí být správcem vykonáváno bezplatně. Jednoznačným případem, kdy správce očividně brání předání osobních údajů, je tedy stanovení poplatků za tento proces.

Uplatnění práva na přenositelnost nicméně nemá vliv na další práva. V praxi výkon tohoto práva vypadá tak, že správce umožní předání osobních údajů jinému správci, pokud však subjekt zároveň požaduje, aby původní správce už jeho osobní údaje nezpracovával, musí uplatnit také právo na výmaz.

5.7.1 Právo na přenositelnost a jeho vliv na práva třetích osob

Ustanovení o právu na přenositelnost obsahuje také úpravu vztahující se k právům jiných osob, jejichž osobní údaje jsou součástí těch, u nichž je právo prováděno. Obecné nařízení stanovuje, že *„nesmí být nepříznivě dotčena práva a svobody jiných osob“* [84]. Z uvedeného vyvstává řada otázek, přičemž interpretační mezeru z velké části doplňuje stanovisko WP 29.

Dle stanoviska nebudou porušena práva třetích osob za splnění dvou podmínek – iniciující subjekt využívá práva na přenositelnost pro své osobní potřeby a nový správce bude používat osobní údaje ke stejnému účelu.

Pokud se fyzická osoba rozhodne převést svůj účet od jedné bankovní instituce k druhé, je zcela pochopitelné, že předmětem tohoto přesunu nebudou pouze jeho osobní údaje, ale také těch osob, které na jeho účet uskutečnily transakce. Přesun osobních údajů třetích osob nebude odporovat Obecnému nařízení, pokud bude sloužit původnímu účelu, tedy např. pro vedení historie transakcí, kterou využívá subjekt – osoba iniciující přesun. Pokud by však

[82] Guidelines on the right to data portability 2016/679 (WP 242 rev.01) adopted on 13 December 2016 as last Revised and adopted on 5 April 2017. In: *Ec.europa.eu* [online]. str. 16 [cit. 2020-03-30]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[83] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 143.
[84] Čl. 20 odst. 4 Obecného nařízení.

sekundární bankovní instituce tyto získané kontakty využila k oslovení třetích osob k marketingovým účelům, jedná se o jednoznačné porušení práv.[85]

5.8 Právo vznést námitku

Obecné nařízení umožňuje dle čl. 21 subjektům údajů podávat námitky proti zpracování osobních údajů, a to kdykoliv během zpracování, ať už se jedná o automatizované pracování včetně profilování. O tomto právu musí být subjekt obeznámen separátně od ostatních informací.

Obecné nařízení přímo definuje tři situace, proti nimž lze vznést námitku proti zpracování, které se pojí ke zvláštním povinnostem správce.

První situace nastává, pokud zpracování probíhá na základě právního titulu oprávněného zájmu správce, veřejného zájmu nebo při výkonu veřejné moci. V takovém případě musí správce omezit zpracování na dobu, během níž přezkoumá, zda je žádost přiměřená a důvodná. Pokud ano, přistoupí k věcnému posouzení námitky. V případě, že správce používá jako právní titul oprávněný zájem a následně je subjektem vznesena námitka proti zpracování, musí vypracovat tzv. balanční test. Jeho účelem je zhodnocení, zda oprávněný zájem správce převažuje nad právy a svobodami subjektu osobních údajů.[86] Důkazní břemeno náleží správci. Pokud prokáže, že oprávněný zájem převažuje nad zájmy subjektu, může ve zpracování pokračovat, o čemž subjekt musí být informován. Pokud ne, osobní údaje nadále nesmí být zpracovávány.

Druhým případem je zpracování za účelem přímého marketingu. Pokud subjekt vznese námitku proti zpracování za účelem přímého marketingu, účinky jsou absolutní. V případě této námitky nedochází k žádnému posouzení a správce jí vždy musí vyhovět[87], tedy rovnou pozbývá možnost pro tento účel osobní údaje zpracovávat. Účel možnosti podat tuto námitku je především zacílen na ochranu práv osob méně zkušených v ochraně osobních údajů, zejména pak na seniorní část občanů.

[85] Guidelines on the right to data portability 2016/679 (WP 242 rev.01) adopted on 13 December 2016 as last Revised and adopted on 5 April 2017. In: *Ec.europa.eu* [online]. str. 12 [cit. 2020-03-30]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[86] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 250.
[87] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 148.

Třetím případem je vznesení námitky proti zpracování osobních údajů pro účely vědeckého či historického výzkumu nebo pro statistické účely, pokud nejde o zpracování nezbytné z důvodu veřejného zájmu. Nulíček a kol. v Praktickém komentáři jako příklad uvádějí právě zpracování pro statistické účely, kdy v případě podané námitky správce přezkoumá, zda je nezbytné zpracovávat osobní údaje konkrétního člověka, pokud patří do množiny velkého okruhu sledovaných subjektů. V takovém případě zpracování není ve veřejném zájmu.[88] Dle mého názoru je tato možnost dána nízkým povědomím laické veřejnosti o tomto institutu, kdyby však docházelo k hromadnému uplatňování svého práva proti zpracování právě za statistickým účelem, tvorba jakýchkoliv statistik by byla značně ztížena.

5.9 Automatizované individuální rozhodnutí a profilování

Obecné nařízení v čl. 22 obsahuje právo subjektu osobních údajů nebýt předmětem výhradně automatizovaného rozhodování včetně profilování, které by pro něj mělo právní dopad. Týká se to procesu rozhodování, který probíhá výlučně výpočetní technikou, aniž by obsahoval jakýkoliv zásah člověka.[89] Toto právo, byť se veřejnosti může jevit jako zcela nový institut, bylo obsaženo již v předchozí právní úpravě.

Pro užití automatizovaného individuálního rozhodování určuje tři výjimky:

- je-li nezbytné k uzavření či plnění smlouvy mezi správcem a subjektem;
- dal-li subjekt k jeho použití výslovný souhlas;
- je-li umožněno právem Evropské unie či právem členského státu.[90]

Bod dva a tři jsou poměrně jednoznačné, avšak výklad prvního bodu se může jevit jako problematický. Stanovisko WP 29 uvádí přehled důvodů pro užití automatického individuálního rozhodování. Je jím především zvýšení důslednosti a korektnosti, kdy výpočetní technika napomůže předcházet lidským chybám či diskriminaci, dále snižuje riziko pro správce v případě posouzení bonity a v neposlední řadě také zvyšuje rychlost a efektivnost procesu.[91] Příkladem, kdy

[88] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 253.
[89] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi, str. 122.
[90] Čl. 22 odst. 2 Obecného nařízení.
[91] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01) adopted on 3 October 2017 as last Revised and Adopted on 6 February

typicky dochází k uplatnění bodu č. 1, jsou poskytovatelé spotřebitelských úvěrů, kteří užívají počítačové systémy k posouzení úvěruschopnosti žadatele o úvěr.[92]

Pokud správce užívá automatizované individuální rozhodování, musí přijmout adekvátní opatření na ochranu práv, svobod a zájmů subjektu. Jedná se zejména o možnost přístupu a zásahu správce do automatizovaného rozhodování a právu subjektu vyjádřit se k takovému způsobu rozhodování, popřípadě možnost takové rozhodnutí napadnout.

