Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Bakalářská práce

GDPR a jeho implementace v konkrétní právnické osobě

Blanka Blažková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Blanka Blažková

Veřejná správa a regionální rozvoj – k.s. Hradec Králové

Název práce

GDPR a jeho implementace v konkrétní právnické osobě

Název anglicky

GDPR and its implementation in a specific legal person

Cíle práce

Tato Bakalářská práce se bude zabývat problematikou implementace GDPR do státní správy. Konkrétně na České správě sociálního zabezpečení Hradec Králové. Hlavním cílem bude analýza rizik zpracování osobních údajů. Vedlejším cílem bude posouzení nárůstu administrativy, časová případná finanční nákladnost a možnosti zefektivněním provádění povinného nařízení GDPR.

Metodika

Práce bude rozdělena na dvě části. Teoretická část se bude zaměřovat na právní úpravu v oblasti ochrany osobních údajů, včetně vysvětlení relevantních pojmů, které budou čerpány z příslušné legislativy a ověřených internetových zdrojů. Česká správa sociálního zabezpečení a potažmo okresní správy sociálního zabezpečení zpracovávají osobní údaje a osobní údaje zvláštní kategorie za účelem výkonu agendy nezbytné pro výběr pojistného na sociálním zabezpečení, pro provádění důchodového a nemocenského pojištění a lékařské posudkové služby v souladu s právním řádem České republiky a Evropské unie. Z tohoto důvodu v praktické části budou uvedeny a zhodnoceny situace, se kterými úředníci v praxi setkávají. Tyto informace budou zjišťovány formou nestrukturovaného rozhovoru či anketním dotazováním na OSSZ spadajících kompetentně pod ČSSZ Hradec Králové. Pomocí GAP analýzy bude zjišťován rozdíl mezi současným stavem a stavem požadovaným. Na závěr bude zhodnocena realizace GDPR v praxi.

Doporučený rozsah práce

30-40 stran

Klíčová slova

GDPR, implementace GDPR, správce, zpracovatel, subjekt údajů, citlivý údaj, profilování, dozorový úřad, pověřenec a zásady zpracování osobních údajů

Doporučené zdroje informací

Janečková, Eva. GDPR. Praktická příručka implementace. Praha : Wolters Kluwer ČR, a. s., 2018. str. 136. ISBN 978-80-7552-248-1.

Jasnečková, Eva. GDPR – Řešení problémů v praxi obcí. Praha : Grada Publishing, a.s., 2019. str. 256. ISBN 978-80-247-2925-1.

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

Navrátil, Jiří a a kolektiv. GDPR pro praxi. Plzeň : Aleš Čermák, s.r.o., 2018. str. 339. ISBN 978-80-7380-689-7.

Nezmar, Luděk. GDPR: Praktický průvodce implementací. Praha : Grada Publishing, a.s., 2018. str. 304. ISBN 978-80-271-0668-4.

Novák, Daniel. Zákon o ochraněosobních údajů a předpisy související. Komentář. Praha : Wolters Kluwer, a.s., 2014. str. 504. ISBN 978-80-7478-665-5.

PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR): Zákon o zpracování osobních údajů : komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. Komentátor. ISBN 978-80-7502-396-4.

Vlachová , Barbora a Maisner, Martin. Zákon o zpracování osobních údajů. Komentář. Praha : C. H. Beck, 2019. str. 163. ISBN 978-80-7400-6.

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

Žůrek, J. Praktický průvodce GDPR. Olomouc: ANAG, 2017, 223s. ISBN 978-80-7554-097-3.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Mgr. Michal Reichert, DiS.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 9. 3. 2022

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 3. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 11. 03. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "GDPR a jeho implementace v konkrétní právnické osobě" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 12. 3. 2023 _____

Poděkování

Rád(a) bych touto cestou poděkovala Mgr. Michalu Reichertovi, DiS za rady a připomínky, které mi pomohly při psaní bakalářské práce. Dále bych chtěla poděkovat své rodině, a zvláště manželovi za trpělivost a podporu v době studií.

GDPR a jeho implementace v konkrétní právnické osobě

Abstrakt

Bakalářská práce se zabývá legislativní úpravou GDPR a její implementací do české právní úpravy ve formě zákona o ochraně osobních údajů v oblasti státní správy, a to konkrétně v České správě sociálního zabezpečení. V teoretická část práce se zaměřuje na vymezení GDPR, historický vývoj včetně základních zásad Obecného nařízení. V další části jsou popsány práva subjektu údajů a role v oblasti GDPR. Poslední teoretická část se obšírněji věnuje dozorovému úřadu v podobě Úřadu pro ochranu osobních údajů.

V praktické části formou dotazníkového šetření je zjišťována povědomost o zpracování osobních údajů a úspěšná implementace GDPR do praxe úředníků na ČSSZ Hradec Králové a spádových OSSZ v Královehradeckém kraji. Dotazníkové šetření bude především cílit na každodenní potkávání se s danou problematikou a jestli jsou údaje zpracovávány automatizovaně nebo zda došlo k časové nebo administrativní nákladnosti

Klíčová slova: GDPR, implementace GDPR, správce, zpracovatel, subjekt údajů, citlivý údaj, profilování, dozorový úřad, pověřenec a zásady zpracování osobních údajů

GDPR and its implementation in a specific legal person

Abstract

The bachelor thesis deals with the legislative regulation of GDPR and its implementation into the Czech legislation in the form of the Personal Data Protection Act applied in the field of state administration, specifically in the Czech Social Security Administration. The theoretical part of the thesis focuses on the definition of GDPR and historical development, including the basic principles of the General Regulation. The next section describes the rights of the data subject and its roles in the framework of GDPR. The last theoretical part deals more extensively with the supervisory authority, which is performed by the Office for Personal Data Protection.

The practical part uses the form of a questionnaire survey, which examines the awareness of personal data processing and the successful implementation of GDPR in the practice of officials, specifically at the Czech Social Security Administration in Hradec Králové and the subordinary district social security administrations in the whole Hradec Králové Region. The questionnaire survey primarily aims to reveal what is the daily encounter with the issue, and to answer the question of whether the data is processed automatically or whether there was a time or administrative cost.

Keywords: GDPR, GDPR implementation, controller, processor, data subject, sensitive data, profiling, supervisory authority, data protection officer, principles of personal data processing

Obsah

Seznam obrázků

Seznam příloh

Seznam použitých zkratek

GDPR – 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.

EU – Evropská unie

OÚ – Osobní údaj

ČSSZ – Česká správa sociálního zabezpečení

OSSZ – Okresní správa sociálního zabezpečení

Obecné nařízení – viz. GDPR

1 Úvod

Cílem bakalářské práce je zhodnocení implementace Nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „GDPR“) do státní správy, a to konkrétně v České správě sociálního zabezpečení Hradec Králové a jejich spádových OSSZ.

Teoretická část si klade za úkol popsat zákonný rámec v oblasti ochrany osobních údajů a jeho implementaci do české legislativy v podobě zákona na ochranu osobních údajů. První část bude zaměřena obecně na GDPR včetně jeho historického vývoje. Obšírněji zde budou rozebrány základní zásady GDPR zejména zásada zákonnosti, korektnosti a transparentnosti čí přesnosti nebo minimalizace údajů atd. Dále pojmy jako je osobní údaj, zvláštní kategorie osobních údajů, profilování a pseudonymizace osobních údajů. Další téma směřuje na otázku, jaké práva mají subjekty osobních údajů, jako například právo na informace, právo na přístup k osobním údajům, právo vznést námitku nebo podat stížnost u dozorového úřadu a jiné. Nebudou opomenuty okruhy témat zabývající se souhlasem se zpracováním osobních údajů, role a odpovědnosti v GDPR. Závěrečná teoretická část je zaměřena na dozorový úřad, jehož činnost v České republice vykonává Úřad pro ochranu osobních údajů. Kromě historie dozorového úřadu zde budou popsány pravomoci a hlavní úkoly.

Praktická část se zaměřuje na implementaci GDPR do České správy sociálního zabezpečení v Hradci Králové a do Okresních správ sociálního zabezpečení spadajících pod působnost ČSSZ Hradec Králové. Pomocí dotazníkového šetření bude zjišťováno, jaká je míra povědomí a pochopení aspektu GDPR u úředníků ČSSZ. Dotazník bude především zaměřen na každodenní potkávání se s danou problematikou. Jako například s jakým typem osobních údajů se setkávají, z jakého důvodu jsou tyto údaje zpracovávány a zda zpracovaní probíhá automatizovaně či nikoliv. V neposlední řadě bude šetřeno, zda implementací GDPR došlo k navýšení časové nebo administrativní náročnosti.

Závěrem dojde k zhodnocení dotazníkového šetření a stanovení možného řešení ke zlepšení stávající situace.

2 Cíl práce a metodika

2.1 Cíl práce

Tato Bakalářská práce se bude zabývat problematikou implementace GDPR do státní správy. Konkrétně na České správě sociálního zabezpečení Hradec Králové. Hlavním cílem bude analýza rizik zpracování osobních údajů. Vedlejším cílem bude posouzení nárůstu administrativy, časová případná finanční nákladnost a možnosti zefektivněním provádění povinného nařízení GDPR.

2.2 Metodika

Práce bude rozdělena na dvě části. Teoretická část se bude zaměřovat na právní úpravu v oblasti ochrany osobních údajů, včetně vysvětlení relevantních pojmů, které budou čerpány z příslušné legislativy a ověřených internetových zdrojů. Česká správa sociálního zabezpečení a potažmo okresní správy sociálního zabezpečení zpracovávají osobní údaje a osobní údaje zvláštní kategorie za účelem výkonu agendy nezbytné pro výběr pojistného na sociálním zabezpečení, pro provádění důchodového a nemocenského pojištění a lékařské posudkové služby v souladu s právním řádem České republiky a Evropské unie. Z tohoto důvodu v praktické části budou uvedeny a zhodnoceny situace, se kterými úředníci v praxi setkávají. Tyto informace budou zjišťovány formou nestrukturovaného rozhovoru či anketním dotazováním na OSSZ spadajících kompetentně pod ČSSZ Hradec Králové. Pomocí GAP analýzy bude zjišťován rozdíl mezi současným stavem a stavem požadovaným. Na závěr bude zhodnocena realizace GDPR v praxi.

3 Teoretická východiska

Teoretická část se bude zaměřovat na právní úpravu v oblasti ochrany osobních údajů, včetně vysvětlení relevantních pojmů, které budou čerpány z příslušné legislativy, odborné literatury a ověřených internetových zdrojů.

3.1 GDPR

Přijetím 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 musí každá instituce, organizace, obec nebo společnost, která zpracovává osobní údaje splnit požadavky tohoto nařízení. [1]

3.1.1 Historie GDPR

1. října 1985 vstoupila v platnost Úmluva Rady Evropy č. 108, která měla na zřeteli automatizované zpracování osobních dat. Tuto smlouvu ratifikovali všechny členské státy EU kromě Turecka.[2]

Aby byla zajištěna ve všech členských státech Unie vysoká úroveň ochrany osobních údajů byla vytvořena v roce 1995 Směrnice 95/46 /ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Cílem této směrnice bylo specifikovat jednotný rozsah pro práci s osobními údaji a sjednotit právní předpisy v této oblasti v jednotlivých členských státech. [3]

Směrnice se časem stala zastaralá, a to hlavně z důvodu prudkého technologického pokroku zvláště v informačních technologiích. Dalším důvodem byla vlastní zákonná úprava legislativy každého jednotlivého členského státu. I když vycházela, s již zmíněné Směrnice 95/46/ES, se v mnoha aspektech lišila a tato skutečnost nesla s sebou určité obtíže.[4]

V prosinci 2009 podle článku 29 byla zřízena pracovní skupina, jako nezávislá evropská pracovní skupina, která se zabývala principy ochrany osobních údajů. Stanoviska

[1] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s.13.
[2] Tamtéž, s.14.
[3] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s.14.
[4] Tamtéž, s 14.

vydaná touto skupinou přispěla k počáteční debatě o reformě ochrany osobních údajů. Ve svých stanoviscích se věnuje několika oblastem, převážně k posílení postavení subjektu údajů, odpovědnosti správců, či postavení dohledového orgánu a později definici osobních údajů, k pojmu souhlas a k přenesené pravomoci. [5]

Výslednou podobu Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 96/46 ES (obecné nařízení o ochraně osobních údajů) schválil Evropský parlament 27. dubna 2016. Nařízení EU jsou závazná a přímo aplikovatelná v celém svém rozsahu pro všechny členské země. Nařízení začalo platit 25. května 2018 po předchozím zavedením do vnitrostátních legislativ zemí EU. [6]

3.1.2 **GDPR a české zákony**

Vývoj ochrany osobních údajů na území České republiky začal přijetím zákona č. 87/1862 Sb.z.s., o ochraně svobody osobní a zákonem č. 88/1862 Sb.z.s., na ochranu svobody domovní. V roce 1920 byl schválen Ústavní zákon č. 293/1920 Sb. z. a n., o ochraně svobody osobní, domovní a tajemství listovního. V dalších letech se zmínky o ochraně osobních údajů objevují v české legislativě objevují v kontextu s úpravou norem pro vydávání a držení dokladů, které osobní údaje obsahují. Koncem 20. století se ochrana osobních údajů dostává více do právních norem. Nejdříve zákonem 256/1992 Sb., o ochraně osobních údajů v informačních systémech, pak přišla na řadu Listina základních práv a svobod, vyhlášená Usnesením předsednictva České národní rady č. 2/1993 Sb. A v roce 2000 byl schválen zákon č. 101/2000 Sb., o ochraně osobních údajů, který platí dodnes.[7]

