Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Ochrana osobních údajů v České republice podle nového nařízení Evropské unie

Bc. Milena Brožová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Milena Brožová

Veřejná správa a regionální rozvoj

Název práce

Ochrana osobních údajů v České republice podle nového nařízení Evropské unie

Název anglicky

General Data Protection Regulation in the Czech Republic

Cíle práce

Cílem této práce je popsat změny v oblasti ochrany osobních údajů, které přináší nové obecné nařízení Evropské unie, zjistit, jaké má nařízení dopady na organizaci sociálních služeb a na základě vyhodnocení zjištěných poznatků předložit návrhy netechnických opatření, které budou aktivně nápomocny implementaci nařízení.

Metodika

Pro teoretickou část práce budou vyhledány a soustředěny relevantní právní předpisy a odborná literatura. Tyto odborné zdroje budou analyzovány. Na základě poznatků získaných v teoretické části práce bude zvolena vhodná metoda pro sběr dat nutných k vypracování praktické části práce. Získaná data budou vyhodnocena a na základě jejich porovnání s výsledky teoretické části práce bude navrženo řešení směřující k eliminaci zjištěných nedostatků.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Osobní údaj, zpracování, obecné nařízení, právo, ochrana, zabezpečení, informace.

Doporučené zdroje informací

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).Dostupné z www:http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&rid=1

NEZMAR, L. GDPR: Praktický průvodce implementací. Praha: Grada Publishing, 2017.ISBN 978-80-271-0668-4

Praktická personalistika. Olomouc: Nakladatelství Anag. ISSN 2336-5072. MK ČR E 21766

Škorničková, E. : www.gdpr.cz

Úřad pro ochranu osobních údajů: www.uoou.cz

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.Dostupný ve Sbírce zákonů České republiky

ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

JUDr. Daniela Světlíková

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 7. 11. 2018

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 12. 11. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 21. 02. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Ochrana osobních údajů v České republice podle nového nařízení Evropské unie" jsem vypracovala samostatně pod vedením vedoucího diplomové 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 diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 18. 03. 2019 _____

Poděkování

Ráda bych touto cestou poděkovala vedoucí mé diplomové práce JUDr. Daniele Světlíkové za vstřícnost a odborné rady při psaní této diplomové práce. Dále bych ráda poděkovala vedení organizace, kde jsem prováděla vlastní výzkum, za poskytnutí prostoru a podkladů pro vlastní část práce.

Mé velké poděkování směřuji ke svým blízkým za podporu a trpělivost.

Ochrana osobních údajů v České republice podle nového nařízení Evropské unie

Abstrakt

Tato diplomová práce se věnuje problematice ochrany osobních údajů, jak ji pojímá obecné nařízení Evropské unie. Diplomová práce je rozdělena na část teoretických východisek a na část vlastní práce.

Část teoretických východisek se zabývá analýzou právních předpisů, přednostně obecným nařízením o ochraně osobních údajů, a jeho interpretací, používá metodu deskripce. Jsou zde objasňovány nosné prvky důležité pro soulad zpracování osobních údajů s obecným nařízením. Analýza právních předpisů je průběžně doplňována odbornými interpretacemi.
V textu jsou používány přímé a nepřímé citace, které jsou označovány a odkazovány na zdroje formou poznámkou pod čarou.

Vlastní práce zkoumá analyticky proces implementace obecného nařízení ve vybrané organizaci sociálních služeb. K výzkumu je použito studium dokumentů a následných rozhovorů se zaměstnanci organizace.

Po vyhodnocení poznatků zjištěných primárním výzkumem, porovnaných s poznatky v teoretické části, byla navržena vhodná opatření. K diskuzi bylo dáno téma jmenování pověřence pro ochranu osobních údajů a získávání informačních zdrojů, a dále téma provedení pravidelného proškolování stávajících i nových zaměstnanců. Doporučen byl návrh konceptu vnitřního předpisu pro stanovení organizačních a technických opatření, který je aktivní nápomocí v implementaci obecného nařízení o ochraně osobních údajů.

Klíčová slova: Osobní údaj, zpracování, obecné nařízení, právo, ochrana, zabezpečení, informace.

General Data Protection Regulation in the Czech Republic

Abstract

This diploma thesis focuses on the personal data protection in accordance with the European Union regulation. This work is divided into a theoretical and practical part.

The theoretical part focuses on the analysis of legal regulations, in particular General Data Protection Regulation and its interpretations. The method used is description. This part explains the fundamental points of the regulation which are important for processing personal data in accordance with General Data Protection Regulation. The analysis of the legal regulations is complemented with expert interpretations.
Both direct and indirect quotes are used in the text. The sources of the quotes are marked and listed in footnotes.

The practical part analytically studies the process of implementation of General Data Protection Regulation in a specified social services institution. The research is conducted with the usage of documentation and subsequent interviews with the employees of the institution.

After the evaluation of primary research findings, suitable measures were suggested. The appointment of Data Protection Officer was proposed as well as a periodical training of both current and new employees. A draft of an inner regulation was written and recommended. The purpose of this regulation is to set measures which help with implementation of General Data Protection Regulation.

Key words: personal data, processing, General Data Protection Regulation, law, protection, provision, information

Obsah

1 Úvod 10

2 Cíl práce a metodika 12

2.1 Cíl práce 12

2.2 Metodika 12

3 Teoretická východiska 15

3.1 Obecné nařízení v souvislosti s vývojem ochrany osobních údajů v České republice 15

3.2 Osobní údaj 16

3.2.1 Zvláštní osobní údaje 19

3.2.2 Osobní údaj – rodné číslo 20

3.3 Zpracování osobních údajů 20

3.3.1 Správce osobních údajů, zpracovatel osobních údajů 22

3.3.2 Zásady zpracování osobních údajů 23

3.4 Práva subjektů osobních údajů 28

3.5 Omezení práv a zásad zpracování 34

3.6 Proces naplnění souladu zpracování osobních údajů s obecným nařízením 35

3.6.1 Vnitřní analýza 35

3.6.2 Záznamy o činnostech zpracování 36

3.6.3 Posouzení vlivu na ochranu osobních údajů 37

3.6.4 Předchozí konzultace s dozorovým úřadem 38

3.6.5 Pověřenec pro ochranu osobních údajů 39

3.6.6 Kodexy chování 39

3.6.7 Zabezpečení osobních údajů a jeho porušení 41

3.6.8 Předávání osobních údajů do třetích zemí 42

4 Vlastní práce 44

4.1 Rozsah a charakteristika osobních údajů 44

4.2 Zákonné tituly ve zpracování osobních údajů 46

4.3 Výkon práv subjektů osobních údajů 49

4.4 Vnitřní analýza a opatření z analýzy plynoucí 49

4.5 Aktualizace stavu 58

5 Výsledky a diskuse 59

5.1 Zhodnocení teoretických vstupů 59

5.1.1 Zhodnocení dopadů na organizaci sociálních služeb 60

5.2 Výsledky zjištění z analýzy vybraného subjektu 60

5.2.1 Náměty k diskuzi ze získaných poznatků a vhodná opatření: 60

6 Závěr..... 68

7 Seznam použitých zdrojů 70

7.1 Odborná literatura 70

7.2 Právní předpisy..... 70

7.3 Ostatní literatura..... 71

7.4 Internetové zdroje..... 71

Seznam grafů

Graf č. 1 Procentní vyjádření kategorií zpracovávaných osobních údajů na celkovém rozsahu……..45

Graf č. 2 Procentní podíl zákonných titulů……...46

Seznam tabulek

Tabulka č. 1 – Náhled popisu osobních údajů…….....50

Tabulka č. 2 – Struktura identifikace zpracování…….54

Tabulka č. 3 – Záznam o činnostech zpracování – kamerový systém……. 56

1 Úvod

Každý člověk je nositelem osobních údajů. Jsou používány v rozličných situacích, ať soukromého rázu, společenského nebo obchodního. Používání osobních údajů však neopravňuje druhého jedince ke zneužití osobních údajů. Jak je řečeno v Listině základních práv a svobod: „ *Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života a každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“*[1]

V Českém právním řádu jsou k naplnění práva na ochranu před neoprávněným zasahováním do soukromí zakotveny práva a povinnosti v zákoně č. 101/ 2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Vzhledem k mezinárodní spolupráci již dochází ke zpracování osobních údajů nejen na území České republiky, ale dále i v prostoru globálním. Mnohé je umožněno rozvojem informačních technologií, zejména internetového prostředí. Zákon č. 101/2000 Sb. musí být tomuto přizpůsoben, nastavuje proto také podmínky pro migraci osobních údajů do jiných států.

Nelze opomenout fakt, že se společnost celkově dále vyvíjí, má nové potřeby, vznikají nové komunikační prostory, tím i nové komunikační nástroje, spravování společnosti se stává komplikovanějším, dochází k velkému počtu zpracovatelských operací v informačních systémech různých struktur. Na jedné straně jsou nastalé potřeby a velké množství zpracování osobních údajů, na straně druhé stojí riziko zneužití těchto údajů. Tím vyvstává potřeba vytvoření nové právní úpravy, která by reagovala na současný společenský stav ve zpracování osobních údajů, a to v širším mezinárodním měřítku. Zásady a pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů v prostoru Evropské unie jsou zpracovány v obecném nařízení Evropského parlamentu a Rady 2016/679. Jak je vyjádřeno v nařízení, účelem této směrnice je „ *harmonizovat právní předpisy“*[2] v oblasti ochrany práv osob právě v souvislosti se zpracováním osobních údajů.

[1] Zákon č. 23/1991 Sb., ústavní zákon, kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské federativní republiky, v platném znění, čl. 10, odst. 2, odst. 3

[2] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), recitál 3

Ve svém pojetí toto nařízení představuje, jak uvádí autor Žůrek, *daleko „důmyslnější a propracovanější systém ochrany osobních údajů při jejich zpracování“*[3] v současnosti v prostoru Evropské unie.

Vzhledem k tomu, že se jedná o nařízení Evropské unie, jakožto nejsilnější právní normy, jsou jím vázány všechny členské státy, tedy i Česká republika. Tato právní norma má přednost před vnitřním právem členských států, je jim nadřazena, dává však možnost členským státům některá ustanovení upravit, případně upřesnit nebo doplnit, vnitrostátní právní normou.

Obecné nařízení jako evropská právní norma se dotýká i států nečlenských, neboť je závazná pro všechny státy, které vstupují do prostoru Evropské unie obchodně, protože i v těchto vztazích se vyskytují osobní údaje, které podléhají ochraně vyjádřené zmiňovaným nařízením.

Je však důležité zmínit, že obecné nařízení necílí na ochranu osobních údajů zpracovávaných v osobním prostoru, mající osobní povahu. V soukromí musí každý dbát na ochranu svých osobních údajů vlastními silami.

[3] ŽŮREK, J., *Praktický průvodce GDPR,* s. 22

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této práce je popsat změny v oblasti ochrany osobních údajů, které přináší nové obecné nařízení Evropské unie, a zjistit, jaké má nařízení dopady na organizaci sociálních služeb a na základě vyhodnocení zjištěných poznatků předložit návrhy netechnických opatření, které budou aktivně nápomocny naplnění zpracování osobních údajů tak, jak podmínkuje obecné nařízení.

2.2 Metodika

Pro teoretickou část práce budou vyhledány a soustředěny odpovídající právní předpisy a odborná literatura.

První část teoretické části se dotkne vývoje ochrany osobních údajů v České republice s důrazem na vztah dvou právním norem, kterými jsou zákon č. 101/2000 Sb., o ochraně osobních údajů a Nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Evropské nařízení bude v textu uváděno pod zjednodušeným používaným pojmem obecné nařízení o ochraně osobních údajů.
Následně se bude teoretická část věnovat vysvětlení pojmu osobní údaj a jeho kategoriím, nejprve pomocí komparace jak na osobní údaj nahlíží zákon č. 101/2000 Sb., o ochraně osobních údajů a dále jak osobní údaj pojímá obecné nařízení o ochraně osobních údajů.
V teoretické části bude pokračováno analýzou studované stěžejní právní normy – obecného nařízení o ochraně osobních údajů. Analýza se bude zaměřovat na popis jednotlivých institutů obecného nařízení, které jsou zásadními nosnými prvky obecného nařízení o ochraně osobních údajů. Tyto instituty budou za pomoci deskriptivní metody objasňovány v pořadí logické posloupnosti. Nejprve bude pozornost věnována zpracování osobních údajů, institutu správce a zpracovatele osobních údajů, a dále zásadám zpracování osobních údajů. V logické posloupnosti bude v analýze navazováno právy subjektů

osobních údajů a popisem procesu naplnění souladu zpracování osobních údajů s obecným nařízením o ochraně osobních údajů.
Vzhledem k naplnění stanoveného cíle budou hledány odlišnosti pro organizace sociálních služeb, které budou případně v textu teoretických východisek přímo uvedeny.

Obecné nařízení o ochraně osobních údajů bude analyzováno pomocí metody výkladu práva. Prostor k doplnění bude ponechán vhodným interpretacím autorů publikovaným v odborné literatuře. Vhodné interpretace budou hledány v publikaci *Praktický průvodce GDPR* autora Žůrka a v publikaci autora Nulíčka s kolektivem *GDPR/ Obecné nařízení o ochraně osobních údajů, praktický komentář*, a dále v publikaci autora Nezmara *GDPR: Praktický průvodce implementací.* Na podporu studia tématu ochrany osobních údajů bude nahlíženo taktéž do publikace směrované k pověřencům pro ochranu osobních údajů autora Nonnemanna *Praktická příručka GDPR, Příručka pověřence pro ochranu osobních údajů.*
Využito bude taktéž, kde to bude žádoucí, stanovisek Úřadu pro ochranu osobních údajů, případně stanovisek Evropského sboru pro ochranu osobních údajů (dříve pracovní skupina WP 29), a odborných publikovaných článků. Ta budou nalézána pomocí internetových zdrojů.
Internetových zdrojů bude využito taktéž při studiu právních předpisů.

Všechny přímé a nepřímé citace ustanovení právních předpisů, interpretací autorů z odborných publikací a odborná stanoviska budou v textu označovány kurzívou s uvozovkami a odkazovány na svůj zdroj formou poznámky pod čarou.

Ve vlastní práci bude použita metoda analýzy vybraného subjektu. K naplnění cíle bude vybrána organizace sociálních služeb.
Nejprve bude organizace analyzována z pohledu rozsahu a charakteristiky osobních údajů. Následně budou získávána data z pohledu zákonných titulů zpracování osobních údajů a z pohledu výkonu práv subjektů údajů. Získaná data budou komparována, přiměřeně bude ke komparaci dat využito grafů.
Další část bude zaměřena na analytické postupy pro implementaci obecného nařízení o ochraně osobních údajů. Deskriptivní metodou budou analyzovány jednotlivé kroky charakteristické pro posun k souladu zpracování osobních údajů s obecným nařízením. Ve vhodných případech bude popis doplněn tabulkovým znázorněním.

Data potřebná k výzkumu budou získávána studiem dostupných dokumentů ve vybrané zkoumané organizaci a dále budou získávána metodou rozhovoru. Osobní rozhovory budou vedeny s pracovníky organizace, zejména s pracovníky vedení organizace. Otázky k rozhovorům nebudou předem stanoveny. Otázky a téma rozhovorů se budou odvíjet od míry zjištěných dat v dostupných dokumentech organizace.
Veškeré zkoumání bude oproštěno od záznamů osobních údajů. Ve vlastní práci nebudou žádné osobní údaje identifikované nebo identifikovatelné osoby uváděny. Data budou plně anonymizována.

Zjištěné poznatky teoretických východisek a získaná data z vlastní průzkumné práce budou komparována a vyhodnocena. K diskusi budou dána případná zjištěná problematická témata. V případě zjištěného nedostatku, pro který lze navrhnout vhodné opatření, bude takový návrh opatření předložen.

Závěr diplomové práce bude věnován, za pomocí metody syntézy, shrnutí získaných zjištění v problematice ochrany osobních údajů v České republice podle obecného nařízení Evropské unie. Bude souhrnně pojímána teoretická část ve svých poznatcích a vlastní výzkumná část ve svých výsledcích. Zároveň budou shrnuty náměty k diskuzi a případná navržená opatření.

3 Teoretická východiska

3.1 Obecné nařízení v souvislosti s vývojem ochrany osobních údajů v České republice

V České republice začala být ochrana osobních údajů samostatně řešena přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Pozornost zde byla věnována pouze prostředí informačních systémů.

Zásadnějšího kroku bylo dosaženo přijetím zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Jedná se o současnou právní normu, která se věnuje ochraně osobních údajů komplexně, včetně vytvoření dozorového úřadu, kterým je Úřad pro ochranu osobních údajů. Zákon o ochraně osobních údajů zatím zůstává v platnosti v plném znění i přesto, že dne 25. května 2018 nabyla účinnosti nová evropská právní norma – Nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Bylo uvažováno, že nová evropská právní norma plně nahradí rozsah stávajícího zákona č. 101/2000 Sb., o ochraně osobních údajů. V tomto smyslu hovoří autoři Žůrek a Nezmar. Vedle toho staví předpoklad vnitrostátní úpravy některých dílčích aspektů nařízení, autor Žůrek „*přijetím nového zákona*“[4], autor Nezmar „*novelizací*“[5] stávajícího zákona č. 101/2000 Sb., o ochraně osobních údajů..