2018. In: *Ec.europa.eu* [online]. str. 13 [cit. 2020-03-30]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[92] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 149.

6 Povinnosti správců osobních údajů

Právní úprava předchozí ani současná neobsahuje explicitně popsané povinnosti, nýbrž zásady zpracování, přičemž z jejich dodržování správcům povinnosti vyplývají. Je zde zcela patrné zrcadlení v právech subjektů a naopak.

Základní zásady zpracování osobních údajů nejsou v právní úpravě žádnou novinkou. Prvopočátky nalezneme již v Úmluvě OECD, odkud byly převzaty do Úmluvy č. 108 a posléze i do Směrnice č. 95/46/ES.[93]

V Obecném nařízení doznaly téměř všechny zásady změn v podobě zpřesnění a rozšíření, správců se však nejvíce dotknou změny v odpovědnosti. Zpracování osobních údajů v souladu s Obecným nařízením podléhá zásadě zákonnosti, korektnosti a transparentnosti, zásadě účelového omezení, zásadě minimalizace údajů, zásadě přesnosti, zásada omezení uložení, zásada integrity a důvěrnosti a zásada odpovědnosti – tyto budou charakterizovány v následující části.

6.1 Zásada zákonnosti, korektnosti a transparentnosti

Tuto zásadu lze označit jako jeden z nejdůležitějších pilířů právní úpravy ochrany osobních údajů.

Zásada zákonnosti znamená, že pro jakékoliv zpracování osobních údajů musí existovat minimálně jeden doložitelný právní titul. Existence takového titulu je dokladem legitimity účelu zpracování správcem. Pokud správce pozbyde právní titul, je to důvodem pro likvidaci zpracovávaných osobních údajů. Zákonnost také znamená, že zpracování je v souladu s právním řádem, tedy nikoliv pouze s Obecným nařízením, zpracování nesmí být v nesouladu se všemi právními předpisy.

Zásada korektnosti a transparentnosti se vztahuje na jednání správce vůči subjektu, přičemž takové jednání by mělo být co nejvíce otevřené, správce by se měl chovat dle legitimního očekávání subjektu a subjektu by mělo být zcela jasné, jakým způsobem a za jakým účelem jsou jeho osobní údaje zpracovávány. Tato

[93] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 107.

druhá část zásady je odrazem k čl. 12, 13 a 14, které obsahují právo subjektu na transparentnost a informace (viz kap. 5.1 a 5.2).

6.2 Zásada účelového omezení

Druhá zásada je rovněž jednou z nejdůležitějších, a to hlavně z důvodu, že se k ní pojí zásady následující. Zásada účelového omezení dává správci povinnost stanovit *určitý, výslovně vyjádřený* a *legitimní* účel zpracování osobních údajů.

Určitost účelu, byť to na první pohled není zcela zřejmě, představuje pro většinu správců problém. V zájmu správce samozřejmě je, aby účel nebyl určen příliš úzce. Tímto postupem by správce ve zpracování nejvíce omezoval sám sebe. Naopak pokud správce stanoví účel moc obecně (např. účely personálního oddělení), už z podstaty věci se rozhodně nedá nazývat určitým účelem. Zároveň se také nedoporučuje kumulovat více různých účelů do jednoho.[94]

Dalším aspektem této zásady je výslovné vyjádření, tedy o něm informovat subjekt a zároveň vést dokumentaci účelů. Toto lze jednoduše splnit vypracováním záznamů o činnostech zpracování osobních údajů, v nichž jednou z obligatorních informací je stanovení účelu zpracování.

Legitimita účelu se váže i k zásadě zákonnosti, tedy určený účel nesmí odporovat právním předpisům, jimiž je vázán správce.

6.3 Zásada minimalizace údajů

Jak bylo avizováno již kap. 6.2, tato zásada se váže k zásadě omezení účelu, neboť zásada minimalizace údajů ukládá správci povinnost zpracovávat osobní údaje relevantní, přiměřené a pouze v nezbytném rozsahu vzhledem k účelu zpracování, tedy zamezuje, aby správci zpracovávali takové osobní údaje subjektů, které nejsou nezbytně nutné. Můžeme spatřovat zpřísnění zásady oproti Směrnici č. 95/46/ES, která stanovila, že osobní údaje nesmí přesahovat míru vzhledem k účelu.

Tato zásada bývá mnohdy správci lehkomyslně podceňována, což je patrné i z výsledků kontrol ÚOOÚ, během nichž bylo kontrolovaným subjektům často vytýkáno zpracování údajů nad rámec nezbytného rozsahu. Nejčastější porušení

[94] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 110.

této zásady bývá na poli personálního oddělení, kdy zaměstnavatelé v pracovních dotaznících zpracovávají o zaměstnancích údaje, které nejsou nejen nezbytné, ale přímo nadbytečné (např. údaje o počtu vychovávaných dětí, o manželce/manželovi, aniž by zaměstnanec uplatňoval daňové zvýhodnění, údaje o zdravotním stavu, výpisu z rejstříku trestů aj.), zpracovávají kopie osobních dokladů, např. občanských průkazů aj.[95]

6.4 Zásada přesnosti

Zásada přesnosti ukládá správci povinnost zpracovávat jen přesné údaje, které odpovídají skutečnosti a v případě potřeby musí být zavedeny takové postupy, aby mohlo dojít k jejich aktualizaci. Tuto zásadu provádí právo subjektu na opravu a doplnění (viz kap. 5.4).

Správce odpovídá za přesnost údajů, které zpracovává. Pokud zjistí nepřesnost údajů, musí dojit k nápravě bez zbytečného odkladu. Pokud však subjekt sám poskytne nesprávné údaje, za jejich přesnost není správce odpovědný.[96]

6.5 Zásada omezení uložení

Zásada omezení uložení představuje jedno z bezpečnostních opatření a zároveň provádí právo subjektu na výmaz. V této zásadě jsou klíčové dva aspekty – první se týká uchovávání osobních údajů pouze po dobu nepřekračující potřeby účelu, druhá se týká formy, v níž jsou uchovávány, a to ve formě umožňující identifikaci. Jinak lze říci, že správce nesmí uchovávat osobní údaje, pokud zanikne účel zpracování, a musí tak dojít k jejich likvidaci. Vzhledem k aspektu formy osobních údajů je možné brát jako likvidaci taktéž proces anonymizace osobních údajů (viz kap. 4.1.1), pokud je bude chtít správce v takové formě dále zpracovávat.[97]

Předcházení porušení této zásady napomáhá stanovení a dodržování lhůt výmazu osobních údajů. K těmto účelům slouží vypracování spisového a

[95] DEMETEROVÁ, L., HAKROVÁ, K. *A zase to GDPR! Tentokrát poznatky z praxe a auditů aneb nejčastější chyby a jak jim předejít - část I.* [online]. pravniprostor.cz [cit. 2020-04-02]. Dostupné na: https://www.pravniprostor.cz/clanky/ostatni-pravo/a-zase-to-gdpr-tentokrat-poznatky-z-praxe-a-auditu-aneb-nejcastejsi-chyby-a-jak-jim-predejit-cast-i.