Vstoupením platnosti Lisabonské smlouvy, která novelizovala Smlouvu o Evropské unii se Listina základních práv Evropské unie de facto stala formálně její součástí. V listině základních práv a svobod je právo na ochranu osobních údajů vysloveně deklarováno. Listina základních práv a svobod je Ústavou české republiky začleněna do ústavního pořádku České republiky.[8]

Schválením Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 96/46 ES se zákon č. 101/2000 Sb., o ochraně osobních údajů

[5] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s.15-16.
[6] Janečková, E. *GDPR. Praktická příručka implementace.* Praha : Wolters Kluwer ČR, 2018, s. 14.
[7] Navrátil, J. a a kol. *GDPR pro praxi.* Plzeň : Aleš Čermák, 2018, s. 28.
[8] Tamtéž, s. 28.

a o změně některých zákonů se v určitém rozsahu nahrazuje. Po novelizaci tento zákon upravuje jen určitá hlediska týkajících se Úřadu pro ochranu osobních údajů a určité jednotlivé body k dovršení celé sféry ochrany osobních údajů, které nejsou Obecným nařízením upravovány nebo jejich úprava dle Obecného nařízení je povolena na vnitrostátní úrovni. Například u zpracování aspektů osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby je vnitrostátní úprava očekávána.[9]

Proces přijetí zákona o zpracování osobních údajů v České republice byl zdlouhavý, a to i z důvodu opožděného vypracování návrhu zákona a spoustou pozměňovacích návrhů. Kvůli vysoké administrativnímu zatížení naše legislativa neaplikovala zpřísnění podmínek regulace ochrany osobních údajů, i když to GDPR bylo povoleno. 12. března 2019 byl přijat zákon č. 101/2019 Sb., o zpracování osobních údajů, ve kterém byla přímo implementována směrnice 2016/680.[10]

3.1.3 **GDPR – obecné nařízení EU**

GDPR, z anglického názvu General Data Protection Regulation, plným názvem nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46 ES (obecné nařízení o ochraně osobních údajů) tvoří procesní oblast ochrany osobních údajů validní v celém prostoru Evropské unie, která chrání právo na soukromí svých občanů proti neoprávněnému zacházení s jejich daty a osobními údaji.[11]

Jedním z hlavních cílů přijetí Obecného nařízení bylo sjednocení právního rámce ochrany osobních údajů v každém státě Evropské unie, Islandu, Norska a Lichtenštejnska. Dalším záměrem bylo adaptovat právní normy o ochraně osobních údajů novodobým potřebám, hlavně posílit práva osob v jakožto subjektu údajů a sjednotit interpretaci GDPR dozorovými úřady mezi členskými státy Evropské unie, Islandu, Norska a Lichtenštejnska.[12]

[9] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 28.
[10] Vlachová, B., Maisner, M.. *Zákon o zpracování osobních údajů. Komentář.* Praha : C. H. Beck, 2019, s. 3.
[11] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 27.
[12] Janečková, E. *GDPR. Praktická příručka implementace.* Praha : Wolters Kluwer ČR, 2018, s. 30.

3.2 Základní zásady Obecného nařízení (GDPR)

Základní zásady pro zpracování osobních údajů jsou jmenovány v článku 5 odst. 1 Obecného nařízení a formují principy interpretace odpovědnosti správce, který musí být schopen toto dodržení souladu doložit.[13]

3.2.1 Zásada zákonnosti, korektnosti a transparentnosti

Jakékoliv zpracování osobních údajů by mělo být v souladu se zákonnými normami. Pokud by došlo ke zpracování v rozporu s právním řádem nebo by se jednalo o nelegální eventuelně nelegitimní podnět došlo by k porušení zásady zákonnosti. Obecné nařízení v článku 6 odst. 1 uvádí z jakých právních důvodů lze osobní údaje zpracovávat. Pro zpracování musí být splněn minimálně jeden právní důvod, a to v odpovídajícím rozsahu dané podmínky.[14]

Zákonnost zpracování dle článku 6 Obecného nařízení odst. 1:

„a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) 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;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“[15]

---

[13] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 5.

[14] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 35-36.

[15] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6.

Korektnost a transparentnost by měla dotčeným osobám zaručit svobodně se rozhodnout komu údaje poskytnou, za jakým účelem a v jakém rozsahu. Tyto osoby by měly být poučeny o svých právech i rizicích v kontextu se zpracováním osobních údajů. Veškeré informace musí být nejen přístupné, ale i srozumitelné, ideálně v písemné podobě.[16]

3.2.2 **Zásada účelového omezení**

Osobní údaje lze shromažďovat pouze za předem stanoveným účelem, pro který mají být zpracovány. A to metodou a prostředky, které jsou s tímto účelem kompatibilní. Správce musí zajistit, aby nasbírané osobní údaje byly zpracovány pro přesně dané legitimní účely a byly výslovně vyjádřené. Subjekt údajů, na základě plné informovanosti o zpracování svých osobních údajů, má určitou možnost rozhodovat, jak s jeho údaji bude zacházeno.[17]

Za neslučitelné s původními účely podle Obecného nařízení se nepovažuje zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.[18]

3.2.3 **Zásada minimalizace údajů**

V nařízení GDPR je uváděno že zpracování osobních údajů musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.[19]

Správce by měl zabezpečit minimálních rozsah konkrétních informací o subjektu údajů nezbytných pro daný účel zpracování, pro který údaje jsou sbírány. Správce musí doložit k jakému účelu jsou jednotlivé údaje zpracovávány, v opačném případě dochází k porušení zásady minimalizace údajů.[20]

---

[16] Navrátil, J. a a kol. *GDPR pro praxi.* Plzeň : Aleš Čermák, 2018, s. 40-41.
[17] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 40-41.
[18] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 5.
[19] Tamtéž
[20] Janečková, E. *GDPR. Praktická příručka implementace.* Praha : Wolters Kluwer ČR, 2018, s. 7.

3.2.4 **Zásada přesnosti**

Při zpracování osobních údajů musí být zajištěna jejich věcná správnost a je-li to nezbytné jejich aktuálnost. V případě nepřesných údajů musí být tyto údaje okamžitě vymazány nebo opraveny. Přesnost musí být zabezpečena již při sběru dat, tak i v procesu zpracování. Každý, kdo zpracovává osobní údaje, musí přijmout taková opatření, jejich pomocí zajistí, že nebudou zpracovávány nepřesné či chybné osobní údaje, a to v závislosti na rozsahu a okolnostech předmětného zpracování. Správce nebo zpracovatel osobních údajů na základě zákona o ochraně osobních údajů provádí, je-li to vzhledem k účelu zpracování nezbytné, aktualizaci zpracovávaných osobních údajů a tím zajistil korekci zjištěných nepřesností. Závaznost zpracovávat pouze přesné osobní údaje neznamená, že je požadováno zpracovávat jen absolutně správné údaje, neboť nepřesnosti mohli vzniknout již při sběru dat od samotných subjektů údajů, z čehož nelze dedukovat odpovědnost daného správce.[21]

3.2.5 **Zásada omezení uložení**

Úkolem této zásady je zajistit likvidaci osobních údajů, pokud již pominul účel, pro který se informace uchovává nebo pro tento účel již nejsou potřebné a tím snížit nebezpečí, že se tyto údaje stanou zastaralými nebo nepřesnými.[22]

Zásada omezení dle článku 5 Obecného nařízení odst. 1 písmeno e: Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů.[23]

U orgánů veřejné moci je tato zásada zajištěna především díky spisovým a skartačním řádům. Správce po výběru archiválií dokumenty včetně metadat určených k likvidaci zničí.

---

[21] Janečková, E. *GDPR. Praktická příručka implementace.* Praha : Wolters Kluwer ČR, 2018, s. 8.
[22] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 66-67.
[23] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 5.

Vybrané dokumenty s osobními údaji a jejich metadata předá k uložení do příslušného archivu a po potvrzení převzetí vybraných dokumentů k trvalému uložení archivem provede likvidaci všech kopií v informačních systémech spravující dokumenty včetně části jejich metadat. Oprávněná likvidace dokumentů se prokazuje protokolem o provedení skartačního řízení nebo protokolem o provedení výběru archiválií mimo skartační řízení. Obdobný postup je u analogových evidencí.[24]

3.2.6 **Zásada integrity a důvěrnosti**

Správce je povinen vhodným organizačním a technickým opatřením zabezpečit, aby pro každý konkrétní účel daného zpracování, se zpracovávaly pouze nezbytné osobní údaje. Týká se to objemu nasbíraných osobních údajů, rozsahu jejich zpracování, přístupnosti a času jejich uložení. Tím dojde k zajištění, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.[25]

Přiměřená bezpečnost osobních údajů zajistí jejich zabezpečení před neoprávněným a nelegitimním zpracováním, ztracením, zničením nebo poškozením. Integrita v tomto kontextu představuje ochranu nedotknutelnosti osobních údajů a důvěrnost je spojena s neoprávněným zpracováním.[26]

Kromě zajištění důvěrnosti, integrity, dostupnost a odolnost systémů a služeb zpracování musí být zachována schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů, a to pomocí procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Dalším prvkem bezpečného zpracování je pseudonymizace a šifrování osobních údajů.[27]

---

[24] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 44.
[25] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 25.
[26] Navrátil, J. a a kol. *GDPR pro praxi.* Plzeň : Aleš Čermák, 2018, s.43
[27] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 30.

3.2.7 **Zásada odpovědnosti**

Tato zásada nařizuje správci údajů, aby zajistil dodržení všech stanovených zásad Obecným nařízením všude tam, kde dochází ke zpracování osobních údajů. Tuto povinnost musí být schopen doložit.[28]

Zásadu odpovědnosti správce formuje článek 24 Obecného nařízení:

„*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. Tato opatření musí být podle potřeby revidováno a aktualizováno.“*[29]

Správce odpovídá za výběr zpracovatele, který mu musí poskytnout dostatečnou garanci o zavedení vhodných technických a organizačních opatření, které budou principy Obecného nařízení splňovat.[30]

3.3 **Osobní údaje**

Osobní údaje jsou podle článku 4 odstavce 1 Obecného nařízení: „… *veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*[31]

Pokud se určitá informace vztahuje k fyzické osobě a tuto osobu lze na základě těchto údajů jednoznačně identifikovat, je tato informace považována za osobní údaj. To platí také v případě, že informace nevede k přímé identifikaci, ale správce si může opatřit takové údaje, které ve spojením s původní informací vedou k přímé identifikaci subjektu údajů.[32]

---

[28] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 45.
[29] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 24.
[30] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 45-46.
[31] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4.
[32] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 20.

3.3.1 **Zvláštní kategorie osobních údajů**

Původní pojem „citlivé osobní údaje“ dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů je v Obecném nařízení označován jako zvláštní kategorie osobních údajů. Podle článku 9 Obecného nařízení se zakazuje zpracovávání osobních údajů, „… *které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby*.“[33]

Některé údaje, mohou být subjektem údajů považovány subjektivně jako velmi citlivé, ale pokud nejsou jmenovány v článku 9 Obecného nařízení, tak do zvláštní kategorie osobních údajů nespadají.[34]

Mezi zvláštní kategorii osobních údajů spadá i genetický údaj, který se vztahuje k zděděným nebo získaným genetickým znakům fyzické osoby a dávají informace o jejím zdraví a fyziologii. Dalším druhem zvláštní kategorie osobních údajů je biometrický údaj, který umožňuje pomocí konkrétního technického zpracování fyzických či fyziologických znaků nebo znaků chování fyzické osoby jedinečnou identifikaci. Dále sem spadá i údaj o zdravotním stavu, který vypovídá o tělesném nebo duševním stavu fyzické osoby.[35]

3.3.2 **Profilování osobních údajů**

Obecné nařízení definuje profilování jako jednu z forem automatického zpracování osobních údajů, na jehož základě dochází posuzování jistých hledisek souvisejících se subjektem údajů. Konkrétně k analýze nebo odhadu hledisek týkajících se jeho pracovního

[33] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 9.
[34] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 28.
[35] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4.

výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.[36]

3.3.3 **Pseudonymizace osobních údajů**

Pseudonymizace je taková forma zpracování osobních údajů, při které jsou určité údaje zpracovány tak, že nemohou být spojovány s konkrétním subjektem údajů bez doplňujících informací. Aby se zabezpečilo, že tyto informace nebudou spojovány s identifikovanou nebo identifikovatelnou fyzickou osobou musí být zabezpečeno jejich uchovávání pomocí technických a organizačních opatření.[37]

3.4 **Práva subjektu údajů**

Subjektem údajů je identifikovaná nebo identifikovatelná fyzická osoba, ke které se vztahují osobní údaje. Identifikace probíhá buď přímo nebo nepřímo pomocí identifikátoru. Osobní údaje fyzické osoby podnikající spadají pod ochranu Obecného nařízení.[38]

3.4.1 **Právo na informace**

Právo na informace upevňuje dle Obecného nařízení postavení subjektu údajů a posiluje jeho práva. Aby subjekt údajů mohl účinně hájit svá práva a rozhodovat o probíhajícím úkonu zpracování včetně účelu, musí mít plnou informaci podanou ve formě, které porozuměl. Informace musí být stručné, jasné a srozumitelné. Plnění informační povinnosti bylo v minulosti v mnoha případech ignorováno. Zvláště samosprávám a orgánům veřejné správy neměly povědomí o výskytu této povinnosti.[39]

