ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

Dopady GDPR na zvolený ekonomický subjekt

Impacts of GDPR on chosen economic subject

Bc. Marie Velkoborská

Plzeň 2020

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta ekonomická

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Marie VELKOBORSKÁ**
Osobní číslo:	**K18N0140P**
Studijní program:	**N6208 Ekonomika a management**
Studijní obor:	**Podniková ekonomika a management**
Téma práce:	**Dopady GDPR na zvolený ekonomický subjekt**
Zadávající katedra:	**Katedra financí a účetnictví**

Zásady pro vypracování

1. Proveďte literární rešerši studované problematiky (GDPR).
2. Charakterizujte zvolený ekonomický subjekt a analyzujte oblasti ovlivněné GDPR.
3. Určete reálné dopady GDPR do podnikových aktivit a navrhněte řešení problémových oblastí.
4. Shrňte řešenou problematiku.

Rozsah diplomové práce: **60 – 80**
Rozsah grafických prací: **neuveden**
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

- NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU). *2016/679: ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).* In: Brusel: EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE, 2016, ročník 2016, číslo 679. OJ L 119. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1568638421562&uri=CELEX:32016R0679.
- DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *of 24 October 1995 on the protection of indioiduals with regard to the processing of personal data and on the free movement of such data.* In: Luxembourg: The European Parliament, the Council, 1995. OJ L 281. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=cs.
- NAVRÁTIL, Jiří. *GDPR pro praxi.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.
- NULÍČEK, Michal. *GDPR – obecné nařízení o ochraně osobních údajů.* 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

Vedoucí diplomové práce: **Ing. Marie Černá, Ph.D.**
Katedra financí a účetnictví

Datum zadání diplomové práce: **22. října 2019**
Termín odevzdání diplomové práce: **22. dubna 2020**

L.S.

Doc. Ing. Michaela Krechovská, Ph.D.
děkanka

Ing. Pavlína Hejduková, Ph.D.
vedoucí katedry

V Plzni dne 22. října 2019

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma

„Dopady GDPR na zvolený ekonomický subjekt“

vypracovala samostatně pod odborným dohledem vedoucího diplomové práce za použití pramenů uvedených v přiložené bibliografii.

Plzeň dne ……... ……

podpis autora

Poděkování

Tímto bych ráda poděkovala paní Ing. Marii Černé, Ph.D. za vedení této diplomové práce, za její odborné rady a připomínky, a také za ochotu a čas, který mi věnovala.

Dále bych chtěla poděkovat zaměstnancům Magistrátu města Plzně za poskytnutí potřebných materiálů a informací, a za možnost absolvování průběžných konzultací a opakovaných návštěv pracoviště. Za tuto zkušenost děkuji především bezpečnostnímu řediteli magistrátu a referentovi GDPR.

Poděkování patří také zaměstnancům Správy informačních technologií města Plzně a odborníkovi z oblasti IT, který mi byl nápomocen v otázkách technického směru.

Obsah

Úvod ... 8
1 Cíl a metodika práce ... 10
1.1 Cíle práce ... 10
1.2 Metody a postupy zpracování ... 11
2 Obecná východiska GDPR ... 13
2.1 Charakteristika a definice GDPR ... 13
2.1.1 Důležité pojmy ... 13
2.1.2 Hlavní cíle a principy zavedení GDPR ... 14
2.1.3 Zásady a právní důvody zpracování GDPR ... 15
2.1.4 Historický vývoj legislativy sloužící k ochraně osobních údajů ... 16
2.1.5 Stav české legislativy před GDPR ... 18
2.1.6 Další dokumenty související s GDPR ... 20
2.2 Zásadní témata GDPR ... 20
2.2.1 Místní a věcná působnost ... 20
2.2.2 Elektronická komunikace a GDPR ... 21
2.2.3 Pověřenec pro ochranu osobních údajů ... 24
2.2.4 Osobní údaje a zvláštní kategorie osobních údajů ... 25
2.2.5 Zpracování osobních údajů ... 27
2.2.6 Oprava a výmaz osobních údajů ... 30
2.2.7 Ohlašovací povinnost, sankce a pokuty ... 31
3 Magistrát města Plzně ... 33
3.1 Charakteristika ekonomického subjektu ... 33
3.1.1 Základní informace a historie Plzně ... 33
3.1.2 Organizační struktura města Plzně ... 34
3.1.3 Funkce a vztahy ... 35
3.1.4 Informační systémy ... 36
3.2 Analýza ekonomického subjektu ... 37
3.2.1 Systém řízení ... 38
3.2.2 Ochrana osobních údajů před zavedením GDPR ... 39
3.2.3 Proces implementace GDPR ... 40
3.2.4 Ochrana osobních údajů po zavedení GDPR ... 42

4 Dopady GDPR na daný ekonomický subjekt 44
4.1 Funkce pověřence pro ochranu osobních údajů 44
4.2 Nesprávné pochopení evropského nařízení 46
4.3 Administrativní a časová náročnost 47
4.4 Finanční náročnost 49
4.4.1 Náklady na školení 49
4.4.2 Náklady na provedení analýzy 49
4.5 Proces kontroly plnění povinností dle GDPR 50
4.6 Personální gramotnost v problematice a školení zaměstnanců 51
4.7 Technické zabezpečení dat 52
4.7.1 Papírová dokumentace 52
4.7.2 Elektronická dokumentace 53
4.8 Dopady GDPR po dvouletém ustálení 56
5 Návrhová část 58
5.1 Analýza rizik 58
5.1.1 Lidský faktor 60
5.1.2 Technický faktor 62
5.1.3 Externí faktor 64
5.2 Shrnutí a vyhodnocení rizik 65
5.2.1 Zobrazení v matici rizik 65
5.2.2 Riziko úniku dat 68
5.3 Zlepšující opatření a doporučení pro Magistrát města Plzně 71
5.3.1 Opatření ke zvládání kritických rizik 72
5.3.2 Opatření ke zvládání vysokých rizik 74
5.3.3 Opatření ke zvládání středních rizik 76
Závěr 78
Seznam použité literatury 81
Seznam tabulek a obrázků 92
Seznam použitých zkratek 94
Seznam příloh 95

Úvod

Osobní údaje jsou každým rokem cennější a neustále nabírají na své hodnotě. A to zejména v dnešní době, kdy dochází k výraznému rozvoji technologií, a roste tedy i množství příležitostí pro neoprávněné získání těchto dat. Právě proto je zpracování osobních údajů velmi důležitým tématem současnosti, jelikož neznalost bezpečnosti zacházení s osobními údaji může způsobit velké škody jak soukromým osobám, tak společnostem.

Proč je tedy potřeba chránit své osobní údaje? V první řadě je nutné si uvědomit, že se nejedná pouze o ochranu určitých dat, ale také o ochranu základních práv a svobod člověka, které s tím úzce souvisí. Za druhé, nesprávné zacházení s osobními údaji může vést k mnoha nepříjemným situacím – například k odcizení peněz z bankovního účtu. A za třetí, ochrana osobních údajů se promítá také v důvěryhodnosti a spolehlivosti společností poskytujících například produkty či služby. Pro ně je dodržování předpisů ochrany osobních údajů klíčové a jejich ignorace může ohrozit jejich samotnou existenci.

Problematika ochrany osobních údajů tedy není nikterak novou záležitostí a již v minulosti vznikalo mnoho právních předpisů, které toto téma upravovaly. Nicméně, teprve roce 2018 zaznamenala ochrana osobních údajů zásadní milník – účinnosti totiž nabylo nové evropské nařízení známé pod termínem „GDPR“. S tím přišlo i velké množství rozdílných reakcí, jak těch pozitivních, tak těch negativních. Pravdou však je, že se jedná o doposud nejaktuálnější právní předpis z hlediska ochrany osobních údajů, který jednak odpovídá náležitostem dnešní doby, a jednak dává prostor členským státům Evropské unie přizpůsobit si toto nařízení dle vlastních požadavků a potřeb.

Tématem GDPR se zabývá také tato diplomová práce. Konkrétně se zaměřuje na dopady tohoto nařízení na zvolený ekonomický subjekt – Magistrát města Plzně.

Práce je rozdělena do pěti hlavních kapitol.

Úvodní kapitola slouží k představení cíle a metodiky práce.

Druhá kapitola pojednává o GDPR z obecného hlediska. Představuje základní charakteristiky tohoto nařízení, důležité pojmy a také historický vývoj ochrany osobních údajů jak v rámci Evropy, tak v rámci území České republiky. Jsou zde definována a popsána také zásadní témata, o kterých nařízení GDPR pojednává.

Praktická část práce se již vztahuje ke zvolenému subjektu, tedy k Magistrátu města Plzně. Třetí kapitola je rozdělena do dvou částí. Ta první se zaobírá charakteristikou subjektu – základními informacemi týkajícími se fungování magistrátu. Druhá část poté propojuje ekonomický subjekt s nařízením GDPR. Stěžejními body jsou zde koncepce systému řízení v podniku, ochrana osobních údajů před zavedením GDPR, následná implementace GDPR, a shrnutí v podobě představení stavu ochrany osobních údajů po zavedení GDPR.

Čtvrtá kapitola práce již popisuje konkrétní příklady dopadů GDPR na Magistrát města Plzně. Prostředkem ke zjištění těchto informací je kombinace několika metod výzkumu. Jedná se o konzultace, rozhovory a diskuse s vedoucími pracovníky magistrátu a dále o provedení analýzy interních i veřejně dostupných dokumentů a jejich zapracování.

Poslední část práce je zaměřena na představení návrhů a zlepšujících opatření, které vyplývají z předchozích kapitol a jejich výstupů. Je zde využita metoda analýzy rizik, která vychází ze zjištěných dopadů a následně vede ke stanovení opatření, která by mohla výrazně usnadnit a zefektivnit chod subjektu do budoucna (z hlediska ochrany osobních údajů).

1 Cíl a metodika práce

Úvodní kapitola slouží jako prostředek k seznámení s cíli práce. Jsou zde také vymezeny metody a postupy zpracování – nejdůležitější zdroje, o které se diplomová práce opírá, a zvolené metody výzkumu.

1.1 Cíle práce

V rámci této práce je vymezen hlavní cíl a několik cílů vedlejších.

Hlavním cílem práce je identifikovat a vyhodnotit dopady nařízení GDPR na konkrétní ekonomický subjekt a vypracovat návrh opatření směřujících ke zlepšení situace sledovaného subjektu v této oblasti.

Prostředkem k dosažení tohoto cíle bude provedení analýzy subjektu – Magistrátu města Plzně, a to prostřednictvím rozhovorů a konzultací s vedoucími pracovníky. Budou definována potenciální rizika plynoucí z ochrany osobních údajů, která společně s nalezenými dopady poslouží jako podkladový materiál pro tvorbu návrhů vedoucích k omezení či odstranění těchto rizik, a následně k zefektivnění chodu subjektu v oblasti ochrany osobních údajů (GDPR).

Práce čtenáři poskytne konkrétní příklady týkající se řešení této problematiky a definuje, jak bylo při zavádění GDPR reálně postupováno, jak toto nařízení ovlivnilo chod daného subjektu, a zejména pak, jaké jsou výstupy a hodnocení implementace GDPR po téměř dvou letech fungování.

Vedlejší cíle:

- provést literární rešerši sledované oblasti,
- představit Magistrát města Plzně z hlediska systému řízení,
- analyzovat průběh zavádění GDPR,
- analyzovat současný stav z hlediska ochrany osobních údajů (GDPR),
- identifikovat globální hrozby v oblasti zabezpečení osobních údajů.

Pro lepší přehlednost byly definovány následující výzkumné otázky, k jejichž zodpovězení dojde v rámci praktické části této práce.

Jaké jsou dopady GDPR na chod ekonomického subjektu?

Jakou funkci má v subjektu pověřenec pro ochranu osobních údajů? Jakým zaškolením prošel pověřenec před výkonem této pozice? Jak byl tento člověk zvolen či vybrán?

Jaké výhody a nevýhody přineslo nové nařízení sledovanému subjektu?

S jakými překážkami se subjekt musel/musí potýkat a jaké skutečnosti naopak usnadnily jeho chod?

Jakou metodiku ochrany osobních údajů subjekt využíval před zavedením nového nařízení a co se změnilo?

Jaká byla celková časová, finanční a administrativní náročnost implementace GDPR?

Jak subjekt hodnotí implementaci nařízení GDPR po roce (2 letech)?

Jaký je proces kontroly plnění GDPR?

1.2 Metody a postupy zpracování

Práce čerpá ze dvou hlavních kategorií zdrojů.

Prvním zdrojem jsou právní předpisy, knižní materiály, dokumenty a články týkající se jak přímo GDPR, tak ochrany osobních údajů obecně. Tyto zdroje budou využity pro zpracování teoretické části práce.

Jak teoretická, tak zejména pak praktická část je konzultována s odborníky na ochranu osobních údajů. Těmi jsou především zaměstnanci z oddělení bezpečnosti Magistrátu města Plzně, kteří mají na starost právě GDPR. Druhou kategorií zdrojů je tedy samotný ekonomický subjekt.

Vedlejším, avšak neméně důležitým zdrojem, jsou informace čerpané na základě konzultací s odborníkem v oblasti IT.

Právní předpisy a další dokumenty týkající se ochrany osobních údajů

Nejdůležitějším pramenem, o který se celá práce opírá je *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)*. Přestože zákon vešel v platnost již v roce 2016, účinnost

tohoto nařízení byla odložena až na 25. května 2018. Důvodem byla vysoká časová náročnost a velké množství povinností souvisejících s jeho aplikací (Navrátil, 2018).

Příčinou vzniku nového nařízení byla neaktuálnost a nedostatečnost původního nařízení, tedy *směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*. S rozvojem technologií a automatizací zpracování osobních údajů bylo tedy potřeba nastavit novou jednotnou směrnici pro všechny členské státy Evropské unie (Navrátil, 2018).

V České republice platil do roku 2018 *zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.* Ten byl v uvedeném roce nahrazen novým evropským nařízením. Teprve 24. dubna 2019 byla v České republice schválena adaptační legislativa k GDPR, a s ní vešel v platnost nový zákon. Tím je *zákon č. 110/2019 Sb., o zpracování osobních údajů.*

Dále práce čerpá z portálů evropských i českých institucí. Jako příklad lze uvést *Úřad pro ochranu osobních údajů (The Office for Personal Data Protection)* či *Evropský sbor pro ochranu osobních údajů (European Data Protection Board).*

Magistrát města Plzně

Část práce, týkající se Magistrátu města Plzně, se opírá o několik zdrojů.

V první řadě jsou to rozhovory a konzultace se zaměstnanci magistrátu, jejichž pracovní náplní je, mimo jiné, ochrana osobních údajů. Důležitým zdrojem je také aktivní účast v diskusi s vedoucími pracovníky Magistrátu města Plzně na téma zabezpečení osobních údajů a dalších záležitostí týkajících se ochrany dat (včetně samotného nařízení GDPR a budoucnosti tohoto nařízení). Práce se opírá také o informace získané v průběhu návštěv a pozorování pracoviště magistrátu.

Dále práce čerpá z internetových stránek města Plzně a dokumentů veřejně přístupných na těchto stránkách. Podstatnou součástí jsou také interní dokumenty a další informace získané na základě již uvedených konzultací, diskusí a rozhovorů uskutečněných v průběhu zpracovávání práce.

Část práce je podložena také informacemi získanými od zaměstnanců Správy informačních technologií města Plzně.

2 Obecná východiska GDPR

Následující kapitola má za úkol seznámit čtenáře se základními náležitostmi GDPR. V první části kapitoly dojde k vysvětlení této zkratky. Budou představeny všechny podstatné pojmy, hlavní cíle, principy zavedení, a také právní stránka věci. Dále bude znázorněn historický vývoj ochrany osobních údajů jak v České republice, tak v Evropské unii obecně.

Druhá část kapitoly pak poslouží k vysvětlení hlavních témat v oblasti GDPR – budou zde uvedeny důležité body tohoto nařízení.

2.1 Charakteristika a definice GDPR

Pod všeobecně známou zkratkou GDPR se skrývá anglický název *General Data Protection Regulation*, v českém překladu jde tedy o *Obecné nařízení o ochraně osobních údajů*. Tato zkratka není nikterak stará, vznikla až společně se samotným nařízením.

S GDPR také, mimo jiné, přišla povinnost jmenovat pověřence pro ochranu osobních údajů (DPO), jehož pracovní náplní je dohled nad zpracováním osobních údajů, informační a poradenská činnost.

Důležité je zde také vymezit rozdíl mezi nařízením a směrnicí, a vysvětlit, proč je GDPR právě nařízením. Účel *směrnice* spočívá v tom, že členským státům (například Evropské unie) je předložen požadovaný výsledek, kterého by měly v určitém období dosáhnout. Záleží však na jejich uvážení, jak k dané situaci přistoupí a jakým způsobem daný cíl naplní.

Oproti tomu *nařízení* je uplatňováno ve všech zemích Evropské unie jednotně a nemusí se tedy implementovat do vnitrostátního práva (Europa.eu, n. d.)

2.1.1 Důležité pojmy

V nařízení Evropského parlamentu a Rady (EU) 2016/679 (dále uváděno také pouze jako „nařízení“, „evropské nařízení“ či „obecné nařízení“) se objevuje nespočet pojmů, které jsou nezbytné pro úplné pochopení procesů GDPR. V této části budou představeny pouze některé z nich – ty, které jsou nejzásadnější (článek 4 obecného nařízení). V dalších částech práce budou tyto pojmy vysvětleny detailněji a uvedeny do souvislostí.

Nejdůležitějším pojmem je *osobní údaj*, který znázorňuje veškeré informace o fyzické osobě. Fyzická osoba je označována jako *subjekt údajů*. Subjektem údajů není osoba právnická.

Zpracování osobních údajů značí jakékoli operace s osobními údaji, které jsou prováděny s pomocí či bez pomoci automatizovaných postupů (shromažďování, zaznamenávání, pozměnění, vyhledání, používání, výmaz a další)

Na rozdíl od subjektu údajů, *správce osobních údajů* je fyzická či právnická osoba, orgán veřejné moci nebo například agentura, která určuje účely a prostředky zpracování osobních údajů.

Zpracovatel osobních údajů je fyzická či právnická osoba, orgán veřejné moci nebo například agentura, která zpracovává osobní údaje pro správce (článek 4 obecného nařízení).

2.1.2 Hlavní cíle a principy zavedení GDPR

Článek 1 obecného nařízení (Předmět a cíle) uvádí následující:

1. *„Toto nařízení stanoví pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla týkající se volného pohybu osobních údajů.*
2. *Toto nařízení chrání základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů.*
3. *Volný pohyb osobních údajů v Unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán.“*

Obecně lze konstatovat, že důvodů zavedení GDPR je hned několik. Různé zdroje a články[1] hovoří zejména o zastaralosti původní směrnice, její roztříštěnosti a vysoké administrativní zátěži.

Dle Navrátila (2018, s. 30) jsou cíle zavedení GDPR následující:

1) *„Přizpůsobení právní regulace ochrany osobních údajů poměrům dnešní doby“*.

To odpovídá problematice zastaralosti a nutnosti modernizace původní směrnice.

[1] gdpr.cz, n. d.; MVČR, 2019a; Nezmar, 2017.

2) *„Sjednocení práva ochrany osobních údajů ve všech zemích Evropské unie a dalších zemích, na které dopadá.“*

Navrátil zde poukazuje na roztříštěnost a nesourodost původních právních předpisů napříč zeměmi Evropské unie.

3) *„Posílení práv v oblasti ochrany osobních údajů všech osob, které jsou subjekty údajů a dosáhnout sjednoceného výkladu GDPR dozorovými úřady jednotlivých zemí Evropské unie.“*

Vzhledem ke stoupající míře elektronické komunikace a využití informačních technologií je potřeba klást mnohem větší důraz na ochranu osobních údajů, jelikož tato data jsou v dnešní době mnohem jednodušeji napadnutelná a zneužitelná než dříve.

4) *„Posílení důvěryhodnosti Evropské unie a jejích členských zemí (i dalších zemí, které musí GDPR implementovat) pro jiné země, které mají zájem na rozvoji obchodu s Evropskou unií a s tím souvisejícím předáváním osobních údajů mezi zeměmi.“*

Ochrana osobních údajů je důležitá nejen v rámci jednoho státu či mezi státy Evropské unie, ale také v rámci světového měřítka.

2.1.3 Zásady a právní důvody zpracování GDPR

Jedním z klíčových bodů evropského nařízení jsou také zásady zpracování osobních údajů, kterými je subjekt (pověřenec pro ochranu osobních údajů) povinen se řídit a poctivě je dodržovat. Jedná se o následující (článek 5 obecného nařízení):

- *„zákonnost, korektnost, transparentnost“*,
- *„účelové omezení“* (shromažďování pro určité, výslovně vyjádřené a legitimní účely),
- *„minimalizace údajů“* (omezení na nezbytný rozsah ve vztahu k účelu zpracování),
- *„přesnost“* (případně aktuálnost údajů),
- *„omezení uložení“* (uložení pouze po nezbytnou dobu),
- *„integrita a důvěrnost“*.

2.1.4 Historický vývoj legislativy sloužící k ochraně osobních údajů

Ochrana osobních údajů a obecně ochrana soukromí nebyla vždy běžnou součástí života člověka. Až do středověku se veškeré osobní a intimní životní události odehrávaly víceméně veřejně (až na výjimky) a první zvrat přišel až s náboženskými válkami a s tím souvisejícím pronásledováním osob s odlišným náboženským vyznáním (Navrátil, 2018).