[96] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 114.

[97] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 65.

skartačního řádu či záznamů o činnostech zpracování. V obou těchto dokumentech je evidována lhůta, po jejímž uplynutí musí dojít k likvidaci osobních údajů.

6.6 Zásada integrity a důvěrnosti

Tato zásada cílí na zabezpečení osobních údajů, které má předcházet neoprávněnému či protiprávnímu zpracování, ztrátě, zničením nebo poškozením.[98]

Tato zásada úzce souvisí s čl. 32 Obecného nařízení, nicméně už jen tím, že požadavek na zabezpečení osobních údajů byl včleněn do základních zásad práva na ochranu osobních údajů vypovídá o jeho důležitosti. Nelze však stanovit jednotné požadavky na zabezpečení komplexně pro všechny správce a druhy zpracování. Proto Obecné nařízení obsahuje výčet možností, jak zabezpečení provést, přičemž následná aplikace musí být individualizovaná dle potřeb správců a musí odpovídat povaze, rozsahu a účelům zpracování.[99]

6.7 Zásada odpovědnosti

Ustanovení Obecného nařízení, které stanovuje zásadu odpovědnosti, lze rozdělit do dvou částí. První část ukládá správci odpovědnost za splnění povinností vyplývajících z předchozích zásad. Tato odpovědnost byla zakotvena již v předchozí právní úpravě. Zcela nová je však druhá část tohoto ustanovení, která správci ukládá povinnost být schopen dodržení povinností doložit.

Tato nová povinnost představuje poněkud revoluční pojetí a přístup k ochraně osobních údajů. Ve své podstatě představuje požadavek na proaktivní přístup správce, který spočívá v přijetí účinných postupů a pravidel zajišťujících soulad zpracování se zásadami Obecného nařízení a zároveň vedení doložitelné dokumentace těchto postupů.

Obecné nařízení za tímto účelem přináší celou řadu nových institutů, které dokládají provedení zásad. Mezi ně můžeme zařadit například zavedení technických a organizačních opatření, vedení záznamů o činnostech zpracování, jmenování pověřence pro ochranu osobních údajů či posouzení vlivu na ochranu

[98] Čl. 5 odst. 1 písm. f) Obecného nařízení.
[99] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 65.

osobních údajů.[100] Těmto novým institutům bude věnována následující část této kapitoly.

6.8 Nové instituty v povinnostech správců osobních údajů

6.8.1 Zabezpečení a ohlašování případů porušení

Jak již bylo zmíněno v kap. 6.6, mezi základní povinnosti správce patří přijetí bezpečnostních opatření, přičemž se ponechává na jeho uvážení, jaké prostředky zvolí. Správce musí přihlédnout k druhu osobních údajů, které zpracovává, ke způsobu zpracování, míře rizika a dalším aspektům.

Pokud dojde k porušení zabezpečení osobních údajů, Obecné nařízení ukládá správci povinnost tento „bezpečnostní incident" oznámit. Tato povinnost není v českém právním řádu úplnou novinkou, dříve se však týkala pouze poskytovatelů elektronických komunikací. S účinností Obecného nařízení už dopadá na každého správce osobních údajů. Porušením se rozumí jakýkoliv zásah do zabezpečení, který by mohl mít za následek riziko pro subjekty, jejichž osobní údaje správce zpracovával.[101] Pokud k němu dojde, má správce dvojí ohlašovací povinnost. Správce musí *„bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o incidentu dozvěděl"* [102], věc oznámit dozorovému úřadu. Pokud dojde k incidentu u zpracovatele, nahlašuje ho správci. Oznámení o porušení zabezpečení, které je podáváno k ÚOOÚ, musí obsahovat následující náležitosti:

- *„(a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;*
- *(b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;*
- *(c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;*

[100] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 269.
[101] LUPIEŃSKÁ, P. *Hlášení bezpečnostních incidentů – co stanovuje zákon o kybernetické bezpečnosti a co GDPR?* [online]. pravniprostor.cz [cit. 2020-04-05]. Dostupné na: https://www.pravniprostor.cz/clanky/pravo-it/hlaseni-bezpecnostnich-incidentu-co-stanovuje-zakon-o-kyberneticke-bezpecnosti-a-co-gdpr.
[102] Čl. 33 odst. 1 Obecného nařízení.

- *(d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.“*[103]

Zde ovšem povinnosti správce nekončí, neboť pokud je míra rizika vysoká, musí dojít ještě ke splnění druhé oznamovací povinnosti, a to samotnému subjektu údajů, jehož se potenciální riziko týká. Zde je však obsah nesporně užší, správce by ho měl informovat o možných důsledcích porušení, jaká navrhl nápravná opatření a také kontaktní údaje na pověřence pro ochranu osobních údajů.

Správce nemá povinnost ohlašovat takové porušení zabezpečení, při kterém je velmi nepravděpodobné, že dojde k riziku ve formě úniku dat.

Zavedení komplexní povinnosti hlásit bezpečnostní incidenty je zcela logickým krokem vzhledem ke kybernetizaci a množství uchovávaných osobních údajů v informačních systémech, ale také vzhledem k neustále se zvyšujícímu počtu kybernetických útoků. Nicméně ohlášení incidentu dozorovému úřadu a subjektu může mít řadu negativních následků.

Subjekt může nabýt domnění, že správce nedostatečně zabezpečil osobní údaje a může se rozhodnout pro uplatnění svého práva na výmaz. Ovšem daleko závažnější dopad zde bude mít oznámení dozorovému úřadu. Nejen že správce znatelně upozorní na nedostatky v zabezpečení, což by mohlo následně vyústit v kontrolu[104], a to buď dle kontrolního plánu ÚOOÚ anebo i z podnětu subjektu, jehož osobní údaje jsou ohroženy. Dále by následkem ohlášení porušení zabezpečení mohl ÚOOÚ usoudit, že primárně došlo k porušení základní zásady Obecného nařízení, a to integrity a důvěrnosti, a udělit tak správci pokutu. I přes tyto možné negativní následky by měl mít správce na paměti, že neoznámení porušení zabezpečení je ve všech ohledech mnohem vážnější porušení Obecného nařízení s výrazně vyšší sankcí.