V recitálu 60 Obecného nařízení je uvedeno, že pro zajištění spravedlivého a transparentního zpracování je správce povinen poskytnout subjektu údajů veškeré další informace, s přihlédnutím ke konkrétním okolnostem a kontextu, v němž jsou osobní údaje

[36] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4.
[37] Tamtéž, čl. 4.
[38] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 30.
[39] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 48.

zpracovávány. Další informace se týkají profilování a jeho případných důsledcích. Pokud subjekt údajů je povinen údaje poskytnout musí mít informace o důsledcích neposkytnutí údajů.[40]

V okamžiku shromažďování osobních údajů od subjektu údajů nebo pokud jsou získány z jiného zdroje, tak v přiměřené lhůtě, má správce povinnost informovat subjekt údajů. To samé platí, jestliže jsou údaje sděleny jinému příjemci, subjekt údajů musí být informován o jejich prvním sdělení tomuto příjemci. Pokud se údaje budou zpracovávat pro jiný účel, než byly shromažďovány, tak před jejich zpracováním o tom subjekt údajů musí informován.[41]

V případě, že subjekt údajů tyto informace má, nebo zpřístupnění těchto údajů je přímo stanoveno legislativní normou, nebo poskytnutí informací není možné, povinnost poskytovat informace není uložena. Při zpracování prováděného pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely by poskytování informací vyžadovalo neúměrné úsilí. Z tohoto důvodu není vyžadována povinnost poskytnout informace. [42]

3.4.2 **Právo na přístup k osobním údajům**

Toto právo subjektů údajů umožňuje získat od správce potvrzení a doplňkové informace, na základě své aktivní žádosti, zda jeho osobní údaje jsou nebo nejsou zpracovávány a k těmto osobním údajům získat přístup. Týká se to následujících informací:

- Za jakým účelem jsou osobní údaje zpracovávány
- Zpracovávány jsou dotčené osobní údaje, podle jakých kategorií osobních údajů
- Kterým příjemcům nebo kategorii příjemců budou nebo byly osobní údaje zpřístupněny
- Jaký je časový rámec, po který budou osobní údaje uloženy a bodle jakého měřítka budou skartovány

[40] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 60.
[41] Tamtéž, recitál 61.
[42] Tamtéž, recitál 62.

- Zda je právní nárok na opravu nebo výmaz osobních údajů nebo jejich omezení při zpracování a právo vznést námitku proti tomuto zpracování
- Zda legislativa umožňuje podat stížnost u dozorového úřadu
- Pokud údaje nejsou získány od subjektu údajů přímo, jaké jsou veškeré dostupné informace o zdroji
- Jestli dochází automatizovanému rozhodování, včetně profilování[43]

Právo na přístup k osobním údajům může subjekt údajů uplatnit kdykoliv během zpracování dotčených osobních údajů, ale i v případě, že jeho údaje zpracovávány nejsou. Forma žádosti v Obecném nařízení není stanovena. Tudíž může mít jak písemnou, tak ústní formu a lze ji uplatnit i na dálku prostřednictvím e-mailu, telefonu nebo i jinou formou. Vždy musí dojít k přesné identifikaci žadatele a jeho ztotožnění se subjektem údajů.[44]

Správce žádost musí zpracovat do jednoho měsíce po obdržení žádosti a případě velkého množství žádostí nebo ve složitějších případech může být tato lhůta prodloužena o další dva měsíce. Vždy musí správce žadatele informovat o prodloužení lhůty a z jakého důvodu k tomuto prodloužení došlo.[45]

3.4.3 **Právo na opravu**

V případě, že o subjektu údajů jsou evidovány nepřesné osobní údaje, má právo na opravu. V kontextu účelu zpracování má subjekt údajů právo na doplnění osobních údajů, a to i poskytnutím dodatečného prohlášení. Správce tak musí učinit bez zbytečného odkladu. Sám správce nemá povinnost aktivně vyhledávat nepřesné osobní údaje o subjektu údajů, ani požadovat každoroční aktualizaci těchto údajů.[46]

3.4.4 **Právo na výmaz**

Podle článku 17 Obecného nařízení má subjekt údajů právo, „… *aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce*

[43] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 15.
[44] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 67.
[45] Tamtéž, s. 70
[46] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 71-72.

má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů":[47]

- Pro původní účely již nejsou potřebné
- Došlo k odvolání souhlasu, na jehož základě byly údaje zpracovány, a není existence právního důvodu pro další zpracování
- Subjekt údajů podá námitku proti zpracování
- Došlo k protiprávnímu zpracování osobních údajů
- Pokud příslušný orgán rozhodl o vymazání osobních údajů
- Pokud došlo ke shromažďování v souvislosti s nabídkou služeb a zboží[48]

Existují výjimky z povinnosti výmazu, a to při realizaci práva na svobodu projevu a informace, při výkonu veřejné moci, z důvodu veřejného zajmu v oblasti veřejného zdraví, pro účely archivace ve veřejném zájmu, vědeckého či historického výzkumu, pro statistické účely a pro určení, výkon nebo obhajobu právních nároků.[49]

3.4.5 **Právo na omezení zpracování**

Právo na omezení zpracování dává subjektu údajů možnost, aby správce v případě, že subjekt neuznává přesnost osobních údajů nebo podal námitku proti zpracování či zpracování není legitimní a subjekt údajů odmítá výmaz, došlo k omezení zpracování. To samé platí v případě, že pro účely zpracování správce osobní údaje již nepotřebuje, ale subjekt údajů tyto údaje chce využít pro určení, výkon nebo obhajobu právních nároků. Pokud dojde k omezení zpracování osobních údajů, k jejich znovu zpracování je potřeba souhlas subjektu údajů.[50]

3.4.6 **Právo na přenositelnost údajů**

Pokud je zpracování osobních údajů založeno na souhlasu nebo smlouvě, anebo se provádí automatizovaně můžou být tyto údaje předány jinému správci. Tyto údaje musí být

[47] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 17.
[48] Tamtéž, čl. 17.
[49] Navrátil, J. a a kol. *GDPR pro praxi.* Plzeň : Aleš Čermák, 2018, s. 119.
[50] Tamtéž, s. 120.

ve strukturovaném, běžně požívaném a strojově čitelném formátu. Povinností správce není používat systémy zpracování, které jsou kompatibilní s jinými organizacemi.[51]

Právem na přenositelnost údajů nesmí být negativně dotčena práva a svobody jiných osob. Správce musí zvážit, jestli nedošlo poškození práv jiné osoby zejména v případě, že se osobní údaje týkají více než jedné osoby. Bez souhlasu všech subjektů nesmí dojít k sdílení údajů. [52]

3.4.7 **Právo vznést námitku**

Obecné nařízení podle článku 21 dává právo subjektu údajů vznést námitku proti zpracování osobních údajů, které se jej týkají, a to včetně profilování. Správce může údaje dále zpracovávat v případě existence oprávněných důvodů pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků. Námitku může subjekt údajů vznést v souvislosti se zpracováním nutným pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, za účelem přímého marketingu, včetně profilování a pro účely vědeckého, historického výzkumu a statistiky. Správce je povinen pozastavit zpracování osobních údajů, jestliže neprokáže oprávněné důvody pro zpracování.[53]

3.4.8 **Právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování**

V základních pojmech Obecného nařízení v článku 4 je definováno profilování jako *„jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k* rozboru *nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu“*[54]

[51] Navrátil, J. a a kol. *GDPR pro praxi.* Plzeň : Aleš Čermák, 2018, s. 90.
[52] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 90.
[53] Tamtéž, s. 91
[54] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4.

Právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování má subjekt údajů za podmínky, že se ho to právním způsobem dotýká. Právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování nelze uplatnit kdy se jedná o rozhodnutí potřebné k uzavření nebo plnění smlouvy mezi subjekty údajů a správcem údajů, povoleno právem Evropské unie, které se vztahuje na správce a které vymezuje vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů; nebo založeno na výslovném souhlasu subjektu údajů. Jestliže dojde k odmítnutí automatizovaného zpracování správce realizuje vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí.[55]

3.4.9 **Právo podat stížnost u dozorového úřadu**

Každý subjekt údajů, aniž jsou dotčeny jeho jakékoliv legitimní prostředky ochrany, má právo podat stížnost u dozorového úřadu, jestliže se domnívá, že zpracováním jeho osobních údajů je porušeno Obecné nařízení. Stížnost může podat u některého dozorového úřadu, zejména v členském státě svého obvyklého bydliště, místa výkonu zaměstnání nebo místa, kde došlo k údajnému porušení. Dozorovým úřadem v České republice je Úřad pro ochranu osobních údajů.[56]

Pokud subjekt údajů předpokládá, že došlo k poškození jeho práv v souvislosti s Obecným nařízením, nemusí stížnost u dozorového úřadu podat sám, ale může pověřit podání stížnosti, konkrétní neziskový subjekt, organizaci nebo sdružení, které jsou zřízeny v souladu s právem členského státu, jejichž statutární cíle jsou ve veřejném zájmu a které působí v oblasti ochrany osobních údajů. Neziskový subjekt, organizace nebo sdružení nesmí bez souhlasu subjektu údajů požadovat náhradu škody.[57]

[55] Navrátil, J. a a kol. *GDPR pro praxi.* Plzeň : Aleš Čermák, 2018, s.122.
[56] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 99.
[57] Janečková, E. *GDPR. Praktická příručka implementace.* Praha : Wolters Kluwer ČR, 2018, s. 99.

3.5 Souhlas se zpracováním osobních údajů

Obecné nařízení definuje souhlas jako*: „ … jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“*[58]

3.5.1 Souhlas

Souhlas se zpracováním osobních údajů je nejpodstatnější segment úkonů v rámci Obecného nařízení. Správce odpovídá, že souhlas bude splňovat následující kritéria, a to že bude svobodný, konkrétní, informovaný a jednoznačným projevem vůle.[59]

Svoboda souhlasu označuje skutečnou volbu subjektu údajů mezi přijetím nebo odmítnutím podmínek souhlasu zpracování osobních údajů. V případě orgánů veřejné moci, kdy Obecné nařízení předpokládá jistou nerovnováhu mezi dvěma subjekty, je nepravděpodobné, že za všech okolností této konkrétní situace bude souhlas udělen svobodně.[60]

Přesnou specifikací účelu zpracování je naplněna podmínka konkrétnosti, ale i ta nemusí být vyžadována. „*Například e-shop, který potřebuje od zákazníka jeho adresu, nemusí uvádět, že adresa bude použita za účelem dodání zboží zákazníkovi. To lze zahrnout pod obecné zpracování osobních údajů za účelem plnění smlouvy.“* Je k tomu potřebný souhlas se založením zákazníkova účtu a informování zákazníka, že data budou použita k plnění jeho objednávek.[61]

V případě udělení souhlasu formou písemného prohlášení, který se týká rovněž jiných skutečností, dle Obecného nařízení, musí být souhlas jasně od těchto skutečností odlišitelný. Musí jasně prokazatelné, že subjekt údajů si je vědom toho, že dává souhlas a v jakém rozsahu.[62]

Subjekt údajů musí být dostatečně informován o účelu zpracování, pro který je souhlas udělen. Správce je povinen podat jasné informace o existenci prováděných operací

[58] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4.
[59] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 131.
[60] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 104.
[61] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s.130.
[62] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 42.

zpracování a jejich účelech, které korespondují se zásadou spravedlivého a transparentního zpracování.[63]

Ke správné informovanosti subjektu údajů je kromě informacích o účelu zpracování, typu údajů, které budou shromažďovány a používány doplnit údaje o správci, existenci práv souhlas odvolat a o možných rizicích předávání údajů.[64]

Jednoznačným potvrzením v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení dává subjektu údajů souhlas ke zpracování osobních údajů. Souhlas lze dát pouze aktivním jednáním subjektu údajů, a to například zaškrtnutím políčka při návštěvě internetové stránky s navrhovaným zpracováním jeho osobních údajů. Mlčení nebo nečinnost nejsou považovány za souhlas.[65]

3.5.2 **Odvolání souhlasu**

Subjekt údajů může kdykoliv svůj souhlas se zpracováním osobních údajů odvolat. V Obecném nařízení se uvádí, že odvolání souhlasu se zpracováním musí být stejně snadné jako jej poskytnout. Správce se musí přesvědčit ve shodě s Obecným nařízením, jestli existují i jiné důvody, na jejichž základě může ve zpracování pokračovat. V opačném případě musí na základě odvolání souhlasu subjektu údajů pozastavit další zpracování.[66]

Veškeré operace zpracování osobních údajů, které proběhly před odvoláním souhlasu zůstávají legitimní, ale správce musí pozastavit veškeré dotčené zpracovatelské činnosti. Správce musí tyto data buď smazat nebo anonymizovat, jestliže neexistují právní důvody pro jejich další zpracování.[67]

3.5.3 **Zpracování osobních údajů bez udělení souhlasu**

Zpracování osobních údajů je možné i bez souhlasu se zpracováním. Nejčastějším důvodem je zpracování nezbytné k plnění uzavřené smlouvy, pokud je subjekt údajů účastníkem. A to za předpokladu, že se tak děje na žádost subjektu údajů. Náleží jsem

[63] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 130.
[64] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 107.
[65] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 32.
[66] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 131.
[67] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 106.

shromažďování základních informací o subjektu údajů před vytvořením nebo splněním požadavků smlouvy. Údaje, které nesplňují účel smlouvy do zpracování nelze začlenit.[68]

Pokud zpracování správci ukládá zákon, tak i v tomto případě proběhne zpracování bez souhlasu. Je vždy nutné tuto právní normu zkontrolovat a shromažďovat jen nejnutnější objem dat. Tato situace se týká například bank, ve spojení legislativní normou proti praní špinavých peněz.[69]

Orgány veřejné správy při zpracování, které je nezbytné pro účel prováděný ve veřejném zájmu nebo při výkonu veřejné moci pověřené správcem, není souhlas nezbytný. Stejná podmínka platí při zpracování osobních údajů za účelem ochrany veřejného zájmu.[70]

3.6 Role a odpovědnost v rámci GDPR

Obecné nařízení klade důraz na odpovědnost a povinnosti správce i zpracovatele při výkonu práv subjektu údajů.[71]

3.6.1 Správce

Obecné nařízení správce definuje jako fyzickou nebo právnickou osobu, orgán veřejné moci, agenturu nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Jsou-li účely a prostředky tohoto zpracování určeny legislativní normou Evropské unie nebo jejích členských států, je možné určit správce nebo zvláštní kritéria pro jeho určení dané právem jednotlivých států nebo Evropské unie.[72]

V pravomocích správce je rozhodnout, které osobní údaje a kým budou shromažďovány, po jakou dobu budou údaje uchovávány, o nutnosti souhlasu a informovanosti subjektu údajů, o možné míře rizika pro subjekt údajů a tím i o ochraně dat a v prvé řadě o účelu zpracování těchto dat.[73]

[68] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 131.
[69] Tamtéž, s. 131.
[70] Tamtéž, s. 132.
[71] Tamtéž, s. 150.
[72] Novák, D. *Zákon o ochraněosobních údajů a předpisy související. Komentář.* Praha : Wolters Kluwer, 2014. s.114.
[73] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 150.