Na základě ustanovení Směrnice 95/46/ES byla založena pracovní skupina WP29. Do doby nabytí účinnosti obecného nařízení o ochraně osobních údajů působila jako pomocná ruka k uchopení této problematiky. Vydávala dokumenty, které jsou vodítky a výkladovým materiálem obecného nařízení. Ke dni nabytí účinnosti obecného nařízení již přestala být pracovní skupinou, nadále však působí jako Evropský sbor pro ochranu osobních údajů, který bude nadále vydávat pokyny a doporučení k problematice. Lze předpokládat, že sbor při tvorbě doporučení bude vycházet z poznatků z praxe zavedeného obecného nařízení.

[4] ŹŮREK, J., *Praktický průvodce GDPR,* s. 19
[5] NEZMAR, L., *GDPR: Praktický průvodce implementací,* s. 28

Dokumenty Evropského sboru pro ochranu osobních údajů jsou k dispozici na webových stránkách Úřadu pro ochranu osobních údajů: www.uoou.cz

3.2 Osobní údaj

Zákon o ochraně osobních údajů vymezuje pojmem osobní údaj *„jakoukoliv informací týkající se určeného nebo určitelného subjektu údajů“*[6]. Pro určitelnost subjektů dále zákon říká: *„Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*[7] Z tohoto pojetí lze usuzovat, že osobní údaj je údajem, na základě kterého lze fyzickou osobu identifikovat či určit, o kterou osobu se jedná.

Obdobně hovoří o osobním údaji obecné nařízení, když specifikuje osobní údaj jako *„ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů).“*[8] Za identifikovatelnou osobu, jak shodně uvádí v souladu s nařízením, Nezmar a Úřad pro ochranu osobních údajů, považuje *„fyzickou osobu, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, lokační údaje, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*[9]
Okruh doposud všeobecně známých osobních údajů, kterými jsou například jméno a příjmení, rodné číslo, tzn. údaje k přímé identifikaci osoby, obecné nařízení rozšiřuje okruh o další identifikační prvky, které mají vazbu ke konkrétní fyzické osobě, a kterými lze osobu identifikovat nepřímo. Jako příklad uvádí Žůrek *„ údaj o platu nebo odměnách konkrétního zaměstnance, a to nejen označeného jménem a příjmením, ale např. i jedinečným označením pozice, kterou zastává, jelikož podle ní je identifikovatelný.“*[10] Pro

[6] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění, § 4 písmeno a)
[7] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění, § 4 písmeno a)
[8] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) čl. 4, odst. 1
[9] NEZMAR, L., *GDPR: Praktický průvodce implementací,* s. 31 – 32
[10] ŽŮREK, J., *Praktický průvodce GDPR,* s. 40

názornost lze použít porovnání pracovních pozic v organizaci. Zaměstnává-li organizace deset dělníků a nejsou-li označeni jménem, nelze toto definovat jako osobní údaj, jelikož nelze identifikovat konkrétní osobu. Zaměstnává-li však jednoho ředitele, jde o jedinečnou pracovní pozici, a v tomto případě se jedná o nepřímou identifikaci, již jde tedy o osobní údaj. Stejně lze postupovat v případě služebních (pracovních) telefonních čísel. Je-li uvedeno telefonní číslo do organizace neutrální (zpravidla recepce, základní telefonní číslo), nelze jej spojit s konkrétní osobou, nejedná se tudíž o osobní údaj. Užívá-li však telefonní číslo jen jeden konkrétní zaměstnanec, jde opětně o nepřímou identifikaci konkrétní osoby, v takovém případě je taktéž dané telefonní číslo nutno považovat za osobní údaj. Dalším příkladem nepřímé identifikace osoby je IP adresa. Jak uvádí Nezmar společně s Úřadem na ochranu osobních údajů, „ *IP adresa je osobním údajem vždy, když se vztahuje k určené nebo určitelné osobě, a to od prvního použití IP adresy v provozu"*.[11] Klasifikaci osobního údaje přiřazuje obecné nařízení taktéž síťovým identifikátorům například adresám internetového protokolu, identifikátorům cookies nebo identifikátorům lokace a rádiovým frekvencích, a to v případě, pokud jsou přiřazeny konkrétní fyzické osobě k využití jejího zařízení a aplikací, neboť, jak zdůvodňuje obecné nařízení ve svém recitálu, „ *tímto způsobem mohou být zanechány stopy, které mohou být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají, použity k profilování fyzických osob a k jejich identifikaci*".[12] Z tohoto důvodu se lze na serverech setkat s vyžadováním souhlasu s použitím cookies, lokace, apod.

Jsou-li však osobní údaje anonymizovány, nemohou se vztahovat ke konkrétní osobě a posloužit k její identifikaci, proto v nich, ve smyslu obecného nařízení, nelze nadále osobní údaj spatřovat.

Jinak je však posuzován pseudonymizovaný údaj. Obecné nařízení nahlíží na „*pseudonymizaci zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby*

[11] NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 277, Úřad pro ochranu osobních údajů, www.uoou.cz

[12] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), recitál 30

bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné osobě.“[13] Jedná se o taková zpracování, kdy je přímý identifikační údaj skryt pod kód, klíč, tím nelze již přiřadit ke konkrétní osobě konkrétní informace bez použití dodatečné informace.
Pro názornost lze uvést následující příklady vazeb konkrétních údajů:

Příklad č. 1 Popis údajů

jméno	příjmení	bydliště	věk	měsíční mzda
Josef	Josefský	Josefská 1, Josefov	30	40000

Ve výše uvedeném popisu jsou údaje navázány k osobě, osobu lze identifikovat, proto všechny údaje, tj. jméno, příjmení, bydliště, věk a měsíční mzda je nutno považovat za osobní údaje podléhající obecnému nařízení.

Příklad č. 2 Popis údajů

jméno	příjmení	bydliště	věk	měsíční mzda
			30	40000

Ve výše uvedeném popisu jsou údaje jméno, příjmení, bydliště plně vymazány, zničeny, úplně zlikvidovány. Ostatní uvedené údaje nedokáží osobu identifikovat, určit, jsou považovány za údaje anonymizované, již na ně není pohlíženo jako na osobní údaje, proto obecnému nařízení nepodléhají.

Příklad č. 3 Popis údajů

jméno	příjmení	bydliště	věk	měsíční mzda
101			30	40000

Ve výše uvedeném popisu jsou údaje typu jméno, příjmení, bydliště skryty pod číselný klíč, tím jsou tyto údaje pseudonymizovány. Identifikační vazba však, byť skrytě, trvá, je proto nutno na tyto údaje pohlížet jako na osobní údaje ve smyslu obecného nařízení.

[13] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), článek 4, bod 5

Jak uvádí autorka Škorničková: „ *Pseudonymizace osobních údajů je proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost*.“[14] Správce tak má možnost sbírat další data s menším bezpečnostním rizikem. Autor Žůrek spatřuje výhodu pseudonymizace, mimo jiné, taktéž při předávání dat jinému subjektu, což demonstruje na typické ukázce zdravotnického výzkumu, „*kdy jsou předána za určitým účelem výzkumnému ústavu data o zdravotním stavu deseti pacientů, kteří jsou označeni číselnými klíči, tím je výzkumný ústav nedokáže ztotožnit s konkrétními osobami*“[15]. Lze konstatovat, že pseudonymizaci snižuje některá rizika při zpracování osobních údajů. Proto, jak uvádí autor Žůrek, „ *i Obecné nařízení nabádá správce, aby ve vhodných případech pseudonymizaci využívali.*“[16]

Obecné nařízení se nevztahuje na osobní údaje zemřelých osob, uděluje však pravomoc členským státům k nastavení pravidel pro zpracování osobních údajů zesnulých.

3.2.1 Zvláštní osobní údaje

Zvýšená ochrana je věnována v obecném nařízení podskupině osobních údajů - zvláštním osobním údajům, které svou charakteristikou výrazně zasahují do soukromí. Jedná se o údaje, které vypovídají o rasové, etnické, politické, náboženské, filozofické či odborové identitě osoby a dále genetické, biometrické údaje sloužící k jedinečné identifikaci fyzické osoby, údaje o zdravotním stavu, sexuálním životě či sexuální orientaci. Tato skupina údajů je v zákoně o ochraně osobních údajů označována jako citlivé údaje. Oproti zákonu o ochraně osobních údajů obecné nařízení již neuvažuje o národnostní identitě jako o zvláštním osobním údaji, stejně tak o údaji o odsouzení za trestný čin. Nicméně se zabývá rozsudky v trestních věcech a trestných činů v souvislosti s jejich rozsáhlým zpracováním.
Přesto, že se citlivé údaje objeví, nemusí se nutně jednat o zpracování citlivých osobních údajů. Autor Nonnemann tento fakt posuzuje na pořizování kamerového záznamu a fotografií. „*Pořizování kamerového záznamu či fotografií není v běžném režimu považováno za zpracování citlivých osobních údajů, ačkoliv z nich lze odvodit informaci o rasovém či etnickém původu, o náboženském přesvědčení či některé biometrické údaje*

[14] https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/
[15] ŹŮREK, J., *Praktický průvodce GDPR,* s. 43- 44
[16] ŹŮREK, J., *Praktický průvodce GDPR,* s. 43

zachycených osob. O zpracování citlivých osobních údajů by se jednalo tehdy, pokud by úmyslem správce bylo citlivé údaje aktivně využívat, např. k identifikaci osob podle jejich chůze, k evidování počtu návštěvníků podle etnického původu atd.“[17]

3.2.2 Osobní údaj – rodné číslo

Pozornosti je třeba věnovat rodnému číslu, který je samostatným osobním údajem. Není vyjmenován v kategorii zvláštních osobních údajů, proto by bylo možno na něj nahlížet jako na běžný osobní údaj a zpracovávat jej dle obecných právních titulů obecného nařízení. Jak upozorňuje autor Nonnemann, tyto „*obecné právní tituly na zpracování rodného čísla uplatnit nejdou*“[18]. Rodné číslo má svoji specifičnost, neboť jeho užití je dáno zvláštním právním předpisem, konkrétně zákonem č. 133/2000 Sb., o evidenci obyvatel a o rodných číslech, který ve svém paragrafu 13c stanovuje právní důvody, na základě kterých je možno rodné číslo využívat. Ve zjednodušené formulaci lze právní důvody vyjádřit jednak činností státní správy, soudů a notářů, dále stanovené zvláštním zákonem nebo se souhlasem nositele rodného čísla, případně jeho zákonného zástupce. Z uvedeného je patrno, že rodné číslo nelze používat automatizovaně, i zde musí být oprávněný právní titul. Byť je rodné číslo specifickým osobním údajem, je třeba na jeho zpracování vztahovat zásady dané obecným nařízením, o kterých bude pojednáno dále.

3.3 Zpracování osobních údajů

Za zpracování osobních údajů je považována „*jakákoliv operace nebo soubor operací s osobními údaji nebo soubory údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování omezení, výmaz nebo zničení*.“[19] Takto vnímá zpracování osobních údajů obecné nařízení. Z uvedeného lze usuzovat, že jakoukoliv operací je zde myšlen každý proces, při němž se

[17] NONNEMANN,F., *Praktická příručka GDPR*, s. 37
[18] NONNEMANN,F., *Praktická příručka GDPR*, s. 24
[19] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), článek 4, bod 2

s osobními údaji pracuje, počínaje přijetím osobního údaje a jeho zničením konče. Je třeba se zastavit u pojmu „ automatizovaný postup“. Tento pojem není definován ani v zákoně o ochraně osobních údajů, ani v obecném nařízení. Autoři Radičová a Burian nalézají vodítko k výkladu tohoto pojmu v mezinárodní úpravě oblasti ochrany osobních údajů, a to v Úmluvě 108, v které se odkazují na definici automatizovaného zpracování, kde je uvedeno automatizovaným postupem „*ukládání na nosiče dat, provádění logických a/nebo aritmetických operací s těmito daty, jejich změna, výmaz, vyhledávání nebo rozšiřování“*[20]. Velkou měrou se týkají automatizované postupy oblasti internetu, což autor Nonnemann demonstruje na výkladu Soudního dvora EU, který „*vyložil, že již pouhé umístění několika málo údajů na internet představuje jejich zpracování automatizovanými prostředky."* [21]

Zajímavým náhledem na to, zda se jedná o zpracování osobních údajů je oblast Facebooku. Do okamžiku, kdy vstupují do této oblasti soukromé osoby v soukromé rovině, nejedná se o zpracování osobních údajů. V okamžiku, kdy zde kterákoliv společnost „*zřídí fanouškovskou stránku, dostává se do pozice správce osobních údajů těch uživatelů, kteří tuto fanouškovskou stránku používají*“[22]. V tomto smyslu i vyznívá autorem Nonnemannem prezentované vyjádření generálního advokáta Soudního dvora.

V úvodu je zmiňován fakt, že obecné nařízení necílí na ochranu osobních údajů v osobním prostoru. Na tomto místě je proto třeba doplnit, že pravidla zpracování osobních údajů jsou závazná „*v souvislosti s činnostmi provozovny správce nebo zpracovatel“*[23] Volně odvozeno – pro všechny, kteří provozují jakouko-li ekonomickou činnost. To znamená veškeré firmy, drobní živnostníci, ale taktéž neziskové organizace, orgány veřejné moci, nehledě na předmět působnosti a nehledě na právní formu, kteří se v pojetí obecného nařízení stávají správcem zpracování osobních údajů.

[20] https://www.epravo.cz/top/clanky/profilovani-ve-svetle-noveho-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-104926.html
[21] NONNEMANN,F., *Praktická příručka GDPR*, s. 27
[22] NONNEMANN,F., *Praktická příručka GDPR*, s. 29
[23] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), článek 3, bod 1

3.3.1 Správce osobních údajů, zpracovatel osobních údajů

Obecné nařízení za správce považuje subjekt, který *„sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů“*[24] Účel je tedy ten hlavní faktor, s kterým jsou spjaty povinnosti správce při zpracování osobních údajů a je tedy na správci, jakým způsobem si účel nebo účely konkretizuje. Vždy musí být účel zpracování *„legitimní a nesmí být protiprávní.“*[25] Zde je patrná souvislost se zásadou zákonnosti, o které bude pojednáno dále.

Nebude se jednat o výjimku, že správce bude zpracovávat stejné osobní údaje pro více účelů. Jako příklad lze uvést zaměstnanecké osobní údaje, které mohou být účelově vymezeny ke zpracování v rámci plnění pracovní smlouvy, ale stejně tak k plnění zákonných povinností v oblasti nemocenského pojištění, stejně tak pro potřeby benefitových programů. Bude se však lišit rozsah zpracování osobních údajů pro jednotlivé účely. Zatímco pro benefitový program může stačit jméno a příjmení, pro účely nemocenského pojištění bude třeba zpracovávat například taktéž rodné číslo a bydliště.

Správce může pro jednotlivý účel nebo více účelů osobní údaje zpracovávat sám nebo může k tomu pověřit jinou fyzickou či právnickou osobu. V takovém případě se pověřená osoba stává zpracovatelem osobních údajů. Odpovědným za soulad zpracování osobních údajů s obecným zařízením je správce, nikoli zpracovatel, proto by si měl správce počínat obezřetně a pověřit takové zpracovatele, kteří „*poskytují dostatečné záruky*“[26]. Kolektiv autorů hovoří zejména o odborné znalosti a spolehlivosti zpracovatele. Společně s autorem Žůrkem se shodují na úpravě vztahu správce a zpracovatele právním aktem nebo smlouvou. Nejčastěji se bude jednat o smlouvu o zpracování osobních údajů, jejíž náležitosti, jak uvádí autor Žůrek, vyjmenovává obecné nařízení v článku 28, odstavci 3. Ve shrnutí náležitostí se jedná zejména „ *o předmět a dobu trvání zpracování, povahu a účel zpracování, typ osobních údajů a kategorie subjektů údajů*“[27]. Autor Žůrek upozorňuje na další povinnosti zpracovatele, které by ve smluvním dokumentu měly být

[24] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), článek 4, bod 7

[25] ŽŮREK, J., *Praktický průvodce GDPR,* s. 56

[26] BOGNÁROVÁ,V. a kolektiv, *GDPR 2018 v praxi, Sborník vzorů a návodů pro mzdové účetní a personalisty,*s. 28

[27] ŽŮREK, J., *Praktický průvodce GDPR,* s. 89

stanoveny, tak, jak jsou popsány ve zmiňovaném článku a odstavci věnovaném vztahu správce a zpracovatele. Tyto povinnosti lze charakterizovat jako povinnosti spojené se zajištěním bezpečného zpracování osobních údajů povinnosti vyplývající z řídící pozice správce vůči zpracovateli. Autor Žůrek upozorňuje na nutnou písemnou podobu takové smlouvy, autor Nezmar zmiňuje možnost zakomponovat příslušná smluvní ustanovení do jiné smlouvy, která je uzavírána správce a zpracovatelem v rámci jiného vztahu. Typickým příkladem může být smlouva o vedení účetnictví, kdy je pro organizaci, v tomto případě zároveň pro správce, účetnictví zpracováváno externí osobu, nikoli vlastním zaměstnancem, a tato externí osoba je zároveň pověřeným zpracovatelem osobních údajů. Smluvní strany uzavřou obchodní vztah, nic jim nebrání v tom, aby dotčené náležitosti zařadily mezi ustanovení smlouvy o vedení účetnictví.