Ke dni 1. 10. 2019 ÚOOÚ evidoval 600 případů ohlášení porušení zabezpečení od účinnosti Obecného nařízení.[105]

[103] Čl. 33 odst. 3 Obecného nařízení.
[104] MORÁVEK, J. Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie? *Právní rozhledy*. 2018, č. 13–14, s. 487–493.
[105] MARCÍN, V. *Poznatky Úřadu z ohlašování porušení zabezpečení osobních údajů*. [online]. uoou.cz [cit. 2020-04-05]. Dostupné na:

6.8.2 Posouzení vlivu na ochranu osobních údajů a předchozí konzultace

Posouzení vlivu na ochranu osobních údajů neboli *DPIA* (z anglického názvu *Data Protection Impact Assessment*) je zcela novým institutem, který reflektuje přístup založený na riziku. Tento nástroj slouží k posouzení, zda zpracování osobních údajů představuje pro subjekty vysoké riziko, či nikoliv. Z toho vyplývá, že se tato povinnost nevztahuje na všechny subjekty ani veškerou jejich činnost.

Předchozí právní úprava obsahovala posouzení rizik, což se od posouzení vlivu dle Obecného nařízení liší v mnoha ohledech. Posouzení rizik dle ZOOÚ podléhalo oznamovací povinnosti ÚOOÚ, zde však docházelo k četným pochybením, kdy správci neoznamovali pouze riziková zpracování, ale všechna, čímž toto posouzení ztratilo smysl.[106] Dalším rozdílem je forma posouzení, kdy v případě posouzení rizik nebyla obligatorní písemná forma, kdežto u posouzení vlivu dle Obecného nařízení lze ze stanovených obsahových náležitostí usuzovat, že je povinné písemné vyhotovení.[107]

Posouzení vlivu má povinnost vyhotovit správce, který s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování usoudí, že zpracování zvláště za použití nových technologických prostředků představuje vysoké riziko pro práva a svobody subjektů údajů. K vyhotovení posouzení dochází zpravidla před zahájením zpracování. ÚOOÚ vytvořil seznam operací, u nichž je požadováno posouzení vlivu vytvořit.[108] Nejčastějším druhem operace, u níž je posouzení prováděno, je monitorování subjektů údajů, a to například kamerovým systémem či zpracování biometrických údajů, kterým je třeba biometrický podpis či snímání otisků prstů.

Pokud správce ustanovil pověřence pro ochranu osobních údajů, musí si vyžádat jeho posudek k posouzení vlivu.

---

https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=37161&n=poznatky%2Duradu%2Dz%2Dohlasovani%2Dporuseni%2Dzabezpeceni%2Dosobnich%2Dudaju&p1=2567.

[106] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 121.

[107] NEŠPŮREK, R., ŠUCHMAN, J., JAROŠ, J. *GDPR: Kdy a jak posuzovat vliv zpracování na ochranu osobních údajů a kdy konzultovat dozorový orgán?* [online]. pravniprostor.cz [cit. 2020-04-05]. Dostupné na: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/gdpr-kdy-a-jak-posuzovat-vliv-zpracovani-na-ochranu-osobnich-udaju-a-kdy-konzultovat-dozorovy-organ.

[108] *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (DPIA)* [online]. uoou.cz [cit. 2020-04-05]. Dostupné na: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940.

Samotné posouzení vlivu musí obsahovat uvedené náležitosti:

- *„systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;*
- *posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;*
- *posouzení rizik pro práva a svobody subjektů údajů;*
- *plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.“*[109]

Vyhotovením posouzení vlivu však tato povinnost pro správce nekončí. Je nezbytné provádět pravidelné aktualizace, neboť se používané technologie mohou měnit a riziko by mohlo zpracování představovat až s nástupem těchto změn.

Pokud se vypracováním posouzení vlivu včetně zahrnutí zamýšlených opatření na zmírnění rizik identifikuje pravděpodobnost vysokého rizika, musí dojít ke konzultaci zpracování osobních údajů s dozorovým úřadem. V rámci přezkumu tohoto zamýšleného zpracování může v souladu s čl. 58 Obecného nařízení ÚOOÚ uplatnit některou ze svých pravomocí, zejména by mohlo jít o vyzvání správce k uvedení procesu zpracování do souladu s Obecným nařízením předepsaným způsobem, omezení zpracování či úplný zákaz.[110]

Posouzení vlivu na ochranu osobních údajů je dalším z nástrojů, který dokládá soulad s Obecným nařízením. Důležitým hlediskem je ovšem i kvalita zpracování tohoto dokumentu. Pokud k tomuto institutu správce přistoupí pouze jako ke splnění povinnosti, může dokument zpracovat nesprávně, a dojít tak k výsledku posouzení, který neodpovídá skutečnému stavu.

[109] Čl. 35 odst. 7 Obecného nařízení.
[110] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 357.

6.8.3 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů neboli *DPO* (z anglického *Data Protection Officer*) je pro české správce osobních údajů naprosto novým institutem, neboť předchozí právní úprava neobsahovala ani obdobu tohoto.

Hned první odstavec čl. 37 Obecného nařízení, který je věnován pověřenci, obsahuje, za jakých okolností je povinné pověřence jmenovat, a to z toho důvodu, že takové zpracování může mít za následek vyšší riziko, a proto je potřeba dohled nezávislé osoby s jistým stupněm odbornosti. Jedná se o následující případy:

- *„zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;*
- *hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;*

  nebo
- *hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.“*[111]

Kromě výše uvedených situací je zároveň možné pověřence jmenovat dobrovolně, přičemž v takovém případě se na něj budou vztahovat stejná pravidla a povinnosti dle čl. 37 až 39 jako na povinně jmenovaného pověřence. WP 29 ve svých pokynech k institutu pověřence pro ochranu osobních údajů také uvádí, že pokud správce nemá povinnost jmenovat pověřence a nechce tak učinit ani dobrovolně, má ještě třetí možnost, a to pověřit externího poradce či vlastního zaměstnance úkoly, které se týkají zpracování osobních údajů.

Obecné nařízení samo o obě neobsahuje nikterak podrobný výčet požadavků, která by měl pověřenec splňovat. Mnohem šířeji se k tomuto tématu vyjádřily pokyny WP 29. Dle pokynu by měl pověřenec disponovat adekvátní úrovní odborných znalostí dle činnosti správce. Tedy pokud půjde o správce, jehož zpracování zahrnuje velké množství osobních údajů v několika systémech, přičemž

[111] Čl. 37 odst. 1 Obecného nařízení.

velkou část osobních údajů bude tvořit zvláštní kategorie, musí tomuto odpovídat i úroveň odbornosti daného pověřence. Zároveň se pokyny vyjadřují k profesním kvalitám pověřence, do nichž by měla spadat dobrá znalost nejen Obecného nařízení, ale i souvisejících právních předpisů a zároveň znalost evropské a vnitrostátní praxe v oblasti ochrany osobních údajů. Měl by také dobře znát situaci správce, její vnitřní fungování, procesy, při nichž dochází ke zpracování osobních údajů a postupy a prostředky zabezpečení.[112]

Správce pro úlohu pověřence pro ochranu osobních údajů může vybrat osobu z řad vlastních zaměstnanců či zvolit externího odborníka na základě smlouvy o poskytování služeb.