Odpovědností správce je dodržování povinností plynoucích z Obecného nařízení a respektování zásad zpracování osobních údajů. Správce musí být schopen tento soulad s Obecným nařízením doložit.[74]

V případě společného zpracování dvou a více správců, ještě před započetím zpracování musí dojít k určení, a to transparentním způsobem, podílů na odpovědnosti a povinnostmi mezi těmito správci.[75]

Při zpracování osobních údajů správce musí dodržovat tyto zásady:

- Zásada férového a zákonného zpracování
- Zásada omezení účelem
- Zásada minimality
- Zásada kvality údajů
- Zásada přístupu subjektu údajů k informacím včetně práva na opravu osobních údajů
- Zásada obecného zpřístupnění údajů
- Zásada bezpečnosti a odpovědnosti[76]

3.6.2 **Zpracovatel**

Zpracovatelem dle článku 4 odstavce 8 Obecného nařízení je jakýkoliv fyzická nebo právnická osoba, orgán veřejné moci nebo agentura či jiný subjekt, který pro správce zpracovává nebo má přístup k osobním údajům, které jsou správcem shromažďovány.[77]

V souladu s požadavky Obecného nařízení při provádění zpracování zpracovatelem, kterého pověřil správce, musí správce akreditovat pouze takového zpracovatele, který poskytne dostatečné záruky, zejména pokud jde o odborné znalosti, spolehlivost a zdroje, že zavede opatření, technického a organizačního charakteru, která budou splňovat požadavky tohoto nařízení, včetně požadavků na bezpečnost zpracování. Tato povinnost správce by se měla prokázat dodržováním schváleného kodexu chování nebo schváleného mechanismu pro vydávání osvědčení zpracovatelem. Pokud zmocnění zpracovatele nevyplývá přímo

[74] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 124.
[75] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 151.
[76] Novák, D. *Zákon o ochraněosobních údajů a předpisy související. Komentář.* Praha : Wolters Kluwer, 2014. s.139-151.
[77] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 151.

z právního předpisu, musí být mezi správcem a zpracovatelem uzavřena písemná smlouva ve které bude stanoven předmět a doba trvání zpracování, povaha a účely zpracování, typ osobních údajů a kategorie subjektů údajů, s přihlédnutím ke konkrétním úkolům a povinnosti zpracovatele v souvislosti se zpracováním, jež má být provedeno, a riziko pro práva a svobody subjektů údajů. Po dokončení zpracování jménem správce by zpracovatel měl na základě rozhodnutí správce osobní údaje vrátit nebo vymazat, jestliže se nepožaduje uložení osobních údajů podle práva Evropské unie nebo členského státu, které se na zpracovatele vztahuje.[78]

3.6.3 **Pověřenec pro ochranu osobních údajů**

Pověřence pro ochranu osobních údajů jmenuje buď správce nebo zpracovatel eventuelně ho jmenují oba. Obecné nařízení ukládá povinnost jmenovat pověřence vždy když zpracování je prováděno orgánem veřejné moci nebo veřejným subjektem. Výjimkou jsou soudy jednající v rámci svých soudních pravomocí. Další situace, která vyžaduje jmenování pověřence vzniká, pokud hlavní činností správce nebo zpracovatele spočívají ve zpracování, které má požadavky na rozsáhlé, pravidelné a systematické sledování subjektu údajů. Za podmínky spočívající v rozsáhlém zpracování zvláštní kategorie údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů je povinné pro správce nebo zpracovatele pověřence jmenovat.[79]

Jmenování pověřence ochrany osobních údajů dle souladu s Obecným nařízením musí být na základě jeho profesních kvalit, odborných znalostí legislativy v oblasti ochrany osobních údajů a schopností vykonávat povinnosti stanovené v Obecném nařízení. Jeho profesní kvalifikace se musí týkat informační bezpečnosti, odbornou znalostí problematiky vztahující se činnosti dané organizace, zkušenosti s implementací, s analýzou rizik a způsobem zpracování osobních dat klientů. Pověřenec musí chápat kontext s procesy organizace, jejímu záměru, a to vše v souvislosti s GDPR.[80]

---

[78] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 81.

[79] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 157.

[80] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2018, s. 165-166.

Recitál 39 Obecného nařízení udává, které úkoly spadají do povinností pověřence. Úkolem pověřence je všem účastníkům zpracování poskytnout informace a odborné poradenství vyplývajícím z ochrany osobních údajů včetně jejich povinností. Dalším úkolem pověřence je dohlížení na dodržováním souladu s tímto nařízením a dalšími předpisy Unie nebo členských států a s koncepcí správce a zpracovatele z hlediska ochrany osobních údajů, včetně rozdělení odpovědnosti. Pověřenec musí být schopen prokázat, že procesy v organizaci jsou ve shodě s požadavky Obecného nařízení, a to jak v teoretické rovině, tak v běžném uplatňování těchto procesů. Za dokumentaci a její bezpečné uchovávání zodpovídá pověřenec. Pomocí této dokumentace organizace stvrzuje účinnost svých opatření a funkčnost systému. Mezi povinnosti pověřence se řadí i poskytování poradenství na požádání, a to hlavně z důvodu posouzení účinku na ochranu osobních údajů a analýzy rizik. Zajišťuje přímý kontakt s dozorovým úřadem, jakožto s kontrolním orgánem, se kterým spolupracuje.[81]

Pověřenec pro ochranu osobních údajů při plnění svých úkolů a povinností je vázán tajemstvím nebo důvěrností, v souladu s právem Unie nebo členského státu a správce nebo zpracovatel musí zajistit, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.[82]

3.7 **Dozorový úřad**

Jednotlivé členské země si stanoví jeden nebo více nezávislých orgánů veřejné moci, kteří budou pověřeny kontrolou plnění povinností vyplývající z Obecného nařízení z důvodu chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie. Legislativou jednotlivých členských států se upravují základní podmínky zřízení dozorového úřadu, jeho kvalifikace, způsobilosti, jmenování členů atd. V České republice je dozorovým úřadem Úřad pro ochranu osobních údajů a jeho záležitosti upravuje zákon č. 110/2019 Sb., o zpracování osobních údajů.[83]

[81] Tamtéž, s.167.
[82] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 39.
[83] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 149.

3.7.1 **Historie**

Jako nezávislý správní orgán byl 1. června 2000 zřízen Úřad pro ochranu osobních údajů. V září 2000 návrhem Senátu a jmenováním prezidentem České republiky stal RNDr. Karel Neuwirt jeho prvním předsedou. Postupně se úřad začal ujímat úkolů, které mu stanovil zákon č. 101/2000 Sb., o ochraně osobních údajů. Mezi tyto povinnosti náleží vedení registru, plnění požadavků vyplývajících z mezinárodních smluv, vyřizování stížností na porušení zákona, poskytování konzultací a osvětová činnost. V témže roce mu přibyla další povinnost, a to udělování a odebírat akreditace na základě zákona o elektronickém podpisu. Tu to povinnost převzalo v roce 2004 tehdejší Ministerstvo informatiky ČR. V průběhu času se kompetence úřadu rozšiřují. K těm nejpodstatnějším lze zařadit dozor nad oblastí šíření obchodních sdělení na základě zákona o některých službách informační společnosti. [84]

V roce 2006 došlo k nejvýznamnější osvětové činnosti. Sérií seminářů v rámci tříletého vzdělávacího projektu Ochrana osobních údajů ve vzdělání, který byl akreditován Ministerstvem školství, mládeže a tělovýchovy, úspěšně prošlo 211 pedagogů z celé České republiky. Ve stejném roce byla Úřadu pro ochranu osobních údajů svěřena v rámci přípravy na vstup České republiky do Schengenského informačního systému činnost k vytvoření podmínek, které požadovala z hlediska ochrany osobních údajů evropská evaluační komise. V dubnu 2010 se v Praze konala konference evropských komisařů ochrany dat a soukromí. N a této konferenci byla přijata Rezoluce k problematice dalšího vývoje v oblasti ochrany osobních údajů a soukromí. Dle této rezoluce je zejména nezbytné:

- *„trvat na úrovni národní i v EU na jasném stanovení, kdo nese odpovědnost za zpracování a ochranu osobních údajů. Dále trvat na tom, že souhlas subjektu údajů je jedním ze základních předpokladů zákonného zpracování dat, a dále trvat na přísných, zákonem stanovených ochranných opatřeních pro druhotné využívání osobních údajů. A také usilovat o to, aby rozsah veškerých byrokratických opatření souvisejících s ochranou osobních údajů zůstal omezený;*
- *vyžadovat, aby před přijetím nových zákonných opatření nebo nasazením nových informačních technologií byl vzat v úvahu koncept „privacy by design“ nebo, v případě nutnosti, bylo provedeno náležité a prokazatelné posouzení dopadů*

[84] Historie. Úřad pro ochranu osobních údajů [online]. [cit. 19.2.2022]. https://www.uoou.cz/historie/ds-1061/archiv=0.

v takové míře, aby případné narušení soukromí nepřevážilo nad zamýšlenou účinností chystaného právního opatření nebo informační technologie;

- *usilovat na národní i evropské úrovni o vytvoření úplné soustavy pravidel pro ochranu osobních údajů ve všech oblastech (včetně boje proti zločinu a terorismu);*
- *usilovat o přijetí celosvětových závazných standardů ochrany osobních údajů založených na mezinárodních standardech vypracovaných v roce 2009 na Konferenci o ochraně dat v Madridu a dále také podporovat úsilí Rady Evropy prosadit přistoupení zemí třetího světa k Úmluvě 108 a jejímu dodatkovému protokolu.“*[85]

S nástupem platnosti Obecného nařízení, které nahradilo dřívější poradní orgán – pracovní skupinu WP29, zřídil úřad na svých webových stránkách rubriku, kde jsou aktuální relevantní informace k dané problematice. [86]

V následujících letech Úřad pro ochranu osobních údajů uspořádal velké množství seminářů, školení, konferencí a přednášek, jako například s Právnickou fakultou

Univerzity Karlovy mezinárodní konferenci Právo na informační sebeurčení.[87]

V roce 2020 dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím přibyla úřadu další nová agenda, v rámci, které se na úřad obrací klienti s žádostí o sdělení informací. [88]

Současným předsedou Úřadu pro ochranu osobních údajů je Mgr. Jiří Kaucký, kterého jmenoval do funkce na návrh Senátu prezident republiky Miloš Zeman. [89]

3.7.2 **Úkoly dozorového úřadu**

K hlavním činnostem dozorového úřadu dle zákona č. 110/2019 Sb., o zpracování osobních údajů:

„a) provádí dozor nad dodržováním povinností stanovených zákonem při zpracování osobních údajů,

[85] Rezoluce k problematice dalšího vývoje v oblasti ochrany osobních údajů a soukromí. Úřad pro ochranu osobních údajů [online]. [cit. 19. 2. 2022]. https://www.uoou.cz/rezoluce-k-problematice-dalsiho-vyvoje-v-oblasti-ochrany-osobnich-udaju-a-soukromi/ds-1695/archiv=0&p1=1659
[86] Historie. Úřad pro ochranu osobních údajů [online]. [cit. 19.2.2022]. https://www.uoou.cz/historie/ds-1061/archiv=0.
[87] Tamtéž
[88] Tamtéž
[89] Tamtéž

b) ověřuje zákonnost zpracování osobních údajů na podnět subjektu údajů podle § 31,

c) přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování osobních údajů a informuje o jejich vyřízení,

d) projednává přestupky a ukládá pokuty,

e) poskytuje konzultace v oblasti ochrany osobních údajů,

f) informuje veřejnost o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním osobních údajů,

g) informuje správce a zpracovatele o jejich povinnostech v oblasti ochrany osobních údajů a

h) vykonává další působnost stanovenou mu zákonem.“[90]

Dle zákona o zpracování osobních údajů je Úřad pro ochranu osobních údajů centrální dozorový úřad pro ochranu osobních údajů. A jeho činnost spočívá zejména v monitorování, zvyšování povědomí, vymáhání a kontrole uplatňování obecného nařízení a dalších předpisů upravujících některé otázky ochrany osobních údajů. [91]