Obecné nařízení se v článku 28 a v článku 29 zmiňuje o možnosti, kdy může zpracovatel zapojit do zpracování dalšího zpracovatele. Autor Žůrek tento stav pojmenovává „řetězením zpracovatelů“, který popisuje „*zapojením dalšího zpracovatele, a sice ze strany zpracovatele, čímž vznikne řetěz správce →zpracovatel 1 → zpracovatel 2 atd.“*[28] Dikce obecného nařízení tento stav nevylučuje, ale v souvislosti s nastavením smluvního vztahu mezi správcem a zpracovatelem a zajištěním záruky zpracovatele, je vhodné možnost dalšího zpracovatele vymezit smluvně, stejně tak je vhodné, aby si správce dalšího zpracovatele prověřil a posoudil jeho kvality. Zásadním faktem je, že bez souhlasu správce je navazování dalšího zpracovatele zakázáno.

3.3.2 Zásady zpracování osobních údajů

Obecné nařízení ve svém článku 5 charakterizuje zásady, které musí být uplatňovány při činnostech zpracování osobních údajů. Zásady lze vykládat jako zásadní principy určující, jak může správce, případně zpracovatel, s osobními daty nakládat. Článek 5 zároveň správci ukládá povinnost dodržování zásad, a činí jej odpovědným za doložení dodržování těchto zásad.

[28] ŽŮREK, J., *Praktický průvodce GDPR*, s. 91

Zásada zákonnosti

Zásadu zákonnosti lze spatřovat v dostatečném odůvodnění, proč se musí dotčené osobní údaje zpracovávat. Správce musí disponovat dostatečným právním titulem k danému účelu zpracování osobních údajů. Z dikce článku 6 obecného nařízení lze právní tituly shrnout pod následující volby, pro které je zpracování osobních údajů nezbytné:

- splnění smlouvy,
- splnění právní povinnosti,
- ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci,
- oprávněné zájmy příslušného správce či třetí strany,

a dále pokud subjekt k danému účelu či k více účelům udělil souhlas se zpracováním osobních údajů. Všechny právní tituly jsou si rovny. Pro zákonné zpracování postačuje, pokud správce disponuje pro daný účel jedním právním titulem. Pokud například zpracovává osobní údaje pro účel sjednání pracovního poměru pracovní smlouvou, jedná se o nezbytnost pro splnění smlouvy. Tento právní titul je plně zákonný a není třeba vyžadovat souhlasu se zpracováním osobních údajů. Naopak, pokud by v tomto případě souhlas vyžadován byl, jednalo by se o protiprávní jednání.

Takto lze usuzovat i v dalších vyjmenovaných právních titulech. Právní titul splnění právní povinnosti se vztahuje na povinnosti uložené veřejnoprávními předpisy, při kterých je nutno osobní údaje zpracovávat. V takovýchto případech taktéž není relevantní souhlas nositele osobních údajů.

Právní titul ochrany životně důležitých zájmů lze spojit se situací krajní nouze a měl by být využit v případě, kdy nelze z objektivních důvodů využít jiného právního titulu. Jako příklad uvádí autor Nulíček „*zpracování osobních údajů oběti nehody, která nedokáže dát souhlas*“[29].

Právní titul zaměřující se na úkoly ve veřejném zájmu je spojen primárně s činnosti orgánů veřejné moci. Pro příklad lze uvést správní řízení, evidence živnostenských oprávnění, evidence motorových vozidel, činnosti zastupitelstev.

Právní titul oprávněný zájem považuje autor Nulíček za jeden z nejflexibelnějších právních titulů. Jak už právní titul naznačuje, musí být zájem správce považován skutečně za oprávněný a tento zájem nesmí být převážen zájmy a základními právy dotčeného nositele

[29] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 132

osobních údajů. Vzhledem k této limitaci doporučuje autor Nonnemann „*provést test přiměřenosti (balanční test), při kterém správce zváží, jak silný je jeho zájem*“[30] v poměru k zásahu do práv dotčených osob při daném zpracování osobních údajů. „*Zpracování lze provádět tehdy, je-li tento zásah přiměřený“*[31]. Jako příklad uvádí autor Nonnemann problematiku kamerového zařízení ve veřejně přístupných prostorách, kdy je legitimním oprávněným zájmem správce například ochrana majetku, ale pro přiměřenost zásahu je třeba „*věnovat pozornost nastavení kamer, aby monitorovaly přístupné prostory v nezbytném rozsahu“*[32]. Úřad pro ochranu osobních údajů provádění balančního testu stanovuje povinně ve svém vyjádření: „*Správce je povinen provést balanční test, neboli test proporcionality, pro každé zpracování osobních údajů, které hodlá vykonávat na základě právního důvodu oprávněného zájmu“*[33].

Zákonné zpracování osobních údajů může být založeno taktéž na souhlasu subjektu osobních údajů se zpracováním. Obecné nařízení získávání takového souhlasu velmi limituje a stanovuje požadavky, za kterých lze souhlas přijmout jako legitimní. V článku 4 bodu 11) se rozumí „*souhlasem subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“*[34]. Z uvedené definice vyplývá, že subjekt údajů by měl sám jednoznačně projevit souhlas, bez jakéhokoliv nátlaku nebo negativních důsledků, pokud souhlas neudělí. Zároveň je třeba souhlas vymezit konkrétním účelem nebo účely a subjekt osobních údajů musí být přesně informován o všech skutečnostech, týkajících se dotčeného zpracování osobních údajů tak, aby se mohl svobodně rozhodnout. Společně s účelem zpracování osobních údajů je třeba konkrétně vymezit i dobu, po kterou bude souhlas udělen. Subjekt údajů má právo kdykoliv udělený souhlas odvolat, v takovém případě pozbývá správce právního titulu ke zpracování předmětných osobních údajů a je povinen učinit jejich výmaz. Než se správce přikloní k zajištění souhlasu, je vhodné se nejprve přesvědčit, zda pro zamýšlený účel

[30] NONNEMANN,F., *Praktická příručka GDPR*, s. 34
[31] NONNEMANN,F., *Praktická příručka GDPR*, s. 34
[32] NONNEMANN,F., *Praktická příručka GDPR*, s. 34
[33] Úřad pro ochranu osobních údajů, https://www.uoou.cz/pravni-duvody-zpracovani/d-27318/p1=3938
[34] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), článek 4, bod 11

nelze použít jiný právní titul pro zpracování osobních údajů. Jak uvádí autor Nulíček: *„Souhlas by měl být využíván pouze v případech, kde není možné využít jiný právní titul.“*[35]

Se zásadou zákonnosti úzce souvisí zásada účelového omezení, neboť od účelu zpracování osobních údajů se odvíjí právní důvod zpracování osobních údajů. Tato zásada má zajistit, aby byly osobní údaje zpracovávány jen pro jasně předem určené účely a nebyly používány k dalším účelům, které jsou s původním účelem neslučitelné. Autor Nezmar neslučitelnost demonstruje na příkladu, kdy „*obvodní lékař zpřístupní seznam pacientů manželce, která provozuje cestovní kancelář, aby mohla nabídnout speciální dovolenou šitou na míru pacienta, který potřebuje rehabilitaci.*“ [36] Účel nabídky speciální dovolené je neslučitelný s účely, pro které obvodní lékař osobní údaje získal.

Účelové omezení se úzce pojí se zásadou minimalizace údajů, neboť ke stanovenému účelu je třeba zpracovávat osobní údaje v nezbytném rozsahu. Lze zde hovořit o určité přiměřenosti rozsahu údajů, kdy je třeba důkladně posoudit, zda požadované údaje jsou pro daný konkrétní účel opravdu potřebné a nezbytné. Zásada se dotýká jak rozsahu zpracování osobních údajů, tak doby jejich uložení a jejich dostupnosti. Doba uložení je určena buď zvláštním předpisem, nebo ji správce stanovuje sám, v takovém případě je vhodné pro soulad s obecným nařízením dané uschovací lhůty odůvodnit. Autor Nonnemann pro takové případy nabízí nápovědu na příkladu „*běžného obchodního vztahu a dobu uschování během trvání smluvního vztahu a po jeho skončení až do uplynutí obecné tříleté promlčecí lhůty dle občanského zákoníku*.“ [37]

Zásada transparentnosti a korektnosti

Tyto zásady nejsou přímo obecným nařízením definovány. Jsou však spojovány s povinností poskytování informací, jako je tomu v recitálu 39, který mimo jiné říká: „*zásada transparentnosti vyžaduje, aby všechny informace a všechna sdělení týkající se zpracování osobních údajů, byly snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků“*[38]. Recitál 58 obecného nařízení

[35] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 164
[36] NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 57
[37] NONNEMANN,F., *Praktická příručka GDPR*, s. 44
[38] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

požadavek transparentnosti navazuje taktéž na poskytování informací nositelům osobních údajů a na poskytování informací určených veřejnosti. Požadavky zmíněné v recitálu 39 doplňuje o „*stručnou podobu informací a ve vhodných případech* o *vizualizační formu podávané informace*, dále stanovuje, *že informace určené veřejnosti mohou být poskytovány v elektronické podobě.*“[39] Korektností lze chápat „správný, společensky přijatelný“ popis zpracování osobních údajů.

K pochopení zásady transparentnosti je nutno se zastavit u jednotlivých pojmů uvedených výše v recitálu 39 a recitálu 58:

Stručnou a transparentní informací je chápána informace jednoduchá, nepřehlcená, odlišená od informací ostatních.

Srozumitelnost informace spočívá v jejím pochopení cílovou skupinou. Pracovní skupina WP 29 směřuje zjištění srozumitelnosti k úrovni průměrného člena cílové skupiny. Správce osobních údajů zřejmě velmi těžko dokáže posoudit míru průměrnosti, vodítkem proto může být spíše charakter cílové skupiny jako takové, což lze demonstrovat na příkladu uváděném autorem Nulíčkem, kdy „*výrobce a prodejce zdravotních a kompenzačních pomůcek pro nevidomé a slabozraké poskytuje na svých webových stránkách informace o zpracování osobních údajů také v audio podobě.*“[40] Srozumitelnosti v této cílové skupině je dosaženo adekvátním způsobem – zvolenou audio formou.

Snadná přístupnost informace je zajištěna tehdy, pokud adresát nemusí informaci dlouze vyhledávat, čehož lze dosáhnout například přímo poskytnutou informací v listinné podobě nebo odkazem na umístění elektronicky zpracované informace.

Použití jednoduchých jazykových prostředků lze spatřovat v poskytnutí informace co nejjednodušším způsobem. Jak uvádí autor Nulíček, měl by se správce „*vyvarovat dlouhých komplexních souvětí a neměl by využívat právnického jazyka.*“[41] „*Neměly by být používány abstraktní a víceznačné pojmy, které dávají prostor pro odlišné výklady“*[42], jak naznačuje pracovní skupina WP 29 ve svém pokynu.

(obecné nařízení o ochraně osobních údajů), recitál 39

[39] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), recitál 58

[40] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 192

[41] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 193

[42] PRACOVNÍ SKUPINA ZŘÍZENA PODLE ČLÁNKU 29 - *Pokyny k transparentnosti podle nařízení 2016/679 přijaty dne 29. listopadu 2017 ve znění naposledy revidovaném a přijatém dne 11. dubna 2018*, s. 9

Zásada přesnosti

Zásada přesnosti je spatřována ve zpracování pouze přesných a aktuálních osobních údajů. Pro správce osobních údajů tato zásada znamená, že pokud se věrohodným způsobem dozví, že zpracovávané osobní údaje nejsou přesné, aktuální, je povinen je opravit nebo vymazat. Pro subjekt osobních údajů je zásada přesnosti aplikována pro zajištění práva na opravu údajů. Je nutno připomenout, že některé právní předpisy přímo ukládají subjektu osobních údajů povinnost nahlášení změn osobních údajů některým správcům osobních údajů. Za příklad lze zde uvést povinnost pojištěnce ve vztahu ke zdravotní pojišťovně.

Zásada integrity a důvěrnosti

Osobní údaje lze klasifikovat jako důvěrná sdělení, která musí být patřičně chráněna a zabezpečena před jejich zneužitím. Od tohoto pojetí lze odvinout zásadu integrity a důvěrnosti, která je promítána právě do zabezpečení zpracování osobních údajů a ochrany osobních údajů samotných. Správce je povinen učinit taková opatření organizačního a technického charakteru, která vytvářejí integrovaný, nebo-li ucelený a propojený systém ochrany osobních údajů a bezpečného zpracování osobních údajů. Volba bezpečnostních prvků by měla odpovídat povaze zpracovávaných osobních údajů a možným škodným následkům při zneužití, náhodné ztrátě nebo náhodným zničením. Příkladem bezpečnostních prvků je šifrování dat, pseudonymizace dat, kamerové systémy, zabezpečovací systémy, heslování přístupu a jiné.

3.4 Práva subjektů osobních údajů

Ve svém recitálu 2 hovoří obecné nařízení o „*respektování základních práv a svobod fyzických osob, zejména právu na ochranu osobních údajů*“[43]. Proto staví jako důležitou součást zpracování osobních údajů posílení práv subjektů osobních údajů. Vedle práva nového na přenositelnost údajů, upravuje ostatní subjektivní práva podrobněji. Správci a zpracovatelé jsou obecným nařízením povinováni k výkonu těchto subjektivních práv

[43] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), recitál 2

závaznými pravidly a postupy, které již byly naznačeny formou zásad. Lze tak na tomto místě připomenout povinnost informovanosti stručným, transparentním, jednoduchým a snadno přístupným způsobem. Postupy zásadou transparentnosti naplňují základní právo na informace.

Právo na informace

Právo na informace zahrnuje povinnost správce poskytnout subjektu osobních údajů přesné a pravdivé informace o zpracování dotčených osobních údajů jeho nositele. Nařízení definuje, které minimální informace je správce povinen subjektu údajů sdělit, a to ve svém článku 13 v případě, že osobní údaje jsou získány od subjektu údajů, a v článku 14 v případě, že osobní údaje nebyly získány od subjektu údajů. Ve shrnutí těchto dvou článků lze konstatovat, že správce poskytne subjektu údajů informace o totožnosti správce a jeho kontaktních údajích, případně taktéž o totožnosti pověřence pro ochranu osobních údajů a jeho kontaktu, dále účely zpracování a jejich právní základy, v případě účelu zpracování na základě oprávněných zájmů správce nebo třetí osoby poskytne informace o těchto oprávněných zájmech. Další minimální informací je případný úmysl správce předat dotčená osobní data do třetí země a právní podklad předání. Informaci o kategorii dotčených osobních údajů je poskytována v případě, že osobní údaje nebyly získány od subjektu údajů. Nepostačuje-li tento minimální obsah informací a je-li to nezbytné pro zajištění spravedlivého a transparentního zpracování, poskytne správce subjektu osobních údajů další informace, z nichž lze jmenovat dobu uložení údajů, informaci o existenci subjektivních práv, skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, a jiné.

S tímto právem je nutno úzce spojit právo na přístup k osobním údajům, neboť jak hovoří článek 15 Obecného nařízení, „ *subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům.“* [44] Rozsah poskytnutých informací již byl zmíněn v předchozím odstavci. Právo na přístup k osobním údajům zahrnuje taktéž poskytnutí kopie zpracovávaných osobních údajů. V předmětném článku obecného nařízení není patrno, zda se jedná o povinnost správce poskytnout subjektu údajů kopie

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

zpracovávaných osobních údajů pokaždé a okamžitě nebo v jen v případě, pokud o to subjekt požádá. Obecné nařízení hovoří o žádostech za další kopie v souvislosti „*s účtováním poplatků za tyto další kopie, kdy se předpokládají administrativní náklady s tímto úkonem spojené"*[45]. Lze tak usuzovat, že první kopie musí být poskytovány zdarma. Vzhledem k tomu že kopie zpracovávaných osobních údajů, jak uvádí autor Nonnemann, se vztahují „ *ke všem údajům, které správce o dané osobě zpracovává, ke všem účelům a ke všem právním důvodům, na jejichž základě tak správce činí"*[46], může se jednat o obsáhlý soubor kopií, bude-li se jednat například o personální a mzdové záležitosti. V souvislosti s právem na přístup informací autor Žůrek hovoří o frekventované otázce poskytnutí záznamu z kamerového systému či záznamu telefonického hovoru, kdy konstatuje, že „*subjekt osobních údajů má právo získat kopii osobních údajů, což evokuje i kopie kamerového záznamu zachycující subjekt údajů či telefonního rozhovoru se subjektem údajů.*"[47]

Ve spojitosti s právem získat kopii osobních údajů obecné nařízení klade podmínku, že „*nesmějí být tímto právem nepříznivě dotčena práva a svobody jiných osob*."[48] Správce tak bude muset v některých případech činit určitá opatření, jak například zmiňuje autor Žůrek v situaci poskytnutí kamerového záznamu, kde „*není vyloučena anonymizace záznamů, aby nebyly vidět zaznamenané jiné osoby.*"[49]

Před poskytnutím přístupu k osobním údajům by měl správce ověřit identitu žadatele o přístup k osobním údajům za „*využití všech vhodných opatření.*"[50] Není definováno, co je myšleno vhodnými opatřeními, zda může či nemůže správce požadovat ověření identity žadatele předložením občanského průkazu nebo zda a jaké musí volit jiné prostředky k tomuto úkonu.