Jako jeden ze zásadních zlomů Navrátil (2018) definuje Velkou francouzskou revoluci, v jejímž průběhu docházelo k rozsáhlému postihování lidí s odlišnými názory.

Právo na soukromí a ochranu osobních údajů mělo však tehdy jiný význam, než pod jakým ho známe dnes. V roce 1888 bylo definováno soudcem Thomasem Cooleym jako „right to be left alone“ čili v češtině „právo být nechán o samotě“ (Prowda, 1995).

Další definice práva na soukromí se objevila o dva roky později (1890) v článku „The Right to Privacy“ (Warren & Brendeis). Autoři zde tvrdí, že toto právo je pouhým vývojem základní zásady ochrany osoby v „common law“ a nejedná se tedy o žádnou novinku.

Nejpodstatnějším obdobím, které v minulosti vedlo k ochraně soukromí, však bylo období nacismu. Po těchto zkušenostech, které pro mnoho lidí znamenaly velké zásahy do soukromí, došlo ke změně chápání původního „práva být nechán o samotě“. V roce 1948 byla proto tato transformace zahrnuta do článku č. 12 Všeobecné deklarace lidských práv (Nulíček et al., 2018).

V roce 1950 byla podepsána takzvaná *Úmluva o ochraně lidských práv a základních svobod* (taktéž Evropská úmluva o lidských právech), která se stala základním pilířem pro pochopení práva na soukromí. Úmluva byla v roce 1992 publikována jako *sdělení č. 209/1992 Sb.* (sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících).

Jejím obsahem byla následující témata:

- povinnost respektovat lidská práva (čl. 1),
- právo na život (čl. 2),
- zákaz mučení (čl. 3),
- zákaz otroctví a nucené práce (čl. 4),
- právo na svobodu a osobní bezpečnost (čl. 5),

- právo na spravedlivý proces (čl. 6),
- zákaz trestu bez zákona (čl. 7),
- právo na respektování rodinného a soukromého života (čl. 8),
- svoboda myšlení, svědomí a náboženského vyznání (čl. 9),
- svoboda projevu (čl. 10),
- svoboda shromažďování a sdružování (čl. 11),
- právo uzavřít manželství (čl. 12),
- právo na účinné opravné prostředky (čl. 13),
- zákaz diskriminace (čl. 14),
- odstoupení od závazků v případě ohrožení (čl. 15),
- omezení politické činnosti cizinců (čl. 16),
- zákaz zneužití práv (čl. 17),
- ohraničení možnosti omezení práv (čl. 18).

Nejvýznamnějším kontrolním orgánem byl v té době Evropský soud pro lidská práva, který vznikl v roce 1959.

Velká změna poté nastala až v 70. letech 20. století s rozvojem technologií. Jedním z prvních dokumentů týkajících se ochrany osobních údajů byla takzvaná *Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat* (také Úmluva Rady Evropy č. 108*)*, která byla zavedena v roce 1981. Českou republikou byla podepsána v roce 2000. Zde byly poprvé oficiálně definovány zásady ochrany osobních údajů, dále také například úprava přeshraničních toků osobních údajů. Obsah úmluvy se stále doplňuje, mění a modernizuje (Navrátil, 2018).

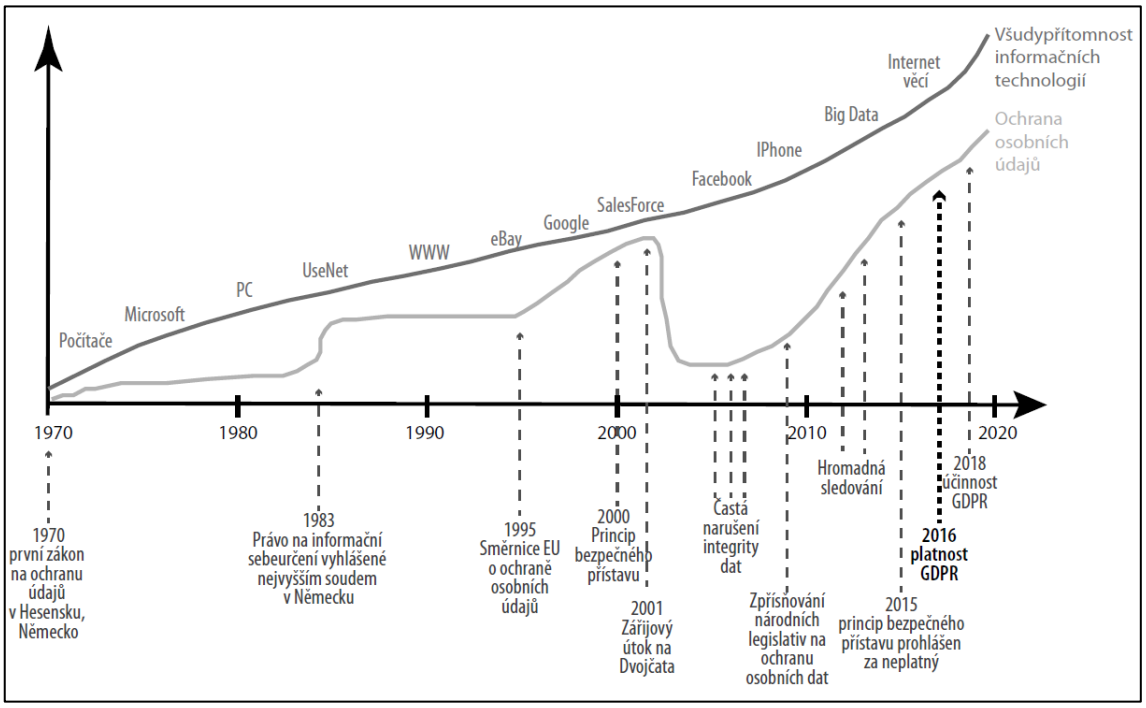
Následující rok (2001) byl zrodem *Lisabonské smlouvy*, která byla součástí ústavního projektu *Deklarace Evropské rady o budoucnosti Evropské unie*. V roce 2000 došlo také k vyhlášení *Listiny základních práv Evropské unie*, která poté doplnila Lisabonskou smlouvu v roce 2009.

Stěžejním dokumentem však byla již zmiňovaná *směrnice Evropského parlamentu a Rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*, která byla vydána v roce 1995. Jejím cílem bylo zajištění fungování jednotného trhu a zajištění účinné ochrany základních práv a svobod fyzických osob (Nulíček et al., 2018).

Její platnost skončila až v květnu 2018, kdy ji nahradilo nové *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).

Následující obrázek znázorňuje vývoj legislativy týkající se ochrany osobních údajů v souvislosti s rozvojem technologií.

Obrázek č. 1: Vývoj legislativy ochrany osobních údajů



Převzato: Nezmar, 2017

2.1.5 Stav české legislativy před GDPR

Česká legislativa související s ochranou osobních údajů se v minulosti opírala o následující zákony a právní předpisy:

- *zákon č. 87/1862 ř. z., pro ochranu svobody osobní,*
- *zákon č. 88/1862 ř. z., pro ochranu svobody domovní,*
- *ústavní zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního,*
- *zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech,*
- *Listina základních práv a svobod č. 2/1993 Sb.*

Evropská směrnice 95/46/ES byla do českého práva zakomponována v podobě *zákona č. 101/2000 Sb., o ochraně osobních údajů.*

Současně se zákonem č. 101/2000 Sb., o ochraně osobních údajů byl v červnu roku 2000 založen Úřad pro ochranu osobních údajů, v jehož kompetencích byl zejména dozor nad dodržováním povinností stanovených v tomto zákoně. Mimo jiné se staral také o vedení registru povolených zpracování osobních údajů, přijímal stížnosti na porušení zákona a také poskytoval konzultační služby či přednášky. V listopadu téhož roku získal také oprávnění udělovat a odebírat akreditace v oblasti ochrany osobních údajů – v roce 2004 však tato zodpovědnost přešla na Ministerstvo informatiky ČR (ÚOOÚ, 2019a).

Jak již bylo řečeno, v dubnu roku 2019 byla přijata adaptační legislativa obecného nařízení, tedy *zákon č. 110/2019 Sb., o zpracování osobních údajů*. Cílem tohoto adaptačního zákona bylo zejména upřesnění práv a povinností, které vyplývaly z nařízení GDPR (§ 1).

Jednou z důležitých změn je udělení výjimky orgánům veřejné moci a veřejným subjektům co se týče rozhodování o sankcích za porušení povinností GDPR (sankce jsou v tomto případě tedy nulové). Výjimka se však nevztahuje na pravomoc dozorových úřadů udělit těmto subjektům napomenutí a nařídit provedení nápravy.

Další změnou je také snížení věkové hranice, kdy je dítě způsobilé k udělení souhlasu. Nařízení GDPR udává hranici 16 let (článek 8), adaptační legislativa tuto hranici posouvá na 15 let.

Dále oproti obecnému nařízení zákon č. 110/2019 Sb. specifikuje tzv. *„zpracování osobních údajů prováděné pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu“* (§ 17).

Společně s adaptačním zákonem vešel v platnost také doprovodný *zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.* Tento zákon se vztahuje konkrétně pouze na orgány veřejné moci a změny v zákonech s tímto související (například změna trestního řádu, změna zákona o Policii ČR, změna zákona o kybernetické bezpečnosti a podobně).

V současné době plní Úřad pro ochranu osobních údajů funkci dozorového úřadu a kontroluje plnění povinností GDPR.

2.1.6 Další dokumenty související s GDPR

Právní předpisy v oblasti ochrany údajů jsou doplňovány dalšími dokumenty, které většinou slouží jako podpůrný materiál pro lepší pochopení právních předpisů.

Těmito zdroji jsou například judikatura Soudního dvora EU, stanoviska dozorových úřadů či pokyny a doporučení Evropského sboru pro ochranu osobních údajů (EDPB – European Data Protection Board).

EDPB je nezávislý orgán, který je tvořen odborníky všech členských států, a který pravidelně vydává pokyny a doporučení týkající se právních předpisů v oblasti ochrany osobních údajů. V květnu 2018 přijal tento orgán pokyny poskytnuté pracovní skupinou 29 (WP29), která společně se zavedením GDPR zanikla a přejmenovala se na EDPB (EDPB, 2019).

2.2 Zásadní témata GDPR

Témat, týkajících se GDPR, je v dnešní době nespočet a stále se objevují témata nová – zejména s rozvojem technologií a novými postupy a metodami zpracování dat.

Následující kapitola slouží k vysvětlení důležitých částí nového evropského nařízení, s důrazem na změny týkající se moderních technologií, zpracování dat prostřednictvím internetové sítě a podobně.

2.2.1 Místní a věcná působnost

Věcná působnost (článek 2)

Nařízení se vztahuje na všechna automatizovaná či částečně automatizovaná zpracování osobních údajů (například webový skript). Týká se ale také neautomatizovaného (manuálního) zpracování těch osobních údajů, které jsou buď již založeny v dané evidenci, nebo do ní mají být teprve zařazeny (například nemocniční kartotéky) – tato data jsou tedy chráněna v případě, kdy jsou určitým způsobem systematicky uspořádána.

Výjimky z věcné působnosti jsou jednak údaje vznikající z činností, které nespadají do oblasti působnosti práva Evropské unie. Další výjimkou je zpracování osobních údajů prostřednictvím činností, které spadají do oblasti společné zahraniční a bezpečnostní politiky Evropské unie. Dále se nařízení nevztahuje na údaje plynoucí z osobních nebo domácích činností (nesmí zde za žádných okolností existovat spojitost s obchodní

či profesní činností). Příkladem je vedení osobního adresáře s kontakty známých. Poslední výjimkou je zpracování osobních údajů za účelem prevence, vyšetřování, odhalování, stíhání trestných činů či výkonu trestů (například boj proti korupci). Tato výjimka je upravena zvláštní směrnicí (2016/680).

Nařízení 2016/679 nemá vliv na uplatňování směrnice 2000/31/ES (o elektronickém obchodu) (Nulíček et al., 2018).

Místní působnost (článek 3)

Nařízení se uplatňuje pro všechny správce nebo zpracovatele osobních údajů v rámci Evropské unie, a to i v případě, kdy zpracování probíhá mimo EU. Zpracování však musí souviset s činnostmi, které se týkají:

a) nabídky zboží nebo služeb daným subjektům v EU,
b) monitorování chování subjektů (v rámci EU) – prostřednictvím cookies, IP adresy, MAC adresy zařízení či dalších geolokačních údajů (Nulíček et al., 2018).

Problematika monitorování je více popsána v následující podkapitole.

2.2.2 Elektronická komunikace a GDPR

Primárním právním předpisem z hlediska elektronických komunikací *směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích)*.

Tato směrnice byla do českého práva zakomponována *zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů* (zákon o elektronických komunikacích) a *zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů* (zákon o některých službách informační společnosti).

Již v lednu roku 2017 byl však předložen takzvaný *návrh nařízení Rady a Evropského parlamentu o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)*. Toto plánované nařízení je více známo pod názvem „ePrivacy Regulation“ (European Commission, 2017).

Zatímco původní směrnice se zaměřovala pouze na tradiční telekomunikační operátory, nové nařízení by mělo stanovit povinnosti i dalším společnostem a poskytovatelům služeb, jako jsou například:

- Whatsapp, Facebook, Skype,
- fyzické a právnické osoby poskytující přímou marketingovou komunikaci (direct marketing),
- majitelé webových stránek,
- majitelé aplikací, které zahrnují elektronickou komunikaci,
- poskytovatelé přístupu k internetu,
- telekomunikační firmy (Secure Privacy, 2020).

Nařízení původně mělo vejít v platnost v květnu roku 2018 a sloužit tak jako doplněk GDPR, nicméně toto datum se odložilo a v dnešní době stále není známo, kdy k nabytí účinnosti dojde. V listopadu roku 2019 byl návrh opět zamítnut (IAPP, 2019).

GDPR se v současné době pojí s několika pojmy. Jedná se zejména o cookies, IP adresu, MAC adresu a cloudové služby.

Cookies jsou krátké datové soubory, které se ukládají do počítače během prohlížení internetových stránek. Mohou být uloženy i online (synchronizace prostřednictvím účtu Google) (Google, 2020a). Portál je tak schopen zaznamenat kompletní informace o návštěvě a slouží zejména ke sledování počtu návštěvníků, k výběru reklam a podobně.

I některé z těchto údajů jsou považovány za údaje osobní (bod 30), jedná se pak zejména o takzvané sledovací cookies, které mají za cíl právě sledování daného uživatele (například návštěvnost stránek konkrétního e-shopu).

Jsou definovány tři druhy cookies:

- funkční (technické) cookies – GDPR se na ně nevztahuje,
- výkonnostní cookies (slouží k měření návštěvnosti webových stránek a tvorbu statistik) – požadují souhlas subjektu údajů,
- marketingové cookies – požadují souhlas subjektu údajů (Svět IT, 2019).

Při vstupu na webovou stránku je provozovatel povinen umístit lištu či nějaké upozornění o sběru cookies (současně s informacemi o používání souborů cookies) – návštěvník má následně možnost se vyjádřit, zda se sběrem těchto informací souhlasí či nikoliv.

Obrázek č. 2: Notifikace o sběru cookies

Převzato: ČEZ, 2020

Takzvaná **IP adresa** (IP = Internet Protocol) značí řadu čísel, která označuje daný počítač komunikující prostřednictvím tohoto internetového protokolu (IP). IP adresa tedy slouží k určení polohy zařízení a identifikaci uživatele či počítačové sítě, kterou uživatel využívá (například síť univerzity) (Janevski, 2003).

IP adresa tedy může být osobním údajem.

MAC adresa (MAC = Media Access Control), označovaná také jako fyzická adresa, představuje unikátní číslo, které slouží k identifikaci daného síťového prvku (síťové karty, routery, switche a podobně) (Cafourek, 2010).

Stejně jako v případě IP adresy se může jednat o osobní údaj.

Cloud neboli cloudová služba slouží zejména k uchovávání dat online. Některá z těchto dat mohou být také považována za osobní údaje. V pracovním procesu se cloud nejčastěji využívá pro ukládání databáze zákazníků či zaměstnanců či pro účel provozu webových stránek a aplikací. Každý člověk, který využívá služby cloudu pro účel podnikání, je minimálně správcem, případně zpracovatelem osobních údajů, a nese tedy za svou činnost plnou zodpovědnost (cloudflare.com, 2019).

2.2.3 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů (dále jako „DPO“ = Data Protection Officer či „pověřenec“) je speciální pracovní pozice jmenovaná správcem či zpracovatelem osobních údajů. Dle nařízení má DPO povinnost dohlížet, zda dochází k souladu zpracování osobních údajů s nařízením, dále poskytuje správci rady ohledně skutečností spojených s tímto tématem.

Jmenovat pověřence pro ochranu osobních údajů je povinné v případech, kdy (článek 37, odst. 1):

a) *„zpracování provádí orgán veřejné moci či veřejný subjekt“* (s výjimkou soudů),
b) *„hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektu údajů“,*
c) *„hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10“.*

V případě *pravidelného a systematického monitorování subjektu údajů* se jedná například o provoz telekomunikační sítě, cílenou reklamu prostřednictvím e-mailu, monitorování prostřednictvím kamer, sledování polohy na základě lokalizačních údajů a mnohé další (WP29, 2019).

Pojem *rozsáhlé zpracování* označuje například zpracování cestovních dat osob používajících městskou hromadnou dopravu, zpracování dat v rámci obchodní činnosti banky či pojišťovny či zpracování údajů o pacientech v rámci činnosti nemocnice. Naopak v případě zpracování dat, která *nejsou rozsáhlá*, se jedná například o údaje o pacientech, které zpracovává jeden konkrétní lékař (WP29, 2019).

Pokud tedy společnost neprovádí rozsáhlé, pravidelné a systematické zpracování osobních údajů, jmenování pověřence pro ochranu osobních údajů není povinné, ale pouze dobrovolné.

Dle článku 37 může existovat jeden pověřenec pro více podniků, pokud je však snadno dosažitelný. Odstavec 5 (článek 37) určuje, že pověřenec musí být jmenován na základě profesních kvalit, zejména na základě odborných znalostí práva a praxe v oblasti ochrany

osobních údajů. Tyto kvality však nejsou jasně definovány. Pokyny WP29 uvádí, že pověřenec by měl disponovat vědomostmi z oblasti národní i evropské legislativy a mít praxi v oboru ochrany osobních údajů. Nezbytná je samozřejmě také znalost evropského nařízení. Dále pracovní skupina doporučuje znalost oboru podnikání dané organizace, znalost informačních systémů a bezpečnosti dat (WP29, 2019).

2.2.4 Osobní údaje a zvláštní kategorie osobních údajů

Rozdíl mezi původním zákonem (respektive původní směrnicí) a novým nařízením lze najít i v definici pojmu osobní údaj. Pro srovnání lze využít následující tabulku.

Tabulka č. 1: Definice pojmu osobní údaj

Zákon č. 101/2000 Sb. (§ 4)	**Nařízení č. 2016/679 (článek 4)**
„ … jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“	*„ …veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například **jméno**, identifikační číslo, **lokační údaje**, **síťový identifikátor** nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*

Zdroj: zákon č. 101/2000 Sb. (§ 4), nařízení č. 2016/679 (článek 4), zvýraznila M. V.
Zpracovala: Marie Velkoborská, 2020

Obecné nařízení tedy nově obsahuje také jméno, lokační údaje a síťový identifikátor. Nicméně žádný z právních předpisů přesně neurčuje, o jaké konkrétní údaje se jedná.

Na základě nového nařízení (článek 4) lze za osobní údaje považovat následující:

- jméno a příjmení,
- pohlaví,
- datum a místo narození,
- rodné číslo,
- trvalý pobyt,
- rodinný stav,
- záznamy (fotografie, video, hlasový záznam),

- kontaktní údaje (e-mailová adresa, telefonní číslo),
- síťové identifikátory (IP adresa, MAC adresa),
- lokační údaje (GPS, Google, mobilní aplikace),
- identifikační čísla (občanský průkaz, řidičský průkaz, ISIC, DIČ, …),
- dosažené vzdělání,
- příjem.

Mezi další osobní údaje patří kontaktní údaje (e-mailová adresa, telefonní číslo) či číslo soukromého bankovního účtu.

Zvláštní kategorií jsou takzvané *citlivé osobní údaje*. Tato kategorie zahrnuje následující:

- rasový či etnický původ,
- politické názory,
- náboženské či filozofické vyznání,
- členství v odborech,
- zdravotní stav (tělesné i duševní zdraví),
- sexuální orientace,
- trestní delikty či pravomocné odsouzení osob.

Do citlivých údajů řadíme také *genetické* a *biometrické údaje* (Nezmar, 2017).

Genetické údaje nařízení definuje jako *„osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby“* (článek 4, odst. 13). Biometrické údaje jsou osobní údaje technického charakteru, díky kterým je možné osobu identifikovat – například snímek obličeje, hlas, otisk prstu či podpis (článek 4).

Anonymizované osobní údaje jsou v podstatě protipólem osobních údajů – jedná se o údaje, které nejsou nikterak spojeny s konkrétní osobou (článek 26).

Pseudonymizace je metoda sběru dat o osobě, jejíž identita není známa. Příkladem mohou být například kódované údaje (článek 26).