Zástupcům odborných, profesních a průmyslových sdružení poskytuje poradenství v oblasti ochrany osobních údajů. Konzultace je poskytována správcům ale i osobám, které mají podezření, že jejich zpracování osobních údajů je v rozporu s legislativou. Některé výstupy z konzultací jsou zveřejněny na webových stránkách úřadu, pro jejich využití dalšími zpracovateli. Úřad uděluje konzultace i Parlamentu ČR, vládě a dalším orgánům a institucím, zejména v souvislosti s legislativou.[92]

Podle správního a kontrolního řádu vykonává úřad kontrolní a správní činnost, a to hlavně přijímání a vyřizování stížností, řešením úkolů, které vedou ke zkvalitnění a prohloubení ochrany osobních údajů nejen v celé Evropské unii, ale i v mikrosvětě jednotlivých správců.[93]

[90] Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 110, § 54.
[91] Role Úřadu pro ochranu osobních údajů. Úřad pro ochranu osobních údajů [online]. [cit. 19. 2. 2022]. https://www.uoou.cz/role-uoou/ds-4726
[92] Tamtéž
[93] Role Úřadu pro ochranu osobních údajů. Úřad pro ochranu osobních údajů [online]. [cit. 19. 2. 2022]. https://www.uoou.cz/role-uoou/ds-4726

3.7.3 **Pravomoci dozorového úřadu**

V rámci Obecného nařízení pro dozorový úřad určujeme tři okruhy pravomocí. A to vyšetřovací pravomoci, nápravné pravomoci a povolovací a poradní pravomoci.[94]

Vyšetřovací pravomoci Úřadu pro ochranu osobních údajů umožnuje nařídit správci a zpracovateli, aby došlo k poskytnutí veškerých informací a přístupů k osobním údajům, které potřebují k plnění svých úkolů, provádět audit ochrany údajů, přezkoumávat osvědčení, získat přístup do všech prostor, kde správce a zpracovatel působí.[95]

Nápravné pravomoci úřad využívá k upozornění správce nebo zpracovatele, že zpracováním může dojít k porušení nařízení, udělit napomenutí nebo správní pokutu, pokud již k porušení došlo. Tato pravomoc opravňuje nařídit správci či zpracovateli vyhovění žádostem subjektu údajů o výkon jejich práv, uvedení zpracování do souladu s Obecným nařízením, nařídit opravu nebo výmaz osobních údajů a umožňuje mu odebrat osvědčení. [96]

Mezi povolovací a poradní pravomoci náleží vydávat stanoviska určená Parlamentu ČR, vládě a dalším orgánům a institucím, zejména v souvislosti s legislativou ohledně ochrany osobních údajů, vydávat stanoviska ohledně kodexu chování, vydávat osvědčení a akreditace, povolovat a přehmat smluvní doložky o ochraně údajů a schvalovat závazná podniková pravidla. [97]

[94] Janečková, E. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, 2019, s. 151-152.
[95] Tamtéž, s. 151.
[96] Tamtéž, s. 151-152.
[97] Tamtéž, s. 152.

4 Vlastní práce

4.1 Vymezení praktické části

Praktická část bude zaměřená na implementaci GDPR a problematických aspektů, které s tím souvisejí, ve státní správě, konkrétně v České správě sociálního zabezpečení (dále jen „ČSSZ“) Hradec Králové. Nejprve je třeba představit ČSSZ a její fungování. Následně bude vysvětlena činnost ČSSZ, tedy budou především nastíněna data, se kterými pracuje, jak tato data zpracovává apod. Následně práce předloží způsob zpracování osobních dat v ČSSZ Hradec Králové, tedy v spádových OSSZ Jičín, Trutnov, Náchod, Hradec Králové, Rychnov nad Kněžnou.

Dále praktická část zhodnotí anketní průzkum, který proběhl prostřednictvím dotazníků, které byly pracovníkům ČSSZ v uvedených OSSZ předány, jakým způsobem dochází k implementaci GDPR. Dojde k detekci problematických aspektů při implementaci GDPR v uvedených oblastech a pomocí GAP analýzy bude zjištěn rozdíl mezi požadovaným stavem a stavem současným.

4.1.1 ČSSZ jako součástí státní správy a její organizace

Aby bylo možné pochopit, s jakým osobními údaji ČSSZ, resp. její okresní pobočky pracují, je třeba nejprve vymezit postavení ČSSZ v rámci státní správy ČR a následně pojednat o struktuře a organizaci Okresních správ sociálního zabezpečení.

ČSSZ je správní institucí, která zabezpečuje spolu s Ministerstvem práce a sociálních věcí (dále jen „MPSV“) a dalšími institucemi sociální zabezpečení. ČSSZ a okresní správy sociálního zabezpečení jsou podle zákona správními úřady.

Organizační struktura:

- Ústřední ředitel ČSSZ
    - Ústředí ČSSZ
        - Organizační útvary přímo řízené ústředním ředitelem,
        - Sekce ekonomická,
        - Sekce provozní,
        - Sekce sociálního pojištění,
        - Sekce provádění důchodového pojištění,
        - Sekce informačních a komunikačních technologií,
    - Pracoviště ČSSZ,

- OSSZ (okresní správy sociálního zabezpečení)[98]

OSSZ se dále pro výkon svých povinností v oblasti sociálního zabezpečení dělí do jednotlivé odbory podle § 109 zákona č. 582/1991 Ab., o organizaci a provádění sociálního zabezpečení. V čele OSSZ stojí ředitel, kterého jmenuje a odvolání ústřední ředitel ČSSZ.

Odbory v rámci OSSZ jsou:

a) **Odbor sociálního pojištění**, který provádí koordinaci a usměrňování sociálního pojištění. Především rozhoduje ve věcech nemocenského pojištění zaměstnanců a současně připravuje podklady pro výplatu dávek. Současně zpracovává údaje o vzniku nebo zániku nemocenského pojištění a vede agendu pojištěnců, kteří jsou pracovně neschopní. Kromě toho zpracovává žádosti o dávky. Současně zpracovává vyjádření pro soudní exekutory. [99]

b) **Oddělení nemocenského pojištění** – zpracovává a provádí nemocenské pojištění zaměstnanců, a kromě toho poskytuje metodickou a instruktážní pomoc subjektům nemocenského pojištění. Zároveň rozhoduje ve věci pojistného, pokut, které jsou za porušení nebo nesplnění povinností ukládány. Současně zpracovává agendu související se vznikem, trváním a zánikem pojistného poměru.[100]

c) **Oddělení důchodového pojištění** – provádí a metodicky kontroluje provádění důchodového pojištění. Vede evidence subjektů pojištění. Vede soupisy a doklady dávek. Vyřizuje žádosti ohledně důchodového pojištění. [101]

d) **Oddělení OSVČ** – provádí důchodové a nemocenské pojištění osob samostatně výdělečně činných (dále jen „OSVČ“). Dále rozhoduje o dávkách nemocenského a důchodového pojištění a současně kontroluje dodržování termínů a měsíčního výměřovacího základu pro výši záloh. [102]

e) **Oddělení registru pojištěnců a registru zaměstnavatelů** – provádí kontrolu nemocenského pojištění zaměstnanců podle stanovených právnících předpisů. Jeho úkolem je sledovat povinné subjekty, zda dodržují zákonná pravidla s ohledem na pojištění zaměstnanců. Také vede registr pohledávek, o kterých rozhoduje. [103]

[98] Profil organizace. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/web/cz/profil-organizace
[99] Popis organizační struktury OSSZ. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/web/cz/popis-organizacni-struktury-ossz
[100] Tamtéž
[101] Tamtéž
[102] Tamtéž
[103] Tamtéž

f) **Odbor výběru pojistného v rámci územní působnosti příslušné OSSZ** – zodpovídá za koordinaci a usměrňování provádění sociálního pojištění. Současně sleduje dodržování platební povinnosti pojistných subjektů v sociálním zabezpečení. Současně je zodpovědný za přípravu podkladů pro rozhodnutí o povolení splátek pojistného a penále.[104]

g) **Oddělení účtárny pojistného a dávek** – dohlíží na dodržování platební povinnosti zaměstnavatelů v sociálním zabezpečení a vystavuje výkazy nedoplatků zaměstnavatelům. Kromě toho kontroluje a účtuje Přehledy o výši pojistného. [105]

h) **Oddělení vymáhání pojistného a provádění exekučních srážek** – sleduje a eviduje pohledávky OSSZ a současně o nich rozhoduje. Ve spolupráci s dalšími orgány vykonává působnost v oblasti pojištění nemocenského, důchodového atd. Současně podává návrhy na nařízení exekuce prováděné soudními exekutory a spolupracuje s peněžními ústavy.[106]

i) **Oddělené kontroly** – poskytuje metodické a instruktážní zastřešení kontrolovaných subjektů v oblasti zaměstnanosti, včetně povinností zaměstnavatelů, především pro účel systémů sociálního zabezpečení v oblasti sociálních dávek.[107]

j) **Oddělené lékařské posudkové služby** – plní úkoly OSSZ v oblasti posouzení zdravotního stavu a pracovní schopnosti fyzických osob. Současně toto oddělení rozhoduje o ukončení dočasné pracovní neschopnosti nebo potřeby ošetřování, a to v případě, že ji neukončí ošetřující lékař.[108]

k) **Oddělení vnitřní správy** – zajišťuje přípravu podkladů pro zadávání veřejných zakázek malého rozsahu, tedy veřejných zakázek mimo režim zákona. Připravuje a předkládá pracovišti ČSSZ požadavky na nákup materiálu, případně jiného drobného majetku. [109]

4.1.2 Zpracování osobních údajů v OSSZ v Královéhradeckém kraji

Zpracování osobních údajů se řídí Nařízením Evropského Parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, následně pak adaptační

[104] Popis organizační struktury OSSZ. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/web/cz/popis-organizacni-struktury-ossz
[105] Tamtéž
[106] Tamtéž
[107] Tamtéž
[108] Tamtéž
[109] Tamtéž

právní normou, tedy zákonem č. 110/2019 Sb., o zpracování osobních údajů. Dále také musí zaměstnanci postupovat podle interních aktů, mezi které je možné zařadit *Politiku ochrany osobních údajů v ČSSZ* a *Pokyny pro zpracování osobních údajů* a prováděcími metodickými instrukcemi. [110]

Politika ochrany osobních údajů je zpracovávána za účelem nastavení pravidel ochrany osobních údajů, které jsou v rámci ČSSZ, tedy konkrétně OSSZ zpracovávány. Hlavními cíli této politiky pak je:[111]

a) Stanovení způsobu ochrany osobních údajů v OSSZ tak, aby zaměstnanci postupovali v souladu s požadavky zákona č. 101/2000 Sb., o ochraně osobních údajů v platném znění, Nařízením Evropského Parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES a zákona č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění,
b) zajištění trvalé shody ochrany osobních údajů v celé ČSSZ,
c) uplatnění této Politiky především v oblasti ochrany osobních údajů, tedy jejich zpracování a předávání dalším subjektům dle zákonných norem,
d) určení odpovědnosti, a to především za:
    a. naplňování požadavků výše uvedených právních předpisů, tedy dodržování zákonných norem,
    b. registraci u Úřadu pro zpracování osobních údajů,
    c. určení vnitřních předpisů tak, aby osobní údaje byly zpracovávány v souladu se zákonnými normami a Politikou.

Politika je platná pro všechny zaměstnance ČSSZ, ale i pro externí pracovníky, kteří jsou zaměstnáni v ČSSZ například na základě dohod o pracovní činnosti apod. Politika dále vymezuje pojmy jako:

a) osobní údaje – informace, které mohou identifikovat konkrétní osobu,
b) zpracování – operace s osobními údaji nebo soubory, které obsahují osobní údaje,
c) evidence – soubor osobních údajů, který je přístupný podle zvláštních kritérií.

Hlavním principem pro zpracování osobních údajů dle Politiky ČSSZ je znalost charakteristiky a účelu zpracování osobních údajů, tedy jedná se o informace, které jsou

[110] *Politika ochrany osobních údajů* (2019). Česká správa sociální zabezpečení (interní dokument). *Pokyny pro zpracování osobních údajů* (2020). Česká správa sociální zabezpečení (interní dokument).
[111] *Politika ochrany osobních údajů* (2019). Česká správa sociální zabezpečení (interní dokument), s. 5.

důležité pro zajištění efektivní ochrany osobních údajů. Tyto informace pak musí být uvedeny v Záznamu o zpracování osobních údajů, které by měly být uloženy u vedoucího jednotlivých oddělení. [112]

Pokud jde o charakteristiku zpracování osobních údajů pak dle Politiky jsou:

a) osobní údaje a citlivé osobní údaje osob vedené v agendách a spisech,
b) osobní údaje zaměstnanců ČSSZ, které jsou nezbytné pro personální a mzdové potřeby jsou vedeny v souladu s právními předpisy.

ČSSZ má také pověřence pro ochranu osobních údajů, který při plnění svých úkolů bere ohled na riziko spojené se zpracováním osobních údajů a přihlíží také ke kontextu, povaze a rozsahu zpracování. Pověřenec současně poskytuje informace a poradenství správcům osobních údajů, stejně jako ostatním zaměstnancům, kteří se podílení na zpracování osobních údajů. Pověřenec dále monitoruje soulad s národní a evropskou legislativou a podporuje zvyšování povědomí a odborné přípravy pracovníků, kteří jsou zapojení do činností, které obsahují zpracování osobních údajů. Pověřenec také poskytuje poradenství manažerovi kybernetické bezpečnosti, a to především ve věcech posouzení vlivu na ochranu osobních údajů, analýzu rizik a jejich uplatňování a monitorování. Kromě toho zpracovává pravidelné hodnocení řízení ochrany osobních údajů pro Úřad pro ochranu osobních údajů.