Úkolem pověřence je především zajišťovat soulad činnosti správce osobních údajů s Obecným nařízením. Za tímto účelem mu musí správce poskytnout všechny relevantní informace, které potřebuje, aby mohl vykonávat činnost poradenství řádně. Pověřenec poskytuje svá stanoviska a vyjádření, pokud se jedná například o posouzení vlivu aj. Zároveň působí jako prostředník mezi správcem na jedné straně a subjekty osobních údajů či dozorovým úřadem na straně druhé.

6.8.4 Záznamy o činnostech zpracování

Záznamy o činnostech zpracování jsou jedním z klíčových dokumentů, jimž správce dokládá soulad s Obecným nařízením. Povinnost vést tyto záznamy nahrazuje dříve známou oznamovací povinnost dozorovému úřadu, kterou správcům ukládala předchozí právní úprava. Na rozdíl od předchozí oznamovací povinnosti správce nyní pouze vede ve své dokumentaci záznamy, které dozorovému úřadu předloží na vyžádání, a umožní tak jejich kontrolu a monitorování procesů zpracování osobních údajů.

Obsah těchto záznamů se liší, zdali je vede správce či zpracovatel, který má rovněž povinnost tyto dokumenty vést.

Obsahové náležitosti záznamů o činnostech zpracování pro správce jsou následující:

[112] Guidelines on Data Protection Officers (‘DPOs’) (WP 243 rev.01) adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017. In: *Ec.europa.eu* [online]. str. 11-12 [cit. 2020-04-06]. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

- *„jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;*
- *účely zpracování;*
- *popis kategorií subjektů údajů a kategorií osobních údajů;*
- *kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;*
- *informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;*
- *je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;*
- *je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.“*[113]

Oproti tomu se obsahové náležitosti pro zpracovatele týkají pouze písmen a), c), e) a g). V příloze č. 1 a č. 2 této práce jsou přiloženy vzorově vyplněné záznamy o činnostech zpracování v případě správce a v případě zpracovatele.

Záznamy, stejně jako posouzení vlivu, musí být pravidelně aktualizovány, neboť zde může často docházet ke změnám.

Obecné nařízení obsahuje výjimku z povinnosti zpracovávat záznamy o činnostech zpracování, a to pro správce, kteří mají menší počet zaměstnanců než 250, pokud zpracování nepředstavuje riziko, zpracování není příležitostné nebo správce zpracovává zvláštní kategorii osobních údajů či rozsudky ve věcech trestních.[114] Poněkud zmatečně může působit příležitostnost zpracování, neboť jakékoliv zpracování nese určité znaky pravidelnosti a systematičnosti, přičemž čistá náhodnost zpracování je velmi nepravděpodobná. Z toho důvodu lze přistoupit k názoru, že tato výjimka se bude vztahovat na správce, jenž zpracovává osobní údaje velmi malého množství a nízkého počtu účelů.

[113] Čl. 30 odst. 1 Obecného nařízení.
[114] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 165.

6.8.5 Kodexy chování

Kodexy chování lze charakterizovat jako určitý souhrn pravidel, jak dodržovat soulad Obecného nařízení pro určité odvětví. Odvětvím se rozumí v tomto případě okruh správců, kteří mají stejnou nebo obdobnou činnost zpracování.

Obsahem kodexů chování jsou upřesňující pokyny, jak provádět určitá ustanovení Obecného nařízení určitým sektorem správců. V čl. 40 odst. 2 je obsažen demonstrativní výčet oblastí, které může kodex chování upravovat. Patří mezi ně například upřesnění oprávněných zájmů správců či postupy, jak uplatňovat práva subjektů. Demonstrativnost tohoto výčtu znamená, že kodex chování nemusí obsahovat úplně všechny oblasti, které uvádí výše zmiňovaný článek a zároveň tvůrci kodexů mohou přidat další oblast úpravy mimo tento výčet.

Tvůrcem kodexů může být jeden či více správců dohromady. Vypracovaný kodex poté předloží k posouzení a schválení příslušnému dozorovému úřadu. Pokud se jedná o kodex, který by se vztahoval na činnost správců z více členských států, dozorový úřad tento kodex předloží ke schválení Evropskému sboru pro ochranu osobních údajů.[115]

Nespornou výhodou kodexu chování je, že správce, který kodex dodržuje, zároveň prokazatelně dokládá soulad své činnosti s Obecným nařízením. Prokazuje zavedení technických a organizačních opatření k zabezpečení zpracování a dokládá plnění povinností. Zároveň se k dodržování kodexu přihlíží, pokud by měla být správci uložena pokuta za porušení Obecného nařízení.[116]

K dohledu nad dodržováním kodexu je ustanoven subjekt, který bude pověřen akreditací. Aby ji získal, musí splňovat určité parametry. Těmi jsou především dobrá znalost samotného kodexu chování, práva na ochranu osobních údajů, činnost správců, na kterou se kodex vztahuje, nezávislost a odlišnost zájmů, aby nedocházelo ke střetu. Zároveň také musí prokázat stanovení postupů, díky nimž bude docházet ke kontrole dodržování kodexů.

[115] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 168.
[116] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR - obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer, 2018, str. 384.

6.8.6 Vydávání osvědčení

Tento institut je opět zcela novou možností, jehož cílem je napomáhání dokládání souladu s Obecným nařízením. Osvědčení může mít formu známek či pečetí, které mají signalizovat jednoznačným a srozumitelným způsobem, že prováděné zpracování správcem je v souladu s Obecným nařízením. Rozdíl oproti kodexům chování je ten, že se nevztahuje na určitou činnost správců daného odvětví.

Akreditovat subjekty k vydávání osvědčení může dozorový úřad či vnitrostátní akreditační úřad. V České republice je tímto subjektem Český institut pro akreditaci, o. p. s.[117] Vydávání akreditací za účelem vydávání osvědčení probíhá v souladu se zákonem č. 90/2016 Sb., o posuzování shody stanovených výrobků při jejich dodávání na trh.[118] Subjekty, které žádají o udělení akreditace k vydávání osvědčení musí obdobně jako v případě kodexů chování splňovat určitá kritéria. Jsou jimi především odborná znalost právní úpravy ochrany osobních údajů, předmětu osvědčení, nezávislost a neexistence střetu zájmů. Také musí doložit stanovení postupů k vydávání, přezkumu a odebírání osvědčení.

Osvědčení se vydává maximálně na dobu tří let, přičemž existuje možnost obnovy, pokud správce stále splňuje podmínky pro udělení. Pokud však přestane tyto podmínky plnit, subjekt pro vydávání osvědčení ho může také odebrat.

[117] *Úřad k vydávání osvědčení o ochraně osobních údajů podle GDPR* [online]. uoou.cz [cit. 2020-04-08]. Dostupné na: https://www.uoou.cz/urad-k-vydavani-osvedceni-o-ochrane-osobnich-udaju-podle-gdpr/d-23896.

[118] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Nakladatelství ANAG, 2018, str. 170.