---

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

[46] NONNEMANN,F., *Praktická příručka GDPR*, s. 52

[47] ŽŮREK, J., *Praktický průvodce GDPR*, s. 130

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

[49] ŽŮREK, J., *Praktický průvodce GDPR*, s. 131

[50] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v jed souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), recitál 64

Právo na opravu a doplnění

Toto právo lze přiřadit k zásadě přesnosti. Mají-li být osobní údaje přesné, je třeba v případě potřeby učinit jejich opravu nebo je doplnit. Potřebnost opravy či doplnění se odvíjí od stanoveného účelu zpracování osobních údajů. V tomto smyslu se nejedná o automatické časové revize osobních údajů. Spíše je zde předpokladem aktivita subjektu osobních údajů, který tímto správce informuje o nepřesnosti či neúplnosti svých osobních údajů a správce je povinen zareagovat a nejdéle do jednoho měsíce údaje ve své databázi opravit či doplnit. Vždy se bude jednat o osobní údaje aktuálně zpracovávaná, Jak uvádí autor Nulíček, „ *historická data není nutné zpětně měnit*“.[51]

Právo na výmaz („právo být zapomenut“)

Toto právo je spojeno se situací, kdy subjekt osobních údajů požádá správce o výmaz svých osobních údajů, které správce doposud zpracovával. Správce má k naplnění tohoto práva povinnost dotčené osobní údaje odstranit, ale pouze za předpokladu, že osobní údaje již „*nejsou potřebné pro účely, pro které byly zpracovávány, již pominul právní důvod zpracování nebo byl odvolán souhlas, na základě kterého byly osobní údaje zpracovávány. Dále se může jednat o situaci protiprávního zpracování osobních údajů*“[52]. Článek 17 Obecného nařízení hovoří taktéž o výmazu osobních údajů, které byly shromažďovány v souvislosti s nabídkou služeb informační společnosti. Obecné nařízení stanovuje situace, v kterých i přes žádost subjektu údajů k výmazu nedojde, pokud je zpracování pro tyto situace nezbytné. Zde je třeba zmínit především výkon a obhajobu právních nároků, dále veřejný zájem v oblasti ochrany zdraví, v oblasti vědeckého a historického výzkumu a pro statistický účel, a dále v oblasti práva na svobodu projevu a informace. Autor Žůrek připomíná, že „ *i samotná likvidace osobních údajů je operací zpracování, za kterou správce odpovídá.*“[53]

Právo na omezení zpracování

Toto právo subjekt osobních údajů uplatní v případech, pokud je zpochybněna přesnost osobních údajů a je požadována jejich oprava nebo subjekt vznesl námitku proti

[51] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 227
[52] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 17
[53] ŽŮREK, J., *Praktický průvodce GDPR*, s. 133

zpracování. K omezení zpracování dojde i za situace, kdy již sice pominul účel zpracování, ale subjekt osobních údajů je potřebuje pro výkon nebo obhajobu právních nároků. V takovém případě bude mít správce dotčené osobní údaje uložené, což je samo o sobě operace zpracování, a nebude je nadále pro žádný jiný účel zpracovávat. Osobní údaje jsou tím v omezeném zpracování. Autor Žůrek k tomuto připomíná definici omezeného zpracování v obecném nařízení, které omezeným zpracováním rozumí „*označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu*.“[54] Lze tak dovodit, že osobní údaje omezené ve zpracování musí být k tomuto označeny nebo jak napovídá recitál 67, „*přesunuty do jiného systému, znepřístupněny uživatelům, tak aby nemohly být prováděny další zpracovatelské operace*“[55]

Omezené zpracování se předpokládá vždy na omezenou dobu, jde tedy o dočasný stav, dokud nebudou dány podmínky pro standardní zpracování osobních údajů nebo nedojde k naplnění podmínek pro likvidaci osobních údajů.

Právo vznést námitku

Obecné nařízení dává subjektu osobních údajů možnost vznést námitku proti zpracování. Jedná se o situace, kdy, jak uvádí autor Nezmar, „ *konkrétní osoba nedostane možnost uplatnit některé ze svých práv, třeba právo na výmaz.*“ [56] Námitku může subjekt osobních údajů vznést proti zpracování osobních údajů, které je nezbytné pro splnění úkolů ve veřejném zájmu nebo výkonu veřejné moci, dále které je nezbytné pro účely oprávněných zájmů správce či třetí strany, dále pokud jsou osobní údaje zpracovávány pro účely přímého marketingu, a to včetně profilování ve všech případech.

Po dobu, než správce prokáže závažné oprávněné důvody pro zpracování, bude se jednat o omezené zpracování. V každém případě musí správce námitku posoudit. V případě zpracování za účelem oprávněných zájmů správce nebo třetí osoby je správce povinen, jak uvádí autor Nonnemann „*znovu provést balanční test, kterým je poměřována váha*

[54] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 4; ŽŮREK, J., *Praktický průvodce GDPR,* s. 134

[55] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), recitál 67

[56] NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 91

oprávněného zájmu a přiměřenost zásahu do jejich práv.“[57] V případě, že byla vznesena námitka proti zpracování za účelem přímého marketingu, obecné nařízení přímo stanovuje požadavek dále osobní údaje nezpracovávat.

Právo na přenositelnost údajů

Toto právo je novým právem, které obecné nařízení předkládá. Lze uplatnit v případech, kdy subjekt poskytl své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu a zpracování osobních údajů je založeno na souhlasu nebo pro plnění smlouvy a je prováděno automatizovaně. Nápovědou poskytnutých osobních údajů subjektem, na které by mohlo být uplatněno právo na přenositelnost údajů, dle autora Žůrka ve vodítku pracovní skupiny WP29 mohou být například „*údaje z GPS aplikace o pohybu uživatele, historie vyhledávání nebo naměřené zdravotní hodnoty prostřednictvím chytrého zařízení*“.[58] Jak shrnuje autor Nonnemann, cílem tohoto nového práva je „ *usnadnit mobilitu služeb, především v prostředí internetu*.“[59] Z toho je patrno, že se jedná o prostředí informačních technologií, čemuž napovídá i další podmínka technické proveditelnosti přenosu údajů. Otázkou je, zda všichni správci disponují takovým technickým vybavením, který by přenos osobních údajů ve strukturovaném a strojově čitelném formátu umožňoval. Z tohoto pohledu autor Nulíček odkazuje na výzvu v recitálu 68 obecného nařízení „*směřující na správce, kteří by měli rozvíjet interoperabilní řešení, která umožní a zjednoduší přenositelnost osobních údajů*.“[60] Interoperabilita je zde významově vysvětlena jako „*schopnost interakce různých nesourodých organizací, která přispívá k dosažení vzájemně prospěšných a dohodnutých společných cílů a zahrnuje sdílení informací a znalostí mezi organizacemi pomocí podnikových procesů, které tyto organizace podporují, na základě výměny údajů mezi jejich systémy IKT*.“[61]

Je vhodné zde připomenout hledisko bezpečnosti. Rizikovost přenosu údajů může být spatřována jednak směrem od subjektu osobních údajů ke správci, a dále směrem od jednoho správce ke druhému. V tomto smyslu autor Žůrek upozorňuje na obavu stávajících správců z možného úniku dat, za který by stávající správce byl odpovědný a byl by

[57] NONNEMANN,F., *Praktická příručka GDPR*, s. 61
[58] ŽŮREK, J., *Praktický průvodce GDPR*, s. 138
[59] NONNEMANN,F., *Praktická příručka GDPR*, s. 60
[60] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 244
[61] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 244-245

„*prvním podezřelým z porušení zabezpečení ochrany osobních údajů*“[62], pokud by neprokázal, že únik nenastal na jeho straně. Obecné nařízení zřejmě nepředpokládá, že by se nový správce bránil přijetí přenesených údajů. Touto záležitostí se nezabývá. Lze tak usoudit, že nový správce může příjem přenesených dat odmítnout a v rámci zásady transparentnosti odmítnutí zdůvodnit.

Právo nebýt předmětem automatizovaného rozhodnutí, včetně profilování

Jak vyplývá z popisu tohoto práva, bude se toto právo dotýkat pouze automatizovaného zpracování osobních údajů a to za předpokladu, že má automatizované rozhodování pro subjekt osobních údajů právní či obdobné účinky. Volně přiblíženo se jedná o stavy, kdy o situaci jedince rozhoduje počítačový program bez lidského faktoru. Typickým příkladem je profilování zákazníků firmy nebo klientů finanční instituce., kdy jsou automatizovanými procesy subjekty rozděleny do nastavených profilů. Mezi typické způsoby profilování řadí autor Nezmar například „*rozhodnutí o solventnosti, hodnocení pracovního výkonu, zjištění místa pohybu.*“[63] Právo nebýt předmětem automatizovaného rozhodnutí dává subjektu osobních údajů možnost opětného posouzení situace správcem, a to přímo jeho zaměstnancem. Toto právo nelze použít, pokud je automatizované rozhodnutí přípustné, neboť je nezbytné k uzavření nebo plnění smlouvy, je založeno na výslovném souhlasu subjektu údajů, nebo které je povoleno za splnění vhodných opatřeních v rámci evropského nebo národního práva. Takovou výjimkou je automatizované individuální rozhodování „*pro účely monitorování podvodů a daňových úniků a jejich předcházení.*“[64]

3.5 Omezení práv a zásad zpracování

Práva a povinnosti, vztahující se ke zpracování osobních údajů a jejich ochraně, mohou být evropským nebo národním právem dle článku 23 obecného nařízení v některých případech omezena, zejména v souvislosti se zajištěním národní a veřejné bezpečnosti a obrany státu, v souvislosti s ochranou nezávislosti soudnictví, v souvislosti s odhalováním a stíháním trestných činů.

[62] ŽŮREK, J., *Praktický průvodce GDPR,* s. 140
[63] NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 93
[64] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 259

3.6 Proces naplnění souladu zpracování osobních údajů s obecným nařízením

Zajištění souladu zpracování osobních údajů s obecným nařízením je odpovědností správce osobních údajů, jak vyplývá přímo s ustanovení článku 24 odst. 1 obecného nařízení, které povinuje správce „ *s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavést 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 revidována a aktualizována.*“[65] Jak je z textu patrno, je třeba vnímat realizaci naplnění souladu s obecným nařízením jako soubor činností a opatření. Autor Nezmar doporučuje přistoupit k procesu celé realizace „*formou projektového řízení a realizaci rozplánovat do několika postupných kroků*“[66]

3.6.1 Vnitřní analýza

První krok spatřuje autor Nezmar v provedení analýzy, která „*definuje rozdíl mezi stavem stávajícím a stavem požadovaným*“[67], to znamená, jakými procesy probíhalo zpracování osobních údajů doposud a co je třeba změnit, aby byly splněny všechny požadavky obecného nařízení. Analýza se proto dotýká souhrnně jak samotných osobních údajů, tak procesů zpracování, právních titulů, zabezpečení osobních údajů listinných i elektronicky zpracovávaných, přenosů osobních údajů, kontroly smluvních závazků týkajících se osobních dat a předávání osobních údajů třetím stranám. Analýza se musí zaměřit na všechny organizační úseky, které se dostávají do kontaktu s osobními údaji. Analyzovat je třeba „*veškeré dokumenty upravující zpracování osobních údajů, vnitřní směrnice, smlouvy s dodavateli apod.“*[68]

„*Zpráva o provedené analýze by měla přehledně obsahovat zjištěné nálezy a doporučení, měla by umožnit identifikovat rizika a problémy, které vyžadují řešení a měla by*

[65] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 24, odst.1
[66] NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 96
[67] NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 96
[68] BOGNÁROVÁ,V., *GDPR 2018 v praxi, Sborník vzorů a návodů pro mzdové účetní a personalisty*, s.40

identifikovat všechny oblasti, kde je zapotřebí akce k dosažení souladu s obecným nařízením“.[69]

Následující kroky nutně vedou k zajištění všech nutných opatření, která vyplynula z analýzy a která jsou nutná k zajištění souladu zpracování osobních údajů s Obecným nařízením.

3.6.2 Záznamy o činnostech zpracování

Obecné nařízení ve svém článku 30 ukládá správci povinnost vést záznamy o činnostech zpracování. Autorka Kohútová považuje záznamy o činnostech zpracování „*za základní složku interní administrativy z pohledu obecného nařízení, neboť tyto záznamy mohou sloužit jako výchozí bod pro orientaci ve zpracování.*“[70] Obecné nařízení požaduje v záznamech uvést údaje související se zpracováním osobních údajů, a to zejména „*identifikaci a kontakt správce a pověřence pro ochranu osobních údajů, dále účely zpracování, kategorie subjektů osobních údajů, kategorie osobních údajů a příjemců, a dále informace o předání osobních údajů do třetí země.*“[71] Povinnost vést záznamy o činnostech zpracování dopadá taktéž na zpracovatele osobních údajů, obsahově v užším rozsahu oproti správci, nicméně nesmí chybět zejména „*identifikace a kontakt zpracovatele a pověřence pro ochranu osobních údajů, dále kategorie zpracování pro správce, a taktéž informace o případném předání osobních údajů do třetí země.*“[72] Jak uvádí autor Žůrek, „*velká část informací ze záznamů o činnostech zpracování se kryje s informacemi poskytovanými subjektu údajů, mohou proto být tyto záznamy vhodným podkladem i pro výkon práv subjektů údajů, především pokud jde o právo k přístupu k informacím.*“[73]

Povinnost vést záznamy o činnostech zpracování není poplatná pro všechny správce a zpracovatele. Výjimku z této povinnosti mají podniky a organizace, které „*zaměstnávají méně než 250 zaměstnanců, a jejichž zpracování osobních údajů nepředstavuje riziko pro práva dotčených subjektů osobních údajů, jejich zpracování osobních údajů lze považovat*

[69] NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 96

[70] *Metodické aktuality Svazu účetních 4/2018,* s.17

[71] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 30

[72] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 30

[73] ŽŮREK, J., *Praktický průvodce GDPR*, s. 158

za příležitostné a nezpracovávají zvláštní kategorii osobních údajů, ani nezpracovávají osobní údaje týkající se trestných činů a rozsudků v trestních věcech"[74]. Pro názornost tohoto pojetí vynětí z povinnosti vést záznamy o činnostech zpracování lze uvést příklad „*vedení personální agendy u správce, který zaměstnává 200 osob, zpracování osobních údajů pro pracovněprávní účely není považováno za rizikové*"[75], lze tedy uplatnit výjimku. Pokud však tato organizace s 200 zaměstnanci zpracovává v rámci „*své hlavní činnosti informace o zdravotním stavu*"[76], nelze výjimku uplatnit, neboť zpracovává zvláštní kategorii osobních údajů.

Správci a zpracovatelé, na které se vztahuje výjimka z povinnosti vést záznamy o činnostech zpracování, mohou vést tyto záznamy zcela dobrovolně, neboť jak již bylo zmíněno, mohou sloužit jako orientační a podkladová pomůcka ve zpracování osobních údajů.

3.6.3 Posouzení vlivu na ochranu osobních údajů

Tomuto institutu je třeba se věnovat v kontextu s pravděpodobným vysokým rizikem pro práva subjektů osobních údajů. „*Rizikem lze rozumět popis určité události a jejích důsledků společně s odhadem její závažnosti a pravděpodobnosti*"[77]. Smyslem posouzení je identifikovat a zhodnotit rizika pro práva a svobody subjektů osobních údajů, která mohou vznikat nebo vznikají při zpracování osobních údajů. Jak uvádí Evropský sbor pro ochranu osobních údajů (dříve pracovní skupina WP29) ve svém pokynu, „*odkaz na „práva a svobody" subjektů údajů se především týká práv na ochranu údajů a soukromí, může však také zahrnovat jiná základní práva, jako např. svobodu projevu, svobodu myšlení, svobodu pohybu, zákaz diskriminace, právo na svobodu, svědomí a náboženské vyznání"*[78]. O posouzení vlivu na ochranu osobních údajů lze v této souvislosti hovořit jako o určitém řízení rizik nebo-li„ *souboru koordinovaných činností určených k řízení a omezení rizika v*

[74] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 30

[75] ŽŮREK, J., *Praktický průvodce GDPR*, s. 158 - 159

[76] NONNEMANN,F., *Praktická příručka GDPR*, s. 64

[77] Úřad pro ochranu osobních údajů, *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, s. 7

[78] Úřad pro ochranu osobních údajů, *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, s. 7

určité organizaci“[79], jak ostatně naznačuje Obecné nařízení ve svém článku 35 věnovaném obsahu posouzení, kde hovoří o „*systematickém popisu zamýšlených operací, posouzení nezbytnosti a přiměřenosti operací, posouzení rizik a plánovaných opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatřeních a mechanismů k zajištění ochrany osobních údajů*“[80].