Politika současně nastavuje opatření pro ochranu osobních údajů, které je možné rozdělit na opatření organizační a dále pak na opatření technická. Pokud jde o organizační opatření, jedná se především o taková opatření, která spočívají v pravidelném školení zaměstnanců v oblasti ochrany osobních údajů, dále pak v kontrole provádění zpracování osobních údajů dle zákonných norem a nastavení takových postupů, které zabezpečí, aby zpracování osobních údajů bylo v souladu s národními i evropskými normami.[113]

Kromě toho se dále vyhodnocují na ČSSZ rizika, mezi která patří například porušení vnitřních postupů a norem, která následně mohou mít za cíl poškození celého resortu ČSSZ. Proto, aby nedocházelo k rizikovým situacím zpracovává ČSSZ metodiky a pracovní postupy pro zaměstnance tak, aby bylo možné efektivně předcházet rizikovým situacím.[114]

Hlavními zásadami, kterými se zpracování údajů v ČSSZ řídí je zásada zákonnosti, zásada korektnosti a transparentnosti, zásada omezení účelu, zásada minimalizace údajů,

[112] *Politika ochrany osobních údajů* (2019). Česká správa sociální zabezpečení (interní dokument), s. 15.
[113] *Tamtéž*, s. 21.
[114] *Tamtéž*, s. 27.

zásada přesnosti, zásada omezení uložení, zásada integrity a důvěrnosti a zásada odpovědnosti. [115]

Zásada zákonnosti je obecně považována za nejdůležitější, neboť spočívá v dodržování české i evropské legislativy a spočívá v přístupu, že osobní údaje je možné zpracovávat pouze na základě zákonného důvodu. Zásada korektnosti a transparentnosti pak spočívá především ve skutečnosti, že správce v případě zpracování osobních údajů musí subjektu, jehož údaje jsou zpracovávány, sdělit účel zpracování a následně pak údaje nesmí být zpracovány v případě absence takového účelu.

Zásada omezení účelu spočívá ve skutečnosti, že údaje musí být shromažďovány pro určité, a to výslovně vyjádřené legitimní účely a nesmějí být zpracovávány takovým způsobem které těmto účelům neodpovídá. Zásada minimalizace údajů představuje povinnost zpracovat osobní údaje přiměřeně, relevantně a pouze v takovém rozsahu, který je nezbytně nutný pro účel zpracování. Zásada přesnosti vyjadřuje nutnost zpracovat osobní údaje v jednoznačné podobě a v případě potřeby aktualizované. Zásada omezení uložení stanoví, že osobní údaje by měly být uloženy ve formě, která umožní identifikaci subjektu údajů po dobu ne delší, než je nezbytně nutné pro účely, pro které jsou tyto údaje zpracovávány.

Zásada integrity a důvěrnosti spočívá v požadavky zabezpečit osobní údaje prostřednictvím vhodných technických prostředků nebo organizačních opatření tak, aby osobní údaje byly chráněny před neoprávněným nebo protiprávním zpracováním, případně před ztrátou nebo zneužitím. Zásada odpovědnosti pak propojuje všechny výše uvedené zásady zpracování osobních údajů a zavazuje správce osobních údajů, aby zvažovali a průběžně vyhodnocovali hrozby zneužití osobních údajů, ke kterým může během jednotlivých fází zpracování osobních údajů dojít.

Základní povinnosti zaměstnanců při vzniku událostí při nakládání s osobními údaji jsou následující:

a) Zaměstnanec, který se o události dozvěděl je povinen toto nahlásit. Zaměstnanec je povinen nahlásit i jen podezření na vznik takové události. Následně je pak nutné rozhodnout, zda se jedná o takovou událost, která je nutná nahlásit na Úřad pro ochranu osobních údajů, nebo může být vyřízena bez jeho informování.

[115] *Pokyny pro zpracování osobních údajů* (2020). Česká správa sociální zabezpečení (interní dokument).

b) V případě, že je nutné událost ohlásit na Úřad pro ochranu osobních údajů, je nutné uvést především popis události (jakým způsobem došlo k porušení postupů/pravidel apod.), kategorii osobních údajů, kterých se tato událost týkám jejich množství apod. Do informace pro Úřad pro ochranu osobních údajů je nutné uvést i jméno a kontakt na pověřence ČSSZ. Porušení pravidel zpracování osobních údajů ohlašuje na Úřad pro ochranu osobních údajů pověřenec.[116]

Do souvislosti se zpracováním osobních údajů je nutné dát také pravidla chování zaměstnanců, které je vymezeno jednak zákonem č. 234/2014 Sb., o státní službě, ale pro zaměstnance ČSSZ, resp. OSSZ i Služebním předpisem náměstka ministra vnitra pro státní službu ze dne 14. prosince 2015, kterým se stanoví pravidla etiky státních zaměstnanců.[117] Tento dokument je třeba zmínit především proto, že vymezuje obecně pravidla chování zaměstnanců ve státní službě, které je možné aplikovat i na shromažďování osobních údajů a nakládání s nimi, resp. jejich zpracování.

Hlavními zásadami tohoto předpisu je zásada zákonnosti, tedy, že zaměstnanec vykonává službu v souladu s ústavním pořádkem a zákony. To znamená, že již zde je stanoven obecný rámec povinnosti dodržování zákona č. 101/2000 Sb., o ochraně osobních údajů.

Na závěr nutné uvést, jaké typy osobních údajů jsou na ČSSZ zpracovávány. Podle dokumentu *Informace o zpracování osobních údajů* [118]jsou to následující údaje:

- Identifikační údaje,
- Adresní údaje,
- Kontaktní údaje,
- Údaje pro provádění nemocenského pojištění,
- Údaje pro provádění důchodového pojištění,
- Údaje pro provádění lékařské posudkové služby,
- Údaje o výběru pojistného,

[116] *Pokyny pro zpracování osobních údajů* (2020). Česká správa sociální zabezpečení (interní dokument), s. 12.
[117] Služební předpis náměstka ministra vnitra pro státní službu ze dne 14. prosince 2015, kterým se stanoví pravidla etiky státních zaměstnanců. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/documents/20143/99686/eticky_kodex_CSSZ_sluz.pdf/78cb9806-07e0-8a28-6321-60999ca2e0f2
[118] Informace o zpracování osobních údajů. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/documents/20143/227251/Informace+o+zpracov%C3%A1n%C3%AD+osobn%C3%ADch+%C3%BAdaj%C5%AF+-+interaktivn%C3%AD+let%C3%A1k.pdf/e14db7d5-16d4-1620-5414-4ef667d77d3b

- Údaje, evidované na základě požadavků práva Evropských společenství a podle mezinárodních smluv o sociálním zabezpečení,
- Majetkové a finanční údaje.[119]

Zvláštní kategorii pak ještě tvoří údaje jako jsou zdravotní stav a trestní záležitosti.[120]

4.2 Dotazníkové šetření

Dotazník byl vytvořen tak, aby bylo možné následně vyhodnotit, jak probíhá implementace ochrany osobních údajů a rizika spojená GDPR. První otázka se soustředí na identifikaci typu osobních údajů, s jakými pracovníci OSSZ pracují. Otázka č. je: 1. *S jakými typy OÚ (osobní údaje) pracujete? Prosím o uvedení konkrétních typů (jméno, rodné číslo atd.)*.

Další se soustředí na identifikaci právního důvodu, na jehož základě pracovníci shromažďují osobní údaje. Cílem této otázky je zjistit, zda pracovníci vědí, jaký tento právní důvod je a na dotázání ho mohou klientům zodpovědět. Další otázka se následně soustředí na typ zpracování osobních údajů, tedy jakým způsobem jsou osobní údaje zpracovány (automatizované/manuální).

Dále je cílem dotazníkového šetření zjistit, zda pracovníci OSSZ vedou záznamy o činnostech zpracování OÚ a jakým způsobem a současně jakým způsobem jsou subjekty, jejichž údaje jsou zpracovávány, informovány o účelu zpracování jejich údajů.

Další otázky se týkaly rizik při zpracování osobních údajů. Jakým způsobem je zabezpečen neoprávněný přístup k údajům. Dále je snahou zjistit, jestli nedochází k neoprávněnému zpracování údajů a zda jsou při zpracování využívány konkrétní přístupy jako je např. anonymizace nebo pseudonymizace a zda je užití těchto způsobů práce s osobními údaji časově nebo administrativně náročné. Další otázka se zaobírá, jakým způsobem se řeší neaktuální a nesprávné údaje. Poslední otázka se soustředí na znalosti postupu, jaký má OSSZ při událostech s osobními údaji.

[119] Informace o zpracování osobních údajů. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/documents/20143/227251/Informace+o+zpracov%C3%A1n%C3%AD+osobn%C3%ADch+%C3%BAdaj%C5%AF+-+interaktivn%C3%AD+let%C3%A1k.pdf/e14db7d5-16d4-1620-5414-4ef667d77d3b

[120] Tamtéž

4.2.1 **Sběr dat a vyhodnocení**

Poté, co byly dotazníky vytvořeny byly zaslány přes kontaktní emaily nacházející se na dostupných internetových zdrojích na jednotlivé pobočky OSSZ – tedy do Hradce Králové, Jičína, Rychnova nad Kněžnou a Trutnova. Z veřejně dostupných informací bylo zjištěno, že v ČSSZ v Hradci Králové pracovalo k březnu 2021 celkem 65 zaměstnanců,[121] v OSSZ v Rychnově nad Kněžnou k 1. březnu 2021 celkem 49 zaměstnanců [122] a v Trutnově ke dni 4. 3. 2021 celkem 70 zaměstnanců.[123] Pro obvod Jičín se tuto informaci nepodařilo zjistit. Nicméně je možné, alespoň řádově, odhadnout počet všech zaměstnanců v okresech Královéhradeckého kraje, kterých je kolem dvou set.

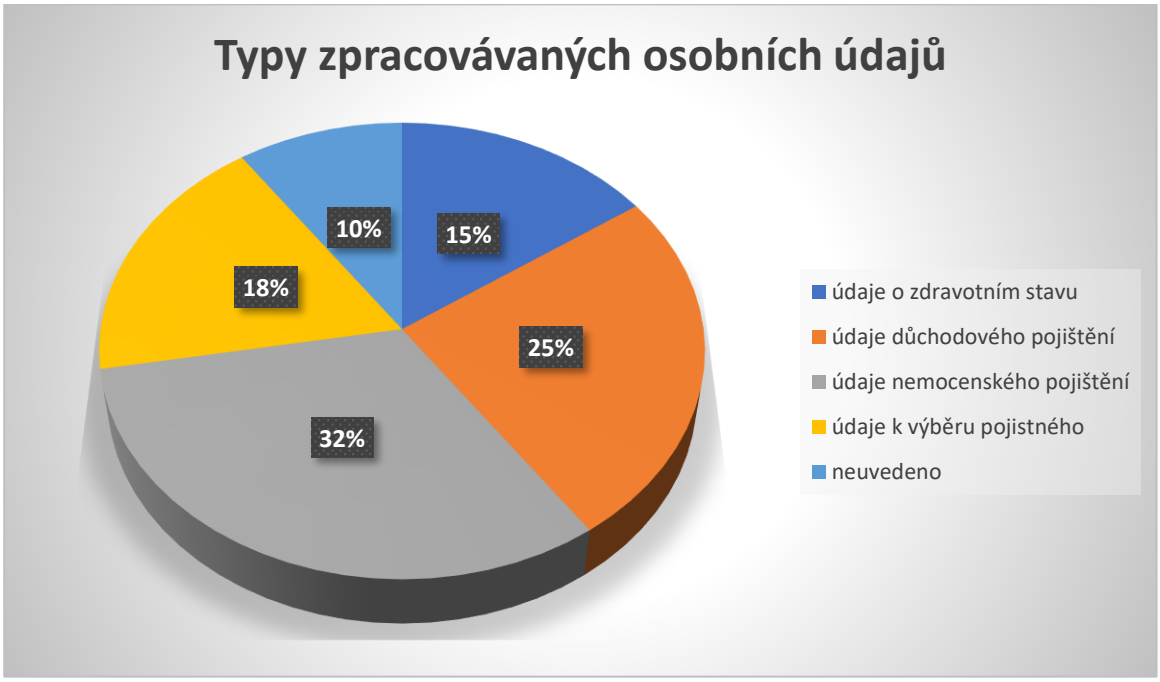
Vyplněných dotazníků se vrátilo zpět 72, tedy něco přes třicetšest procent. Pokud jde o jednotlivé dotazníku bylo zjištěno:

V případě typů zpracovaných údajů se na všech dotaznících objevily identifikační údaje (tedy jméno, příjmení, adresy apod.), nicméně další údaje, které jsou zpracovávány, se v dotaznících lišily, a to následujícím způsobem:

a) 11 respondentů uvedlo, že zpracovává zdravotní stav,
b) 18 respondentů uvedlo, že zpracovává údaje důchodového pojištění,
c) 23 respondentů uvedlo, že zpracovávají údaje nemocenského pojištění,
d) 13 respondentů uvedlo, že zpracovává údaje pro výběr pojistného,
e) 7 respondentů neuvedlo další specifické údaje.