7 Ochrana soukromí během nouzového stavu v souvislosti s vyhlášením pandemie Covid-19

Od přelomu roku 2019-2020 se celý svět potýká s pandemií virové choroby covid-19, následkem čehož byl v březnu 2020 v České republice vyhlášen nouzový stav dle čl. 5 a násl. ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky. V souvislosti se snahou zabránit nekontrolovanému šíření nemoci vydalo Ministerstvo zdravotnictví na základě usnesení vlády č. 250 mimořádné opatření čj. MZDR 12398/2020-1/MIN/KAN, které mj. upravuje tzv. „orientační trasování" polohy osob, u nichž bylo prokázáno onemocnění covid-19. Jedná se o velmi nekonvenční zásah do osobních údajů. Důvodem pro zvýšenou pozornost s ohledem na zásah do soukromí je spolupráce soukromoprávních společností s orgány veřejné moci a vytvoření projektu „Chytrá karanténa".

7.1 Projekt Chytrá karanténa a zásah do osobních údajů

Poté, co fyzická osoba zjistí, že je pozitivní na nákazu onemocněním covid-19, musí označit všechny osoby, se kterými přišla do styku, a tak eliminovat další nevědomé šíření prostřednictvím jí možných nakažených. Za tímto účelem byl vytvořen projekt „Chytrá karanténa", který spočívá v trasování nakažených občanů a vytváření tzv. paměťových map. Potřebné údaje jsou poskytovány soukromoprávními společnostmi, kterými jsou mobilní operátoři či bankovní instituce, které poskytnou údaje, kde se dotyčná osoba nacházela během doby, kdy již byla přenašečem, a s kým se mohla dostat do styku. Poskytnutí těchto informací nicméně předchází souhlas nakaženého s předáním těchto údajů.

Do značné míry jde o citlivou problematiku, neboť dojde k poskytnutí osobních údajů dotyčného ve spojitosti s místem a časem, tedy dojde k poměrně velkému zásahu do jeho soukromí. Zároveň jsou zpracovávány osobní údaje třetích osob, tedy potenciálně nakažených, které na základě dodaných údajů informuje příslušná hygienická stanice o možné nákaze a posléze otestuje.

Zpracování je podmíněno velmi přísnými mantinely, kterými je striktně vymezený účel a doba zpracování. Ve věci účelu je jednoznačně dané pro mobilní operátory i bankovní instituce, že zpracování je možné pouze za použití nezbytných operací a výlučně za účelem řešení pandemie. Mimořádné nařízení ministerstva

stanovuje dobu nezbytně nutnou ke zpracování osobních údajů, v případě jejich neanonymizované podoby se jedná o časový úsek, který nepřekračuje šest hodin.

Právním titulem, jak bylo již výše zmiňováno, je souhlas subjektu údajů. Nicméně z vyjádření ÚOOÚ ze dne 2. 4. 2020[119] vyplývá, že jako mnohem příhodnější se jeví právní titul zpracování ve veřejném zájmu dle čl. 6 odst. 1 písm. e) Obecného nařízení.[120] Z uvedeného lze usuzovat, že vláda ČR zvolila přístup mnohem mírnější a ohleduplnější s ohledem k právu na ochranu osobních údajů.

Dle mého názoru je však tento krok zbytečný vzhledem k vážnosti situace a existenci adekvátního právního titulu, kterým je zpracování na základě veřejného zájmu, kterým nastalá situace bezesporu je. Byť se Obecné nařízení vyznačuje především ochranou subjektů údajů, existují situace, kdy je možné ochranu soukromí omezit. Tou je bezpochyby, byť nevědomé, veřejné ohrožení šířením nebezpečné nemoci. Tímto je naplněna podmínka veřejného zájmu, neboť zde ochrana veřejného zdraví značně převáží zájem jednotlivce na ochranu soukromí.

[119] *Úřad se vyjádřil k mimořádnému opatření ministerstva zdravotnictví v souvislosti s projektem chytrá karanténa* [online]. uoou.cz [cit. 2020-04-09]. Dostupné na: https://www.uoou.cz/urad-se-nbsp-vyjadril-k-nbsp-mimoradnemu-opatreni-ministerstva-zdravotnictvi-v-nbsp-souvislosti-s-nbsp-projektem-chytra-karantena/d-41505.

[120] Čl. 6 odst. 1 písm. e) Obecného nařízení: Zpracování je zákonné …. pokud je zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.

Závěr

Autorka si v úvodu stanovila za stěžejní úlohu této práce posouzení dopadů účinnosti Obecného nařízení na práva a povinnosti subjektů a správců osobních údajů. Jak již bylo nastíněno v úvodu, v průběhu přijetí této „revoluční“ úpravy osobních údajů byly vyvolávány značné kontroverze a jednalo se o jeden z nejvíce diskutovaných právních aktů Evropské unie posledních let.

Pro lepší pochopení obsahu Obecného nařízení byly zprvu popsány historické souvislosti ochrany osobních údajů, resp. jejich vývoj, a to ať už globálního měřítka či pouze na území České republiky.

Následně byly popsány okolnosti a důvody vedoucí k přijetí Obecného nařízení, přičemž byl kladen důraz především na cíle přijetí nové právní úpravy a na změny, které přináší. Následně došlo k analýze samotného Obecného nařízení, a to nejprve z hlediska jeho působnosti a posléze z hlediska definování základních pojmů, na kterých je úprava osobních údajů postavena, přičemž byly zohledněny právě změny, které tyto pojmy přinesly.

Vzhledem k posouzení dosud uvedených kapitol lze zhodnotit, že naprosto revolučním právním předpisem Obecné nařízení není. Lze tak usuzovat z poměru terminologie, kterou Obecné nařízení převzalo ze Směrnice č. 95/46/ES, ale také z poměru práv a povinnosti, které byly převzaty a práv a povinností, které jsou nové a tvoří skutečně faktický přínos Obecného nařízení. Z uvedeného vyvstala další otázka, zda Obecné nařízení reflektovalo současné, ale i budoucí potřeby osobních údajů. Nezastavitelný vývoj technologie hrál zásadní roli již při vytváření Obecného nařízení a v tomto ohledu lze jednoznačně říct, že změna právní úpravy byla nezbytná, neboť Směrnice č. 95/46/ES na aktuální potřeby nestíhala reagovat a ze značné části již byla neaplikovatelná. Zda však Obecné nařízení zvládne reagovat na aktuální stupeň vývoje technologie a kybernetizace je věcí druhou. Někteří odborníci se domnívají, že již při přijetí nové právní úpravy byla pozadu zhruba o pět let. Dle mého názoru byl tento stav z hlediska zákonodárce nedostatečně posouzen a zcela určitě tato právní úprava nebude ani zdaleka stačit na rychlost vývoje let následujících. S jistotou lze říct, že změna právní úpravy ochrany osobních údajů přijde mnohem dříve, než zákonodárce předpokládal, neboť bude muset reagovat na nedostatečnost současného stavu Obecného nařízení. V tomto případě by bylo na místě disponovat větší dávkou předvídavosti a snažit

se vytvořit takový právní předpis, který bude schopný reflektovat potřeby nejen aktuální, ale především i ty budoucí.