Nejčastěji se bude povinnost posouzení vlivu plnit v případech, kdy se jedná o systematické a rozsáhlé vyhodnocování osobních aspektů subjektů osobních údajů automatickým rozhodováním, jakým je např. „*posuzování platební historie zájemce o úvěr*“[81], nebo v případě systematického monitorování veřejně přístupných prostorů, jakým je např. „*městský kamerový systém*“[82]. Taktéž při zpracování zvláštní kategorie osobních údajů je třeba se na provedení posouzení vlivu na ochranu osobních údajů zaměřit. Zde lze uvést příklad „*nemocničního informačního systému, kde dochází ke zpracování genetických a zdravotních údajů pacientů.“*[83]

Důležitou úlohu zde má pověřenec pro ochranu osobních údajů, neboť je-li jmenován, správce jej žádá o „*posudky, a to zejména v otázkách, zda posouzení provádět, jakou metodiku zvolit, jaká opatření přijmout, zda je posouzení provedeno správně*“.[84]

3.6.4 Předchozí konzultace s dozorovým úřadem

Povinnost předchozí konzultace s dozorovým úřadem vychází následně ze zjištění provedené posouzení vlivu na ochranu osobních údajů. Povinnost se na správce vztahuje tehdy, pokud je závěrem posouzení vlivu na ochranu osobních údajů, že zpracování má za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika, a dále za situace, že i přesto, že opatření přijme, je zde možnost „zbytkového“ vysokého rizika. Předchozí konzultace s dozorovým úřadem je taktéž povinná pro situaci, kdy správce nemůže identifikovatelné vysoké riziko žádnými opatřeními odstranit.

---

[79] Úřad pro ochranu osobních údajů, *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679*, s. 7

[80] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 35, odst. 7

[81] NONNEMANN,F., *Praktická příručka GDPR*, s. 79

[82] NONNEMANN,F., *Praktická příručka GDPR*, s. 79

[83] Úřad pro ochranu osobních údajů, *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679*, s. 13, NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 105

[84] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 350

3.6.5 Pověřenec pro ochranu osobních údajů

Důležitost pověřence pro ochranu osobních údajů lze odvodit z úkolů, k jejichž výkonu je obecným nařízením pověřen. Jak hovoří článek 39 Obecného nařízení, „*poskytuje pověřenec informace a poradenství ve zpracování osobních údajů, monitoruje soulad zpracování s Obecným nařízením, je kontaktní osobou pro dozorový úřad, s kterým spolupracuje"*[85]. Správci a zpracovatelé se mohou na pověřence obracet se všemi záležitostmi týkajícími se zpracování osobních údajů, ať ve věcech klasifikovaných jako běžných nebo ve věcech, které správcům a zpracovatelům činí obtíže nebo si nejsou jisti se správností výkladu či posouzení. Na pověřence lze v této souvislosti pohlížet jako na nezávislého kvalifikovaného odborníka zastřešující soulad zpracování osobních údajů s obecným nařízením u jednotlivých správců a zpracovatelů, u kterých je jmenován. Povinnost jmenovat pověřence pro ochranu osobních údajů nedopadá na všechny správce a zpracovatele. Dle článku 37 Obecného nařízení jej musí jmenovat takoví správci a zpracovatelé, kteří se zabývají „*rozsáhlým zpracováním zvláštních kategorií osobních údajů nebo rozsáhlým a systematickým monitorováním subjektů údajů, a dále orgány veřejné moci a veřejné subjekty s výjimkou soudů jednajících v rámci své soudní pravomoci*".[86] Zpracovatelé a správci, kteří k tomuto institutu nejsou povinováni, se mohou rozhodnout o dobrovolném jmenování pověřence. V pozici pověřence pro ochranu osobních údajů se vždy musí jednat o osobu „*s dostatečnou znalostí práva a praxe zpracování osobních údajů*".[87]

3.6.6 Kodexy chování

Každé odvětví má ve zpracování osobních údajů svá specifika. Jak hovoří obecné nařízení ve svém článku 40, jsou „*podporovány kodexy chování, které mají přispět k řádnému uplatňování tohoto nařízení s ohledem na povahy různých odvětví provádějících*

[85] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 39

[86] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 37

[87] NONNEMANN,F., *Praktická příručka GDPR*, s. 139

zpracování“[88]. Je tak dána možnost zástupcům určitých odvětví zpracování těchto kodexů, které upřesňují jednotlivá pravidla obecného nařízení s ohledem na specifika daného odvětví. Každý kodex musí být schválen dozorovým úřadem, který posoudí, zda jsou kodexová pravidla chování v souladu s obecným nařízením. Přijetím kodexu chování správcem či zpracovatelem se tento kodex stává pro správce a zpracovatele závazným a tím i, jak uvádí autor Nulíček, „*se správce a zpracovatel podřizuje dalšímu kontrolujícímu subjektu, který dohlíží na dodržování kodexu chování*“.[89] Kontrolováním dodržování kodexu chování je zde myšleno monitorování schválených kodexů chování dle článku 41 obecného nařízení prováděné akreditovaným subjektem. Tím však není dotčena pravomoc dozorového orgánu v oblasti zpracování osobních údajů, kterým je v České republice Úřad pro ochranu osobních údajů. Monitoring se, dle článku 41 obecného nařízení, netýká zpracování prováděného orgány veřejné moci a veřejnými subjekty.

Ministerstvo práce a sociálních věcí má uveřejněn kodex chování aplikovatelný pro poskytovatele sociálních služeb, v poloze, jak je v dokumentu uvedeno, „*doporučeného metodického postupu, který bude řízen a aktualizován MPSV*“[90] Z uvedeného lze usoudit, že se nejedná o kodex chování schválený dozorovým úřadem. Ministerstvo práce a sociálních věcí dále, v dokumentu, uvádí, že „*auditní činnost prováděná v systému výkonu sociální politiky bude podrobně zpracována po ustálení výkladové praxe a především po ustavení dozorového úřadu, který bude mít kompetenci vydávat podmínky udělení osvědčení pro ochranu osobních údajů a zavádění pečetí a známek dokladujících ochranu údajů pro účely prokázání souladu s nařízením GDPR*“[91]. Je zde poukazováno na potřebu akreditace již výše zmíněných kontrolních subjektů.

[88] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 40

[89] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 385

[90] MPSV, *Doporučený postup č. 02/2018, kterým se v rámci metodického a koncepčního vedení MPSV vypracovává Kodex chování ve smyslu čl. 40 Obecného nařízení o ochraně osobních údajů – GDPR pro potřeby výkonu sociální politiky*, s. 29

[91] MPSV, *Doporučený postup č. 02/2018, kterým se v rámci metodického a koncepčního vedení MPSV vypracovává Kodex chování ve smyslu čl. 40 Obecného nařízení o ochraně osobních údajů – GDPR pro potřeby výkonu sociální politiky*, s. 29

3.6.7 Zabezpečení osobních údajů a jeho porušení

Zabezpečení osobních údajů nelze vnímat jako nový požadavek obecného nařízení, neboť samotné zabezpečení by mělo pro správce a zpracovatele být samozřejmostí od samého počátku zpracování osobních údajů i před nabytím účinnosti obecného nařízení. V důsledku problémů s úniky informací, ať již vzniklými samotným lidským faktorem nebo kybernetickými hrozbami, klade obecné nařízení na bezpečnost osobních údajů daleko větší důraz. V této souvislosti ukládá správcům a zpracovatelům osobních údajů obecné nařízení povinnosti k zajištění maximální možné bezpečnosti osobních údajů. Každý správce a zpracovatel je povinen zhodnotit možná rizika a „*provést adekvátní technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku*“[92]. V přístupu posuzování rizik je třeba se zaměřit nejen na zabezpečení IT systémů, ale taktéž, jak uvádí autor Nulíček, na „*lidský faktor, fyzické prostředí, ve kterém jsou systémy umístěny, a nakonec na bezpečnost, kterou poskytují při zpracování nejrůznější subdodavatelé a obchodní partneři správce či zpracovatele*.“[93]

Je zde spojitá linka s posouzením vlivu na ochranu osobních údajů, neboť jsou řešena rizika a souvislá bezpečnostní opatření. Autor Žůrek hovoří v souvislosti s digitálně zpracovávanými daty o „*zavedení mechanismů zjišťování neoprávněného přístupu či nestandardních činností v síti, samozřejmé aktualizace bezpečnostních opatření a přezkušování jejich funkčnosti“*[94]. Nabízí zde jako možný vhodný prostředek takzv. penetrační test pro zjištění slabin zabezpečení. Směrem k lidskému faktoru upozorňuje autor Žůrek na možné „*podceňování proškolení zaměstnanců z hlediska IT zabezpečení“*[95]. Jak sám uvádí, „*řádným proškolením a upozorněním na různá aktuální rizika lze významně předejít bezpečnostní hrozbě“*[96].

I přes všechna opatření může dojít k porušení zabezpečení osobních údajů. Obecné nařízení vykládá „*porušením zabezpečení osobních údajů porušení zabezpečení, které vede*

[92] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 32

[93] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 315
[94] ŽŮREK, J., *Praktický průvodce GDPR*, s. 93
[95] ŽŮREK, J., *Praktický průvodce GDPR*, s. 94
[96] ŽŮREK, J., *Praktický průvodce GDPR*, s. 94

k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů."[97]
Pro tuto situaci má obecné nařízení povinnostní postupy. Předně je správce povinen bez zbytečného odkladu, pokud možno do 72 hodin od doby, kdy se o porušení zabezpečení osobních údajů dozvěděl, toto porušení dozorovému úřadu nahlásit. Dále musí správce porušení zdokumentovat, a představuje-li porušení vysoké riziko pro subjekt údajů, je povinen tento subjekt informovat, pokud nezavedl náležitá technická a organizační opatření a tato opatření nebyla použita. Určení míry rizika autor Nezmar krátce objasňuje: „*Při určování míry rizika je nutné vycházet z kategorie osobních údajů, které byly porušením zabezpečení dotčeny. Vyšší riziko budou vždy představovat zvláštní kategorie osobních údajů (např. údaje o zdravotním stavu), případně údaje, jimiž lze způsobit subjektu údajů újmu či zásah do jeho práv (např. únik přihlašovacích údajů do elektronického bankovnictví)".*[98]
Autor Nulíček upozorňuje na rozlišení porušení zabezpečení a bezpečnostního incidentu. Jak uvádí, „*všechna porušení zabezpečení jsou zároveň bezpečnostními incidenty, ne všechny bezpečnostní incidenty představují zároveň porušení zabezpečení, protože se nemusejí týkat osobních údajů (např. únik obchodního tajemství)*"[99].

Zbývá zde připomenout, že všechna opatření se jednoznačně musí vztahovat nejen na osobní údaje elektronicky zpracovávané, ale i na osobní údaje v listinné podobě.

3.6.8 Předávání osobních údajů do třetích zemí

Tato problematika je řešena v obecném nařízení jako „*specifická část s vlastními instituty a pravidly, do kterých navíc velmi intenzivně vstupují evropské soudy*"[100].
Třetími zeměmi jsou zde myšleny země mimo prostor Evropské unie. Předávání je zpracovatelskou operací a je třeba na tuto operaci pohlížet pravidly zpracování osobních údajů, především učinit opatření k ochraně osobních údajů. V této souvislosti uvádí autor

[97] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), čl. 4

[98] NEZMAR, L., *GDPR: Praktický průvodce implementací*, s. 41
[99] NULÍČEK, M., *GDPR/Obecné nařízení o ochraně osobních údajů, praktický komentář,* s. 320
[100] NONNEMANN,F., *Praktická příručka GDPR*, s. 141

Nonnemanno „*ověření, zda se v konkrétním případě jedná o tzv. bezpečnou zemi dle rozhodnutí Evropské komise, vyjednání standardních smluvních doložek nebo zdokumentování a schválení tzv. závazných podnikových pravidel*.“[101]

Výčet třetích zemí, hodnocených jako bezpečné, zveřejňuje Evropská komise na svých webových stránkách a průběžně jej, na základě hodnocení, aktualizuje. Je zde vhodné se krátce zmínit o vnitropodnikových pravidlech. Jak uvádí autor Žůrek, jsou „*primárně určena pro velké skupiny podniků, u nichž dochází k opakovanému vzájemnému předávání*“ [102]osobních údajů. Pravidla musí stanovovat podmínky v souladu s obecným nařízením, s použitím zásad pro zpracování osobních údajů. Pravidla mohou být použita, jsou-li schválena nejen dozorovým úřadem, ale taktéž, jak uvádí autor Žůrek, Evropským sborem pro ochranu osobních údajů.

[101] NONNEMANN,F., *Praktická příručka GDPR*, s. 140
[102]ŽŮREK, J., *Praktický průvodce GDPR*, s. 148

4 Vlastní práce

Pro vlastní práci je vybrán subjekt, jehož hlavní činností je poskytování sociálních služeb. Subjekt je příspěvkovou organizací zřízenou územně samosprávným celkem.

4.1 Rozsah a charakteristika osobních údajů

Velikostně odpovídá organizace rozsahu do 100 zaměstnanců a do 100 uživatelů služby. Organizace je správcem osobních údajů. Zpracovatele osobních údajů v současné době nevyužívá.

Organizace zpracovává osobní údaje:

- zaměstnanců a jejich rodinných příslušníků,
- uživatelů, kterým poskytuje sociální služby a jejich rodinných příslušníků,
- obchodních partnerů,
- ostatních, které nelze podřadit pod výše uvedené.

Organizace má zpracovány identifikace zpracování, které poskytují informace o:

- vstupu informace,
- správci,
- subjektu údajů,
- právním základu zpracování,
- zda se jedná o zvláštní kategorii osobních údajů, identifikátorech (osobní údaje),
- použitých technických a organizačních opatřeních,
- uložení osobních údajů,
- době zpracování,
- odpovědné osobě za zpracování a organizačním útvaru a
- případné poznámky k identifikaci.

Z jednotlivých identifikací zpracování lze shrnout následující rozsah zpracování:

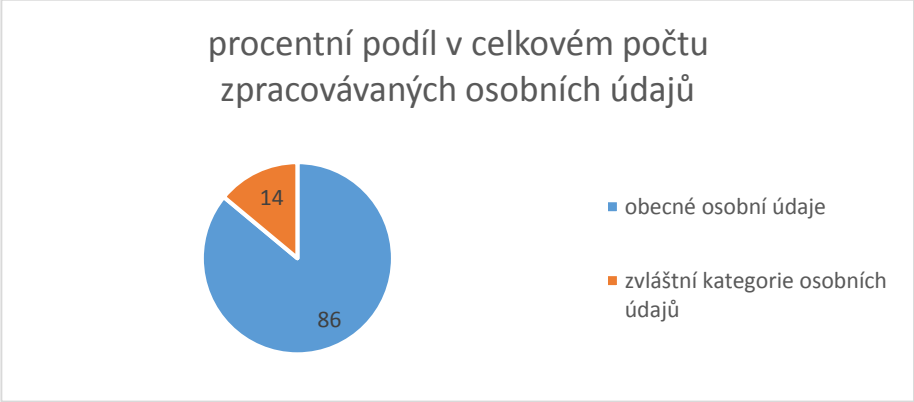
- zaměstnanecké osobní údaje- jméno a příjmení, titul, osobní zaměstnanecké číslo, datum narození, místo narození, rodné příjmení, rodné číslo, rodinný stav, bydliště, státní příslušnost, služební telefonní kontakt, služební kontaktní e-mail, plat,

dosažené vzdělání a kvalifikace, fotografie; u rodinných příslušníků se jedná o jméno a příjmení, rodné číslo, bydliště,

- osobní údaje uživatelů, kterým je poskytována sociální služba - jméno a příjmení, titul, datum narození, místo narození, rodné příjmení, rodné číslo, bydliště, státní příslušnost, zdravotní stav včetně diagnózy, biometrické údaje, příjem, fotografie**;** u rodinných příslušníků jméno a příjmení, titul, telefonní číslo, kontaktní e-mail, bydliště; u zákonných zástupců jméno a příjmení a bydliště,
- osobní údaje obchodních partnerů – jméno a příjmení, titul, kontaktní telefonní číslo, kontaktní e-mail,
- osobních údaje ostatních – jméno a příjmení

V následujícím grafu je procentuálně vyjádřen rozsah zpracovávaných osobních údajů obecných a osobních údajů zařazených do zvláštní kategorie osobních údajů.

Graf č. 1 Procentní vyjádření kategorií zpracovávaných osobních údajů na celkovém rozsahu



Zdroj: data od organizace, zpracování vlastní

Z grafu je patrná převaha zpracování obecných osobních údajů, které tvoří 86 % z celkového rozsahu. Do zvláštní kategorie osobních údajů, které tvoří 14 % z celkového rozsahu, lze přiřadit zdravotní stav uživatelů sociální služby včetně diagnózy, biometrické údaje uživatelů sociální služby a fotografie uživatelů sociální služby a zaměstnanců.