Následující tabulka znázorňuje příklad anonymizovaných údajů (zaznačeno modře) a pseudonymizovaných údajů (zaznačeno červeně)

Tabulka č. 2: Anonymizované a pseudonymizované údaje

Jméno a příjmení	Adresa	Věk	Pohlaví	Měsíční příjem
Jan Novák	Nová 5, Praha	35	muž	30 000 Kč
012345		35	muž	30 000 Kč

Zdroj: nařízení č. 2016/679 (článek 4), 2016
Zpracovala: Marie Velkoborská, 2020

Definovat pojem osobní údaj není tak jednoduché, jak se na první pohled zdá, a to zejména proto, že ani nařízení GDPR neuvádí konkrétní příklady. Obecně lze však konstatovat, že o osobní údaj se jedná vždy v případě, kdy je možné na základě dané informace identifikovat konkrétní osobu. Jako příklad lze uvést jméno Jan Novák – vzhledem k velkému množství osob s tímto jménem se v tomto případě nejedná o osobní údaj. Pokud je se jménem spojeno například i datum narození či trvalý pobyt, lze zjistit, o jakého člověka se jedná – poté lze hovořit o osobním údaji, který podléhá nařízení GDPR.

2.2.5 Zpracování osobních údajů

Článek 6 obecného nařízení definuje zpracování osobních údajů jako zákonné v případě splnění alespoň jedné z následujících podmínek:

a) subjekt údajů udělil souhlas se zpracováním,
b) zpracování je nezbytné pro splnění smlouvy,
c) zpracování je nezbytné pro plnění právní povinnosti,
d) zpracování je nezbytné pro ochranu životně důležitých zájmů osoby,
e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu,
f) zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, (vyjma situací, kdy mají přednost zájmy nebo základní práva a svobody subjektu údajů, zejména pokud je subjektem dítě).

Informovanost subjektů o zpracovávání dat a udělování souhlasu

Dle evropského nařízení (článek 4, odst. 11) je *„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“*.

„Svobodný“ je souhlas v případě, že má subjekt údajů možnost volby a není na něj uvalen nátlak, zastrašování či klamání (Nulíček et al., 2018). Nařízení v bodě 43 uvádí několik příkladů či situací, kdy může být svoboda souhlasu diskutabilní. První případ se týká situace, kdy existuje jasná nerovnováha mezi subjektem údajů a správcem – zvláště v případě, kdy správce je zároveň orgánem veřejné moci.

Dále je zde popsán případ, kdy subjektu údajů není umožněno souhlasit pouze s některými částmi zpracování a je tedy nucen souhlasit se zpracováním celkově. Nulíček (2018) uvádí, že se jedná například o zpracování dat prostřednictvím mobilních aplikací, kdy subjekt údajů nemá možnost souhlasit pouze s konkrétními funkcemi dané aplikace. Řešením by mohl být takzvaný „členěný souhlas“.

„Konkrétnost“ souhlasu vypovídá o tom, že existuje konkrétní účel zpracování údajů. Specifikace účelu či účelů zpracování je podstatným bodem, který je nutné uskutečnit před samotným zpracováním dat. Tím lze zabránit či omezit takzvané neplánované rozšiřování funkcí (function creep[2]), které může vyvrcholit ve ztrátu kontroly nad zpracováním osobních údajů (Nulíček et al., 2018).

„Informovaný“ je souhlas v případě, kdy je subjekt údajů obeznámen se všemi okolnostmi a skutečnostmi – zejména pak s totožností správce, účely zpracování, konkrétními operacemi, s možností souhlas odvolat a tak dále (Nulíček et al., 2018).

Souhlas musí být také „jednoznačný“ čili musí být na první pohled jasné, že subjekt údajů vyjadřuje souhlas se zpracováním svých osobních údajů a udělení svolení je tedy jasně označeno (Nulíček et al., 2018).

Zároveň článek 7 obecného nařízení uvádí, že správce je povinen nějakým způsobem doložit, že subjekt údajů se zpracováním svých osobních údajů souhlasil a zároveň si je vědom toho, že má právo svůj souhlas kdykoli odvolat.

Záznamy o činnostech zpracování

Bez ohledu na to, zda je souhlas udělen písemnou či ústní formou, správce údajů by měl vést záznam o udělení souhlasu, který by měl obsahovat následující (ICO, 2019):

[2] „Function creep“ je postupné rozšiřování způsobů využití technologie nebo systému nad rámec původního účelu (zejména pokud to vede k potenciálnímu narušení soukromí) (Collins, 2020).

a) kdo souhlas udělil (jméno subjektu údajů, případně uživatelské jméno či IP adresa),
b) kdy k udělení souhlasu došlo (kopie datovaného dokumentu či elektronický záznam obsahující například časovou známku),
c) o čem byl subjekt údajů informován (kopie dokumentu včetně všech podmínek),
d) jakým způsobem byl souhlas udělen (písemné prohlášení či elektronický záznam),
e) zda byl souhlas odvolán.

Profilování

Dalším důležitým pojmem, o který se nařízení opírá, je takzvané *profilování*.

Jedná se o princip automatizovaného zpracování dat, které slouží k následnému vyhodnocení či předvídání některých aspektů dané fyzické osoby. Lze zde hovořit například o kvalitě pracovního výkonu, ekonomické situaci, zdravotním stavu, osobních zájmech, typu chování či pohybu a umístění dané osoby (ÚOOÚ, 2019b).

Přestože je tento pojem nově definován (článek 71 obecného nařízení), o novinku se nejedná – metoda profilování se využívá například i v bankovnictví v případě žádosti klienta o hypotéku. Banka prostřednictvím profilování tímto způsobem zjišťuje, zda je dotyčný schopný hypotéku splácet. Dalším využitím je také monitorování návštěvníků internetových stránek z hlediska toho, o jaké produkty mají zájem a následné cílení reklamy (ÚOOÚ, 2019b).

Co se týče souhlasu, v případě profilování není vždy potřeba – zapotřebí je pak výhradně za předpokladu, že má správce v plánu operovat s citlivými údaji.

S tématem profilování souvisí také pojem *automatizované rozhodování*. Jedná se o rozhodování za pomoci výpočetních technologií čili s absencí jakéhokoliv lidského faktoru. Dle článku 22 (odst. 2) může automatizované rozhodování správce využít pouze v případech, kdy je:

a) nezbytné k uzavření nebo plnění smlouvy mezi subjektem a správcem údajů,
b) povoleno právem Unie nebo právem členského státu,
c) založeno na výslovném souhlasu subjektu údajů.

Dále je nutné, aby správce údajů sám provedl či přijal (na základě práva Unie či členského státu) vhodná opatření na ochranu práv a svobod a poskytl dostatečné informace subjektům, kterých se automatizované rozhodování týká.

2.2.6 Oprava a výmaz osobních údajů

Právo na opravu značí možnost opravení nepřesnosti osobních údajů, a to bez zbytečného odkladu (článek 16).

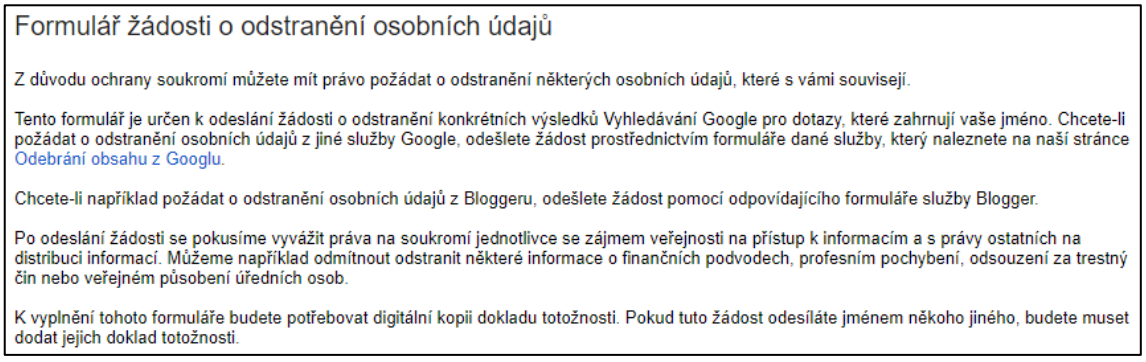
Právo na výmaz („právo být zapomenut“) umožňuje subjektu údajů požadovat kompletní likvidaci osobních údajů, a to v případě, že má požadavek následující důvod (článek 17):

a) osobní údaje již nejsou potřebné,
b) subjekt údajů odvolá svůj souhlas,
c) existence námitek proti zpracování,
d) protiprávní zpracování,
e) nutnost výmazu z důvodu splnění právní povinnosti,
f) shromáždění údajů souviselo s nabídkou služeb informační společnosti.

Právo být zapomenut nabízí v současné době například Google, který dává uživatelům k dispozici takzvaný „Formulář žádosti o odstranění osobních údajů“ (viz obrázek níže).

Pro vyplnění je potřeba uvést zemi původu, jméno, kontaktní údaj, kopii dokladu totožnosti. Následně už stačí uvést údaje, které chce dotyčný odstranit (dle adresy URL), a z jaké důvodu tak činí. V závěru je nutné poskytnout digitální podpis.

Obrázek č. 3: Právo na výmaz


Formulář žádosti o odstranění osobních údajů

Z důvodu ochrany soukromí můžete mít právo požádat o odstranění některých osobních údajů, které s vámi souvisejí.

Tento formulář je určen k odeslání žádosti o odstranění konkrétních výsledků Vyhledávání Google pro dotazy, které zahrnují vaše jméno. Chcete-li požádat o odstranění osobních údajů z jiné služby Google, odešlete žádost prostřednictvím formuláře dané služby, který naleznete na naší stránce Odebrání obsahu z Googlu.

Chcete-li například požádat o odstranění osobních údajů z Bloggeru, odešlete žádost pomocí odpovídajícího formuláře služby Blogger.

Po odeslání žádosti se pokusíme vyvážit práva na soukromí jednotlivce se zájmem veřejnosti na přístup k informacím a s právy ostatních na distribuci informací. Můžeme například odmítnout odstranit některé informace o finančních podvodech, profesním pochybení, odsouzení za trestný čin nebo veřejném působení úředních osob.

K vyplnění tohoto formuláře budete potřebovat digitální kopii dokladu totožnosti. Pokud tuto žádost odesíláte jménem někoho jiného, budete muset dodat jejich doklad totožnosti.

Převzato: Google, 2020b

Právo na omezení zpracování je možné uplatnit v případě, že (článek 18):

a) *„subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit,*
b) *zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití,*
c) *správce již osobní údaje nepotřebuje, ale subjekt je požaduje pro určení, výkon nebo obhajobu právních nároků,*
d) *subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.“*

Právo na přenositelnost údajů značí právo subjektu údajů osobní údaje získat a předat jinému správci.

2.2.7 Ohlašovací povinnost, sankce a pokuty

Dle článku 32 je jakékoli porušení zabezpečení osobních údajů správce nutno nahlásit v ideálním případě do 72 hodin od okamžiku uvědomění. Porušení se hlásí příslušnému dozorovému úřadu.

Ohlášení musí obsahovat:

a) popis povahy daného případu porušení zabezpečení osobních údajů,
b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů (či jiného kontaktního místa),
c) popis pravděpodobných důsledků porušení,
d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení (článek 32).

Sankce, pokuty

O problematice ukládání správních pokut hovoří článek 83, jehož součástí jsou také konkrétní sankce za porušení povinností zpracování osobních údajů. Horní hranice výše těchto pokut je v rámci nařízení rozdělena do následujících dvou kategorií, a to na základě toho, jakého porušení se správce údajů dopustil.

a) pokuta ve výši 10 000 000 EUR (nebo až do výše 2 % celkového obratu za předchozí rok – vybrána je vyšší hodnota),

b) pokuta ve výši 20 000 000 EUR (nebo až do výše 4 % celkového obratu za předchozí rok – vybrána je vyšší hodnota).

Evropský sbor pro ochranu osobních údajů (EDPB) vydal speciální dokument týkající se uplatňování a stanovování pokut. Ten by měl sloužit jako podklad pro jednotlivé dozorové úřady – v případě České republiky se jedná o již zmiňovaný Úřad pro ochranu osobních údajů (ÚOOÚ).

Na základě zásad uvedených v obecném nařízení EDPB vydal několik základních pravidel pro ukládání pokut (WP253, 2017).

1) *„Porušení nařízení by mělo mít za následek uložení ‚rovnocenných sankcí'."* (s. 5)

Sankce v jednotlivých členských zemích by měly být co nejsoudržnější, aby nedocházelo k překážkám v rámci volného pohybu osobních údajů, co se vnitřního trhu týče (bod 13 obecného nařízení).

2) *„Stejně jako všechna nápravná opatření zvolená dozorovými úřady by i správní pokuty měly být ‚účinné, přiměřené a odrazující'."* (s. 6)

Udělování pokut a jejich výše by vždy mělo být adekvátní k rozsahu porušení povinností. Účelem pokuty je odradit správce či zpracovatele od případného opakování porušení svých povinností – plní tedy i preventivní funkci. Zároveň by však sankce měly být přiměřené ekonomické situaci státu i osoby (fyzické či právnické osoby). Výše pokuty by v žádném případě neměla být likvidační (Nulíček et al., 2018).

3) *„Příslušný dozorový úřad provede posouzení ‚v každém jednotlivém případě'."* (s. 6)

Každý případ porušení povinností v souvislosti s obecným nařízením musí být posuzován individuálně.

4) *„Harmonizovaný přístup ke správním pokutám v oblasti ochrany údajů vyžaduje aktivní účast dozorových úřadů a výměnu informací mezi nimi."* (s. 7)

Dle obecného nařízení (článek 83, odst. 7) si může každý stát stanovit pravidla, zda a do jaké výše je možné ukládat pokuty orgánům veřejné moci a veřejným subjektům. Na základě toho zákon č. 110/2019 Sb., o zpracování osobních údajů vylučuje orgány veřejné moci a veřejné subjekty z udílení správních pokut (§ 62, odst. 5).

3 Magistrát města Plzně

Jako ekonomický subjekt byl pro potřeby této práce zvolen Magistrát města Plzně (dále také jako „MMP“ či pouze „magistrát“).

Subjekt byl vybrán z důvodu předpokladu vyšší důvěryhodnosti poskytovaných informací (dle názoru autorky práce), jelikož se jedná o subjekt působící ve státním sektoru. U soukromých subjektů může pravděpodobněji docházet ke zkreslení údajů a informací za účelem například pozitivní reklamy. Naopak subjekty státního sektoru mají většinu informací transparentních a je tedy mnohem jednodušší dostat se ke skutečným datům.

Zároveň je nutné si uvědomit, že Magistrát města Plzně je úřadem. Subjekt tedy každodenně zpracovává velké množství osobních údajů, a to nejen svých zaměstnanců, ale také občanů města Plzně a spřízněných institucí (základních škol, divadel, hřbitovů a dalších). Důraz na zabezpečení osobních údajů je tedy významnou součástí běžného chodu magistrátu, a právě z toho důvodu je Magistrát města Plzně vhodným subjektem pro zpracování tohoto tématu.

3.1 Charakteristika ekonomického subjektu

Tato podkapitola je určena k představení zvoleného subjektu a také k charakteristice jednotlivých funkcí a aktivit města Plzně (potažmo tedy i magistrátu).

3.1.1 Základní informace a historie Plzně

Plzeň je čtvrtým největším městem České republiky a zároveň metropolí Plzeňského kraje. Žije zde téměř 192 000 obyvatel (ČSÚ, 2019) a rozloha činí 13 767 hektarů.

Výhodou je například její dobrá dostupnost – nachází se pouhou hodinu jízdy z Prahy směrem na západ. Nejzajímavější na Plzni však je její bohatá historie a s tím související malebné historické centrum, které se může pyšnit hned několik dominantami – gotickou katedrálou svatého Bartoloměje, renesanční radnicí, divadlem J. K. Tyla či Velkou synagogou. Je zde možnost návštěvy několika muzeí a galerií, parků, barů, hospod, restaurací, a to vše v blízké vzdálenosti od centra.

Nejznámější je však Plzeň díky produkci světoznámého piva Pilsner Urquell, které se zde vaří již od roku 1842.

Plzeň také nedávno získala titul Evropské hlavní město kultury 2015. Tato skutečnost stála za velkým nárůstem kulturních událostí. Mimo jiné došlo na základě této skutečnosti také k výstavbě Nového divadla, které se pyšní neotřelým moderním designem.

Mezi další zajímavé turistické atraktivity patří také Techmania Science Center s vlastním moderním planetáriem, Historické podzemí, Zoologická a botanická zahrada, Dinopark či Muzeum loutek a strašidel (Plzen.eu, 2018).

3.1.2 Organizační struktura města Plzně

Nejvyšším orgánem v rámci města je *Zastupitelstvo města Plzně*, jehož součástí je 47 členů.

Pod něj spadá *Rada města Plzně* se svými 9 členy. Jedním z členů je také *primátor* města Plzně, kterým je v současné době Mgr. Martin Baxa. Zároveň je primátor nejvyšším orgánem **Magistrátu města Plzně** a je zodpovědný za *náměstky primátora* a *členy rady*[3]. Hlavní činností primátora je veřejné vystupování ve prospěch města, řízení a svolávání jednání zastupitelstva a rady, schvalování právních předpisů a plnění úkolů starosty či hejtmana Plzeňského kraje.

Náměstci primátora zastupují primátora v době jeho nepřítomnosti, jsou odpovědni za tvorbu návrhů a vnitřních norem města a také kontrolují jejich dodržování. Dále monitorují činnost rozpočtových a příspěvkových organizací. Členové Rady města Plzně plní stejnou funkci jako náměstci s výjimkou zastoupení primátora.

Pozice primátora je zároveň nadřazená *tajemníkovi magistrátu*. Ten je zodpovědný za samotnou činnost Magistrátu města Plzně. Má na starosti vše související s jednotlivými úřady, potažmo jejich řediteli. Plzeňský magistrát disponuje čtyřmi úřady, jedná se o:

- Úřad správních agend,
- Úřad ekonomický,
- Úřad technický,
- Úřad služeb obyvatelstvu.

Úřady se následně dělí na *odbory* (kanceláře) a *oddělení*. Tyto útvary mají vždy svého vedoucího.

[3] Organizační struktura v grafické podobě je k dispozici v příloze A.

Konkrétně za GDPR a oblast ochrany osobních údajů je zodpovědný bezpečnostní ředitel Magistrátu města Plzně a referent GDPR. Ti jsou součástí Kanceláře tajemníka MMP (Organizační řád Magistrátu města Plzně, 2019).

3.1.3 Funkce a vztahy

Nadřízeným útvarem města Plzně je Krajský úřad Plzeňského kraje. Zároveň Plzeň spolupracuje s úřady a magistráty dalších měst České republiky.

Magistrát města Plzně se zabývá plněním jak všech činností v oblasti samostatné působnosti, tak v oblasti přenesené působnosti. Konkrétně postavení a působnost MMP definuje *zákon č. 128/2000 Sb., o obcích*, dále pak *obecná vyhláška města Plzně č. 1/2003* a jiné právní předpisy.

Dále magistrát spolupracuje se Zastupitelstvem města Plzně a s Radou města Plzně. Také úzce komunikuje s městskými obvody, které sice mají vlastní orgány samosprávy, ale v některých oblastech se jejich činnosti prolínají (Statut města Plzně, 2019).

V rámci svých činností se Magistrát města Plzně dostává do kontaktu s množstvím různých subjektů. Jedním z příkladů jsou městské (příspěvkové) organizace, mezi které patří následující (Plzen.eu, 2019a):

- Správa informačních technologií města Plzně,
- Útvar koncepce a rozvoje města Plzně,
- Útvar koordinace evropských projektů města Plzně,
- Správa veřejného statku města Plzně,
- Divadlo Josefa Kajetána Tyla,
- Divadlo ALFA,
- Plzeň – TURISMUS,
- základní školy a jídelny,
- mateřské školy,
- Zoologická a botanická zahrada města Plzně,
- Městský ústav sociálních služeb města Plzně,
- Dětské centrum Plzeň.

Magistrát také kooperuje s dalšími společnostmi s majetkovým podílem města, mezi které patří například Čistá Plzeň, s.r.o., PMDP, a.s. či Měšťanská Beseda Plzeň,

s.r.o. Důležitou funkci v činnostech Magistrátu mají také neziskové organizace, kterou je například Nadace 700 let města Plzně.

Nelze opomenout také finanční instituce – Úřad práce, zdravotní pojišťovny či Finanční úřad.

Mimo státní sektor Magistrát města Plzně komunikuje také se soukromými společnostmi, a to zejména v souvislosti s veřejnými zakázkami. Jejich průběh a všechny související materiály jsou zveřejněné na internetových stránkách z důvodu nutné a velmi důležité transparentnosti (Plzen.eu, 2019c).

Pro tyto potřeby jsou občanům i dalším zájemcům k dispozici dvě aplikace:

- Investiční záměry (Plzen.eu, 2020),
- Dokumenty k veřejným zakázkám (Tenderarena.cz, 2020).

3.1.4 Informační systémy

Magistrát města Plzně disponuje několika informačními systémy, které mají velký vliv na zpracovávání a uchovávání údajů, a to včetně těch osobních. Pro potřeby této práce budou zmíněny pouze ty nejdůležitější v této oblasti.