Hlavní část této diplomové práce spočívala v kapitolách následujících, ve kterých došlo k popsání současných práv subjektů osobních údajů a také povinností správců osobních údajů.

Pokud jde o práva subjektů osobních údajů, bylo zjištěno, že tato práva byla značně rozšířena a tím jednoznačně posíleno postavení subjektu údajů jakožto slabší strany ve vztahu ke správci osobních údajů. Avšak dodržování práv subjektů správci není jediné hledisko, které je třeba v tomto stavu zohlednit. Přístup samotných subjektů je rovněž velice důležitým aspektem, což, jak se v praxi ukazuje, si subjekty často neuvědomují, přistupují k těmto právům zcela ledabyle a sami na ochranu osobních údajů nedbají. Důsledkem uvedeného se stávají tato práva pouze prázdnými ustanovení, která tak v praxi nepřináší kýžený výsledek ochrany slabší strany, který byl zákonodárcem zamýšlen.

V kapitole věnující se povinnostem správců osobních údajů byly následně analyzovány nové instituty, které předchozí právní úprava neznala, a bylo tak potřebné je osvětlit, neboť i v praxi tyto nové instituty působí poněkud nejednoznačně a není příliš jasné, jak mají být konkrétní instituty aplikovány. Z této práce je patrné, že počet povinností správců osobních údajů značné vzrostl, což přineslo v praxi mnoho problémů, neboť na tuto rozsáhlou změnu museli správci zareagovat a důsledně se připravit, aby jejich činnost v okamžiku účinnosti byla v souladu s Obecným nařízením. Je ovšem důležité posoudit, zda k této povinnosti správci přistoupili jen za účelem, aby byla splněna formálně vypracováním interních dokumentů dokládajících soulad, nicméně je neaplikovali do praktické činnosti zpracování osobních údajů, anebo zda skutečně zohlednili podstatu povinností jim uložených Obecným nařízením v praxi. V ideálním případě bude obsah Obecného nařízení v praxi skutečně reflektován, v opačném budou veškeré interní dokumenty k doložení souladu pouhým formálním úkonem, který ovšem nebude mít materiální využití. Ve světle uvedených skutečností je třeba zohlednit i účelnost finančních prostředků, které byly vynaloženy za účelem souladu s Obecným nařízením. Dle mého názoru je nezbytné k naplnění účelu a smyslu Obecného nařízení, aby správci nepřijímali různé směrnice a metodiky jen jako

formální krok za účelem splnění povinnosti doložení souladu, ale aby docházelo zároveň k naplnění těchto dokumentů a aplikování v praxi.

V úplném závěru této práce byla zmíněna zcela aktuální problematika osobních údajů ve vztahu k celosvětové pandemii, a to konkrétně na základě čeho může během nouzového stavu dojít k omezení práva na soukromí, resp. k zásahu do osobních údajů, kde hlavním faktorem je v této souvislosti především veřejný zájem.

Resumé

This diploma thesis is focused on the changes brought by Regulation 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 (hereinafter referred to as the „General Data Protection Regulation" or „GDPR"), in particular on selected impacts on the rights and obligations of data subjects and controllers. Given the fact, that GDPR is just four years old legislative act, it is not clear yet, how GDPR benefits to rights of data subjects and obligations of controllers in practice. First of all, there is a short summary of the history of personal data and its protection for the purpose of analysing the changes brought by GDPR. Afterwards this thesis answers a question about the legal form of this act. The main part of this thesis is dedicated to rights of data subjects and obligations of controllers, especially the new impacts brought by this legal act. An analysis of rights of data subjects shows an extension of the rights but also a problem with the attitude of data subjects themselves to protecting their data. As well as extension of the rights of data subjects there is an extension in obligations of controllers because GDPR brought so many new tools for harmonizing data process with the legal act. However, there is also a problem with the attitude of controllers if they made steps for just formal conformity with GDPR or if they really implement methods according to GDPR into the data processing operations.

Seznam příloh

Seznam použitých zdrojů

Odborná literatura a komentáře

1. European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2018, 402 s. ISBN 978-92-871-9849-5.
2. NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 339 s. ISBN 978-80-7380-689-7.
3. NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017, 304 s. Právo pro praxi. ISBN 978-80-271-0668-4.
4. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR - obecné nařízení o ochraně osobních údajů*. *Praktický komentář*. 2. vydání. Praha: Wolters Kluwer, 2018, 580 s. ISBN 978-80-7598-068-7.
5. PATTYNOVÁ, J., SUCHÁNKOVÁ, L., ČERNÝ, J. a kolektiv. Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář. Praha: Leges. 488 s.
6. VOIGT, P., Axel von dem Bussche. The EU General Data Protection Regulation (GDPR): a practical guide. Cham: Springer. 383 s.
7. ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: Nakladatelství ANAG, 2018, 343 s. ISBN 978-80-7554-152-9.

Právní předpisy

1. Deklarace práv člověka a občana z roku 1789.
2. Evropská úmluva o ochraně lidských práv a základních svobod.
3. Mezinárodní pakt o občanských a politických právech.
4. 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.*
5. Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.*

6. Směrnice Evropského parlamentu a Rady 95/46/ES, ze dne 24. října 1995 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.*
7. Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (č. 115/2001 Sb. m. s.).
8. Usnesení č. 2/1993 Sb., usnesení předsednictva České národní rady *o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky.*
9. Ústavní zákon č. 293/1920 Sb., *o ochraně svobody osobní, domovní a tajemství listovního.*
10. Všeobecná deklarace lidských práv z roku 1948.
11. Zákon č. 101/2000 Sb., *o ochraně osobních údajů a o změně některých zákonů.*
12. Zákon č. 110/2019 Sb., *o zpracování osobních údajů.*
13. Zákon č. 87/1862 Sb.z.s., *o ochraně svobody osobní.*
14. Zákon č. 256/1992 Sb., *o ochraně osobních údajů v informačních systémech.*

Odborné články a příspěvky

8. DEMETEROVÁ, L., HAKROVÁ, K. *A zase to GDPR! Tentokrát poznatky z praxe a auditů aneb nejčastější chyby a jak jim předejít - část I.* [online]. pravniprostor.cz Dostupné na: https://www.pravniprostor.cz/clanky/ostatni-pravo/a-zase-to-gdpr-tentokrat-poznatky-z-praxe-a-auditu-aneb-nejcastejsi-chyby-a-jak-jim-predejit-cast-i.
1. DEMETEROVÁ, L., HAKROVÁ, K. *A zase to GDPR! Tentokrát poznatky z praxe a auditů aneb nejčastější chyby a jak jim předejít - část II.* In: *Pravniprostor.cz* [online]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/ht-a-zase-to-gdpr-tentokrat-poznatky-z-praxe-a-auditu-aneb-nejcastejsi-chyby-a-jak-jim-predejit-cast-ii.
2. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01) adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018. In: *Ec.europa.eu* [online]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
3. Guidelines on Data Protection Officers (‘DPOs’) (WP 243 rev.01) adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017. In:

Ec.europa.eu [online]. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

4. Guidelines on the right to data portability 2016/679 (WP 242 rev.01) adopted on 13 December 2016 as last Revised and adopted on 5 April 2017. In: *Ec.europa.eu* [online]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
5. Guidelines on transparency under Regulation 2016/679 (WP260 rev.01) adopted on 29 November 2017. In: *Ec.europa.eu* [online]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
9. KRÁL, R. Nařízení v ES. In: HENDRYCH, D. a kol. Právnický slovník. In: Beck-online.cz [online databáze]. 3. vydání. Praha: C. H. Beck, 2009. [cit. 2019-02-09]. Dostupné z: https://www-beck-online.cz.
6. LUPIEŃSKÁ, P. *Hlášení bezpečnostních incidentů – co stanovuje zákon o kybernetické bezpečnosti a co GDPR?* [online]. pravniprostor.cz. Dostupné na: https://www.pravniprostor.cz/clanky/pravo-it/hlaseni-bezpecnostnich-incidentu-co-stanovuje-zakon-o-kyberneticke-bezpecnosti-a-co-gdpr.
7. MARCÍN, V. Poznatky Úřadu z ohlašování porušení zabezpečení osobních údajů. [online]. uoou.cz. Dostupné na: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=37161&n=poznatky%2Duradu%2Dz%2Dohlasovani%2Dporuseni%2Dzabezpeceni%2Dosobnich%2Dudaju&p1=2567.
8. MORÁVEK, J. Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie? Právní rozhledy. 2018, č. 13–14, s. 487–493.
9. *Nejdůležitější pojmy.* [online] In: *Uoou.cz*. Dostupné z: https://www.uoou.cz/3-nejd-lezit-jsi-pojmy/d-27293.
10. NEŠPŮREK, R., ŠUCHMAN, J., JAROŠ, J. GDPR: Kdy a jak posuzovat vliv zpracování na ochranu osobních údajů a kdy konzultovat dozorový orgán? [online]. pravniprostor.cz Dostupné na: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/gdpr-kdy-a-jak-posuzovat-vliv-zpracovani-na-ochranu-osobnich-udaju-a-kdy-konzultovat-dozorovy-organ.
11. *Nové přístupy a povinnosti*. [online] In: *Uoou.cz*. Dostupné z: https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=4744.
12. Opinion (WP 136) 4/2007 *on the concept of personal data* adopted on 20th June. In: *Ec.europa.eu* [online]. Dostupné z:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

13. Opinion (WP216) 05/2014 *on Anonymisation Techniques* adopted on 10 April 2014. In: *Ec.europa.eu* [online]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
14. Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (DPIA) [online]. uoou.cz. Dostupné na: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940
15. SLANINA, Jan. Právo být zapomenut a další dopady rozsudku SDEU C-131/12 Google Spain. [online]. *In: epravo.cz* [cit. 2020-03-29]. Dostupné na: https://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-sdeu-c-13112-google-spain-94498.html.
16. Stanovisko Úřadu pro ochranu osobních údajů č. 3/2011 *Ochrana osobních údajů podnikajících fyzických osob*. Dostupné z: https://www.uoou.cz/files/stanovisko_2011_3.pdf.
17. ŠKORNIČKOVÁ, Eva. *Právo na přístup k osobním údajům prověří připravenost na GDPR.* [online]. *In: Gdpr.cz* Dostupné na: https://www.gdpr.cz/blog/pravo-na-pristup-k-osobnim-udajum-proveri-pripravenost-na-gdpr/.
18. *Upozornění na změnu v posuzování systémů využívajících biometrické údaje (dříve "Stanovisko č. 1/2017 - Biometrická identifikace nebo autentizace zaměstnanců").* In: *Uoou.cz* [online]. Dostupné z: https://www.uoou.cz/upozorneni-na-zmenu-v-nbsp-posuzovani-systemu-vyuzivajicich-biometricke-udaje-drive-quot-stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu-quot/d-29048/p1=3069.
19. *Úřad k vydávání osvědčení o ochraně osobních údajů podle GDPR* [online]. uoou.cz. Dostupné na: https://www.uoou.cz/urad-k-vydavani-osvedceni-o-ochrane-osobnich-udaju-podle-gdpr/d-23896.
20. *Úřad se vyjádřil k mimořádnému opatření ministerstva zdravotnictví v souvislosti s projektem chytrá karanténa* [online]. uoou.cz. Dostupné na: https://www.uoou.cz/urad-se-nbsp-vyjadril-k-nbsp-mimoradnemu-opatreni-ministerstva-zdravotnictvi-v-nbsp-souvislosti-s-nbsp-projektem-chytra-karantena/d-41505.

Judikatura

1. Soudní dvůr: Rozsudek ze dne 13. května 2014, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, bod 14, 15.

Přílohy

Záznam o činnostech zpracování - správce

Záznam o činnostech zpracování **Čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů (GDPR)** **Správce:** **Pověřenec pro ochranu osobních údajů:**
I. Účely zpracování
Zpracování osobních údajů na základě smlouvy o vedení personální a mzdové agendy
Čl. 6 odst. 1 písm. c) GDPR - zpracování nezbytné pro plnění právní povinnosti: - zákon č. 563/1991 Sb., o účetnictví **Čl. 6 odst. 1 písm. b)** GDPR - zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů
II. Kategorie subjektů údajů
Zaměstnanci
III. Kategorie osobních údajů
Jméno, příjmení, číslo účtu
IV. Kategorie příjemců
Příslušný finanční úřad
V. Plánované lhůty pro výmaz kategorií osobních údajů
K výmazu a skartaci dochází po uplynutí zákonných lhůt: - účetní doklady, účetní knihy, odpisové plány, inventurní soupisy, účtový rozvrh, přehledy – 5 let - účetní záznamy, kterými účetní jednotky dokládají vedení účetnictví – 5 let
VI. Obecný popis technických a organizačních bezpečnostních opatření
Dokumenty jsou uloženy v šanonech v uzamykatelné skříni v kanceláři účtárny, která je rovněž uzamykána v nepřítomnosti zaměstnanců, popřípadě jsou dokumenty uloženy v uzamykatelném archivu. Systém vydávání klíčů je upraven vnitřním dokumentem.

Záznam o činnosti zpracování – zpracovatel

Záznam o činnostech zpracování **Čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů (GDPR)** **Správce:** **Pověřenec pro ochranu osobních údajů:**
I. Kategorie subjektů údajů
Zaměstnanci
II. Kategorie osobních údajů
Jméno, příjmení, číslo účtu
III. Kategorie příjemců
Osobní údaje nebudou předávány do třetích zemí nebo mezinárodním organizacím.
IV. Obecný popis technických a organizačních bezpečnostních opatření
Dokumenty jsou uloženy v šanonech v uzamykatelné skříni v kanceláři účtárny, která je rovněž uzamykána v nepřítomnosti zaměstnanců, popřípadě jsou dokumenty uloženy v uzamykatelném archivu. Systém vydávání klíčů je upraven vnitřním dokumentem.