[121] Žádost o poskytnutí informace. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/documents/20143/950750/%C3%9Ast%C5%99ed%C3%AD+%C4%8CSSZ.pdf/7fe6df6b-fafb-60a2-8fe3-426aff7cb491.
[122] Žádost o poskytnutí informace. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/documents/20143/950750/OSSZ+Rychnov+nad+Kn%C4%9B%C5%BEnou.pdf/80439ccc-f4d4-71c8-55c4-b94e77d7bf57
[123] Žádost o poskytnutí informace. Česká správa sociálního zabezpečení [online]. [cit. 28. 2. 2022]. https://www.cssz.cz/documents/20143/950750/OSSZ+Trutnov.pdf/0064f439-267a-900d-224b-4f5791e2ada5.

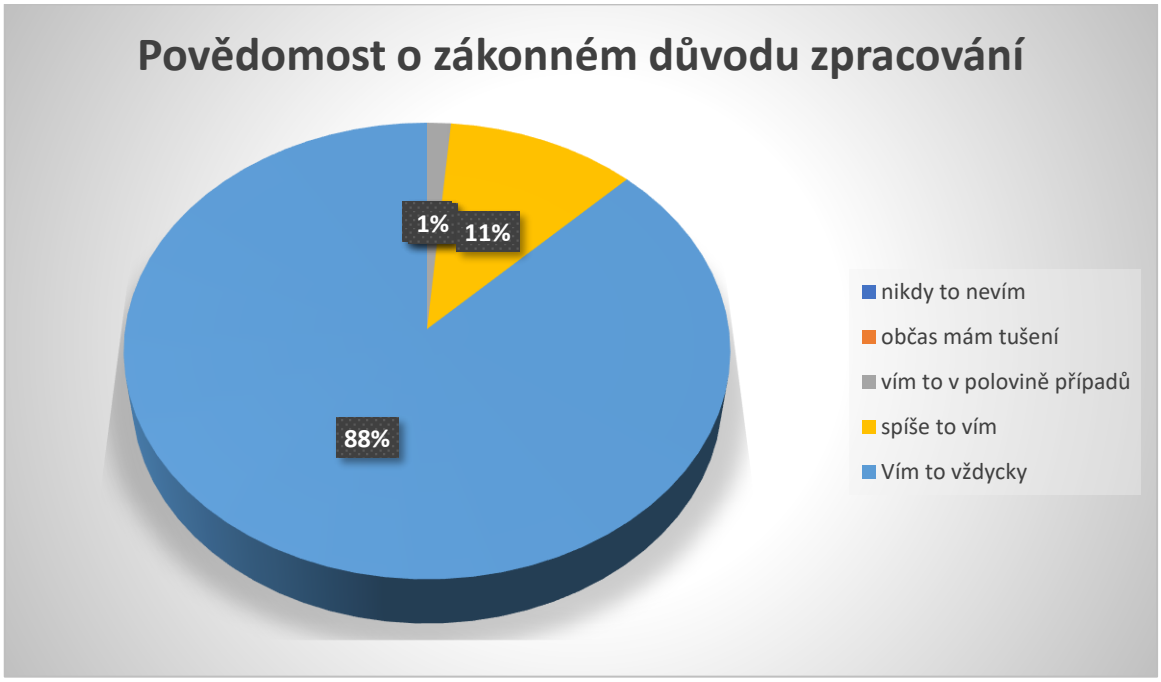
Obrázek 1: Graf č. 1 Typy zpracovávaných osobních údajů[124]



Ve druhé otázce byla pozornost zaměřena na zákonný důvod zpracování osobních údajů, kde bylo identifikováno, zda pracovníci OSSZ jsou si vědomi zákonného důvodu, z jakého data zpracovávají. Je třeba konstatovat, že výsledek tohoto šetření je velmi důležitý, protože z průzkumu vyplynulo, že 63 respondentů vždy zná zákonný důvod zpracování osobních údajů, 8 respondenti to většinou vědí a v jednom případě bylo uvedeno, že vím to v polovině případů. (graf č. 2).

[124] Vlastní výzkum, zpracování vlastní

Obrázek 2: Graf č. 2 Povědomost o zákonném důvodu zpracování[125]



Následující otázka byla zaměřena na skutečnost, zda zaměstnanci OSSZ zpracovávají osobní údaje manuálně (papírově, tedy např. prostřednictvím formulářů apod.) nebo automaticky (za použití výpočetní techniky). Jak vyplynulo z odpovědí, přestože to nebylo v možnostech uvedeno, 62 respondentů zaškrtlo obě možnosti, 6 potom pouze možnost automatickou 4 respondenti uvedli pouze manuální zpracování. Dá se tedy vyvodit, že způsob, jakým jsou údaje v OSSZ zpracovávány je především prostřednictvím výpočetní techniky, nicméně některé dílčí činnosti u konkrétních agent je stále prováděno manuálně.

[125] Vlastní výzkum, zpracování vlastní

Obrázek 3: Graf č. 3 Typy zpracování osobních údajů[126]

V případě záznamů o zpracování osobních údajů, byly pouze čtyři odpovědí kladné.

Obrázek 4: Graf č. 4 Vedení záznamů o činnostech zpracování OÚ[127]

[126] Vlastní výzkum, zpracování vlastní
[127] Vlastní výzkum, zpracování vlastní

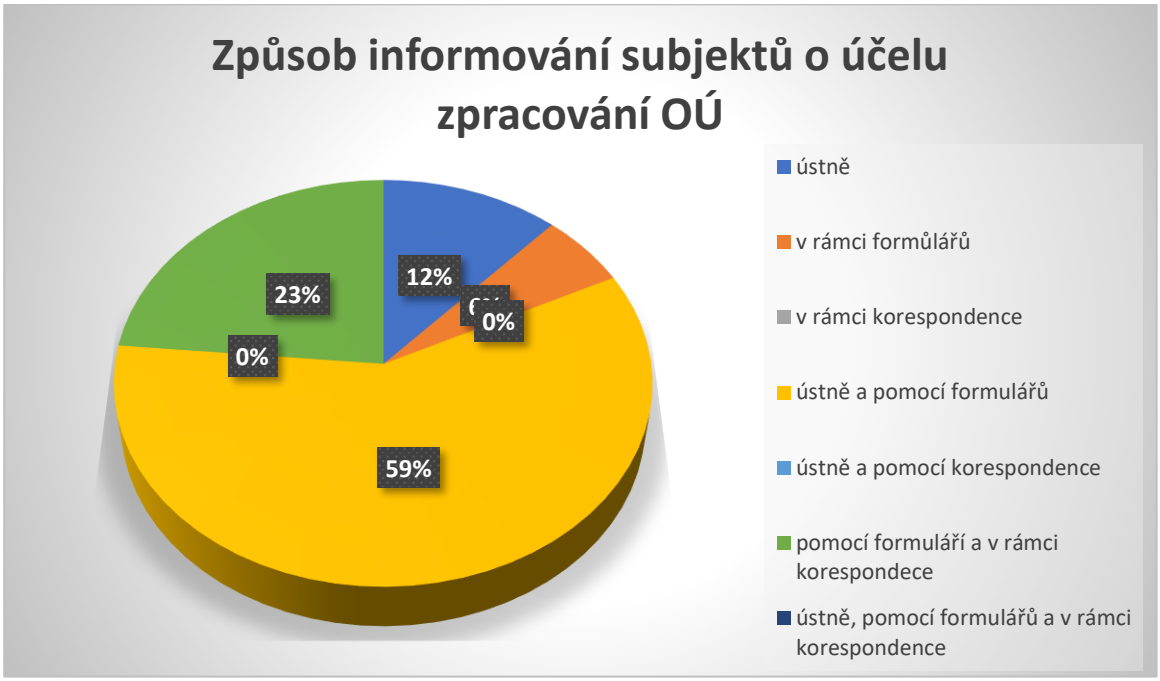
Další otázkou byla snaha zjistit, kdo konkrétně vede záznamy o činnostech zpracování OÚ, přičemž ve čtyřech případech se jednalo o respondenty, 12 respondentů uvedlo, že to nevědí a zbytek, tedy 54 respondentů uvedlo, že se jedná o vedoucího. Je tedy možné shrnout, že vedení záznamů o činnostech zpracování OÚ je svěřeno vedoucím oddělení nebo menších jednotek. Pokud jde o administrativní náročnost, V jedné bylo uvedeno, že „*administrativní a časová náročnost je značná a bylo by třeba výstupy, kterými jsou zpravidla zprávy včetně excelové tabulky, zkrátit*.“ I další tři respondenti uváděli, že vedení je hodně administrativně a časově náročné. Dá se tedy shrnout, že přestože došlo k určité koncentraci zodpovědnosti za vedení záznamů o činnostech zpracování OÚ, je otázkou, zda toto zpracování by nebylo vhodné určitým způsobem zjednodušit nebo zautomatizovat.

Šestá otázka soustředila pozornost na informování subjektů osobních údajů, kdy všechny shromážděné odpovědi bylo možné rozdělit do tří způsobu informování subjektů osobních údajů:

a. ústní sdělení
b. formulace o GDPR je přímo součástí formuláře, který subjekty OÚ vyplňují
c. formulace o GDPR je součásti korespondence se subjekty OÚ.

Většina respondentů využívala kombinaci všech výše uvedených způsobů. Zde se dá soudit, že plnění zákonné informační povinnosti není časově ani administrativně náročné.

Obrázek 5: Graf č.5 Způsob informování subjektů o účelu zpracování OÚ[128]



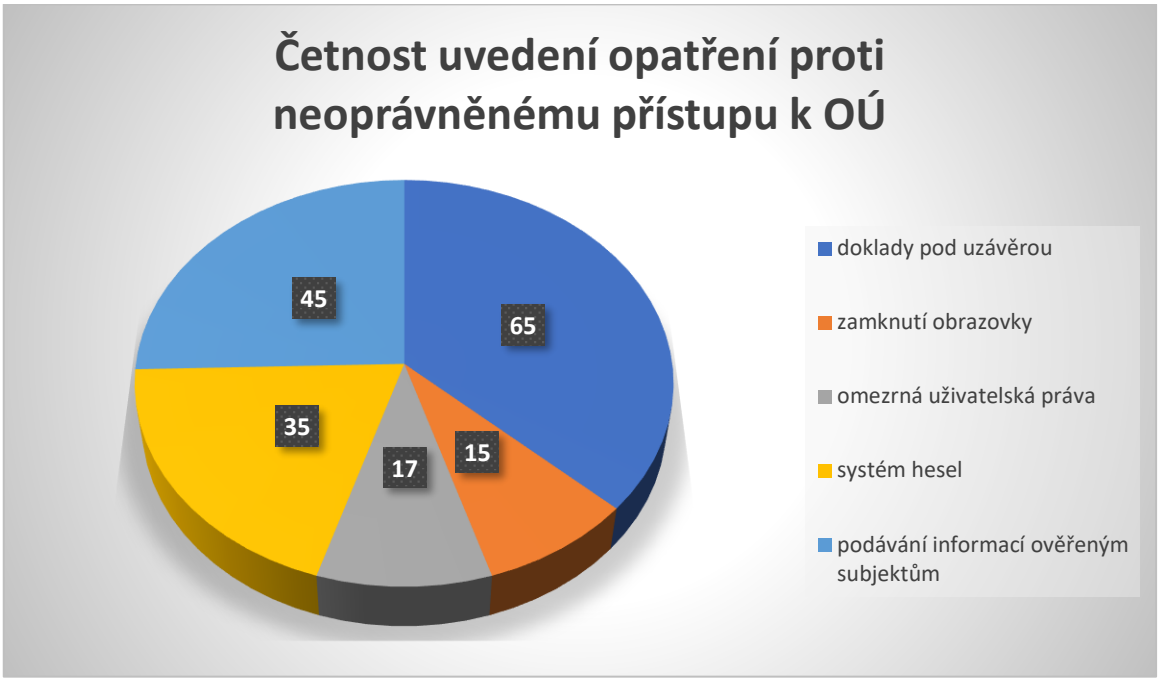
Další otázka byla zaměřena na opatření proti neoprávněnému přístupu k osobním údajům. Zde respondenti uváděli několik opatření, která jsou dána vnitřními předpisy organizace.

a. Veškeré doklady po ukončení zpracování musí být pod uzávěrou
b. Zamknutí obrazovky při odchodu od PC
c. Systém uživatelských práv omezující přístup k OÚ
d. Systém hesel
e. Podávání informací jen subjektům, kterých se to týká

V této otázce se ukázala dobrá povědomost úředníků o zabezpečení osobních údajů proti neoprávněnému přístupu k osobním údajům, protože 65 respondentů uvedlo, že veškeré doklady musí být po ukončení zpracování pod uzávěrou. Ale i další možná opatření byla uváděna ve vysoké četnosti (graf č. 6). Zde je možné se domnívat, že rizika spojená s neoprávněným přístupem k osobním údajům jsou na ČSSZ Hradec Králové a na OSSZ Královehradeckého kraje minimalizována.

[128] Vlastní výzkum, zpracování vlastní

Obrázek 6: Graf č. 6 Četnost uvedení opatření proti neoprávněnému přístupu k OÚ[129]



Osmá otázka se zabývá neoprávněným zpracováním osobních údajů. Na tuto otázku konkrétně odpovědělo jen 13 respondentů. Ostatní buď napsali, že neví nebo tuto otázku nechali nezodpovězenou. Dva respondenti uvedli, že pomocí anonymizace a 11 respondentů uvedlo, že ověřují identitu subjektu, u které zpracovávají osobní údaje. Zde by bylo možné navrhnout buď automatické anonymizace nebo vymazaní osobních údajů po uplynutí stanovené lhůty, či výmaz osobních údajů z vyřazené IT techniky atd.