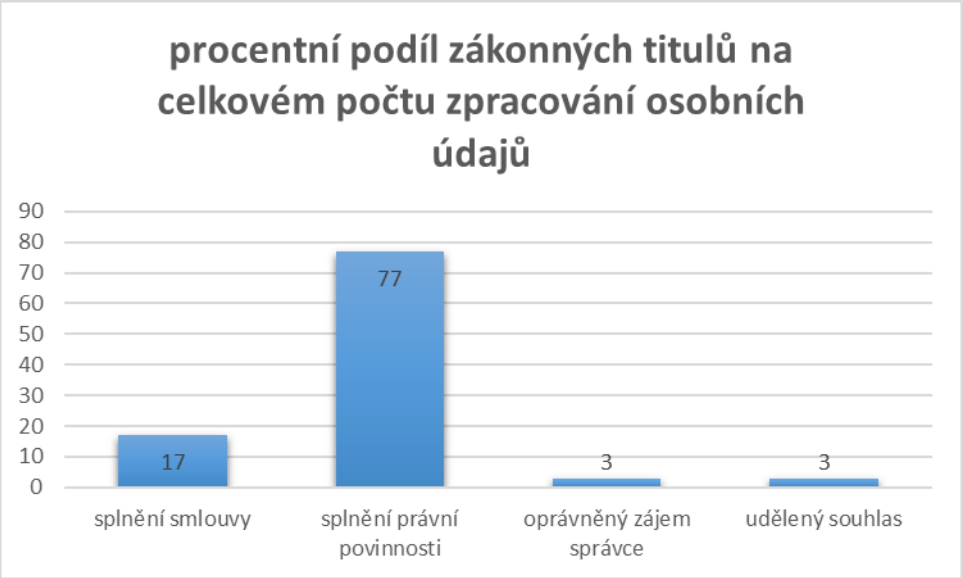
4.2 Zákonné tituly ve zpracování osobních údajů

Ve spojitosti se stanovenými účely zpracování jednotlivých osobních údajů jsou vysledovány zákonné prováděné zpracování:

- nezbytné pro splnění smlouvy,
- nezbytné pro splnění právní povinnosti,
- nezbytné pro účely oprávněných zájmů správce,
- na základě uděleného souhlasu subjektem osobních údajů pro jeden či více konkrétních účelů.

Procentní vyjádření jednotlivých zákonných titulů znázorňuje následující graf.

Graf č. 2 Procentní podíl zákonných titulů



Zdroj: data od organizace, zpracování vlastní

Graf ukazuje s největším procentním podílem 77 % zákonný titul splnění právní povinnosti, v 17 % jde o zákonný titul splnění smlouvy, 3 % náleží zákonnému titulu oprávněného zájmu a 3 % náleží zákonnému titulu souhlasem.

Splnění právní povinnosti je v této organizaci směrováno k vlastnímu fungování organizace, dále směrem k zaměstnanecké oblasti a směrem k uživatelům sociální služby.

Z výčtu zákonných norem lze uvést např.:
Zákon č. 563/1991 Sb., o účetnictví
Zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů
Zákon č. 320/2001 Sb., o finanční kontrole
Zákon č. 89/2012 Sb, občanský zákoník
Zákon č. 262/2006 Sb., zákoník práce
Zákon č. 108/2006 Sb., o sociálních službách
Zákon č. 372/2011 Sb., o zdravotních službách
Zákon č. 101/2000 Sb., o ochraně osobních údajů a NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů

Zákonný titul nezbytnosti pro splnění smlouvy je v organizaci směrován v oblasti zaměstnanecké k pracovním smlouvám a dohodám mimo pracovní poměr, v oblasti klientské ke smlouvě o poskytování sociálních služeb, v oblasti dodavatelsko-odběratelských vztahů k dodavatelským smlouvám a objednávkám.

Oprávněným zájmem je pokryt etický kodex externích pracovníků v rozsahu jména a příjmení. Jedná se o pracovníky bezpečnostní agentury, stážisty, apod. Správce zdůvodňuje oprávněný zájem nutností dodržování etického kodexu, a to vzhledem ke kategorii uživatelů sociálních služeb, a potřebnost dokladování, že se dotčený pracovník skutečně seznámil s etickým kodexem, potažmo s pravidly chování ve vztahu k uživatelům sociálních služeb. Odkaz na dodržování pravidel je součástí standardů. Zpracování standardů a jejich používání, dle sdělení, vychází ze zákona o sociálních službách. Tím je možná klasifikace právního titulu splnění právní povinnosti. Pro tuto situaci nemá organizace jasné rozhodnutí, zda se může přiklonit k zákonnému titulu splnění právní povinnosti.

Oprávněným zájmem dále správce pokrývá zpracování osobních údajů příjmení a jména v knize návštěv, a dále kamerový systém. Knihu návštěv odůvodňuje účelem ochrany osob a majetku, kdy má kniha sloužit při případném zjišťování pohybujících se osob. Za účelem ochrany osob a majetku je zaveden i kamerový systém v monitorování vnějších a vnitřních společných prostor. Nejsou monitorovány osobní zóny uživatelů ani zaměstnanců.

Kamerový systém není určen k soustavnému monitorování. Monitorování probíhá on-line, k záznamům mají oprávněný přístup 4 osoby včetně ředitele organizace za dodržení pravidla, že je přístup k záznamu po řádném odůvodnění schválen ředitelem organizace a je řádně zdokumentován protokolem. Do záznamů lze vstoupit jen 5 dní, poté jsou záznamy smazány. Záznamy nelze zvlášť uchovávat. Dle sdělení v současné době k přístupu k záznamu nedošlo.
O kamerovém systému byla předána informace jednak ústně zaměstnancům a uživatelům sociální služby. Písemná informace je uvedena s piktogramem u všech vchodů do areálu i samotných budov v rozsahu, že je objekt monitorován kamerovým systémem.

Uděleného souhlasu je využíváno v oblasti zaměstnanecké zatím pouze pro potvrzení o příjmu, které žádá zaměstnanec vyplnit a následně toto potvrzení předává finanční instituci. Vzhledem k tomu, že organizace si tyto potvrzení uchovává v kopii po stanovenou dobu, kdy si finanční instituce ověřuje sdělené údaje, je třeba udělení souhlasu zaměstnance. Každý takovýto souhlas je konkretizovaný, zaměstnanec je informován o svých právech v ochraně osobních údajů. Taktéž je určen jedinečný kód, pro komunikaci finanční instituce se mzdovým pracovníkem pro případ ověřování údajů. Toto opatření organizace praktikuje v rámci ochrany osobních údajů při telefonické komunikaci, kdy dochází k ověření platových sdělení. Ostatní osobní údaje, vyskytující se v potvrzení o příjmu, organizace telefonicky nepotvrzuje. Ke dni skončení sjednané doby uchování kopie potvrzení, je tato kopie skartována, čímž dochází k výmazu osobních údajů pro účel potvrzení o příjmu. Následně je informace o výmazu osobních údajů poskytnuta písemnou formou zaměstnanci. Dle sdělení byl tento souhlas uplatněn v pěti případech, z toho pouze v jednom došlo k popsanému ověření ze strany finanční instituce.

Uděleného souhlasu využívá organizace dále k pořízení fotografií zaměstnanců a uživatelů z různých akcí, pořádaných pro uživatele sociální služby. Fotografie jsou umísťovány na facebookovské stránce jako prezentace činnosti organizace (poskytovatele sociálních služeb). Souhlasy jsou opětně konkretizovány na danou akci, udělený souhlas v takovémto případě je na dobu jednoho roku. K výmazu a skartaci, vzhledem ke sjednané době, zatím nedošlo.

4.3 Výkon práv subjektů osobních údajů

Organizace zatím nemá zkušenost s řešením situace, kdy by byla požádána nositelem osobních údajů o kopie zpracovávaných osobních údajů nebo byla požádána o výmaz osobních údajů, a muselo být omezeno zpracování. Taktéž zatím nebyly řešeny situace vznesení námitky a požadavku na přenositelnost údajů. Prakticky byly řešeny případy v zaměstnanecké oblasti, kdy zaměstnanci nahlašovali změnu příjmení, změnu rodinného stavu, změnu bydliště, změnu zaměstnání manžela v daňových záležitostech. Osobní údaje byly opraveny v elektronickém systému na základě písemného oznámení zaměstnance, které zároveň bylo uloženo v listinné podobě do osobní složky. V daňové záležitosti změnu vepsal sám zaměstnanec do daňového prohlášení, tak, jak stanovuje právní norma.

Organizace nepoužívá při zpracování osobních údajů automatického rozhodování ani profilování.

4.4 Vnitřní analýza a opatření z analýzy plynoucí

Realizaci nastavení zpracování osobních údajů dle podmínek obecného nařízení předcházelo mnoho přípravných kroků. K ochraně osobních údajů měla organizace nastaveny určité postupy, bylo však zapotřebí zhodnotit, zda jsou dostatečné a nastavit takové, které budou odpovídat požadavkům obecného nařízení. Pro zjištění stavu byla provedena vnitřní analýza odbornou společností, kterou tímto úkolem organizace pověřila.

Vstupní informace ke zmapování rozsahu připravovalo pět zaměstnanců. V rámci popisu osobních údajů se soustřeďovala data o tom, s jakými osobními údaji se pracuje, kdo je zpracovává, kde jsou uložena, na základě jakého zákona, kde se s nimi pracuje (např. počítač, informační systém, apod.), zda a kam jsou přenášena, kde a jak dlouho jsou uložena.

Náhled, jak se připravovala vstupní popisová data, poskytuje následující tabulka.

Tabulka č. 1 – Náhled popisu osobních údajů

ZDROJ	KATEGORIE OSOBNÍCH ÚDAJŮ	PŘÍKLAD	ZPRACOVATEL ZAMĚSTNANEC /EXTERNÍ	LOKACE ULOŽENÍ	SOUVISEJÍCÍ AKTIVA	ZÁKONNÝ DŮVOD	DOBA UCHOVÁNÍ
stávající zaměstnanc-měsíční výkaz	jméno, příjmení, osobní číslo		zaměstnanec	IS, papírová forma v kanceláři xx	tiskárna	zákonná potřeba dle zákoníku práce č.262/2006 Sb.	dle spisového řádu
výpis z rejstříku trestů	jméno a příjmení, rodné příjmení, datum narození, RČ	přímá péče	zaměstnanec xx přijme, zaměstnanci xx předává	osobní složka zaměstnance kancelář xx	písemná forma, předává registrátorovi na krajský úřad	zákonná potřeba,uzavírání prac.poměru	po dobu prac.poměru, poté se vrací zaměstnanci,případná okamžitá skartace
ORP poukazy	jméno, příjmení, titul, rodné číslo, datum narození, zdravotní stav-diagnozy, léčba, doporučení, zdravotní pojišťovna	klienti-vykazování výkonu pojišťovnám	vedoucí sestra, její zástupce, NLZP,ošetřující lékař, zdravotní pojišťovna	IS,dokumentace v kartotéce, ordinující lékař ve své dokumentaci	tiskárna, scanner, pC program lékaře, portály pojišťoven	zákon o zdrav.službách, vyhláška o zdrav.dokumentaci,zákon o veřejném zdrav.pojištění	v rámci archivační doby zdravotnické dokumentace, minim.10 let,
žádost o poskytování soc.služby	jméno a příjmení		zaměstnanec xx	IS, papírová forma v kanceláři xx	tiskárna, scannner, e-mail	zákonná potřeba uzavírání smluv dle zákona 108/2006	po dobu pobytu,při ukončení pobytu dle spis.řádu

Zdroj zpracování: organizace, úprava: vlastní, identifikace místností a příjmení zaměstnanců anonymizovány

Ze zpracovaného popisu údajů mimo jiné vyplynulo, že některé osobní údaje mohou být zpracovávány nadbytečně. Organizace musela proto prověřit nezbytný rozsah osobních údajů. Odpovědní pracovníci hodnotili, zda osobní údaje jsou k dotčenému účelu potřebné, a na základě těchto hodnocení docházelo k postupné minimalizaci osobních údajů.

Příkladově, kde tomu tak došlo, je u žádosti o poskytnutí sociální služby, která je požadována za účelem zaevidování případného zájemce o poskytování sociální služby dle zákonného předpisu. Vzhledem k tomu, že se jedná o potenciálního uživatele sociální služby, osobní údaj čísla občanského průkazu, státní příslušnosti, národnosti ani zdravotní pojišťovny, není pro stanovený účel potřebný. Proto tyto osobní údaje byly ze žádosti vyjmuty a za uvedeným účelem se nezpracovávají.

Další příklad lze uvést v případě předkládání životopisů, kdy není nutno uvádět datum narození, ani rodné číslo, není nutno uvádět věk a stačí jen jeden kontaktní údaj. K tomuto mají vedoucí pracovníci pokyn, že pokud budou v životopise tyto uvedené osobní údaje, bude uchazeč o zaměstnání informován o jejich výmazu. Životopis se po ukončení

výběrového řízení neuschovává, dochází k jeho skartaci a výmazu elektronické podoby, o čemž je uchazeč informován.

K prověření nezbytnosti údajů došlo i u dokumentů, které jsou organizaci předávány, jako je tomu např. u dokladů o absolvování odborných seminářů. Doposud bylo zvyklostí ze strany školících organizací uvádět na osvědčení o absolvování semináře jméno a příjmení zaměstnance a jeho datum narození. Tyto doklady organizace v kopiích uchovává. Osobní údaj datum narození je organizací vyhodnocen jako nepřiměřený, proto požaduje tato osvědčení vystavovat bez osobního údaje datum narození. Dle sdělení se ve dvou případech přesto tento osobní údaj na osvědčeních vyskytl, musel být proto před uschováním anonymizován.

Zároveň popis údajů podal přehled, jaké kategorie osobních údajů jsou zpracovávány. V procesu prověření nezbytného rozsahu došlo k minimalizaci zvláštní kategorie osobních údajů. Konkrétně byl zrušen přístup ke stravovacímu systému zaměstnanců (přihlašování a odhlašování obědů) pomocí otisku prstu, který byl vyhodnocen jako nepřiměřený. Dále byl učiněn výmaz fotografií zaměstnanců a uživatelů sociální služby z webové stránky, neboť se na fotografiích objevovaly osoby, které již nejsou v zaměstnaneckém poměru, ani nejsou uživateli sociální služby, jejich souhlas s uveřejněním by byl obtížně realizovatelný.

Organizace dále prověřovala přístupová uživatelská práva, pro jednotlivé činnosti zpracování prováděné přímo v organizaci a při předávání orgánům veřejné moci. Z tohoto pohledu nebylo třeba dalších úprav, neboť již byly přístupy k informačním systémům, které jsou v organizaci využívány, stanoveny, a taktéž byly stanoveny zmocněné osoby k předávání údajů, jak to vyplývá z jejich náplní práce. K informačním systémům lze přistupovat pouze pomocí přístupových hesel, která jsou pro každého oprávněného jedinečným, tozn. že k systémům nemůže přistoupit nikdo, kdo nemá jedinečné přístupové heslo.

Organizace si dále mapovala, jaké má zavedeny bezpečnostní prvky. V dlouhodobé koncepci se zaměřuje na IT bezpečnost, pravidelně dochází k revizím bezpečnostních bodů a k jejich potřebné obnově. V tomto ohledu organizace nečinila žádná zvláštní nová opatření, pouze došlo k pravidelné aktualizaci počítačové infrastruktury, kdy byla

provedena inventarizace počítačových stanic s přiřazením uživatelů a uživatelských licencí a obnově bezpečnostních IT prvků, včetně zálohovacího zařízení, a taktéž zabezpečenému přístupu na centrální tiskárně.

Dlouhodobě má organizace nastavena opatření k bezpečnému elektronickému předávání dokumentů s osobními údaji dotčeným orgánům veřejné moci. Využívá datovou schránku a zabezpečených portálů s přístupem osobních certifikátů, kde dochází k přenosu pouze zašifrovaných dat. Tyto dvě formy jsou nastaveny prioritně. E-mailové předávání není standardní, pokud k němu dojde, je nastavena povinnost předávané dokumenty heslovat.

Bezpečnostní opatření byla zkontrolována i při používání služebních mobilních telefonů. U každého služebního mobilního telefonu byla zkontrolována přítomnost heslovaného přístupu, případně bylo přístupové heslo doplněno.

Pro ochranu listinných dokumentů je zajištěno bezpečnostní kódování místností. Pozornost věnovala organizace i zabezpečení listinných dokumentů uvnitř místností tam, kde pracují zaměstnanci v nesourodých pracovních pozicích. Dlouhodobě má organizace zabezpečenu personální a mzdovou agendu a sociální agendu v uzamykatelných skříňkách. V důsledku změn dispozic kanceláří musela organizace toto opatření doplnit u nových nábytkových vybavení.

Ve spolupráci s odbornou společností se uskutečnilo školení pro zaměstnance organizace, ve kterém byli zaměstnanci seznámeni se:

- základními pojmy a právními normami týkající se ochrany osobních údajů,
- důvody zavedení ochrany osobních údajů,
- historií a vývojem evropské legislativy v oblasti ochrany osobních údajů,
- co nového přináší obecné nařízení ve srovnání se zákonem č. 101/2000 Sb., o ochraně osobních údajů,
- definicí osobních údajů ze strany obecného nařízení,
- principem odpovědnosti správce,
- novými nástroji pro ochranu osobních údajů,
- principy obecného nařízení (zákonnost/korektnost/transparentnost/omezení účelu/minimalizace/přesnost/integrita a důvěrnost),

- oprávněním ke zpracování (souhlas/smlouva/oprávněný zájem/zákonná povinnost),
- právy subjektů osobních údajů (právo na informaci/námitku/výmaz/omezení zpracování/přenositelnost).

Z rozhovorů se zaměstnanci vyplynulo, že školení vnímají jako obecné, informační, že bylo prezentováno mnoho informací a nejsou si jisti, zda všemu dostatečně porozuměli.