V souvislosti s GDPR je nutné zmínit program **CODEXIS**, což je národní a evropský právní systém. Je k dispozici všem zaměstnancům magistrátu, kteří ho mohou kdykoli využít ať už s cílem dohledání informací týkajících se ochrany osobních údajů či z jiných důvodů.

Dále MMP, stejně jako mnoho dalších ekonomických subjektů, využívá program **SAP**, který v současné době slouží zejména k vedení finančního a mzdového účetnictví. Zároveň je SAP vhodným nástrojem i v souvislosti s GDPR, jelikož splňuje veškeré požadavky na ochranu osobních údajů, které obecné nařízení vyžaduje (SAP, 2019).

Velmi důležitý je z hlediska GDPR program **e-spis**, který slouží k evidenci, správě, archivaci i skartaci písemných dokumentů. Zaměstnanci dále využívají program **i-Faktury**, se kterým pracuje zejména finanční a personální oddělení, či program **Agendio**, který slouží k vedení všech typů agend (včetně těch týkajících se GDPR) a je k dispozici všem zaměstnancům magistrátu (interní zdroje MMP, 2020).

3.2 Analýza ekonomického subjektu

Následující podkapitola (a následně i celá kapitola 4) je sepsána na základě rozhovorů a konzultací se zaměstnanci Magistrátu města Plzně (interní zdroje MMP, 2020). Problematika byla rozebírána zejména s bezpečnostním ředitelem, referentem GDPR a vedoucím Kanceláře tajemníka MMP.

Informace byly zjišťovány jednak prostřednictvím volné diskuse na toto téma a jednak na základě konkrétních či obecných otázek, které byly předem zaslány na e-mailovou adresu MMP[4]. Na některé otázky nebylo možné odpovědět z důvodu nutnosti utajení určitých informací či z důvodu absence některých materiálů.

V průběhu rozhovorů byl veden písemný záznam. Ten byl současně doplňován interními dokumenty MMP, které byly pro potřeby této práce autorce poskytnuty.

V dalších týdnech probíhala taktéž e-mailová a telefonická komunikace, kdy docházelo k upřesňování získaných informací, k dalším konzultacím či k poskytování doplňující dokumentace. Seznam kontaktních osob dle pracovní pozice, jimi poskytované informace a formu přenosu těchto informací znázorňuje následující tabulka.

Tabulka č. 3: Interní zdroje a kontaktní osoby MMP

Zaměstnanec MMP	Poskytované informace	Forma
Bezpečnostní ředitel	Příprava na implementaci GDPR Implementace GDPR a její náročnost Konkrétní příklady z praxe Současný stav ochrany osobních údajů	Konzultace (osobně, e-mail, telefon) Rozhovor Diskuse
Referent GDPR	Papírová i elektronická dokumentace (směrnice, agendy apod.) Konkrétní příklady z praxe Současný stav ochrany osobních údajů	Konzultace (osobně, e-mail) Diskuse
Vedoucí Kanceláře tajemníka	Obecné informace o MMP Ochrana osobních údajů před zavedením GDPR Současný stav ochrany osobních údajů Záležitosti technického charakteru (zabezpečení sítě apod.)	Rozhovor Diskuse

Zpracovala: Marie Velkoborská, 2020

[4] Témata a otázky k rozhovoru jsou k dispozici v příloze B.

Tato kapitola, mimo výše uvedené, čerpá také z internetových stránek Magistrátu města Plzně a veřejně dostupných dokumentů.

První část kapitoly stručně popisuje systém řízení magistrátu. V dalších částech dochází k představení stavu ochrany osobních údajů před zavedením GDPR, průběhu implementace GDPR a stavu ochrany osobních údajů po jeho uvedení v platnost.

3.2.1 Systém řízení

Magistrát města Plzně v současné době využívá takzvaný integrovaný systém řízení (ISŘ), který se skládá z následujících složek (Koncepce integrovaného systému řízení, 2020).

- management kvality (QMS = Quality Management System),
- systém enviromentálního managementu (EMS = Environmental Management Systems),
- systém bezpečnosti a ochrany zdraví při práci (BOZP = Bezpečnost a ochrana zdraví při práci),
- systém managementu hospodaření s energií (EnMS = Energy Management and Saving)[5].

Tento systém je v současné době formován soustavou vnitřních organizačních a řídících norem. Ne vždy tomu tak bylo – v minulých letech byly vnitřní normy formovány odděleně.

První z nich jsou takzvané *směrnice*, které mají označení QS. Jejich hlavní funkcí je stanovení postupů, které jsou uplatněny v hlavních, řídících či podpůrných procesech. Například Organizační řád MMP, který definuje organizační strukturu, funkce a činnosti zaměstnanců či oddělení, je vydán pod označením QS 55-01.

Dále magistrát využívá *instrukce* (QI), které slouží k popisu konkrétních činností. Tyto instrukce jsou pro zaměstnance závazné (nemají pouze informativní funkci). Je tedy nutné je dodržovat.

[5] Certifikát je k dispozici v příloze D.

Další normou jsou *mapy procesů samosprávy* (QM), které popisují jednotlivé činnosti jakožto proces – od vstupů až po výstupy.

Přehled procesů státní správy (QP) stanovuje seznam procesů a takzvané *formuláře* (QF), což jsou šablony sloužící k administrativní činnosti, zpracování a úschově údajů a dat (Organizační řád MMP, 2019).

Pro potřeby ochrany osobních údajů (tedy v současné době zejména pro potřeby GDPR) jsou využívány primárně instrukce a směrnice.

3.2.2 Ochrana osobních údajů před zavedením GDPR

Magistrát města Plzně je státní institucí a jak již bylo zmíněno v předchozích kapitolách, je rozdělen do čtyř základních úřadů, které se následně větví na konkrétní odbory. Všechny tyto složky hojně využívají osobní údaje občanů Plzně. Právě z toho důvodu je ochrana osobních údajů velmi důležitou součástí všech činností probíhajících pod záštitou MMP.

Jak již bylo několikrát řečeno, před GDPR existoval v České republice *zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů*. Na tomto základě byla magistrátem (konkrétně pod záštitou Kanceláře tajemníka) vytvořena instrukce pro ochranu osobních údajů, jejímž cílem bylo informovat o novinkách v problematice ochrany osobních údajů v souvislosti s tímto zákonem. Instrukce se však netýkala pouze zaměstnanců, ale byla rozdělena na dvě části. První část zahrnovala informace využitelné pro zaměstnance Magistrátu města Plzně. Druhá část poté sloužila jako informační zdroj pro externí osoby – klienty, kteří magistrátu v určitě době poskytli své osobní údaje a poté například žádali o uplatnění některého z práv tehdejšího zákona o ochraně osobních údajů (například žádost o výmaz osobních údajů a další).

I před zavedením GDPR tedy Magistrát města Plzně dbal na ochranu osobních údajů a zároveň vytvářel vzorce chování (například v podobě těchto instrukcí) pro ostatní subjekty. Dle vedoucího Kanceláře tajemníka (2020) v tomto *„magistrát dělal více, než musel“*.

Zároveň s rozvojem internetu rostly požadavky na transparentnost státních subjektů – všechny důležité informace se tedy postupně začaly zveřejňovat na internetových stránkách města Plzně.

3.2.3 Proces implementace GDPR

Na základě nového nařízení byl vedoucím Kanceláře tajemníka MMP sestaven postup implementace GDPR, jehož body bylo nutné poctivě dodržovat. Příprava na GDPR byla dle vedení magistrátu nejpodstatnější fází v období implementace. Díky tomu každý zaměstnanec věděl, co dělat a jak se na květen roku 2018 připravit. Tato podkapitola je popisem předem stanoveného postupu – vzhledem k tomu, že i samotná implementace GDPR se dá označovat jako „dopad", veškeré podrobnosti budou rozepsány v následující kapitole popisující dopady (kapitola 4).

V první fázi došlo k úvodnímu **proškolení** vedení daného městského obvodu, vedoucích pracovníků a dalších zaměstnanců podílejících se na implementaci GDPR. Byli určeni konkrétní zaměstnanci (pracovní tým), kteří byli následně odpovědni za provedení analýzy, na jejímž základě byly poté stanoveny návrhy řešení implementace GDPR.

Dále bylo nutné stanovit funkci **pověřence pro ochranu osobních údajů** (krok 2), který v rámci plnění jednotlivých kroků implementace GDPR následně fungoval jako konzultant.

Třetím krokem byla takzvaná **revize**, která byla spojena zejména s analýzou existujícího prostředí. Byly kladeny následující otázky.

a) *„Kde, co máme?"*

Výstupem byl soupis procesů, které využívají osobní údaje. Dále došlo také ke stanovení, o jaké osobní údaje se jedná a určení stupně nezbytnosti zpracovávání těchto údajů. V neposlední řadě bylo potřeba definovat, jakým způsobem zpracování osobních údajů probíhá, po jakou dobu jsou osobní údaje uloženy a jaký prostředek pro úschovu těchto údajů je zvolen. Možnosti uložení jsou například papírová forma, kartotéka, archiv, šanon a skříň, softwarový produkt, databáze, lokální nebo síťová úložiště, používání cloudové služby či e-maily.

b) *„Jakým právem?"*

Magistrát zde odpovídal na otázku, jakým právem, tedy na jakém základě jsou osobní údaje zpracovávány – tedy zda jsou zpracovávány na základě právních předpisů, na základě souhlasu subjektu údajů, na základě smlouvy či na základě plnění veřejného zájmu.

c) *„Jak to chráníme?“*

Součástí odpovědi na tuto otázku byla analýza přístupových oprávnění, bezpečnosti uložení osobních údajů či analýza vnitřních předpisů, které definují nakládání s osobními údaji.

d) *„Kdo?“*

V poslední řadě bylo nutné stanovit, kteří zaměstnanci mají přístup (oprávnění) k osobním údajům, kdo je za co odpovědný, a zda je potřeba doplnit pracovní smlouvu o mlčenlivost zaměstnanců v rámci doložky o ochraně osobních údajů.

Podstatnou součástí implementace GDPR byl čtvrtý krok – rozdílová **analýza**[6], která měla za úkol porovnat a také vyhodnotit současný a žádoucí stav dle GDPR. Tato analýza je i v současnosti využívána pro kontrolu dodržování GDPR a zároveň každoročně dochází k jejímu aktualizování.

Pátým krokem byly **závěry a doporučení** plynoucí z rozdílové analýzy. Jednalo se například o doplnění, revize či vytvoření úplně nových interních předpisů MMP. Dále bylo také podáno doporučení ohledně zavedení nových procesů či technologií a byla ověřena správa dat a jejich záloh.

Na základě předchozí analýzy bylo nutné stanovit další **plán postupu** čili definovat, jakým způsobem budou standardy ochrany osobních údajů integrovány do obecných pravidel bezpečnosti informací MMP. Dále také bylo potřeba stanovit postup pro detekování bezpečnostních incidentů a určit, jakým způsobem se bude porušení zabezpečení řešit.

Následně došlo k **realizaci** a uvedení daných doporučení do praxe.

Nedílnou součástí byla (a stále je) pravidelná **revize**, která mimo jiné zahrnuje také vzdělávání a školení zaměstnanců v této problematice, a zároveň také samotný výkon funkce pověřence pro ochranu osobních údajů.

Všechny výše uvedené kroky (a zejména pak jejich časová náročnost) jsou uvedeny v kapitole 4.3.

[6] Vzorová tabulka je k dispozici v příloze C.

3.2.4 Ochrana osobních údajů po zavedení GDPR

Se zavedením GDPR byla vydána také instrukce s názvem Zpracování osobních údajů – QI 42-03-01, která (stejně jako nové nařízení) nabyla účinnosti 25. května 2018.

> *„Účelem této instrukce je určit závazná pravidla, pokyny, informace a poučení, kterými jsou naplňovány požadavky pro nakládání s osobními údaji stanovené nařízením Evropského parlamentu a Rady (EU) 2016/679…“* (Zpracovávání osobních údajů, 2018)

Instrukce je závazná pro všechny zaměstnance MMP, jejichž náplní práce je, mimo jiné, i zpracování osobních údajů. Instrukce obsahuje následující položky:

- vysvětlení všech potřebných pojmů a zkratek,
- pravomoci a odpovědnosti,
- nakládání s osobními údaji – popis činností:
    - zákonné důvody zpracování,
    - souhlas se zpracováním osobních údajů,
    - žádosti a jejich formy,
    - povinnosti oprávněných osob při zpracovávání osobních či citlivých údajů,
    - pověřenec pro ochranu osobních údajů.
    - zprostředkující speciální osoby,
    - zpracovatelé,
    - kontrola dodržování povinností z pohledu MMP,
- záznamy,
- související dokumentace,
- závěrečná ustanovení,
- přílohy (Zpracovávání osobních údajů, 2018).

Instrukce tedy slouží jako určitá forma shrnutí evropského nařízení ve věcech, které jsou pro zaměstnance magistrátu důležité a potřebné. V současné době se připravuje nová aktualizovaná verze, která by stávající instrukci měla nahradit.

Již byl v práci zmíněn program Agendio. Magistrát totiž využívá takzvaný systém **agend**, které slouží k ujasnění daných záležitostí a činností souvisejících s ochranou osobních údajů. Tyto agendy jsou určené jak pro zaměstnance magistrátu, tak pro tajemníky

obvodů, školy, školky a příspěvkové organizace. Jsou uloženy na sdíleném disku, ke kterému mají všichni výše uvedení přístup.

Agendy objasňující problematiku GDPR zahrnují například následující kapitoly (interní dokumentace MMP, 2020):

1. Účely zpracování,
2. Kategorie subjektu údajů,
3. Kategorie osobních údajů,
4. Kategorie příjemců,
5. Plánované lhůty pro výmaz kategorií osobních údajů,
6. Obecný popis technických a organizačních opatření.

Výhoda těchto agend je taková, že magistrát jasně vytvoří určitá pravidla (v tomto případě dle obecného nařízení), díky čemuž například tajemníci obvodů už toto nemusí řešit a stačí dodržovat body stanovené magistrátem.

V souvislosti s implementací GDPR bylo také nutné podepsat se zákazníky a dodavateli nové smlouvy o zpracování osobních údajů.

4 Dopady GDPR na daný ekonomický subjekt

Čtvrtá kapitola představuje konkrétní dopady GDPR na Magistrát města Plzně. Jejím cílem je zodpovědět otázky týkající se provedených změn, náročnosti implementace GDPR, zabezpečení osobních údajů či případných problémů, se kterými se zaměstnanci museli potýkat.

Následující podkapitoly čerpají z interních zdrojů (interní zdroje MMP, 2020), mezi které patří konzultace, diskuse, rozhovory či různé pracovní dokumenty (více definováno v kapitole 3.2).

Podkapitola týkající se elektronické dokumentace a jejího zabezpečení (4.7.2) je založena (mimo výše uvedené) také na e-mailové komunikaci se zaměstnancem Správy informačních technologií města Plzně (interní zdroje SIT města Plzně, 2020).

4.1 Funkce pověřence pro ochranu osobních údajů

Jako každý jiný úřad a stejně jako každá právnická osoba, Magistrát města Plzně disponuje informacemi, které jsou určeny buďto pouze pro zaměstnance či pouze pro vedení města Plzně. Tato data MMP označuje jako *utajované*.

Proto již před zavedením GDPR v subjektu existovala pracovní pozice, která zajišťovala bezpečnost informací a starala se o veškeré náležitosti související s těmito informacemi. Konkrétně tuto pozici zastupoval bezpečnostní ředitel, který se zodpovídal Kanceláři tajemníka Magistrátu města Plzně.

Se zavedením GDPR tedy bylo zapotřebí stanovit pověřence pro ochranu osobních údajů oficiálně. Zde se z obecného pohledu nabízely dvě možnosti. První možností bylo zvolit si vlastního pověřence pro ochranu osobních údajů, který bude zaměstnancem subjektu, a jehož pracovní náplní bude zajišťovat ochranu osobních údajů pouze pro tento subjekt. Druhá varianta by znamenala využití služeb externího pověřence pro ochranu osobních údajů (externí společnosti), která poskytuje zejména poradenské služby, kontroluje dodržování ochrany osobních údajů dle nařízení a vede záznamy o činnostech zpracování.

Vzhledem k tomu, že Magistrát města Plzně již obdobnou pozicí disponoval, vedení se rozhodlo tyto dvě funkce spojit. Bezpečnostní ředitel tedy v současné době zastává i funkci pověřence ochrany osobních údajů ve spolupráci s kolegyní, která je jako „referent GDPR“ oficiálně uvedena na internetových stránkách města Plzně.

Dá se tedy říci, že MMP má pověřence pro ochranu osobních údajů dva. Oba byli vybráni z vlastních zdrojů čili na pracovní smlouvu a došlo pouze k rozšíření jejich pracovních kompetencí. Na rozhodování o této funkci se podílelo pět osob po dobu jednoho týdne (dle odhadu bezpečnostního ředitele MMP). Díky tomuto kroku tedy nebylo nutné zaškolovat zaměstnance nové, ale pouze obeznámit stávající zaměstnance s náležitostmi souvisejícími s novou funkcí. Vyžadováno bylo v prvotní fázi (ve fázi příprav) pouze nastudování obecného nařízení a následně českého adaptačního zákona. Dále bylo nutné účastnit se školení a vést veškerou dokumentaci související jak s implementací GDPR, tak s jeho dodržováním a kontrolou.

To samozřejmě mělo za důsledek také zvýšenou pracovní zátěž a větší množství administrativy. Pověřenec osobních údajů MMP se totiž nezabývá pouze osobními údaji uvnitř samotného magistrátu, ale stará se i o další subjekty, které pod Magistrát města Plzně spadají. Jedná se zejména o základní a mateřské školy, městské organizace a také jednotlivé obvody. Všechny tyto subjekty měly před zavedením GDPR možnost volby, zda budou chtít využívat služeb pověřence MMP či si zvolí pověřence vlastního. Většina si zvolila možnost využití pověřence MMP. Co se městských obvodů týče, pouze Úřad městského obvodu 2 – Slovany (ÚMO 2) má pověřence vlastního. Z příspěvkových organizací je to pak například Městský ústav sociálních služeb města Plzně, Dětské centrum Plzeň a Správa hřbitovů a krematoria města Plzně.

Dle vedoucího kanceláře tajemníka MMP je funkce pověřence pro ochranu osobních údajů z převážné části poradenskou službou. Nabízí tedy zejména konzultace všem organizacím spadajícím pod město Plzeň, stejně jako zaměstnancům magistrátu.

Jak již bylo řečeno, obvody, školy a příspěvkové organizace vychází v rámci GDPR také z agend magistrátu, což velmi usnadňuje práci pověřence pro ochranu osobních údajů. V počátku je sice nutné agendu vytvořit, nicméně následně dochází k úspoře času z důvodu toho, že je velké množství informací ohledně GDPR uloženo na sdíleném disku (software Agendio). Zároveň se tak magistrát může pojistit, že nedojde k nedorozumění a nepochopení stanovisek obecného nařízení.

Právě z toho důvodu je také velké množství informací a doporučení možné nalézt na internetových stránkách města Plzně, jelikož informovanost a udržitelnost informačních upozornění jsou dle MMP nejpodstatnějšími faktory v rámci GDPR.

4.2 Nesprávné pochopení evropského nařízení

Jedním z nejzásadnějších problémů, který se od zavedení GDPR až po současnost vyskytuje, je dle MMP nesprávné pochopení obecného nařízení. Jak již samotný název vypovídá, jedná se o nařízení *obecné*. Není tedy příliš detailní a nezahrnuje žádné konkrétní příklady či situace, jakým způsobem se při nakládání s osobními údaji zachovat. V některých případech toto nařízení osvětluje český adaptační zákon, nicméně pro laika, který nemá dostatečný přehled o oblasti práva, může být v mnoha případech zavádějící a nepřesný.

Zejména při počátečním „boomu" okolo GDPR začalo docházet k všeobecné panice a vytváření strachu zejména z velkých pokut, které jsou v Obecném nařízení konkrétně vyčíslené (jejich horní hranice). Dle Magistrátu města Plzně se tento strach začal objevovat zejména v rámci vedení mateřských a základních škol, potažmo pak mezi rodiči dětí navštěvujících tyto školy. Velice častým jevem bylo, a stále je, **nadbytečné vyžadování souhlasů**.

Pověřenec pro ochranu osobních údajů MMP dennodenně vyřizoval e-maily a telefonáty zahrnující dotazy ohledně problematiky GDPR. To se týkalo zejména nejasností ohledně zveřejňování fotografií žáků v rámci základních škol (například na nástěnkách).

V souvislosti s tímto vydal Úřad pro ochranu osobních údajů veřejné sdělení.

> *„V úvodu školního roku Úřad pro ochranu osobních údajů upozorňuje na přetrvávající nesprávné chápání souhlasu se zpracováním osobních údajů ve školství. S tím je spojena špatná praxe spočívající ve vyžadování nadbytečných souhlasů rodičů se zpracováním osobních údajů dětí při aktivitách, které jednoznačně patří do povinné náplně činnosti školy anebo s ní úzce souvisí."* (ÚOOÚ, 2019c)

Jedním z příkladů, se kterými se MMP setkal je situace, kdy plzeňská základní škola vyžadovala souhlas rodičů s fotografováním jejich dítěte. Ti ale souhlas neposkytli. Následně pak docházelo k neshodám, jelikož dítě se vlivem tohoto rozhodnutí neobjevilo na oficiálních školních fotografiích.