Pokud šlo o otázku anonymizace nebo pseudonymizace bylo jejím cílem zjistit, zda jsou údaje nějakým způsobem anonymizovány nebo např. „zašifrovány“, když jsou následně zpracovávány. Téměř všechny odpovědi na tuto otázky byly ne, proto se dá shrnout, že pravděpodobně anonymizace nebo pseudonymizace není pro prostředí agend sociálního zabezpečení vhodná. Dva respondenti, kteří na tuto otázku odpověděli ano na anonymizaci, časovou ani administrativní náročnost neudávají.

Jedenáctá otázka soustřeďuje pozornost na neaktuální a nesprávné osobní údaje, a tudíž riziko s jejich zpracováním. Všechny shromážděné odpovědi bylo možné rozdělit do dvou opatření. První je automatické dotazování na aktuální údaje při přihlášení subjektů do systému. A druhé opatření je kontrola dat přímo úředníky buď z registrů nebo dotazem u subjektů. Oba postupy snižují riziko zpracování neaktuálních a nesprávných údajů.

[129] Vlastní výzkum, zpracování vlastní

V případě události související s osobními údaji, tedy např. porušení postupu nebo ohrožení osobních údajů, všichni respondenti uvedli, že jejich organizace mí konkrétní stanovený postup. V jeho popisu pak bylo většinou uváděno, že je třeba informaci o této události nahlásit (vedoucímu, pověřenci apod.) a snažit se zabránit škodám. Nicméně nikdo z respondentů neuvedl, že by se mu někdy událost s osobními údaji stala.

4.2.2 **Shrnutí**

Jak je patrné z výsledků dotazníkového šetření, povědomost o zpracování osobních údajů i implementace GDPR a minimalizace rizik související se zpracováním osobních údajů, jsou na ČSSZ Hradec Králové a OSSZ v Královéhradeckém kraji na vysoké úrovni. Ochrana osobních údajů je nedílnou součástí každodenní práce úředníků. Ať už se jedná o fyzické zabezpečení uzamčením veškerých dokladů s osobními údaji tak i zabezpečení v digitálním prostředí pomocí silných hesel a uživatelských oprávnění. I další riziko, které se týká neaktuálních nebo nesprávných údajů je podchyceno pomocí proaktivního dotazování při přihlášení subjektu do systému a vlastní kontrolou dat, kterou provádějí zaměstnanci z různých registrů i přímým dotazováním u subjektů.

Jedinou problémovou stránkou, co se týká rizik je nepovědomost o opatřeních k neoprávněnému zpracovávání osobních údajů. Zde by bylo možno navrhnout automatickou anonymizaci nebo automatický výmaz osobních údajů po stanovené lhůtě, tak aby nedošlo k administrativní zátěži pro pracovníky.

Zpravidla všichni pracovníci znají zákonný důvod, na jehož základě údaje zpracovávají. Pokud jde o administrativní náročnost, vzhledem ke skutečnosti, že osobní údaje jsou z velké části zpracovávána automatizovaně a bez použití pseudonymizace nebo anonymizace, je administrativní náročnost zanedbatelná, neboť se dá předpokládat, že zpracování údajů by bylo prováděno stejným způsobem bez ohledu na GDPR, ale je to další možnost zvýšení ochrany osobních údajů.

Jediná administrativně náročnější část v postupu zpracování osobních údajů je skutečnost, že někteří pracovníci sdělují účel zpracování osobních údajů a práva subjektu osobních údajů subjektům telefonicky nebo písemně, nicméně vzhledem ke skutečnosti, že opět v některých případech jsou právě tyto zákonné požadavky GDPR uvedeny již přímo ve formulářích, které subjekty vyplňují, nejedná o relevantní administrativní náročnost, která by byla systémová.

Dalším z problematických aspektů je vedení záznamů o činnostech zpracování osobních údajů, které se svěřeno vedoucím pracovníkům. Zde již dotazníky odhalily problém s časovou a administrativní náročností. Proto by bylo vhodné určitým způsobem upravit právě tuto činnost spojenou se zpracováním osobních údajů tak, aby bylo vedené těchto záznamů co nejvíce zautomatizováno (např. vhodným softwarovým systémem) tak, aby bylo možné odstranit časovou a administrativní náročnost.

5 Závěr

Cílem bakalářské práce bylo zhodnocení implementace GDPR do státní správy a analýza rizik spojených se zpracováním osobních údajů, a to konkrétně v České správě sociálního zabezpečení Hradec Králové a jejich spádových OSSZ.

Teoretická část se zaměřila na popsání právní úpravy v oblasti ochrany osobních údajů, a to především Obecným nařízením a jeho implementací do české legislativy v podobě zákona na ochranu osobních údajů. V teoretické části byla zmíněna nejen historie GDPR, ale byly zde rozebrány základní zásady Obecného nařízení a práva subjektu údajů. Další téma se věnovalo souhlasu se zpracováním osobních údajů, rolím a odpovědnosti v GDPR a závěr teoretické části se zaměřil na hlavní úkoly a pravomoci dozorového úřadu.

V praktické části formou dotazníkového šetření byla zjišťována opatření na minimalizaci rizik při zpracovávání osobních údajů, celková povědomost o zpracování osobních údajů a úspěšnost implementace GDPR do praxe úředníků na ČSSZ Hradec Králové a spádových OSSZ v Královehradeckém kraji. Dotazník byl především zaměřen na každodenní potkávání se s danou problematikou.

Dle výsledků dotazníkového šetření byla prokázána vysoká povědomost úředníků ČSSZ Hradec Králové a spádových OSSZ s legislativními povinnostmi vyplývajícími se zpracováním osobních údajů. Většina osobních údajů je zpracovávána na základě zákonného důvodu pro účely vyplácení dávek nemocenského a důchodového pojištění nebo pro účely vymáhání pojistného. ČSSZ a spádové OSSZ zpracovávají i osobní údaje zvláštní kategorie, a to především údaje o zdravotním stavu, které jsou potřebné k výkonu agendy lékařské posudkové služby.

Rizika spojená se zpracováním osobních údajů jsou ze strany ČSSZ minimalizována, a to hlavně nastavením ve vnitřních předpisech organizace, které jsou zaměstnanci povinni dodržovat. Opatření ke znemožnění neoprávněnému přístupu k osobním údajům jsou úředníkům dobře známa a v praxi běžně používána. Neaktuální a nesprávné údaje jsou pravidelně kontrolovány a aktualizovány. Tudíž je sníženo riziko, že by jejich zpracováním došlo k porušení GDPR. Pseudonymizace, anonymizace nebo šifrování není v rámci ČSSZ povinné, ale představuje další možnost zvýšení ochrany osobních údajů. Rizika související s neoprávněným zpracováním osobních údajů nejsou v takové povědomosti úředníků, jak by se dalo očekávat vzhledem k předešlému. Zde by tedy neměla být opomíjena osvěta a vzdělávání pracovníků.

Postupy na zpracování osobních údajů před implementací GDPR do norem ČSSZ byly nastaveny tak, aby byla zajištěna jejich ochrana. Lze tedy předpokládat, že zavedení GDPR nemá významný vliv na současnou změnu zpracování.

Časová a administrativní náročnost vzniká ve většině případů při vedení evidence o činnostech zpracování, která je prováděna obvykle vedoucími pracovníky. Zde je největší potenciál na zlepšení pomocí automatizování těchto záznamů.

Z výsledků dotazníkového šetření vyplývá, že Česká správa sociálního zabezpečení na problematiku implementace GDPR reagovala zodpovědně a jednala v souladu s GDPR.

6 Seznam použitých zdrojů

Odborná literatura:

Janečková, Eva. *GDPR. Praktická příručka implementace.* Praha : Wolters Kluwer ČR, a. s., 2018. str. 136. ISBN 978-80-7552-248-1.

Janečková, Eva. *GDPR - Řešení problémů v praxi obcí.* Praha : Grada Publishing, a.s., 2019. str. 256. ISBN 978-80-247-2925-1.

Navrátil, Jiří a a kolektiv. *GDPR pro praxi.* Plzeň : Aleš Čermák, s.r.o., 2018. str. 339. ISBN 978-80-7380-689-7.

Nezmar, Luděk. *GDPR: Praktický průvodce implementací.* Praha : Grada Publishing, a.s., 2018. str. 304. ISBN 978-80-271-0668-4.

Novák, Daniel. *Zákon o ochraněosobních údajů a předpisy související. Komentář.* Praha : Wolters Kluwer, a.s., 2014. str. 504. ISBN 978-80-7478-665-5.

Vlachová , Barbora a Maisner, Martin. *Zákon o zpracování osobních údajů. Komentář.* Praha : C. H. Beck, 2019. str. 163. ISBN 978-80-7400-6.

Internetové zdroje:

Historie. Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů.* [Online] [Citace: 19. 02 2022.] https://www.uoou.cz/historie/ds-1061/archiv=0&p1=1059.

Informace o zpracování osobních údajů. [Online] [Citace: 28. 02 2022.] https://www.cssz.cz/documents/20143/227251/Informace+o+zpracov%C3%A1n%C3%AD+osobn%C3%ADch+%C3%BAdaj%C5%AF+-+interaktivn%C3%AD+let%C3%A1k.pdf/e14db7d5-16d4-1620-5414-4ef667d77d3b..

Popis-organizacni-struktury-ossz. *ČSSZ.* [Online] [Citace: 27. 02 22.] https://www.cssz.cz/web/cz/popis-organizacni-struktury-ossz.

Profil-organizace. *ČSSZ.* [Online] [Citace: 27. 02 22.] https://www.cssz.cz/web/cz/profil-organizace.

Rezoluce k problematice dalšího vývoje v oblasti ochrany osobních údajů a sou-kromí. Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů.* [Online] [Citace: 19. 2 2022.] https://www.uoou.cz/rezoluce-k-problematice-dalsiho-vyvoje-v-oblasti-ochrany-osobnich-udaju-a-soukromi/ds-1695/archiv=0&p1=1659.

Role, Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů.* [Online] [Citace: 19. 02 2022.] https://www.uoou.cz/role-uoou/ds-4726.

Služební předpis náměstka vnitra pro státní službu. *ČSSZ.* [Online] 14. 12 2015. [Citace: 28. 02 2022.] https://www.cssz.cz/documents/20143/99686/eticky_kodex_CSSZ_sluz.pdf/78cb9806-07e0-8a28-6321-60999ca2e0f2. .

Žádost o poskytnutí informace, Hradec Králové. [Online] [Citace: 20. 02 2022.] https://www.cssz.cz/documents/20143/950750/%C3%9Ast%C5%99ed%C3%AD+%C4%8CSSZ.pdf/7fe6df6b-fafb-60a2-8fe3-426aff7cb491.

Žádost o poskytnutí informace, Rychnov nad Kněžnou. [Online] [Citace: 20. 02 2022.] https://www.cssz.cz/documents/20143/950750/OSSZ+Rychnov+nad+Kn%C4%9B%C5%BEnou.pdf/80439ccc-f4d4-71c8-55c4-b94e77d7bf57.

Žádost o poskytnutí informace, Trutnov. [Online] [Citace: 20. 02 2022.] https://www.cssz.cz/documents/20143/950750/OSSZ+Trutnov.pdf/0064f439-267a-900d-224b-4f5791e2ada5. .

Legislativní dokumenty:

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů): (Text s významem pro EHP). In: THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016. Dostupné také z: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, ročník 2019, částka 47, číslo 110. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=63839

Ostatní zdroje:

Politika ochrany osobních údajů. [Interní dokument]. *ČSSZ*: Česká správa sociálního zabezpečení, 2019.

Pokyny pro zpracování osobních údajů. [Interní dokument]. *ČSSZ*: Česká správa sociálního zabezpečení, 2020.

7 Přílohy

Dotazník:

1. S jakými typy OÚ (osobní údaje) pracujete? Prosím o uvedení konkrétních typů (jméno, rodné číslo atd.).

   _____

2. Při zpracování osobních údajů je Vám známo, z jakého právního titulu tyto informace zpracováváte.
   1 – nikdy to nevím,
   2 – občas mám tušení
   3 – vím to v polovině případů
   4 – spíše to vím
   5 – vím to vždycky

3. Jaký typ zpracování OÚ provádíte?
   a) Automatizované
   b) Manuální zpracování

4. Vedete záznamy o činnostech zpracování OÚ?
   NE – Prosím uveďte, kdo je za Vaši organizaci vede: _____
   ANO – Prosím uveďte, jakým způsobem: _____

5. Je vedení záznamů o činnostech zpracování OÚ administrativně/časově náročné? Prosím, uveďte, jak.

   _____

6. Jakým způsobem informujete subjekty, jejichž OÚ zpracováváte, o účelu zpracování jejich OÚ?

   _____

7. Jakými opatřeními je znemožněn neoprávněný přístup k OÚ?

   _____

8. Jakým způsobem je zabráněno neoprávněnému zpracování OÚ?

   _____

9. Používáte při zpracování OÚ anonymizaci/pseudonymizaci?

   NE

   ANO – Prosím uveďte jakou: _____

10. Pokud byla odpověď na předchozí otázku ANO, je toto zpracování náročnější časově/administrativně?

    ANO

    NE

11. Jakým způsobem jsou řešeny neaktuální a nesprávné OÚ?

    _____

12. Má Vaše organizace stanovený postup, jakým se ohlašují události s OÚ?

    NE

    ANO – Prosím o specifikaci: _____

13. Využil(a) jste někdy výše uvedený postup?

    NE

    ANO – Jak? _____