Pro zajištění informovanosti byl odbornou společností vytvořen dokument o zpracování osobních údajů, který má organizace stále uveřejněn na své webové stránce.
Dokument informuje:

- správci,
- zabezpečení dat,
- dále informace o právech subjektů osobních údajů kam se obrátit s dotazy
- a informace o webových stránkách.

Stávající zaměstnanci byli informováni na školení věnovaném ochraně osobních údajů, které je výše již uvedeno. Informováni o zpracování osobních údajů jsou noví zaměstnanci při jednání o pracovněprávním vztahu a noví uživatelé sociální služby při jednání o poskytování sociální služby.
Informace je taktéž poskytnuta na žádosti o poskytování sociální služby. Jako mírně problematické shledává organizace poskytování informací uživatelům sociální služby. Do poskytování informací zapojil sociální pracovníky, kteří vedou rozhovory a vysvětlují uživatelům obsah informací, v písemné podobě volí větší písmo k přečtení. Zatím se nepodařilo informaci vyjádřit v grafických znacích, které by více uživatelům sociální služby přiblížily podstatu podávané informace. Nyní organizace uvažuje o zpracování předávat informaci taktéž zvukovým záznamem.

Nastaven je v organizaci dlouhodobě spisový řád, který stanovuje pravidla pro archivaci a skartaci dokumentů. Tento řád se zaměřuje na listinnou formu dokumentů. Elektronicky zpracovávané údaje se nearchivují na zvláštní média, jsou po době účelovosti přesunuty do archivu přímo v daném informačním systému.

Pro zdokumentování zpracovávaných osobních údajů organizace vytvořila identifikace zpracování. O identifikaci zpracování je zmiňováno v kapitole 4.1 Rozsah a charakteristika osobních údajů.

Následující tabulka poskytuje na příkladu zpracování smlouvy o poskytování sociální služby zjednodušený náhled, jak jsou informace o zpracování strukturována.

Tabulka č. 2 – Struktura identifikace zpracování

Identifikace zpracování	
název zpracování - SMLOUVA O POSKYTOVÁNÍ SOCIÁLNÍ SLUŽBY	
FORMÁT VSTUPU INFORMACÍ DO ORGANIZACE	žádost o poskytování sociální služby
SPRÁVCE: xxxxxx	ZPRACOVATEL: ne
SUBJEKT OSOBNÍCH ÚDAJŮ	uživatel
PRÁVNÍ ZÁKLAD PRO ZPRACOVÁ	plnění smlouvy
	zákonná povinnost
ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ	ne
IDENTIFIKÁTORY	jméno a příjmení
	datum narození
	bydliště
ZABEZPEČENÍ	ANO
fyzické	ANO uzamčeno, elektronicky zabezpečno
elektronické	přístup do IS na základě oprávnění
ULOŽENÍ OSOBNÍCH ÚDAJŮ	
IS elektronicky	ANO
tištěné	uzamčený prostor
KDE SE DATA NACHÁZEJÍ	kancelář xxx
	IS xxx
DOBA ZPRACOVÁNÍ	po dobu poskytování sociální služby, po ukončení poskytování 10 let
ODPOVĚDNÁ OSOBA ZA ZPRACOVÁNÍ, ÚSEK	sociální pracovník, sociální úsek
POZNÁMKY	sociální složka uživatele

Zdroj zpracování: organizace, úprava: vlastní, identifikace místností a IS anonymizovány

V identifikacích zpracování se v některých případech objevuje více zákonných titulů, jako je tomu ve znázorněném příkladu. Je zde uváděn jak zákonný titul plnění smlouvy, tak zákonný titul právní povinnost (v tabulce jako zákonná povinnost).

Další dokumentací jsou pro osobní údaj zdravotní stav a osobní údaj biometrické údaje (tlak, tepová frekvence), které jsou zařazeny do zvláštní kategorie osobních údajů, zpracované záznamy o činnostech.

Záznam vypovídá:

- o činnosti zpracování, to znamená, zda jde o činnost při přijetí, při zavedení ošetřovatelského plánu, apod.,
- o subjektu osobních údajů, kterého se týká,
- za jakým účelem je osobní údaj zpracován, zda pro identifikaci cílové skupiny sociální služby, zda pro stanovení ošetřovatelských úkonů, apod.,
- komu je předáván, zda lékaři, zdravotnímu personálu,
- jaká je doba uložení, respektive kdy může dojít k výmazu
- jaká jsou technická opatření, to znamená, zda je v listinné podobě, zda je v elektronické podobě a v jaké databázi,
- jaká jsou bezpečnostní a organizační opatření, to znamená, jak jsou zabezpečena oprávněným přístupem do databáze a jak jsou zabezpečena v listinné podobě.

Záznam o činnostech zpracování je zpracován taktéž pro zavedený kamerový systém, neboť je vyhodnocen, že by mohl představovat riziko pro práva a svobody subjektu údajů. Jedná se sice o on-line formu, ale jde o nepřetržitý provoz. Oproti předchozímu záznamu je zde vyloučena informace o konkrétní činnosti zpracování.

Následující tabulka poskytuje náhled na zpracovaný záznam o činnostech zpracování pro kamerový systém.

Tabulka č. 3 – Záznam o činnostech zpracování – kamerový systém

ZÁZNAM O ČINNOSTECH ZPRACOVÁNÍ	**KAMEROVÝ SYSTÉM**
SPRÁVCE	XXXXX
ÚČEL ZPRACOVÁNÍ	Ochrana majetku správce, života a zdraví osob prostřednictvím stálého kamerového systému.
PRÁVNÍ DŮVOD	Oprávněný zájem správce
POPIS KATEGORIE SUBJEKTU ÚDAJŮ	Zaměstnanci, uživatelé sociální služby,příležitostně vstupující osoby do monitorovaného prostoru (dodavatelé, návštěvy, cizí pracovníci).
POPIS KATEGORIE OSOBNÍCH ÚDAJŮ	Podoba a obrazové informace o chování a jednání zaznamenaných osob
INFORMACE POSKYTOVANÉ SUBJEKTŮM ÚDAJŮ	u vstupu do areálu a u všech vchodů do budovy
PŘÍJEMCI OSOBNÍCH ÚDAJŮ	V odůvodněných případech orgány činné v trestním řízení, vedoucí zaměstnaci, případně jiné zainteresované subjekty pro naplnění účelu zpracování (pojišťovna).
PŘEDÁNÍ OSOBNÍCH ÚDAJŮ DO TŘETÍCH ZEMÍ	Není prováděno.
LHŮTA PRO VÝMAZ OSOBNÍCH ÚDAJŮ	Doba uchování záznamu je 5 dní. Záznam zachyceného incidentu je uchován po dobu nezbytnou pro projednání případu a pro právní ochranu.
TECHNICKÁ A ORGANIZAČNÍ BEZPEČNOSTNÍ OPATŘENÍ	On-line provoz. Bezpečnostní kryt, řízený přístup k datům, školení oprávněných osob, vedení záznamů o předání nahrávek oprávněným orgánům a osobám.
POZNÁMKA	Kamerový systém není systematicky sledován a vyhodnocován.

Zdroj zpracování: organizace, úprava: vlastní, identifikace správce anonymizována

V porovnání identifikace zpracování a záznamu o činnostech lze vysledovat podobnou strukturu informací.

Posouzení vlivu na ochranu osobních údajů organizace zatím zpracováno nemá. Organizace vychází ze skutečnosti, že prováděné zpracování osobních údajů není rozsáhlé na regionální, celostátní ani nadnárodní úrovni, ani nedochází k systematickému a rozsáhlému hodnocení osobních aspektů na základě profilování. Jak bylo sděleno, v rámci oborových setkání je diskutováno o různých stanoviscích k tomuto tématu. Nyní jsou v organizaci posuzovány materiály dostupné na webových stránkách Úřadu pro ochranu osobních údajů. Je zvažována konzultace u odborné společnosti.

Taktéž pověřenec pro ochranu osobních údajů zatím není jmenován. Zde je vycházeno z faktu, že pro povinnost jmenovat pověřence pro ochranu osobních údajů neexistuje jednoznačné stanovisko. Organizace tak očekává, zda bude v dohledné době vydáno závazné stanovisko, ale zároveň zvažuje možnost přistoupit ke jmenování pověřence pro ochranu osobních údajů dobrovolně. Náklad na pověřence pro ochranu osobních údajů nemá organizace pro tento rok rozpočtován, zatím zjišťuje v jaké cenové relaci je možno zajistit pověřence pro ochranu osobních údajů externě formou dodávky služby. Úvahu o zajištění pověřence pro ochranu osobních údajů vlastním zaměstnancem organizace zamítla s tím, že stávající zaměstnanci, kteří by mohli činnosti pověřence provádět, osobní údaje zpracovávají, což je neslučitelné s výkonem práce pověřence pro ochranu osobních údajů, a dále již nemají ani volný časový fond ve stávajících pracovních činnostech.

Vzhledem k tomu, že zatím není pro odvětví sociálních služeb závazný kodex chování, nedisponuje s ním ani tato organizace sociálních služeb.
Při sběru dat a v rozhovoru s pracovníkem organizace bylo diskutováno o doporučeném postupu Ministerstva práce a sociálních věcí, který, jak bylo popsáno v teoretické části, zatím není závazným kodexem, ale je možno se k němu přihlásit.

K předávání osobních údajů do třetích zemí v organizaci nedochází, proto nejsou k tomuto žádné dokumenty zpracovány.

4.5 Aktualizace stavu

V současné době je organizace ve fázi, kdy monitoruje nastalé změny a aktualizuje postupy. Od počátečního stavu došlo k personálním změnám, přístupu ke standardům, ke změně počítačového vybavení.

Bezpečnostní technické prvky již má sladěny. Nyní dojde ke změně informačního klientského systému, bude třeba opětně projít moduly s jednotlivými přístupovými právy, zda se nebudou vyskytovat některé osobní údaje v nepřiměřené míře.

Změna nastala taktéž v právních normách zabývající se zdravotnickou dokumentací, i toto nyní prochází kontrolou.

5 Výsledky a diskuse

5.1 Zhodnocení teoretických vstupů

V teoretické části je analyzován evropský právní předpis o ochraně osobních údajů se zaměřením na nosné prvky tohoto nařízení.
Není zde zohledněna nová vnitrostátní úprava, tzv. adaptační zákon. Důvodem toho, že právní předpis není zapojen do teoretické části, je skutečnost, že doposud nedošlo k jeho schválení, není tedy platnou a účinnou právní normou.

Rozpor je znatelný u obecného právního předpisu – zákona č. 101/2000 Sb., o ochraně osobních údajů. Na svém webovém portálu uvádí Úřad pro ochranu osobních údajů informaci: „*Obecným právním předpisem ochrany osobních údajů je zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (účinné znění, obsah), který od 25. května 2018 byl nahrazen GDPR a v budoucnu i českým adaptačním zákonem*“[103]. Ve Sbírce zákonů nebylo nalezeno žádné zrušovací či nahrazovací ustanovení. Z prezentace na webovém portálu Úřadu pro ochranu osobních údajů se jeví zákon č. 101/2000 Sb. jako platný. Tuto skutečnost lze podpořit ustanovením o dozorovém úřadu. Obecné nařízení ukládá členským státům stanovit dozorový úřad. Jediný právní předpis, který dozorový úřad stanovuje je právě jmenovaný zákon č. 101/2000 Sb., o ochraně osobních údajů.

Lze tak konstatovat, že není v současnosti právní jednotnost.

V systému evropského práva je nařízení nejsilnějším právním aktem sekundárního práva Evropské unie a jako takové má obecnou platnost a je závazné pro všechny členské státy, aniž by členské státy přijímaly opatření na státní úrovni, je nadřazeno národní právní úpravě. Je tedy platné tak, jak je formulováno a vnitrostátní úprava je možná jen tam, kde jí k tomu nařízení dává prostor.

Stejné je tomu u obecného nařízení o ochraně osobních údajů, které dává v mnoha případech podnět k vnitrostátní úpravě, která může některé požadavky a některá pravidla zpřesnit či doplnit a upravit, nastavit odchylky, případně omezit práva a povinnosti. Zde je

[103] Úřad pro ochranu osobních údajů, https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=1257&n=pravni-predpisy&p1=1257

možno jmenovat úpravy v oblasti zpracování zvláštní kategorie osobních údajů, v oblasti výzkumných a statistických účelů, v oblasti svobody projevu a informací, zvláště novinářského, v oblasti zpracování osobních údajů zaměstnanců, nastavení věku dítěte pro udělení souhlasu se službami informačních společností. Lze usuzovat, že adaptační zákon může upravit pravidla a podmínky pro zpracování osobních údajů v mnoha odvětvích.

Je třeba zde ještě upozornit na skutečnost, že návrh vnitrostátní legislativní normy, než bude dán ke schválení parlamentu, má být konzultován s dozorovým úřadem. Lze tak usuzovat, že má být konzultován i každý pozměňovací návrh adaptačního zákona, čímž se může schvalovací proces dále prodlužovat.

5.1.1 Zhodnocení dopadů na organizaci sociálních služeb

Pojetí ochrany osobních údajů dle obecného nařízení je obecně uspořádáno pro všechny typy a druhy správců a zpracovatelů osobních údajů. Zohledněná možná specifika odvětví nejsou, jak již bylo zmíněno, zatím adaptačním zákonem upravena. Jediná odlišnost dle odvětví je prokazatelná pouze v přijetí kodexu chování, kde obecné nařízení umožňuje zohlednit specifika odvětví ve stanovení pravidel v rámci kodexu chování. Pro organizace sociálních služeb byl zjištěn kodex chování zpracovaný Ministerstvem práce a sociálních věcí. Tento kodex chování zatím nemůže dostatečně plnit funkci kodexu chování dle obecného nařízení, neboť není splněna podmínka schválení kodexu dozorovým úřadem.

5.2 Výsledky zjištění z analýzy vybraného subjektu

Je zjevné, že organizace přistoupila k požadavkům obecného nařízení aktivně.
Ze sběru dat je znatelné, že přes veškerou snahu nemá organizace vše dořešeno.

5.2.1 Náměty k diskuzi ze získaných poznatků a vhodná opatření:

Je tomu tak např. u posouzení zákonného titulu v případě etického kodexu, zda provést či neprovést posouzení vlivu pro ochranu osobních údajů, zda jmenovat či nejmenovat pověřence pro ochranu osobních údajů.
Dále se lze zastavit u pořizování fotografií, které jsou zařazeny do zvláštní kategorie osobních údajů. Dle vyjádření měla organizace prezentovánu informaci, že fotografie

spadá do zvláštní kategorie osobních údajů, neboť může nést stopu zdravotního stavu, etnického původu apod. K objasnění klasifikace lze však použít stanovisko Úřadu pro ochranu osobních údajů, které prezentuje na své webové stránce. Ze stanoviska vyplývá, že „o zpracování zvláštní kategorie osobních údajů (dříve citlivé údaje) se bude jednat tehdy, pokud by údaje z fotografie byly cíleně zpracovávány ve vztahu ke konkrétní fyzické osobě*, např. by fotografie sloužily jako zdroj získávání informací o nemoci pleti pro lékařský výzkum ve vztahu k identifikovaným či identifikovatelným osobám*."[104] Je tak možnost, že fotografie pořizované za účelem prezentace činnosti organizace, lze ze zvláštní kategorie vyjmout.

K tomu a dalším sporným otázkám je třeba odborného náhledu. Nabízí se zde možnost buď odborných konzultací u společnosti, která se přímo ochranou osobních dat zabývá. Další možností, zde doporučenou, je přistoupit ke jmenování pověřence pro ochranu osobních údajů. Jak vyplývá z povinností a úkolů pověřenců pro ochranu osobních údajů, poskytují záruku souladu zpracování osobních údajů s obecným nařízením a v rámci své činnosti by měli být dostatečně znalostně připraveni na to, aby mohli jednotlivým správcům a zpracovatelům pomoci a poradit ve sporných otázkách.

Do doby než bude připraven k poradenství pověřenec pro ochranu osobních údajů, lze zatím hledat vhodná řešení a stanoviska jednak na webových stránkách Úřadu pro ochranu osobních údajů, kde lze nastavit automatický odběr novinek. Organizace tak bude mít k dispozici nejnovější odborné příspěvky. Jako další vhodná varianta je odběr placeného elektronického zpravodaje pro pověřence pro ochranu osobních údajů. Tato varianta je z pochopitelných důvodů nastavení rozpočtu organizace závislá na možnosti jejího financování.

Z vhodných potřebných opatření, které není nutno opírat o odborný náhled, je nastavení pravidelného proškolování zaměstnanců, která mohou být rozčleněna do několika bloků se zaměřením na jednotlivé pracovní pozice a rozsah jimi zpracovávaných osobních údajů. Školení je vhodné propojit s tématikou kybernetické bezpečnosti, neboť osobní údaje jsou zpracovávány v organizaci jak listinnou, tak elektronickou formou.

[104] Stanovisko Úřadu pro ochranu osobních údajů, https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaj-citlive-udaje/d-27274

Dále je vhodné stanovit rozsah vstupního školení u nových zaměstnanců dle jednotlivých pracovních okruhů. Důležitost pravidelných školení vychází z předpokladu, že nejrizikovějším faktorem je vždy člověk, v zaměstnání pracovník, proto musí být důsledně proškolován směrem k ochraně osobních údajů.