Pověřenec MMP se tedy stejně jako Úřad pro ochranu osobních údajů snaží vysvětlovat zejména subjektům v oblasti školství, že ne všechny osobní údaje se týkají problematiky

GDPR. Co se týče pořizování a zároveň i zveřejňování fotografií souvisejících s činnostmi školy, zde se nejedná o problematiku ochrany osobních údajů, ale o problematiku ochrany soukromí. Ta je zahrnuta v občanském zákoníku (§ 84 – zákon č. 89/2012 Sb.). Není tedy v žádném případě nutné vyžadovat souhlas tohoto typu (ÚOOÚ, 2019d).

4.3 Administrativní a časová náročnost

Z hlediska administrativní a časové náročnosti nastala největší zátěž v době příprav a v době implementace GDPR. Důvod byl zejména ten, že magistrát chtěl být na GDPR důkladně připraven. Následující tabulka zobrazuje jednotlivé kroky implementace GDPR (již vysvětleno v kapitole 3.2.3). Zároveň obsahuje také dobu trvání jednotlivých kroků a přibližný počet zaměstnanců, kteří se na daném kroku podíleli.

Tabulka č. 4: Časová náročnost implementace GDPR

	Časová náročnost	**Počet osob**
1. Úvodní proškolení	8 týdnů	6 školitelů a zhruba 220 proškolených osob
2. Ustanovení funkce DPO	1 týden	5 osob[9]
3. Revize s analýzou existujícího prostředí	4 týdny	110 osob
4. Rozdílová analýza	12 týdnů	2 vedoucí osoby (celkem zhruba 50 účastníků)
5. Závěry a doporučení na základě rozdílové analýzy	6 týdnů	2 osoby
6. Plán postupu a realizace doporučení	4 týdny	2 osoby
7. Pravidelná revize	jednou ročně (8 týdnů)	35 osob

Zdroj: interní zdroje MMP, 2020
Zpracovala: Marie Velkoborská, 2020

Jak již bylo v práci uvedeno, nejzásadnějším krokem v souvislosti s implementací GDPR bylo provedení rozdílové analýzy. Samotná analýza byla zpracována během prvního

[9] Přibližný odhad bezpečnostního ředitele MMP.

čtvrtletí roku 2018 čili zhruba v období 3 měsíců. Dle bezpečnostního ředitele a vedoucího Kanceláře tajemníka MMP byla samotná analýza administrativně nejnáročnější činností (v rámci činností souvisejících s GDPR) a byla také velkým zásahem do běžného chodu magistrátu z časového hlediska. Na analýze se podíleli zejména vedoucí pracovníci jednotlivých odborů, vedoucí Magistrátu města Plzně a další zaměstnanci. Celkem se jednalo zhruba o 50 osob včetně bezpečnostního ředitele a referenta GDPR.

V souvislosti s touto analýzou se každý týden pořádaly porady, kde se rozdělovaly úkoly, docházelo ke kontrole plnění povinností a k případné diskusi a upřesňování informací. Odpovědnou osobou byl v této činnosti vedoucí Kanceláře tajemníka. Klíčovou roli zde hrál však pověřenec pro ochranu osobních údajů, který byl všem zaměstnancům k dispozici, vypomáhal s vyplňováním tabulek a případně od zaměstnanců vyžadoval doplňující informace potřebné pro úspěšné dokončení příprav a implementace GDPR. Zároveň byl všem účastníkům poskytnut podpůrný materiál s návodem, jak při zpracovávání analýzy postupovat[10].

Za velkou výhodu provedené analýzy je považována zejména připravenost na GDPR z hlediska uspořádání osobních údajů a obeznámení zaměstnanců s náležitostmi GDPR.

Velkým přínosem, který v první řadě nebyl cílený, bylo také nastolení pořádku v datech a činnostech subjektu.

Z obecného hlediska provedená analýza odhalila dva zásadní problémy:

1) některé činnosti byly vykonávány na více pracovištích/odborech zároveň,
2) některé souhlasy byly nadbytečné.

Na základě těchto (a jiných) výstupů bylo vedení magistrátu schopno zefektivnit jednotlivé procesy a do budoucna tak minimalizovat množství byrokracie na daných pracovištích.

Tato analýza však neskončila svou platnost s implementací GDPR. Je potřeba ji každoročně aktualizovat, kontrolovat plnění všech povinností dle obecného nařízení a případně doplňovat o nové informace a zlepšující opatření.

[10] Návod pro zaměstnance je k dispozici v příloze E.

4.4 Finanční náročnost

Finanční hledisko je velmi těžko odhadnutelné, jelikož proces implementace GDPR zahrnoval velké množství kroků a valná většina z nich probíhala interně v rámci běžné pracovní doby. Nebyly tedy spotřebovány žádné zásadní finanční prostředky.

4.4.1 Náklady na školení

Jediný magistrátem zaznamenaný výdaj v souvislosti s GDPR se týká úvodních školení, které (viz tabulka č. 4) probíhaly po dobu 8 týdnů v období prosince roku 2017 a února roku 2018. Školení prováděly převážně externí společnosti – tedy za úhradu. V některých případech školení organizoval i krajský úřad Plzeňského kraje či zástupci Ministerstva vnitra České republiky – v těchto případech byla školení bez poplatku.

Celkové náklady za školení včetně časového rozmezí a počtu zúčastněných osob zobrazuje následující tabulka.

Tabulka č. 5: Finanční náročnost školení v problematice GDPR

Časové rozmezí	Prosinec 2017 Únor 2018
Počet školitelů	6
Počet proškolených zaměstnanců	220
Celková částka za školení	70 000 Kč

Zdroj: interní zdroje MMP, 2020
Zpracovala: Marie Velkoborská, 2020

Celkové vynaložené náklady na školení v problematice GDPR tedy činily 70 000 Kč.

4.4.2 Náklady na provedení analýzy

Na samotné analýze pracovalo velké množství zaměstnanců magistrátu a nebylo jasně stanoveno, kolik hodin denně musí analýze věnovat. Na základě údajů poskytnutých Magistrátem města Plzně byl proveden následující odhad.

Analýza probíhala po dobu 3 měsíců v období od ledna do března roku 2018. Na jejím zpracování se podílelo zhruba 50 zaměstnanců magistrátu – jednalo se pouze o interní zaměstnance. Časová náročnost byla zhruba 2 hodiny denně – tedy asi čtvrtina pracovní doby. Vše přehledně zobrazuje následující tabulka.

Tabulka č. 6: Odhad finanční náročnosti

Časové rozmezí	3 měsíce
Počet hodin denně	2
Počet osob	50
Průměrná mzda	26 200 Kč[11]

Zdroj: interní zdroje MMP, 2020
Zpracovala: Marie Velkoborská, 2020

Vezmeme-li v úvahu výše uvedené hodnoty, dostaneme následující výpočet.

3 měsíce x 50 osob x 26 200 Kč / 4 = 982 500 Kč.

Odhadovaná finanční náročnost provedené analýzy GDPR je tedy celkově *982 500* Kč.

Analýzu a poradenství, co se GDPR týče, nabízí v současné době i mnoho firem, jejichž služby se mohou pohybovat v hodnotě desítek až stovek tisíc Kč (dle informací zjištěných MMP). Za velkou výhodu lze tedy považovat skutečnost, že analýza byla prováděna interně – reálně tedy stála pouze čas stávajících zaměstnanců a jejich zdržení od běžných pracovních povinností.

Subjekt pro potřeby této práce neposkytl žádné další materiály související s finanční náročností implementace GDPR. Není tedy v současné době možné přesně stanovit finanční dopad ve sledované oblasti.

4.5 Proces kontroly plnění povinností dle GDPR

Samotné zavedení jakéhokoliv systému ochrany osobních údajů není nikdy konečným bodem. Vše je nutné pravidelně kontrolovat a zjišťovat, zda se jednotlivé činnosti neodchylují od původního plánu a zda je vše dodržováno v souladu s obecným nařízením.

Právě z toho důvodu bylo rozhodnuto o pravidelných schůzích se zaměřením na GDPR, které se pořádají jednou ročně po dobu 8 týdnů. Princip spočívá v tom, že pověřenec pro ochranu osobních údajů (bezpečnostní ředitel) školí takzvané zprostředkující speciální osoby – jedná se o pověřené osoby za každý odbor (většinou jde o vedoucí odboru). Ti se podílí na revizi záznamů o činnostech zpracování osobních údajů a předávají informace dále svým podřízeným. Jedná se o počet 35 osob.

[11] Stanoveno dle platových tabulek (10. platová třída, délka praxe do 15 let).

Cílem těchto porad je mimo jiné:

- obeznámení s novinkami v oblasti ochrany osobních údajů,
- kontrola dodržování všech povinností dle GDPR,
- kontrola aktuálnosti provedené analýzy,
- případné úpravy a doplnění provedené analýzy,
- diskuse a předložení potenciálních návrhů.

Dle MMP je kontrola dodržování povinností dle GDPR v podstatě „klasickou inventurou“.

4.6 Personální gramotnost v problematice a školení zaměstnanců

S příchodem nového nařízení bylo nezbytné všechny zaměstnance s touto problematikou seznámit. Jak již bylo patrné z tabulky č. 4, prvním bodem implementace GDPR bylo úvodní proškolení, které trvalo zhruba 8 týdnů a účastnilo se ho celkem 6 školitelů a zhruba 220 zaměstnanců magistrátu. Zvláštní důraz byl kladen zejména na ty zaměstnance, jejichž hlavní činnost zahrnovala právě nakládání s osobními údaji. Příkladem může být personální oddělení, které zpracovává a uchovává velké množství informací o zaměstnancích magistrátu.

V rámci tohoto školení byla důležitá také informovanost ohledně prováděné analýzy, tedy jak konkrétně postupovat při vyplňování analytických tabulek. Prostředkem poskytování těchto informací byly zejména podpůrné materiály (návody) již zmíněné v předchozích kapitolách.

Pro podpoření gramotnosti v této problematice se v současné době pravidelně pořádají doplňující školení. Také dochází k vydávání již zmiňovaných instrukcí nebo směrnic, které instruují pracovníky o tom, jak mají s osobními údaji zacházet. Veškeré informace jsou podány stručně, avšak výstižně a srozumitelně.

Obecně je dle vedoucího kanceláře tajemníka největší hrozbou lidský faktor (jeho selhání), a právě proto se vedení snaží o neustálé sebevzdělávání i vzdělávání svých zaměstnanců v této problematice.

Velmi často se na pracovišti objevuje problematika neznalosti informačních technologií, zejména pak jejich bezpečnosti. Jedná se například o situace, kdy zaměstnanec obdrží podezřelý e-mail a rozhodne se ho otevřít bez většího přemýšlení nad následky. Magistrát

má sice k dispozici software, kterým monitoruje chování svých zaměstnanců na internetových stránkách, nicméně již nezajistí, že zaměstnanec závadnou internetovou stránku nenavštíví.

Potenciálnímu úniku osobních údajů přes internetovou síť tedy v současné době není možné předejít.

4.7 Technické zabezpečení dat

Zabezpečení dat je pravděpodobně jedno z nejdiskutovanějších témat, co se problematiky GDPR týče. Proto i právě dopady týkající se technického zabezpečení jsou pro každý ekonomický subjekt zásadní, a to zejména po zavedení obecného nařízení. Vedení i zaměstnanci jsou nyní povinni klást mnohem větší důraz na ochranu dat než před změnou zákona. Nedodržování těchto povinností může vést jednak k vysokým sankcím dle nařízení GDPR a jednak k samotnému snížení důvěryhodnosti subjektu.

Technické zabezpečení se však netýká pouze archivování klasické papírové dokumentace, avšak i tato metoda je stále populární, a to zejména na úřadech, kterým je i Magistrát města Plzně. Využívají se zejména kartotéky, archivy, šanony, uzamčené skříně, případně trezory a další zabezpečené prostory. Těmi magistrát disponoval již před zavedením GDPR.

Stále ve větším měřítku jsou v současné době využívány informační technologie, jejichž zabezpečení se často opomíjí a podceňuje. Bezpečnost IT zahrnuje zejména bezpečnost informačních systémů subjektu, jejich ochranu a s tím související ochranu informací a dat, jejichž únik může ohrozit budoucnost jakéhokoliv podniku. Přestože již zmiňované nařízení ePrivacy stále nevešlo v platnost, samotný Úřad pro ochranu osobních údajů upozorňuje na to, že GDPR je důležité vnímat i v souvislosti s elektronickou komunikací (ÚOOÚ, 2020).

4.7.1 Papírová dokumentace

Magistrát města Plzně už před zavedením GDPR velmi dbal na ochranu osobních údajů, nicméně s novým nařízením bylo potřeba stanovit nová pravidla a dodržovat je poctivěji než kdy dříve. Proto byla sestavena nová bezpečnostní opatření, která definuje instrukce MMP o zpracování osobních údajů. Tato opatření se poctivě dodržují, aby se předešlo zneužití těchto dat.

Důležitá bezpečností opatření pro práci s papírovou dokumentací jsou:

- mlčenlivost v souvislosti s osobními údaji,
- uložení nosičů pod neprůhledným uzamčením:
    - kancelář,
    - skříň,
    - trezor,
    - jiný uzamčený prostor,
- zákaz vynášení materiálů obsahující osobní údaje mimo pracoviště,
- povinnost průběžné likvidace pracovních kopií dokumentů ve skartovacím zařízení,
- dodržovat uzamykání kancelářských prostor, pokud se zde nachází volně přístupné nosiče dat (obsahující osobní údaje),
- povinnost informovat vedoucího zaměstnance v případě neoprávněného použití či zpracování osobních údajů, i pokud se jedná pouze o podezření (Zpracování osobních údajů, 2018).

Je nutné zmínit, že dodržování výše uvedeného je úzce závislé na zodpovědnosti zaměstnanců a není v kompetencích vedoucích pracovníků neustále kontrolovat, zda je vše naplňováno (zda dochází k uzavírání dveří, zakládání šanonů a podobně).

Archivy města Plzně jsou umístěny na Radnici města Plzně na náměstí Republiky (dlouhodobé uložení), nebo na pracovišti v Kopeckého sadech (personální oddělení – aktuální data o zaměstnancích).

4.7.2 Elektronická dokumentace

Jednou z příspěvkových organizací Magistrátu města Plzně je pracoviště *Správa informačních technologií (SIT)*, která disponuje vlastním pověřencem pro ochranu osobních údajů. Tato organizace je zodpovědná například za projekt „Záchranka“. Jedná se o aplikaci, která umožňuje záchranné službě rychle vyhledat volajícího prostřednictvím GPS v mobilním telefonu. Druhým příkladem projektu, který vznikl pod záštitou SIT je takzvaný „ChatBot“, což je počítačový program, který umožňuje rychlou komunikaci mezi magistrátem a občanem (například prostřednictvím platformy Messenger). Zároveň však pro MMP spravuje vše související s informačními technologiemi a elektronickou komunikací (SIT MP, 2020; interní zdroje MMP, 2020).

Elektronickou dokumentaci je z obecného hlediska možno spravovat a uchovávat několika způsoby. Mezi ně patří například následující:

- software,
- databáze,
- lokální nebo síťová úložiště,
- cloudová služba,
- e-mail,
- zálohování.

Zálohování dat probíhá v případě MMP na vlastních databázových a dokumentových serverech. Data jsou zálohována na základě vnitřních pravidel a směrnic, a to prostřednictvím diskových polí a pásek v zálohovací knihovně. Archivace dat je taktéž založena na využití pásek.

V síti magistrátu je využíváno několik druhů datových úložišť, která jsou využívána dle způsobu práce s datu (množství dat – kapacita/požadovaný výkon). Vlivem GDPR nebylo nutné pořizovat žádná nová speciální úložiště (interní zdroje SIT města Plzně, 2020).

Magistrát města Plzně má v současné době všechna svá datová úložiště umístěna na území města Plzně. Tato skutečnost však nebývá častým jevem – některá města uchovávají svá data dokonce i v zahraničí. Výhodou lokálního uskladnění je primárně snadná dostupnost, jednoduchá manipulace a možnost důkladné kontroly zabezpečení.

Důležitá bezpečností opatření pro práci s elektronickou dokumentací (pro MMP) jsou:

- mlčenlivost v souvislosti s osobními údaji,
- uložení nosičů osobních údajů (flash disky, paměťové karty) takovým způsobem, aby se k nim nedostala nepovolaná osoba (zejména po dobu nepřítomnosti zodpovědné osoby),
- uložení dat pod přístupovým heslem (v případě uložení v paměti kancelářského počítače),
- zákaz vynášení materiálů obsahující osobní údaje mimo pracoviště (za pomoci nosiče dat),
- povinnost průběžné likvidace pracovních kopií dokumentů ve skartovacím zařízení (CD),

- dodržovat uzamykání kancelářských prostor, pokud se zde nachází volně přístupné dokumenty,
- povinnost informovat vedoucího zaměstnance v případě neoprávněného použití či zpracování osobních údajů, i pokud se jedná pouze o podezření (Zpracování osobních údajů, 2018).

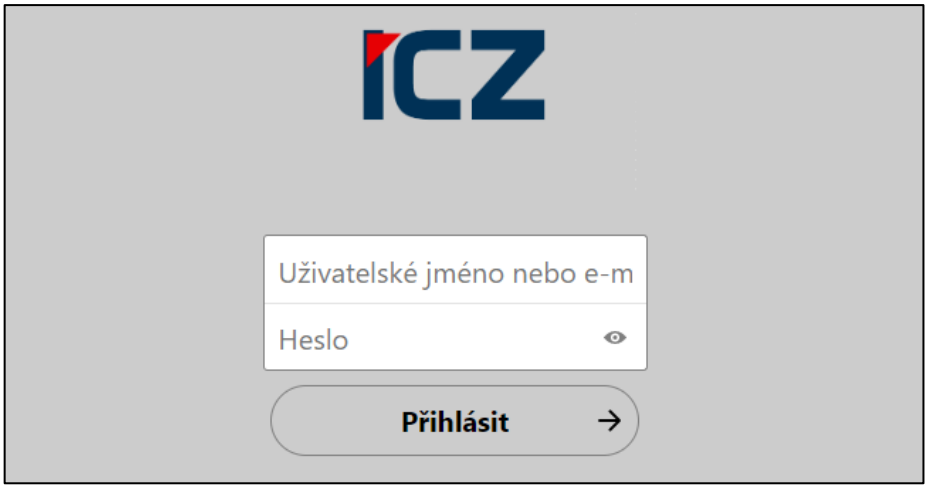
Stěžejní platformou v souvislosti se správou a uchováváním elektronické dokumentace je program **„ICZ e-spis“**. Jedná se o elektronickou spisovou službu, kterou Magistrát města Plzně využívá při práci s dokumenty – konkrétně se stará o příjem, evidenci, oběh, vyřizování, odesílání a ukládání těchto dokumentů. E-spis se mimo jiné zabývá také archivací a skartací těchto dokumentů. Veškeré souhlasy jsou uskutečněny prostřednictvím elektronického podpisu a časového razítka. Elektronický podpis je mimo jiné vyžadován i při podávání žádosti na MMP subjektem údajů. Vše je v souladu s legislativou, tedy včetně legislativy týkající se GDPR. Zaměstnanci magistrátu od počátku nemuseli tyto záležitosti řešit, jelikož program byl po zavedení GDPR aktualizován a modifikován tak, aby odpovídal požadovaným předpisům (ICZ, 2020; interní zdroje MMP, 2020).

Magistrát využívá uzavřenou síť s privátními rozsahy IP adres. V rámci implementace GDPR bylo nutné aktualizovat některé informační systémy takovým způsobem, aby byly v souladu s legislativou (již zmíněno v souvislosti se softwarem e-spis) (interní zdroje SIT města Plzně, 2020).

Celý magistrát pracuje na počítačích značky HP a prostřednictvím operačního systému Windows 10 Pro, který disponuje potřebnými zabezpečeními a antivirovou ochranou. Výběr a instalace těchto technologií probíhá na základě stanovených softwarových standardů, které určuje Správa informačních technologií města Plzně (SIT MP, 2019).

Každý zaměstnanec má k dispozici vlastní pracovní počítač či notebook (dle stanovených standardů), který vyžaduje přihlášení za pomoci uživatelského jména a hesla. Toto heslo je potřeba měnit každé tři měsíce a dodržet pravidlo 8 znaků, alespoň jednoho velkého písmena a jednoho čísla/znaku. Systémy jsou přístupné na základě dvoustupňového přihlášení – nejprve je potřeba přihlásit se do počítače a následně do konkrétního programu, se kterým daný zaměstnanec v současné době pracuje. Pro příklad lze uvést přihlášení do softwaru e-spis (následující obrázek).

Obrázek č. 4: Přihlášení do softwaru e-spis



Převzato: ICZ, n. d.

MMP využívá mnoho různých způsobů zabezpečení dat i celé sítě. Kvůli GDPR se však nenasazovalo žádné zvláštní opatření (interní zdroje SIT města Plzně, 2020).

Jak již bylo zmíněno, základní nedostatky ve zpracovávání elektronické dokumentace lze vidět v softwaru, který monitoruje provoz sítě. Přestože vedení magistrátu ví, jaké webové stránky daný zaměstnanec v uplynulém týdnu navštěvoval, nejsou nastavena žádná opatření, která by tomu zabránila.

4.8 Dopady GDPR po dvouletém ustálení

Nejčastějším problémem, se kterým se Magistrát města Plzně od zavedení GDPR setkává, je nechuť zaměstnanců k dodržování povinností dle instrukcí magistrátu (vytvořených na základě obecného nařízení). Velká část zaměstnanců toto nařízení vnímala jako zbytečnou přítěž. Bylo nutné zúčastnit se potřebných školení, která měla za úkol instruovat zaměstnance ohledně záležitostí spojených s implementací GDPR (průběh příprav na GDPR, analýza GDPR, postupy po zavedení). Také se začalo objevovat množství nových instrukcí, se kterými se zaměstnanci museli seznámit a naučit se je dodržovat.

Nepříliš velká radost z těchto nových povinností se projevila zejména ve snížené motivaci zaměstnanců a neochotě k práci, která souvisela se zabezpečením osobních údajů. Po téměř dvou letech trvání si však zaměstnanci na tuto skutečnost zvykli a nyní přijímají nové pracovní povinnosti (dle GDPR) již jako běžnou každodenní činnost. Lze tedy

konstatovat, že v současné době se přímo na pracovišti MMP žádné interní problémy (v rámci ochrany osobních údajů) neobjevují a vše probíhá v souladu s obecným nařízením.

Přestože platnost GDPR už nějakou dobu trvá, stále se objevují problémy či nejasnosti v obecném nařízení. MMP spravuje ochranu osobních údajů pro velké množství subjektů v Plzni a velice ojediněle dochází k situaci (pochybení), která může být v rozporu s GDPR. V takovém případě magistrát obdrží dopis z Úřadu pro ochranu osobních údajů, který požaduje vysvětlení dané situace. Vše se následně vyřeší či napraví.

Již bylo také uvedeno, že problémem je neznalost či špatné pochopení nařízení GDPR, které vede k dezinformacím, následně ke zbytečným krokům a k vyvolávání paniky. Právě proto se Magistrát města Plzně snaží tuto tématiku osvětlovat jak prostřednictvím agend, instrukcí či veřejně dostupných dokumentů, tak prostřednictvím konzultací se zájemci o informace.

Velkému množství problémů MMP předchází tím, že disponuje vlastním pověřencem pro ochranu osobních údajů. Ten je kdykoli k dispozici a je schopen vše potřebné okamžitě řešit. Magistrát to považuje za velkou výhodu oproti variantě externího pověřence, který má často na starost velké portfolio subjektů a dochází tedy k určité prodlevě, než může s danou záležitostí nakládat.

Z hlediska informačních technologií nedošlo vlivem zavedení GDPR k žádným radikálním změnám či novým opatřením. Byly pouze aktualizovány stávající informační systémy (interní zdroje SIT města Plzně, 2020).

5 Návrhová část

Obecné nařízení je založeno na dvou přístupech. Tím prvním je „princip odpovědnosti správce“, který určuje odpovědnost za dodržování zásad zpracování (článek 5) a následné doložení například záznamu o činnostech zpracování.

Druhým přístupem je „přístup založený na riziku“, který spočívá v tom, že *„správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů“* (MVČR, 2019b).

Poslední kapitola diplomové práce se tedy zabývá zejména problematikou potenciálních rizik souvisejících se zabezpečením osobních údajů. Na základě toho budou vyvozeny závěry, prostřednictvím kterých bude možné definovat návrhy na redukci těchto rizik a uvést další doporučení, která by pomohla efektivnímu řízení MMP z hlediska ochrany osobních údajů.

5.1 Analýza rizik

Pro úspěšné vykonání analýzy rizik je nejprve potřeba daná rizika identifikovat.

Riziko může být z obecného hlediska zapříčiněno několika faktory. V případě Magistrátu města Plzně lze tyto vlivy rozdělit do tří kategorií:

- lidský faktor,
- technický faktor,
- externí faktor.

Veškerá rizika uvedená v následujících podkapitolách jsou sestavena na základě zkušeností čerpaných z návštěv pracoviště Magistrát města Plzně. V těchto zkušenostech jsou obsaženy konzultace, diskuse, rozhovory a pozorování pracovního prostředí (tato kapitola navazuje na kapitolu předchozí – dopady). Veškerá rizika jsou tedy založena na výpovědi zaměstnanců či na subjektivním dojmu autorky práce.

Rizika související s informačními technologiemi (či rizika, která se alespoň částečně dotýkala problematiky technického zabezpečení) byla mimo výše uvedené konzultována také s odborníkem v oblasti IT.

Před sestavením tabulky obsahující tato rizika, je nezbytné definovat dva faktory, na jejichž základě bude sestavena takzvaná matice rizik neboli krizová matice. Jedná se o faktor pravděpodobnosti výskytu rizika v daném čase a faktor závažnosti dopadů na ekonomický subjekt.

Pravděpodobnost výskytu rizika určuje stupeň pravděpodobnosti, že riziko nastane (Mulačová & Mulač, 2013). Jednotlivé stupně a jejich procentuální i slovní vyjádření je znázorněno v následující tabulce.

Tabulka č. 7: Číselné hodnocení pravděpodobnosti výskytu rizika

Hodnota	Pravděpodobnost výskytu rizika [% ročně]	Pravděpodobnost výskytu rizika (slovní vyjádření)
1	<0;5>	Velmi nízká
2	<6;20>	Nízká
3	<21;50>	Možná
4	<51;70>	Vysoká
5	<71;100>	Velmi vysoká

Zdroj: Váchal & Vochozka, 2013
Zpracovala: Marie Velkoborská, 2020

Faktor závažnosti dopadů rizika definuje, jaké dopady a následky se mohou vyskytnout, a jaký budou mít účinek (Mulačová & Mulač, 2013). Jednotlivé stupně a jejich slovní vyjádření znázorňuje následující tabulka.

Tabulka č. 8: Hodnocení závažnosti dopadů rizika

Hodnota	Slovní vyjádření závažnosti potencionálních dopadů
1	Zanedbatelná
2	Malá
3	Střední
4	Významná
5	Fatální (nepřijatelná)

Zdroj: Váchal & Vochozka, 2013
Zpracovala: Marie Velkoborská, 2020

Nutné je také zmínit **faktor významnosti (úrovně rizika)**, jehož hodnota je součinem faktoru pravděpodobnosti a faktoru dopadu.

Přiřazení těchto hodnot rizikům (v následujících podkapitolách) je založeno na subjektivním pocitu autorky (pozorování pracoviště, dedukce), názoru odborníků v dané oblasti (konzultant IT) a výpovědi zaměstnanců magistrátu (DPO a další).

5.1.1 Lidský faktor

Faktor lidského pochybení je zcela jistě nejvýraznějším problémem ve velkém množství organizací. Jinak tomu není ani na pracovišti Magistrátu města Plzně. Příčinou tohoto pochybení může být zejména nedbalost, neopatrnost, neznalost či záměrné zavinění (úmysl).

Všechna rizika zjištěná za pomoci výše uvedených metod jsou zobrazena v následující tabulce (č. 9). Rizika jsou upřesněna ve sloupci popisující toto riziko, následně jim je přiřazen stupeň pravděpodobnosti vzniku (PST) a stupeň dopadu tohoto rizika (dle výše uvedených tabulek).

Tabulka č. 9: Lidský faktor

ID	Název rizika	Popis rizika	PST	Dopad	Význam
1	Nedbalé nakládání s listinnými dokumenty	Nezakládání šanonů Nechávání dokumentů bez dozoru Poskytnutí osobních údajů třetí straně Nesystematická práce s dokumenty Ztráta či náhodné zničení	4	2	8
2	Porušení zabezpečení osobních údajů	Neodhlašování počítače Nechávání klíčů a přístupových karet bez dozoru Neuzamykání kartoték Nechávání otevřených dveří	4	2	8
3	Vynášení informací mimo pracoviště	Nedostatečné zabezpečení (šifrování dat, uzamčení dokumentů, absence neprůhledného obalu) Nedbalost při převozu a neopatrné nakládání s dokumenty Ztráta	3	2	6
4	Nedostatečná znalost GDPR	Nedostatečné nebo vůbec žádné školení zaměstnanců Neochota se vzdělávat Neochota dodržování pokynů, bagatelizace GDPR	3	4	12
5	Neznalost bezpečnosti používání informačních technologií	Otevírání podezřelých či zavirovaných souborů Chybovost při práci s daty obsahující osobní údaje Používání slabých, nebo žádných hesel	5	5	**25**
6	Korupční chování	Poskytnutí osobních údajů třetí straně za úplatu Zatajování korupční činnosti Záměrné zničení nebo zatajení dokumentů Neoprávněná změna	2	5	10
7	Nedodržování bezpečnostních pravidel návštěv	Pochybení vrátnice – umožnění přístupu na pracoviště neoprávněné osobě Pochybení pověřené osoby – umožnění volného pohybu neoprávněných osob bez dozoru	4	4	16
8	Neodborná likvidace vyřazených nosičů dat	Vyhození nefunkčních úložných zařízení a nosičů (harddisk, CD, flash disk a další)	2	3	6

Zdroj: interní zdroje MMP, 2020

Zpracovala: Marie Velkoborská, 2020

Následující tabulka popisuje možné důsledky výše uvedených rizik, které jsou rozděleny do tří po sobě jdoucích fází.

Tabulka č. 10: Důsledky rizik lidského faktoru

První fáze	Druhá fáze	Třetí fáze
Únik, ztráta, změna či případné zneužití osobních údajů	Porušení povinností GDPR Sankce Ztráta zaměstnance Nutnost výběrového řízení Nutnost zaškolení	Časová ztráta Finanční ztráta Ztráta prestiže a důvěryhodnosti

Zdroj: interní zdroje MMP, 2020
Zpracovala: Marie Velkoborská, 2020

Na základě vyhodnocení předchozích dvou tabulek lze usoudit, že nejvýznamnějším rizikem je nedostatečná znalost bezpečnosti používání informačních technologií. Spočívá například v tom, že zaměstnanec otevře jakýkoliv soubor, který obdrží, a to bez přemýšlení nad následky. Pro příklad lze uvést situaci, kdy zaměstnanec personálního oddělení obdrží prostřednictvím e-mailu následující soubor.

Obrázek č. 5: Přijetí PDF souboru

Zpracovala: Marie Velkoborská, 2020

Následně předpokládá, že se jedná například o životopis obsahující osobní údaje uvedeného Jana Nováka, který má zájem o zaměstnání. Ve skutečnosti se však může jednat o počítačový vir, který je pouze velmi dobře skrytý. Pouhým otevřením tohoto souboru pracovník spustí program, který průběžně stahuje všechny magistrátem přijaté osobní údaje. Magistrát si navíc ani nemusí být vědom toho, že nějaká data unikají.

Samozřejmě je však mnohem častější varianta, kdy lze na první pohled snadno odhalit, že se jedná o nebezpečný vir (malware). I za této situace se však stává, že zaměstnanec přesto soubor otevře, protože si neuvědomuje daná nebezpečí a rizika svého chování.

5.1.2 Technický faktor

Technické problémy se zejména v současné době rychlého rozvoje technologií objevují každodenně, a ne každý si plně uvědomuje možné následky těchto problémů (nejen v souvislosti s osobními údaji). Některé dopady navíc nejsou na první pohled zjistitelné, protože samotný problém často není ani odhalen. Právě z tohoto důvodu je této

problematice věnovaná samostatná kapitola, a to i přesto, že některé faktory technického pochybení byly již součástí předchozí tabulky (lidský faktor).

Tabulka č. 11: Technický faktor

ID	Název rizika	Popis rizika	PST	Dopad	Význam
9	Nedostatečný výkon výpočetní techniky	Neschopnost plně vykonávat práci z důvodu stárnutí hardwaru	4	3	12
10	Nedostatečné zabezpečení	Neaktualizovaná virová ochrana Absence pravidel na složitost a opakování hesel	4	5	**20**
11	Výpadky elektřiny	Nefunkčnost, chybějící záložní zdroje	1	4	4
12	Kolaps systému	Přehlcení systému zbytkovými daty	2	4	8
13	Technické chyby	Nečekané technické výpadky (nefunkční síťový prvek)	3	3	9
14	Výpadek zálohování	Nedostatečné úložiště dat Výpadek komunikace s datovým serverem	2	5	10

Zdroj: interní zdroje MMP, 2020
Zpracovala: Marie Velkoborská, 2020

Následující tabulka uvádí důsledky rizik technického charakteru rozdělených do tří fází.

Tabulka č. 12: Důsledky rizik technického faktoru

První fáze	Druhá fáze	Třetí fáze
Únik, pozměnění či případné zneužití osobních údajů	Nutnost technických oprav Nutnost aktualizace a modernizace informačních technologií	Časová ztráta Finanční ztráta Ztráta prestiže a důvěryhodnosti

Zdroj: interní zdroje MMP, 2020
Zpracovala: Marie Velkoborská, 2020

Dle výše uvedeného je nejrizikovějším bodem nedostatečné zabezpečení informačních systémů. Může se jednat například o nedostatečnou ochranu proti virům. To je však v kompetencích Správy informačních technologií města Plzně. Podstatným a z obecného hlediska i velmi běžným jevem je ale absence přísných pravidel na složitost hesel. S tím souvisí i umožnění zaměstnancům tato hesla opakovat či je pouze měnit na podobná (například přidáním jednoho čísla na konec původního hesla).

5.1.3 Externí faktor

Externím faktorem se rozumí jakékoliv vnější vlivy, které mohou nějakým způsobem ohrozit chod subjektu z hlediska ochrany osobních údajů. Tato rizika zobrazuje následující tabulka (včetně jejich ohodnocení).

Tabulka č. 13: Externí faktor

ID	Název rizika	Popis rizika	PST	Dopad	Význam
15	Odcizení dat	Vloupání do skladů za účelem odcizení osobních údajů	1	5	5
16	Narušení IT infrastruktury	Odposlouchávací zařízení síťového provozu	2	4	8
17	Kybernetická špionáž	Malware zaslaný e-mailem	5	5	**25**
18	Kyberterorismus	Neschopnost vykonávat práci vlivem útoku (Ransomware nebo DDos)	3	3	9

Zdroj: interní zdroje MMP, 2020
Zpracovala: Marie Velkoborská, 2020

Následující tabulka opět slouží k popisu důsledků rizik, tentokrát těch externích.

Tabulka č. 14: Důsledky rizik externího faktoru

První fáze	Druhá fáze	Třetí fáze
Únik či případné zneužití osobních údajů	Nutnost aktualizace a modernizace zabezpečení	Časová ztráta Finanční ztráta Ztráta prestiže a důvěryhodnosti

Zdroj: interní zdroje MMP, 2020
Zpracovala: Marie Velkoborská, 2020

Největší hrozbou externího prostředí je kybernetická špionáž, a tedy odcizení osobních údajů prostřednictvím malwaru, který kdokoli může obdržet e-mailem. Únik dat prostřednictvím informačních technologií je v dnešní době mnohonásobně jednodušší a také častější, než klasický případ „vloupání“ do archivů či skladových prostor.

5.2 Shrnutí a vyhodnocení rizik

V předchozí podkapitole byla popsána rizika, která ochrana a zabezpečení osobních údajů může skýtat, a na která by si (i z obecného hlediska) každý správce či zpracovatel měl dávat pozor. V tomto případě je správcem a zpracovatelem osobních údajů ekonomický subjekt Magistrát města Plzně.

Bylo identifikováno a definováno celkem 18 hlavních rizik, která byla rozdělena do tří kategorií dle potenciální příčiny vzniku – dle faktoru lidského, technického a externího. Tato podkapitola je celkovým shrnutím a vyhodnocením těchto rizik prostřednictvím vybrané metody. Touto metodou je již zmiňovaná **matice rizik (krizová matice)**, jejíž zobrazení lze nalézt v první části této podkapitoly (5.2.1).

Druhá část (5.2.2) poté pojednává o tématu úniku dat z globálního hlediska a jeho propojení s kybernetickou bezpečností a GDPR. Jak již bylo uvedeno, problematika úniku dat byla vyhodnocena jako prvotní důsledek nalezených rizik. Zároveň je i samotný únik dat rizikem, které vyplývá z rizik předchozích, a které má další důsledky a generuje další rizika. Jedním z těchto důsledků/rizik je porušení zabezpečení osobních údajů, tedy porušení nařízení GDPR. Právě z tohoto důvodu je tomuto tématu věnovaná samostatná podkapitola, která zároveň navazuje na vyhodnocení matice rizik.

5.2.1 Zobrazení v matici rizik

Než dojde k představení samotné matice rizik, je potřeba definovat prvky, které tato matice obsahuje.

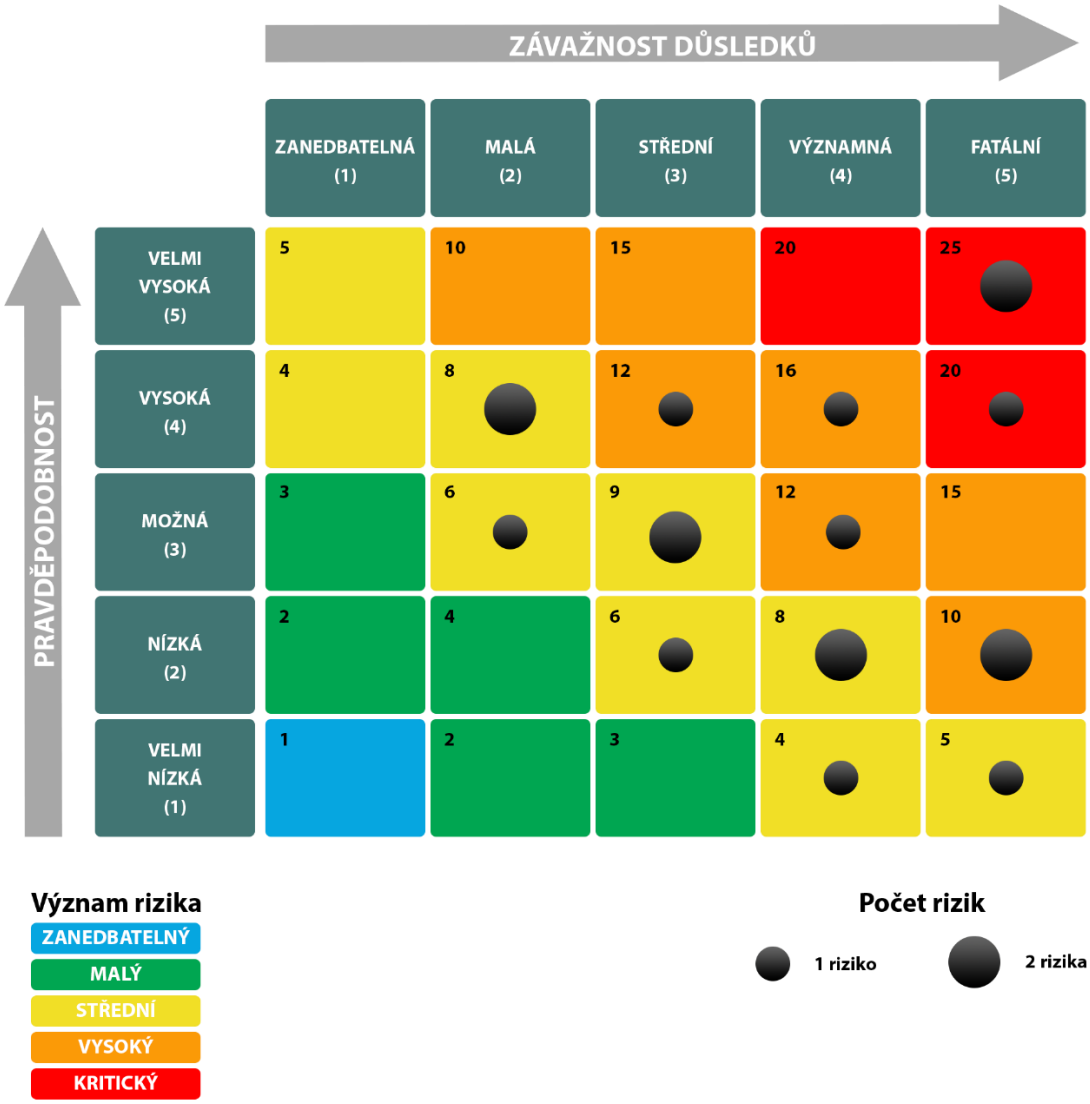
Svislá osa znázorňuje stupeň pravděpodobnosti výskytu rizika a vodorovná osa stupeň závažnosti jeho důsledků (viz vysvětlení faktorů v kapitole 5.1).

Úroveň rizika (jeho významnost) stoupá ve směru z levého dolního rohu do pravého horního rohu. Lze ji rozlišit také barevně – matice je rozdělena na pět oblastí. Na základě tohoto rozdělení může být význam rizika zanedbatelný, malý, střední, vysoký či kritický (Váchal & Vochozka, 2013).

Číslo v levém horním rohu každé buňky udává hodnotu významnosti daného rizika (součin pravděpodobnosti a závažnosti důsledku).

Velikost „puntíků“ znázorňuje počet rizik v dané kategorii významnosti (v dané buňce).

Obrázek č. 6: Zobrazení v matici rizik



Zdroj: Váchal & Vochozka, 2013
Zpracovala: Marie Velkoborská, 2020

Následující tabulka uvádí zjištěný počet rizik v dané kategorii významu rizika.