Na tomto místě je doporučován vnitřní předpis, kterým se organizace v pozici správce osobních údajů zavazuje, včetně svých zaměstnanců, k dodržování obecného nařízení. Jedná se o organizační a technická opatření ve smyslu obecného nařízení v souvislosti se zpracováním osobních údajů. Interní předpis bude součástí základní sady dokumentů pro zajištění souladu s obecným nařízením.

Rozsah a struktura vnitřního předpisu:

1. **Účel vydání předpisu**

Účelem tohoto předpisu je přijmout vhodná organizační a technická opatření k zajištění ochrany osobních údajů v souladu s NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
Tento vnitřní předpis stanovuje účel, k němuž jsou osobní údaje zpracovávány, stanovuje prostředky a způsob zpracování osobních údajů a dokumentuje organizační a technická opatření k zajištění ochrany osobních údajů.

2. **Zásady zpracování osobních údajů**

Při zpracování osobních údajů správce osobních údajů dodržuje zásady:

- zákonnosti,
- korektnosti a transparentnosti,
- účelového omezení,
- minimalizace údajů,
- přesnosti,
- omezení uložení,
- integrity a důvěrnosti

3. Určení a účel zpracovávaných osobních údajů

3.1 Ve vztahu ke svým zaměstnancům zpracovává správce osobní údaje v rozsahu: jméno a příjmení, titul, osobní zaměstnanecké číslo, datum narození, místo narození, rodné příjmení, rodné číslo, rodinný stav, bydliště, státní příslušnost, služební telefonní kontakt, služební kontaktní e-mail, plat, dosažené vzdělání a kvalifikace, fotografie; u rodinných příslušníků se jedná o jméno a příjmení, rodné číslo, bydliště.

Osobní údaje jsou zpracovávány za účelem splnění smlouvy a splnění povinností souvisejících se zaměstnáváním fyzických osob, které vyplývají z právních předpisů především v oblasti zaměstnanosti, nemocenského a důchodového a zdravotního pojištění a v oblasti dani z příjmu fyzických osob.

Ke zpracování pořízených fotografií dochází pouze na základě uděleného souhlasu, který odpovídá požadavkům obecného nařízení o ochraně osobních údajů.

3.1.1 Ve vztahu k uchazečům o zaměstnání zpracovává správce osobní údaje v rozsahu: jméno a příjmení, titul, bydliště, vzdělání a kvalifikace, vše za účelem výběru zaměstnance.

3.2 Ve vztahu k uživatelům sociální služby zpracovává správce osobní údaje v rozsahu: jméno a příjmení, titul, datum narození, místo narození, rodné příjmení, rodné číslo, bydliště, státní příslušnost, zdravotní stav včetně diagnózy, biometrické údaje, příjem, fotografie**;** u rodinných příslušníků jméno a příjmení, titul, telefonní číslo, kontaktní e-mail, bydliště; u zákonných zástupců jméno a příjmení, bydliště.

Osobní údaje jsou zpracovávány za účelem splnění smlouvy a splnění povinností souvisejících s poskytováním sociální služby, jejíž součástí jsou služby zdravotní a ošetřovatelské, které vyplývají z právních předpisů, zejména zákona o sociálních službách a zákona o zdravotních službách.

Ke zpracování pořízených fotografií za účelem prezentace činnosti dochází pouze na základě uděleného souhlasu, který odpovídá požadavkům obecného nařízení o ochraně osobních údajů.

3.2.2 Ve vztahu k zájemcům o poskytování sociální služby jsou zpracovávány osobní

údaje v rozsahu:
jméno a příjmení.

3.3 Ve vztahu k obchodním a jiným partnerům zpracovává správce osobní údaje ve vztahu:
jméno a příjmení, kontaktní telefonní číslo, kontaktní e-mail,
vše k zajištění plnění smlouvy.

3.4 Ve vztahu k ostatním osobám, které se příležitostně vyskytují v objektu správce zpracovává osobní údaje v rozsahu: jméno a příjmení, a to za účelem dodržování etického kodexu chování k uživatelům sociální služby a za účelem ochrany osob a majetku.

3.5 Součástí zpracování je podoba a obrazová informace o chování a jednání osob vyskytujících se v objektu správce v rámci on-line provozu kamerového systému. Kamerový systém je zaveden za účelem ochrany osob a majetku.

4. Prostředky a způsob zpracování osobních údajů

4.1 Zaměstnanecké osobní údaje jsou primárně získávány prostřednictvím osobního dotazníku vyplňovaného zaměstnancem.

4.2 Osobní údaje uživatelů služby jsou získávány primárně prostřednictvím žádostí o poskytování sociální služby.

4.3 Osobní údaje obchodních a jiných partnerů jsou získávány primárně prostřednictvím smluv a nabídek.

4.4 Osobní údaje jsou zpracovávány:
4.4.1 v listinné podobě jednotlivých agend
4.4.2 v elektronické podobě v jednotlivých informačních systémech:

- mzdová a personální agenda v IS xxxx
- účetnictví v IS xxxx
- sociální agenda v IS xxxx

5. Technická a organizační opatření k zajištění ochrany osobních údajů

5.1 Osobní údaje v listinné podobě jsou zabezpečeny v uzamčených skříňkách v elektronicky zabezpečených místnostech:

5.1.1 mzdová a personální agenda v místnosti XXX

5.1.2 účetní agenda v místnosti xxx

5.1.3 sociální agenda v místnostech xxxx

5.1.4 sociálně ošetřovatelská agenda v místnosti xxx

5.2 Osobní údaje elektronické podobě jsou v informačních systémech zabezpečeny přístupovými hesly.

5.3 Jednotlivé PC stanice jsou zabezpečeny přístupovým heslem a v rámci celé počítačové infrastruktury bezpečnostními technickými prvky.

5.4 Přenos dat orgánům veřejné moci je uskutečňován:

5.4.1 prioritně elektronickou formou určenými zaměstnanci datovou schránkou a přístupovými certifikáty

5.4.2 omezeně poštovní službou nebo osobním doručením

6. Uchování a likvidace osobních údajů

6.1 Osobní údaje v listinné podobě jsou uchovávány po uplynutí doby účelovosti dle platného spisového řádu, kde jsou lhůty uchování stanoveny dle zvláštních zákonů, případně dle typového skartačního rejstříku.

6.2 Osobní údaje v informačních systémech mzdové a sociální agendy jsou po uplynutí doby přesunuty do archivního prostředí informačního systému.

6.3 Likvidace osobních údajů probíhá dle pravidel stanovených spisovým řádem.

6.4 Likvidace osobních údajů bez uchování probíhá u osobních údajů uchazečů o zaměstnání ihned po ukončení výběrového řízení.

7. Povinnosti zaměstnanců a jejich odpovědnost při zpracování osobních údajů

7.1 Povinnosti správce osobní údajů plní zaměstnanci správce.

7.2 Zaměstnanci zpracovávají osobní údaje jen v rozsahu oprávnění v rámci stanovených pracovních povinností.

7.3 Zaměstnanci jsou povinni zpracovávat osobní údaje s náležitou odpovědností.

7.4 Zaměstnanci jsou povinni při zpracování osobních údajů dodržovat veškerá bezpečnostní opatření.

7.5 Zaměstnanci jsou povinni jednat tak, aby byl znemožněn neoprávněným osobám přístup ke zpracovávaným osobním údajům, Za tímto účelem jsou zaměstnanci povinni dodržovat následující pravidla:

- Pravidlo čistého stolu (při jednání dbát na zakryté osobní údaje, při odchodu z kanceláře uklidit veškeré dokumenty s osobními údaji do uzamykatelných skříněk)
- Pravidlo bezpečného tisku (dokumenty odnést od tiskárny ihned po vytištění)
- Pravidlo zabezpečené místnosti (vždy zkontrolovat, zda je místnost řádně elektronicky uzamčena a elektronicky zabezpečena)
- Pravidlo ochrany hesla (nesdělovat přístupová hesla jiným osobám, přístupové heslo pravidelně měnit)
- Pravidlo bezpečné sítě (nepřipojovat k počítačové síti žádná vlastní externí zařízení)

7.6 Každý zaměstnanec je vázán mlčenlivostí o osobních údajích a bezpečnostních opatřeních během funkčního pracovněprávního vztahu a i po ukončení pracovněprávního vztahu.

7.7 Veškeré změny ve zpracování osobních údajů zaměstnanec nahlašuje vedoucímu pracovníkovi bezodkladně, aby změny mohly být zařazeny do dokumentace zpracování osobních údajů.

7.8 Zaměstnanec dodržuje stanovené postupy pro výkon práv subjektu údajů a pro nahlašování bezpečnostních incidentů.

8. Závěrečná ustanovení

Tento předpis je závazný pro zpracování osobních údajů

Tento vnitřní předpis nabývá účinnosti dne……

K vnitřnímu předpisu je vhodné připojit již organizací zpracovaný postup pro výkon práv subjektů údajů a zpracovaný postup pro nahlašování bezpečnostních incidentů.

Dále lze uvažovat o vhodnosti připojení zpracovaného seznamu pověřených osob do vstupu datové schránky, seznamu osob s certifikátem a připojení popisu jednotlivých přístupových práv, tzn. popis v rámci jaké pracovní pozice v jakém modulu a s jakými osobními údaji je pracováno v informačních systémech.

Všechny tyto uvažované přílohy lze považovat za organizační a technická opatření. Jejich připojením se stane vnitřní předpis uceleným dokumentovaným souborem přijatých opatření.

6 Závěr

V rámci této diplomové práce byla zkoumána oblast ochrany osobních údajů, jak ji předkládá a stanovuje obecné nařízení o ochraně osobních údajů. Jedná se o novou právní normu Evropské unie, která přináší přísnější pohled na ochranu osobních údajů a nese nové instituty, doposud v České republice nepraktikované.

V teoretické části byla analýza právních předpisů zaměřena na nové prvky ochrany osobních údajů a na celkové nahlížení obecného nařízení na oblast ochrany osobních údajů. Analýza byla doplněna o interpretace autorů odborných publikací. Z analýzy právních norem vyplývá jejich nejednoznačnost. Sdělení Úřadu pro ochranu osobních údajů se odkazuje na novou právní normu, tj. obecné nařízení, která má nahradit dosud používaný zákon č. 101/2000 Sb., o ochraně osobních údajů, s tím, že bude účinný nový adaptační zákon, který bude některá dotčená ustanovení obecného nařízení upřesňovat. Situace je taková, že stávající zákon č. 101/2000 Sb., o ochraně osobních údajů je stále v platnosti a nový adaptační zákon není zatím schválen.

Zároveň se teoretická část snažila nalézt odlišnosti, které by byly charakteristické pro organizace sociálních služeb. Z tohoto pohledu nedošlo ke zjištění odlišností, vyjma odlišnosti v souvislosti s kodexem chování, který by měl být připravován vždy pro určité odvětví vzhledem k rozdílnostem jednotlivých odvětví.

Vlastní práce se orientovala na analýzu vybraného subjektu – organizaci sociálních služeb. Snahou vlastní práce bylo zjistit, jak zdárně se organizace tohoto typu vypořádá s naplněním souladu s obecným nařízením a jaké má obecné nařízení na organizaci dopady. Z pohledu porovnání organizace sociálních služeb s organizacemi jiného typu lze konstatovat odlišnost v rozsahu osobních údajů, kdy vedle zaměstnaneckých a obchodních osobních údajů organizace zpracovává také osobní údaje uživatelů sociální služby.

Ve vybrané organizaci bylo zkoumán celý proces zajišťování souladu s obecným nařízením. Po prozkoumání stavu v organizaci lze konstatovat, že některé podmínky a pravidla obecného nařízení mohou činit obtíže. Pro zajištění souladu s obecným nařízením je třeba náročnější administrativy v popisu a zajištění všech podmínek, které obecné

nařízení požaduje. Nelze se domnívat, že jednou nastavená dokumentace bude sloužit v nezměněné formě několik dalších let. V rámci zásad ochrany osobních údajů bude třeba provádět aktualizační zásahy odvislé od nastalých změn v průběhu zpracování.

Pro aktivní nápomoc při implementaci obecného nařízení do zpracování osobních údajů jsou předloženy návrhy netechnických opatření.

K diskusi je zde předložen návrh jmenování pověřence pro ochranu osobních údajů, který svými vzdělanostními poznatky dokáže posoudit některé sporné záležitosti. Navrhována je taktéž, do doby zajištění pověřence pro ochranu osobních údajů, možnost odborného poradenství společností, zabývající se ochranou osobních údajů a dále informační zjišťování pomocí webových stránek úřadu pro ochranu osobních údajů nebo formou elektronického zpravodaje pro pověřence osobních údajů.

Další doporučení se týká zajištění pravidelného proškolování zaměstnanců v oblasti ochrany osobních údajů a taktéž vstupního školení nových zaměstnanců.

Vzhledem k potřebnosti dokumentace zajištění organizačních a technických opatření pro ochranu osobních údajů je zde doporučen koncept vnitřního předpisu, který bude součástí základní dokumentace pro zajištění souladu zpracování osobních údajů s obecným nařízením.

Na základě poznatků z teoretické části a vlastní práce lze konstatovat, že téma ochrany osobních údajů dle obecného nařízení bude dále dotvářeno stanovisky a doporučeními jak Úřadu pro ochranu osobních údajů, tak Evropského sboru pro ochranu osobních údajů. Lze předpokládat, že k vývoji v oblasti ochrany osobních údajů budou přispívat i poznatky v rámci „dobré praxe“.

Je nutno se dále tématu ochrany osobních údajů věnovat a sledovat, jak se dotčená hlediska vyvíjí, aby každá organizace mohla postupovat přiměřeně s ohledem na nastalý vývoj.

7 Seznam použitých zdrojů

7.1 Odborná literatura

BOGNÁROVÁ,Věra a kolektiv, 2018. *GDPR 2018 v praxi, Sborník vzorů a návodů pro mzdové účetní a personalisty*. Praha: Dashöfer Holding, Ltd. & Verlag Dashöfer, nakladatelství, s.r.o. 262 s. ISBN 978-80-87963-55-5

NEZMAR, Luděk, 2017. *GDPR: Praktický průvodce implementací.* První vydání. Praha: GRADA Publishing, a.s. 304 s. ISBN 978-80-271-0668-4

NONNEMANN, František, 2018. *Praktická příručka GDPR, Příručka pověřence pro ochranu osobních údajů.* První vydání. Praha: Nakladatelství Jiří Nosek – KLIKA. 144 s. ISBN 978-80-88298-10-6.

NULÍČEK, Michal a kolektiv, 2018. *GDPR/ Obecné nařízení o ochraně osobních údajů, praktický komentář.* 2.vydání. Praha: Wolters Kluwer ČR.580 s. ISBN 978-80-7598-068-7.

ŽŮREK, Jiří, 2017. *Praktický průvodce GDPR.* 1. vydání. Olomouc: Nakladatelství Anag. 223 s. ISBN 978-80-7554-097-3.

7.2 Právní předpisy

Zákon č. 23/1991 Sb., ústavní zákon, kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské federativní republiky, v platném znění.

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

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění.

Zákon č. 133/2000 Sb., o evidenci obyvatel a o rodných číslech

7.3 Ostatní literatura

Metodické aktuality Svazu účetních 4/2018.Praha: Svaz účetních České republiky, z.s. 2018.64 s. ISBN 978-80-87367-86-5

7.4 Internetové zdroje

Sbírka zákonů a Sbírka mezinárodních smluv- Ministerstvo vnitra České republiky, zákon č. 23/1991 Sb., ústavní zákon, kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské federativní republiky, v platném znění. Dostupný na www: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=23/1991&typeLaw=zakon&what=Cislo_zakona_smlouvy
Citace 27. 09. 2018

Úřad pro ochranu osobních údajů, 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). Dostupné z www: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31512
Citace 27. 09. 2018

Úřad pro ochranu osobních údajů, Oprava 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). Dostupná odkazově z www: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679R(02)
Citace 27. 09. 2018

Úřad pro ochranu osobních údajů, zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění. Dostupný z www: https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-cervence-2017/ds-3109/archiv=0&p1=1257
Citace 28. 09. 2018

Škorničková E., GDPR. Dostupné z www: https://www.gdpr.cz
Citace 27. 10. 2018

Sbírka zákonů ČR, zákon č. 133/2000 Sb., o evidenci obyvatel a o rodných číslech. Dostupný z www: https://zakonyprolidi.cz/cs/2000-133/zneni-20170701#cast1
Citace 29. 12. 2018

Radičová Z., Burian D., e-právo. Dostupné z www: https://www.epravo.cz/top/clanky/profilovani-ve-svetle-noveho-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-104926.html
Citace 29. 12. 2018

PRACOVNÍ SKUPINA ZŘÍZENA PODLE ČLÁNKU 29 - *Pokyny k transparentnosti podle nařízení 2016/679 přijaty dne 29. listopadu 2017 ve znění naposledy revidovaném a přijatém dne 11. dubna 2018*. Dostupné z www: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31895
Citace 29. 12. 2018

Ministerstvo práce a sociálních věcí, *Doporučený postup č. 02/2018, kterým se v rámci metodického a koncepčního vedení MPSV vypracovává Kodex chování ve smyslu čl. 40 Obecného nařízení o ochraně osobních údajů – GDPR pro potřeby výkonu sociální politiky*. Dostupný z www: https://www.mpsv.cz/cs/13916
Citace 20. 02. 2019