Tabulka č. 15: Významnost

Význam rizika	Počet rizik v kategorii
Zanedbatelný	0
Malý	0
Střední	10
Vysoký	5
Kritický	3

Zpracovala: Marie Velkoborská, 2020

Z tabulky je patrné, že v nejkritičtější kategorii rizik se nachází pouhá tři rizika. Tato rizika jsou však ta nejzásadnější a jejich ignorace by mohla výrazně ohrozit jak chod subjektu obecně, tak procesy související s ochranou osobních údajů (GDPR). Jedná se o následující:

- neznalost bezpečnosti používání informačních technologií (25 bodů[13]),
- kybernetická špionáž (25 bodů),
- nedostatečné zabezpečení informačních technologií (20 bodů).

Pět rizik odpovídá vysoké úrovni rizika, jedná se o následující:

- nedodržování bezpečnostních pravidel návštěv (16 bodů),
- nedostatečný výkon výpočetní techniky (12 bodů),
- nedostatečná znalost GDPR (12 bodů),
- výpadek zálohování (10 bodů),
- korupční chování.

Největší množství rizik se nachází ve střední kategorii úrovně (významu rizika) – celkem 10 rizik:

- technické chyby (9 bodů),
- kyberterorismus (9 bodů),
- narušení IT infrastruktury (8 bodů),
- nedbalé nakládání s listinnými dokumenty (8 bodů),
- porušení zabezpečení osobních údajů (8 bodů),
- kolaps systému (8 bodů),
- neodborná likvidace vyřazených nosičů dat (6 bodů),
- vynášení informací mimo pracoviště (6 bodů),
- odcizení dat (5 bodů),
- výpadky elektřiny (4 body).

Shrnutí

Lze tedy usoudit, že největší hrozby z hlediska možného úniku osobních údajů (tedy porušení zásad nařízení GDPR) je možné nalézt v zabezpečení informačních technologií a bezpečnosti jejich používání. V současné době jsou totiž technologie na takové úrovni,

[13] Hodnota významnosti rizika.

že pro potenciálního „zloděje“ je mnohem jednodušší a efektivnější využít internetovou síť, než se pokoušet vniknout na pracoviště a odcizit osobní údaje v tištěné formě.

Důležité je si také uvědomit, že těmto hrozbám lze zamezit minimálně tím, že zaměstnanci budou vzděláváni v této problematice a budou si uvědomovat, že pouhým jedním „kliknutím“ mohou zapříčinit až zneužití osobních údajů.

O tématu vzdělávání a dalších zlepšujících opatřeních pojednává kapitola 5.4.

5.2.2 Riziko úniku dat

Osobní údaje a kybernetická bezpečnost

V současné době existuje mnoho statistik znázorňujících frekvenci kybernetických útoků, a zároveň mnoho organizací, které tyto statistiky vytváří. Je však prakticky nemožné získat přesný počet úniků dat, jelikož všechny statistiky se odvíjí od toho, zda společnost daný útok (a následný únik dat) nahlásí a zda si je vůbec vědoma, že k útoku došlo. Některé statistiky se shodují či jsou si obsahově velmi podobné, některé jsou naopak velmi odlišné. S přihlédnutím k této skutečnosti (a po analýze několika statistik) lze uvést pro příklad následující informace.

- kybernetické útoky jsou považovány za jedny z pěti největších globálních rizik z ekonomického hlediska (WEF, 2019),
- od roku 2013 do roku 2019 bylo celosvětově odcizeno celkem 9 727 967 988 záznamů, Česká republika v tomtéž období zaznamenala celkem 3 504 000 odcizených záznamů (Varonis, 2020[14]) – jiné statistiky však uvádí až pětkrát vyšší čísla (Cyber Risk Analytics, 2020).

Důležité je také vysvětlit, že existuje rozdíl mezi únikem dat a počtem odcizených záznamů. Únikem dat se rozumí jeden konkrétní úkon, kdy dojde k útoku na internetovou síť dané společnosti. Nejedná se tedy o počet odcizených záznamů – těch může mít mnohonásobně větší množství.

Konkrétní příklady úniků dat v graficky přehledné podobě (a také odkazy na další informace) poskytuje webová stránka *www.informationisbeautiful.com*[15]. Jako příklad

[14] Statistika je k dispozici v příloze F.
[15] Příklad grafického zobrazení úniků dat je k dispozici v příloze G.

nedávného úniku dat lze uvést společnost Facebook, které bylo v září roku 2019 odcizeno 420 milionů záznamů (v rámci jednoho útoku – jednoho úniku dat). Co se státního sektoru týče, na počátku roku 2020 došlo k softwarové chybě v Izraeli. Díky tomu byly odhaleny osobní údaje všech voličů (celkem 6,5 milionu záznamů), což vyvolalo velké obavy ohledně krádeží identit a manipulace s volbami v zemi (Information is Beatiful, 2020; NY Times, 2020).

Kybernetické útoky tedy nejsou v žádném případě cíleny pouze na soukromý sektor, ale dotýkají se i toho státního.

Únik dat obecně

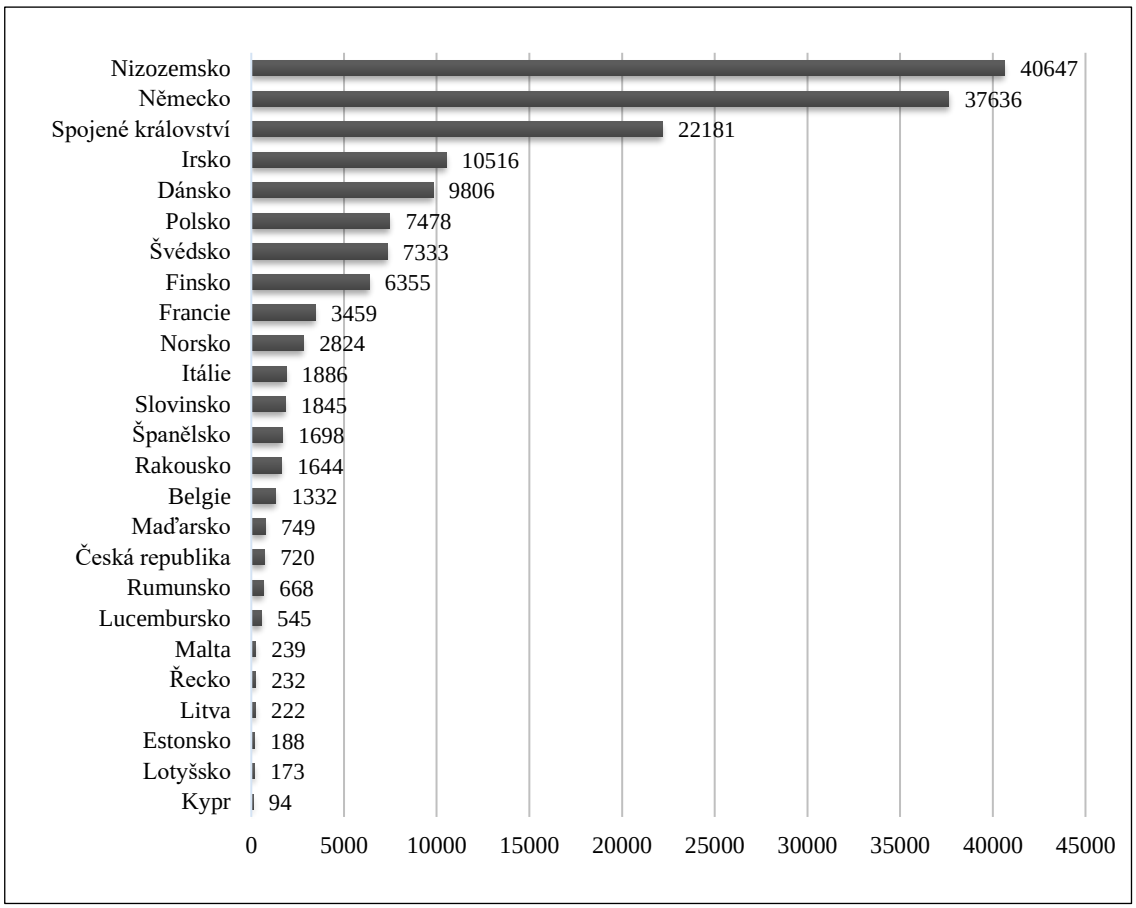
Od roku 2005 do konce roku 2019 bylo ve Spojených státech hlášeno více než 10 000 úniků dat. Oproti tomu v Evropské unii bylo od května 2018 (počátek platnosti GDPR) do konce roku 2019 hlášeno 160 000 úniků dat (DLA Piper, 2020; ITRC, 2020; Statista, 2019).

Důvodem může být to, že Evropská unie má na rozdíl od Spojených států silný zákon o ochraně osobních údajů (GDPR) i zákon o kybernetické bezpečnosti, které nařizují podávání zpráv úředním subjektům. Ve Spojených státech se určitá obdoba evropského GDPR nachází prozatím v přípravné fázi (NY Times, 2019; SC Magazine, 2020).

Z toho lze tedy usoudit, že dopad GDPR z obecného hlediska lze spatřit také ve větší zodpovědnosti, co se týče nahlašování úniků dat.

Následující graf zobrazuje statistiku společnosti DLA Piper, která znázorňuje počet oznámených úniků osobních údajů v období od 25. května 2018 do 27. ledna 2020 (v případě vybraných členských států Evropské unie k lednu 2020).

Obrázek č. 7: Počet oznámených úniků osobních údajů



Zdroj: DLA Piper, 2020
Zpracovala: Marie Velkoborská, 2020

Dle statistik Česká republika v tomto období zaznamenala 720 úniků osobních údajů (DLA Piper, 2020). Je však nutné zdůraznit, že určitá část úniků může být subjekty zatajována či o nich daný subjekt nemusí vůbec vědět. Přesnější statistiky lze tedy pozorovat v průběhu několika dalších let.

Kybernetická bezpečnost a GDPR

GDPR o problematice informačních technologií pojednává pouze z obecného hlediska, a to například v bodě 49, který hovoří o *„zabránění neoprávněnému přístupu k sítím elektronických komunikací a šíření škodlivých kódů a zamezení útokům, jejichž důsledkem je odepření služby, a škodám na počítačových systémech a systémech elektronických komunikací.“*

Úřad pro ochranu osobních údajů se k informačním technologiím vyjadřuje například v souvislosti s ohlašováním případů porušení zabezpečení osobních údajů.

„Je třeba ohlašovat jakékoliv porušení zabezpečení osobních údajů, které může mít za následek riziko pro práva a svobody fyzických osob. Může jít například o ***útok proti počítači, ve kterém jsou osobní údaje zpracovávány, jehož důsledkem je únik osobních údajů, jejich pozměnění nebo jiné zneužití*** (zvýraznila M. V.). *Může jít také např. o ztrátu listinných dokumentů obsahujících osobní údaje, které byly součástí manuálně vedené evidence (kartotéky) fyzických osob nebo byly vytištěny z počítače, ve kterém je taková evidence vedena a obsah těchto dokumentů zakládá riziko pro dotčené osoby (např. ztráta zdravotnické dokumentace.“* (ÚOOÚ, 2019e)

O zpracování osobních údajů mimo jiné pojednává také *zákon č. 181/2014 Sb., o kybernetické bezpečnosti* a zejména pak *vyhláška č. 82/2018 Sb.*, která do tohoto zákona zapracovává nařízení GDPR. Vyhláška definuje konkrétní bezpečnostní opatření z hlediska informačních technologií, která musí subjekt přijmout a je tedy z tohoto pohledu přesnější než GDPR (ITBiz, 2017).

Tyto právní předpisy jsou platné pro poskytovatele služeb elektronických komunikací a subjektů zajišťujících tyto sítě (nejsou platné přímo pro Magistrát města Plzně). Nicméně i přesto by subjekt měl brát tyto právní předpisy alespoň v úvahu, a to zejména v souvislosti se zabezpečením osobních údajů. Bezpečnostní opatření uvedená v této vyhlášce jsou přesně definovaná a každému subjektu by zcela jistě pomohla zabránit případným útokům a zvýšit tak bezpečnost svých osobních údajů.

5.3 Zlepšující opatření a doporučení pro Magistrát města Plzně

V následující části jsou dle jednotlivých stupňů rizik (kritická, vysoká, střední) představena zlepšující opatření a doporučení pro Magistrát města Plzně.

Jedná se o návrhy založené na znalostech čerpaných v průběhu psaní práce (interní zdroje MMP, problematika GDPR a kybernetické bezpečnosti – v teoretické i praktické rovině).

V každé kategorii jsou nejprve daná opatření podrobně rozepsána a v závěru každé podkapitoly je pak k dispozici jejich stručné shrnutí prostřednictvím tabulky.

5.3.1 Opatření ke zvládání kritických rizik

Jedním z opatření (která je možné uskutečnit přímo na pracovišti MMP) je například **přísnost pravidel tvorby uživatelského hesla**. Samotná vyhláška č. 82 uvádí délku hesla minimálně 12 znaků (§ 19) – v současné době MMP požaduje pouhých 8 znaků. Zároveň by mělo heslo splňovat podmínku složitosti, to znamená:

- obsažení velkých i malých písmen,
- obsažení čísel a speciálních znaků (například „*“ či „@“),
- záměna písmen za čísla nebo speciální znaky ve slovech.

Příkladem hesla dle výše uvedeného je například „P@ssw0rd“.

Dále by software neměl povolovat použití častých hesel či hesel obsahujících posloupnosti (například „12345“). Heslo by nemělo být stejné nebo podobné jako uživatelské jméno a zároveň by nemělo být podobné heslům užívaným v předchozích třech obdobích.

Důležité opatření pro MMP je také zákaz uplatňování funkce „zapamatovat heslo“, která sice usnadní zaměstnanci přístup do systému či programu, ale zároveň je přístup otevřený i komukoli dalšímu.

Hesla by se zároveň neměla opakovat (zákaz používání stejného hesla pro více programů zároveň, zákaz používání stejného hesla pro přístup do počítače a pro přístup do daného programu).

Pro zjištění aktuální bezpečnosti hesla není v žádném případě vhodné využívat hojně doporučované internetové stránky jako je například *www.passwordmeter.com*. Je zde riziko úniku hesel do databáze distribuované mezi útočníky.

Přestože zodpovědné užívání osobních hesel zní všeobecně jako nepříliš důležitá věc, právě slabé heslo je jeden z nejčastějších důvodů úniku dat, a lze mu snadno předejít.

Vhodnou variantou, možnou alternativou a také doporučením pro Magistrát města Plzně je „open-source“ software[16] s názvem **KeePass**. Jedná se o nezpoplatněný software, který obsahuje zašifrovanou databázi všech hesel, která zaměstnanec využívá pro vykonávání

[16] Open-source software (OSS) je typ počítačového softwaru, ve kterém je zdrojový kód zpřístupněn na základě licence, v níž držitel autorských práv uděluje uživatelům práva ke studiu, změně a distribuci softwaru komukoli a pro jakýkoli účel (St. Laurent, 2004).

své práce. Přístup do této databáze je chráněn hlavním heslem. To má sice vysoké požadavky na složitost, nicméně jedná se o jediné heslo, které si zaměstnanec musí pamatovat. Po otevření této databáze poté stačí otevřít požadovaný software/internetovou stránku a heslo se automaticky vygeneruje. Databáze nemusí být ani součástí počítače – lze ji přenášet za pomoci jakéhokoliv nosiče (například flash disku). Jedná se o velmi bezpečný způsob uchovávání hesel, jelikož software není nikterak propojen s internetovou sítí – je tedy odolný vůči externím hrozbám (KeePass, 2020).

Co se týče **vzdělávání v oblasti informačních technologií** – v současné době MMP nepořádná žádná pravidelná školení související s touto problematikou. Proto by bylo vhodné tuto formu vzdělávání zavést a seznamovat tak zaměstnance s bezpečností využívání výpočetní techniky, zejména pak s následky nedodržování bezpečnostních pravidel.

Dalším řešením je umožnění participace na rekvalifikačním kurzu v oblasti výpočetní techniky, případně motivace a prostor pro samostudium. Je potřeba docílit toho, aby si zaměstnanci uvědomili, že i pouhé jedno „kliknutí“ může mít fatální následky pro celý subjekt (nejenom z hlediska ochrany osobních údajů) a je nutné vnímat vše, co konkrétní počítač uvádí a hlásí (aktualizace antivirových programů a podobně).

Základní body, které by se zaměstnanci MMP měli naučit dodržovat:

- ochrana před viry a škodlivými programy:
    - schopnost jejich odhalení,
    - respektování aktualizací softwaru,
- odstraňování nepoužívaných a zbytkových souborů (v případě, že to systém umožňuje),
- nestahovat do pracovního počítače soubory osobního typu (fotografie a další),
- nepoužívat vlastní neprověřené (či náhodně nalezené) flash disky,
- udržování dostatečného volného místa na disku (omezení zahlcení počítače),
- odhlašování počítače v době nepřítomnosti,
- vypínání počítače po skončení pracovní doby.

Zaměstnanci mají možnost obrátit se jak na poskytovatele daných informačních systémů (e-spis, Agendio, i-faktury), tak na Správu informačních technologií města Plzně, která má zároveň vlastního pověřence pro ochranu osobních údajů. Ten je schopen zodpovědět

případné dotazy či předat kontakt na povolanou osobu. Vzhledem k tomu, že většina zaměstnanců Magistrátu výpočetní techniku využívá, jedná se o součást pracovní náplně a je potřeba za ni brát plnou zodpovědnost.

Následující tabulka slouží jako shrnutí uvedených opatření k nejvýznamnějším rizikům subjektu.

Tabulka č. 16: Kritická rizika

Riziko	Opatření
Neznalost bezpečnosti používání informačních technologií	Školení v problematice Seznamování s riziky informačních systémů Motivace v sebevzdělávání
Kybernetická špionáž	Zabezpečení informační sítě Dodržování bezpečnostních pravidel
Nedostatečné zabezpečení informačních technologií	Větší přísnost pravidel hesel Využití softwaru KeePass Aktualizace informačních systémů

Zpracovala: Marie Velkoborská, 2020

5.3.2 Opatření ke zvládání vysokých rizik

Aby bylo zaměstnancům umožněno stoprocentně využívat výpočetní techniku pro svou práci, je potřeba dbát i na její výkon. Kancelářské počítače musí být rychlé a musí zvládat veškeré operace související s náplní pracovní pozice. Jelikož se jedná o spotřební zboží, je velmi důležité počítače modernizovat a nepodléhat dojmu, že dané počítače na běžnou kancelářskou práci stačí. S tím souvisí samozřejmě také jejich údržba, kdy lze odkázat opět na problematiku neznalosti používání informačních technologií, a tedy vzdělávání zaměstnanců v této oblasti.

K porušení zabezpečení dat může dojít například i pouhým „proklouznutím“ nepovolané osoby přes ostrahu objektu – vrátnici. Proto je nutné dbát na **dodržování bezpečnostních pravidel návštěv**:

- kontrolovat každou příchozí osobu,
- požadovat průkaz totožnosti,
- vést evidenci návštěv (i v případě, že daná osoba přijde v doprovodu zaměstnance magistrátu).

Co se týče neznalosti GDPR, v této oblasti subjekt nemá velké problémy. Školení jsou pořádána pravidelně a zaměstnanci jsou plně seznámeni s touto problematikou v rámci

své pracovní náplně. Nicméně i přesto se může stát, že magistrát přijme nového zaměstnance, který nebude ihned s problematikou GDPR seznámen. V takovém případě rozhodně nemá smysl vyčkávat do termínu školení, je nutné reagovat rychle a věnovat se GDPR v rámci **úvodního zaškolování**.

Korupční chování je zásadním problémem, který se zatím dle dostupných informací na Magistrátu města Plzně nevyskytl. I přesto je ale potřeba tomuto chování předcházet prostřednictvím určitého interního **protikorupčního programu**, který by měl být ideálně v co nejbližší době sestaven. Tento program by se mohl opírat například o následující body:

- snížení motivace zaměstnanců ke korupci:
    - systém odměňování,
    - systém vzdělávání,
    - komunikace a dobré vztahy na pracovišti,
- definování prostředků odhalení korupčního chování,
- definování sankcí a dalších následků korupčního chování.

Následující tabulka slouží jako shrnutí výše uvedených opatření.

Tabulka č. 17: Vysoká rizika

Riziko	Opatření
Nedodržování bezpečnostních pravidel návštěv	Zvýšení a kontrola dodržování pracovních povinností vrátnice
Nedostatečný výkon výpočetní techniky	Nákup vhodné výpočetní techniky Údržba
Nedostatečná znalost GDPR	Úvodní školení
Výpadek zálohování	Údržba datových úložišť
Korupční chování	Protikorupční program (motivace zaměstnanců)

Zpracovala: Marie Velkoborská, 2020

5.3.3 Opatření ke zvládání středních rizik

Vzhledem k tomu, že rizika střední kategorie významnosti nejsou natolik závažná, není v současné době potřeba zavádět razantní opatření. I přesto je ale nutné těmto rizikům věnovat pozornost, a právě z toho důvodu jsou k dispozici následující doporučení.

Například technickým chybám není ve většině případů možné zabránit – občas se stává, že některé síťové prvky přestanou fungovat (například wifi router). V takovém případě je důležité pouze **rychle reagovat**, okamžitě zjistit, kde došlo k chybě a tuto chybu opravit. Rychlým jednáním lze předejít například neproběhnutí procesu zálohování, které může vést ke ztrátě dat (osobních údajů) a dalším komplikacím. Výpadky elektřiny už v dnešní době nejsou příliš časté, i přesto je však vhodné mít k dispozici **záložní zdroj** (UPS).

Problematika kyberterorismu se týká zejména zabezpečení informačních systémů – již bylo zmíněno v předchozích podkapitolách.

Pro magistrát je důležité pravidelně provádět **audity operačních systémů a sítí**, aby nedocházelo k narušení IT infrastruktury prostřednictvím například odposlechových síťových prvků. Stejně jako další rizika, i toto riziko často vede k úniku osobních údajů a v případě absence auditu (či jiných metod) se narušení IT infrastruktury velmi obtížně odhaluje.

GDPR se však týká i listinných dokumentů obsahujících osobní údaje. Nedbalé nakládání s dokumenty je prvním krokem k úniku osobních údajů (například situace, kdy zaměstnanec nedodržuje pořádek ve svých dokumentech, nechává je ležet na pracovním stole bez dozoru a další případy). Druhým krokem je pak porušení zabezpečení – to znamená, že zaměstnanec nechá dokumenty ležet na stole, a následně opustí kancelář bez jejího uzamknutí. Již bylo zmíněno, že existuje instrukce vydaná MMP, která popisuje veškeré povinnosti související se zabezpečením dokumentů obsahujících osobní či citlivé údaje. Je tedy nutné **motivovat zaměstnance** k dodržování těchto povinností a neustále jim připomínat, že svými činy mohou způsobit únik údajů (například prostřednictvím systému vzdělávání).

Fyzické odcizení dat je jedno z možných rizik a zároveň následků nedostatečného zabezpečení. Je tedy nutné **dodržovat všechna bezpečnostní pravidla** (uzamykat sklady a archivy, zamezit pohyb nepovolaných osob na pracovišti a další).

Zkolabování systému magistrátu lze předejít mnoha způsoby – jedním z nich je **údržba datových úložišť**, která může zamezit zahlcení celého systému při velkém pracovním zatížení. Nedojde tak ke znemožnění vykonávání pracovních povinností souvisejících například i se správou osobních údajů.

Vzdělávat zaměstnance je nutné i v souvislosti s vynášením informací mimo pracoviště (jakým způsobem dokumenty přenášet na jiná pracoviště – například povinnost neprůhledného obalu, dostatečné uzavření a další).

Důležité je věnovat pozornost také **adekvátní likvidaci nosičů dat** – v případě, že dojde ke ztrátě funkčnosti například externího harddisku, neznamená to, že osobní data se z něj již nedají získat. Proto i nevinné vyhození (případně ztráta) například flash disku může způsobit únik osobních údajů. To se týká samozřejmě i likvidace počítačů či jiné výpočetní techniky. Nejvhodnější je fyzické zničení (deformace, probodnutí, skartace) – v současné době pro tyto účely existují speciální stroje.

Shrnutí těchto opatření (vztahujících se ke střední kategorii významnosti rizika) je k dispozici v následující tabulce.

Tabulka č. 18: Střední rizika

Riziko	Opatření
Technické chyby	Rychlé odhalení a reakce na vzniklé problémy
Kyberterorismus	Zabezpečení informačních systémů
Narušení IT infrastruktury	Audity operačních systémů a sítí
Nedbalé nakládání s listinnými dokumenty	Motivace a kontrola zaměstnanců
Porušení zabezpečení osobních údajů	Zvýšená kontrola dodržování bezpečnostních pravidel (uzamykání prostor, bezpečné skladování dokumentů)
Kolaps systému	Údržba datových úložišť
Neodborná likvidace vyřazených nosičů dat	Vzdělávání zaměstnanců v problematice
Vynášení informací mimo pracoviště	Vzdělávání zaměstnanců v problematice
Odcizení dat	Zabezpečení skladových prostor
Výpadky elektřiny	Záložní zdroje – UPS

Zpracovala: Marie Velkoborská, 2020

Závěr

Diplomová práce se zabývala problematikou GDPR a jejími dopady na Magistrát města Plzně. V první polovině práce bylo čtenářům představeno toto evropské nařízení a veškeré náležitosti s tím související. Druhá část práce již pojednávala o problematice GDPR v souvislosti s ekonomickým subjektem.

Hlavním cílem bylo *„identifikovat a vyhodnotit dopady nařízení GDPR na konkrétní ekonomický subjekt a vypracovat návrh opatření směřujících ke zlepšení situace sledovaného subjektu v této oblasti“*. Pro identifikaci těchto dopadů byla využita komunikace s vedoucími pracovníky magistrátu (konkrétně s bezpečnostním ředitelem, pověřencem pro ochranu osobních údajů a vedoucím Kanceláře tajemníka). Informace byly zjišťovány prostřednictvím rozhovorů, konzultací a diskusí. Dále proběhla analýza interních i veřejných dokumentů, pozorování pracoviště, a na základě toho došlo k vyvození následujících závěrů.

Prvním dopadem byla nutnost vytvoření funkce pověřence pro ochranu osobních údajů. Výhoda magistrátu spočívá v tom, že již dříve disponoval pracovní pozicí, jejíž náplní bylo zpracování takzvaných utajovaných informací. Proto při implementaci GDPR došlo pouze k rozšíření kompetencí pracovníka ve funkci bezpečnostního ředitele a nebylo tedy nutné vyhledávat a následně zaškolovat pověřence z externích zdrojů.

GDPR se projevilo také ve zvýšené administrativě a s tím související časové a finanční náročnosti. Magistrát uvádí, že nejnáročnějším obdobím bylo období procesu analýzy GDPR, která znamenala velký zásah do běžných pracovních povinností. Nicméně díky jejímu důkladnému zpracování byl subjekt na samotnou implementaci připraven. Hlavní přínos magistrát vidí v nastolení pořádku v datech. Díky tomu bylo vedení schopno odhalit velké množství chyb, mezi které patří například nadbytečné vyžadování souhlasů či provádění některých činností na více pracovištích zároveň. Nadbytečné vyžadování souhlasů je jeden z nejzásadnějších problémů, se kterými se magistrát stále potýká. Vzhledem k velmi obecnému pojetí nařízení GDPR dochází často ke špatnému porozumění jeho obsahu, což má za důsledek zmatek a chaos zejména ve školství.

Magistrát byl dále vlivem GDPR nucen zintenzivnit množství interních školení. Každoročně se na toto téma pořádá schůze všech vedoucích pracovníků, kde dochází zejména ke kontrole dodržování předpisů či k případným úpravám. S tím souvisí také

nutnost zvýšené personální gramotnosti v problematice, jelikož zaměstnanci jsou povinni seznamovat se s novými předpisy. Pro usnadnění této situace byla sestavena instrukce, která definuje veškerá pravidla a která musí zaměstnanci dodržovat. V souvislosti s GDPR se objevila také hrozba selhání lidského faktoru související s neznalostí informačních technologií.

Pravděpodobně nejzásadnějším dopadem byla modernizace technického zabezpečení (papírové a elektronické dokumentace). Zaměstnanci jsou nyní nuceni dodržovat velké množství bezpečnostních opatření, která definuje již zmiňovaná instrukce. Pro úschovu a zpracování elektronické dokumentace zaměstnancům slouží program E-spis, který splňuje veškeré požadavky dle GDPR. Přístup do programu je zaměstnancům umožněn na základě dvoustupňového přihlášení a hesla je nutné měnit každé tři měsíce.

Lze tedy shrnout, že přestože dopadů bylo mnoho, nejobtížnějším a zároveň nedůležitějším obdobím bylo období příprav a implementace GDPR. S tím souvisí zejména analýza procesů, která odhalila mimo jiné i nedostatky v administrativě, a na jejímž základě bylo vedení magistrátu schopno zefektivnit chod subjektu. Přestože tedy nové nařízení způsobilo nárůst pracovní zátěže a netěšilo se tedy velké oblíbenosti mezi zaměstnanci, z dlouhodobého hlediska je GDPR spíše přínosem.

V poslední části práce byly identifikovány tři hlavní kategorie rizik – lidský faktor, technický faktor a externí faktor, pod které spadá celkem 18 rizik. Prvotním důsledkem těchto rizik je porušení zabezpečení osobních údajů – čili porušení nařízení GDPR.

Nejkritičtějšími riziky jsou v případě MMP neznalost bezpečnosti používání informačních technologií, kybernetická špionáž a nedostatečné zabezpečení technologií. Z toho lze usoudit, že nebezpečí z hlediska porušení ochrany osobních údajů lze nalézt zejména v informačních technologiích. A právě na tyto oblasti by se vedení Magistrátu města Plzně mělo zaměřit. Zlepšujícím opatřením je zavedení větší přísnosti pravidel tvorby hesla a jeho užívání. To souvisí s nutností pravidelného pořádání školení v IT pro všechny zaměstnance magistrátu. Je důležité, aby si každý byl vědom toho, že i pouhým otevřením závadného souboru může subjektu způsobit velké škody. Je tedy nutné dodržovat bezpečnostní pravidla a přísně kontrolovat jejich dodržování.

Úřad pro ochranu osobních údajů v souvislosti s evropským nařízením udává povinnost nahlašovat všechna porušení zabezpečení osobních údajů – tedy i únik dat

prostřednictvím internetové sítě. Z uvedených statistik (viz kapitola 5.2.2) lze usoudit, že možná i díky této povinnosti zaznamenala Evropská unie (v období od května roku 2018 do ledna roku 2020) mnohem větší množství úniků dat než například Spojené státy, které obdobu evropského GDPR teprve připravují.

Velké množství zaměstnanců však stále nebere v úvahu, že v současné době se nebezpečí nachází i ve virtuálním světě a pro útočníka je často mnohem jednodušší se k datům dostat tímto způsobem než fyzicky (zejména pak v případech, kdy zaměstnanci nedodržují bezpečnostní pokyny a nejsou si tohoto rizika vůbec vědomi).

Je statisticky dokázáno, že úniky osobních údajů prostřednictvím internetové sítě se dějí každodenně a velmi často dojde k jejich odhalení až po několika letech (nebo vůbec nikdy).

V současné době (jaro 2020) je problematika kybernetických útoků rozebírána i v médiích (v souvislosti s pandemií), kdy jsou díky tomu ohroženy nemocnice a jejich fungování. Přestože příčina těchto útoků není (pravděpodobně) primárně odcizení osobních údajů, i toto stojí za zmínku v rámci práce. Dokazuje to totiž skutečnost, že internetové sítě jsou velmi křehké a potenciální útočníci využijí každé situace, kdy není zabezpečení věnována absolutní pozornost. To platí i pro úřady včetně Magistrátu města Plzně, který v době této krize funguje v omezeném režimu. Zaměstnanci se tedy do interních systémů připojují často ze svých domovů a využívají komunikace se svými kolegy prostřednictvím sítě. Tato skutečnost razantně zvyšuje riziko úniku osobních dat.

Zejména pak pro úřad (Magistrát města Plzně), který schraňuje velké množství osobních dat o občanech města, by tento únik mohl mít fatální následky. Internetová síť může být sebelépe zabezpečená, ale pokud zaměstnanci nedodržují základní bezpečnostní pravidla (problematika nesprávného užívání hesel, otevírání závadných e-mailů), zabezpečení může být velice snadno prolomeno.

Proto je nutné si uvědomit, že GDPR nespočívá pouze v „nutných podpisech“ či „zbytečné administrativě“, ale i v potenciálu každého subjektu zlepšit zabezpečení své sítě, investovat do vzdělávání svých zaměstnanců v oblasti IT a zamezit tak zbytečným škodám v případě úniku osobních či jiných důležitých dat.

Seznam použité literatury

Tištěné zdroje:

Cafourek, B. (2010). *Windows 7 – kompletní příručka*. Praha: Grada Publishing.

Janevski, T. (2003). *Traffic analysis and design of wireless IP networks*. Boston: Artech House.

Mulačová, V. & Mulač, P. (2013) *Obchodní podnikání ve 21. století.* Praha: Grada Publishing.

Navrátil, J. (2018). *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk.

Nezmar, L. (2017). *GDPR: praktický průvodce implementací.* Praha: Grada Publishing.

Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. & Kovaříková, K. (2018). *GDPR – obecné nařízení o ochraně osobních údajů.* 2. vydání., Praha: Wolters Kluwer ČR.

St. Laurent, A. (2004). *Understanding open source and free software licensing.* California, US: O'Reilly Media.

Váchal, J. & Vochozka, M. (2013). *Podnikové řízení.* Praha: Grada Publishing.

Právní předpisy:

ČESKO. Sdělení č. 209/1992 Sb., sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/39918/1/2

ČESKO. Usnesení č. 2/1993 Sb., usnesení předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky. In: Sbírka zákonů České republiky. 1993, částka 1. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/40453/1/2

ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: Sbírka zákonů České republiky. 2018, částka 43. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/90229/1/2

ČESKO. Zákon č. 89/2012 Sb., občanský zákoník. In: Sbírka zákonů České republiky. 2012, částka 33. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/74907/1/2

ČESKO. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: Sbírka zákonů České republiky. 2000, částka 32. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/49228/1/2

ČESKO. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: Sbírka zákonů České republiky. 2019, částka 47. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/91825/1/2

ČESKO. Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. In: Sbírka zákonů České republiky. 2019, částka 47. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/91826/1/2

ČESKO. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. In: Sbírka zákonů České republiky. 2005, částka 43. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/59921/1/2

ČESKO. Zákon č. 128/2000 Sb., o obcích. In: Sbírka zákonů České republiky. 2000, částka 38. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/49296/1/2

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů České republiky. 2014, částka 75. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/82522/1/2

ČESKO. Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. In: Sbírka zákonů České republiky. 1992, částka 55. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/39975/1/2

ČESKO. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů. In: Sbírka zákonů České republiky. 2004, částka 166. Dostupné také z: https://www.noveaspi.cz/products/lawText/1/58329/1/2

ČESKOSLOVENSKO. Ústavní zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního. In: Sbírka zákonů a nařízení státu československého 1920. Dostupné z: https://www.noveaspi.cz/products/lawText/1/1874/1/2

EUROPEAN UNION. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In: Official Journal L 281. 1995. Dostupné také z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=cs

EVROPSKÁ UNIE. Listina základních práv Evropské unie. In: Úřední věstník Evropské unie C 83/389. 2010. Dostupné také z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:CS:PDF

EVROPSKÁ UNIE. 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). In: Úřední věstník Evropské unie L 119/1. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1568638421562&uri=CELEX:32016R0679

EVROPSKÁ UNIE. Návrh nařízení Rady a Evropského parlamentu o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích). In: Brusel. 2017. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52017PC0010

EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích). In: Úřední věstník Evropské unie L 201. 2002. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32002L0058

OSN (Organizace spojených národů). Všeobecná deklarace lidských práv. In: New York. 1948. Dostupné také z: http://www.lidskaprava.cz/uploads/03_dokumenty/04_uvod/00_VDLP_UDHR-.pdf

RAKOUSKÉ CÍSAŘSTVÍ. Zákon č. 87/1862 ř. z., pro ochranu svobody osobní. In: Říšský zákoník. Dostupné také z: http://alex.onb.ac.at/cgi-content/alex?aid=rgb&datum=18620004&seite=00000243

RAKOUSKÉ CÍSAŘSTVÍ. Zákon č. 88/1862 ř. z., pro ochranu svobody domovní. In: Říšský zákoník. Dostupné také z: http://alex.onb.ac.at/cgi-content/alex?aid=rgb&datum=18620004&seite=00000245

Interní zdroje Magistrátu města Plzně:

Interní dokumentace MMP (2020) – zahrnuje pracovní dokumenty, neoznačené dokumenty a certifikáty, které byly poskytnuty autorce práce v roce 2020.

Interní zdroje MMP (2020) – zahrnuje výpovědi zaměstnanců, konzultace, diskuse, rozhovory.

Koncepce integrovaného systému řízení. Směrnice QS 53-01 (2020). Plzeň: Magistrát města Plzně.

Organizační struktura Magistrátu města Plzně. Příloha č. 1 QS 55-01 (2019). Plzeň: Magistrát města Plzně.

Organizační řád Magistrátu města Plzně. Směrnice QS 55-01 (2019). Plzeň: Magistrát města Plzně.

Statut města Plzně. Úplné znění obecně závazné vyhlášky statutárního města Plzně č. 8/2001, Statut města, ve znění obecně závazných vyhlášek č. 12/2002, 3/2004, 20/2004, 17/2005, 14/2006, 20/2006, 1/2009, 3/2010, 14/2011, 9/2012, 3/2013, 11/2013, 7/2014, 4/2015, 9/2015, 5/2016, 5/2017, 6/2018, 10/2018 a 9/2019 (2019).

Zpracovávání osobních údajů. Instrukce QI 42-03-01 (2018). Plzeň: Magistrát města Plzně.

Interní zdroje Správy informačních technologií města Plzně:

Interní zdroje SIT města Plzně (2020) – zahrnuje informace získané na základě e-mailové komunikace.

Elektronické zdroje – odborné články, výroční zprávy, dokumenty a studie:

Cyber Risk Analytics (2019). *Data Breach QuickView Report*. Cit. 30.03.2020, dostupné z: https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf

European Commission (2017). *Proposal for a Regulation of the European Parliament and of the Council*. Cit. 02.12.2020, dostupné z: https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A52017PC0010

ICO (Information Commissioner's Office) (2019). *GDPR consent guidance for consultation.* Cit. 03.11.2019, dostupné z: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

ITRC (Identity Theft Resource Center) (2020). *2019 End of Year Data Breach Report.* Cit. 10.04.2020, dostupné z: https://www.idtheftcenter.org/2019-data-breaches/

Prowda, J. B. (1995). *Fordham Law Review: Privacy and Security of Data*. Cit. 12.02.2020, dostupné z: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3213&context=flr

Warren, S., & Brandeis, L. (1890). *The Right to Privacy.* Harvard Law Review, 4(5), 193-220. Cit. 12.02.2020, dostupné z: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents

WEF (World Economic Forum) (2019). *The Global Risks Report 2019.* Cit. 30.03.2020, dostupné z: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

WP253 (2017). *Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679*. Cit. 14.11.2019, dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31886

WP29 (2019). *Pokyny 1/2019 týkající se kodexů chování a subjektů pro monitorování podle nařízení 2016/679.* Cit. 18.11.2019, dostupné z: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_cs

Elektronické zdroje – národní a nadnárodní instituce, město Plzeň:

ČSÚ (Český statistický úřad) (2019). *Počet obyvatel ve správních obvodech obcí s rozšířenou působností k 1. 1. 2019.* Cit. 13.11.2019, dostupné z: https://www.czso.cz/documents/10180/91917344/1300721902.pdf/0b87b783-fef2-4b39-8ba6-f3bdeefc8777?version=1.0

EDPB (European Data Protection Board) (2019). *About EDPB.* Cit. 16.12.2019, dostupné z: https://edpb.europa.eu/about-edpb/about-edpb_en

Europa.eu (n. d). *Nařízení, směrnice a další právní akty*. Cit. 19.09.2019, dostupné z: https://europa.eu/european-union/eu-law/legal-acts_cs

MVČR (Ministerstvo vnitra ČR) (2019a). *Co je GDPR*. Cit. 16.11.2019, dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

MVČR (Ministerstvo vnitra ČR) (2019b). *Co nového GDPR přináší.* Cit. 20.03.2019, dostupné z: https://www.mvcr.cz/gdpr/clanek/co-noveho-gdpr-prinasi.aspx

Plzen.eu (2018). *O městě Plzeň*. Cit. 13.10.2019, dostupné z: https://www.plzen.eu/o-meste/o-meste-plzen.aspx

Plzen.eu (2019a). *Příspěvkové organizace města*. Cit. 20.10.2019, dostupné z: https://www.plzen.eu/urad/mestske-organizace/prispevkove-organizace/

Plzen.eu (2019b). *Společnosti s majetkovým podílem města*. Cit. 20.10.2019, dostupné z: https://www.plzen.eu/urad/mestske-organizace/spolecnosti-s-majetkovym-podilem/spolecnosti-s-majetkovym-podilem-mesta.aspx

Plzen.eu (2019c). *Veřejné zakázky*. Cit. 21.10.2019, dostupné z: https://www.plzen.eu/urad/verejne-zakazky/verejne-zakazky.aspx

Plzen.eu (2020). *Investiční záměry*. Cit. 21.02.2020, dostupné z: https://zamery.plzen.eu/

SIT MP (Správa informačních technologií města Plzně) (2019). *Standardy*. Cit. 30.04.2020, dostupné z: https://www.sitmp.cz/sluzby-it/standardy/

SIT MP (Správa informačních technologií města Plzně) (2020). *Inovujeme Plzeň.* Cit. 23.03.2020, dostupné z: https://www.sitmp.cz/

ÚOOÚ (Úřad pro ochranu osobních údajů) (2019a). *Historie Úřadu pro ochranu osobních údajů*. Cit. 16.11.2019, dostupné z: https://www.uoou.cz/historie-uradu-pro-ochranu-osobnich-udaju/ds-1061

ÚOOÚ (Úřad pro ochranu osobních údajů) (2019b). *Základní příručka k ochraně údajů*. Cit. 16.11.2019], dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=1061

ÚOOÚ (Úřad pro ochranu osobních údajů) (2019c). *Praxe s nadbytečným vyžadováním souhlasů ve školství přetrvává.* Cit. 27.02.2020, dostupné z: https://www.uoou.cz/praxe-s-nbsp-nadbytecnym-vyzadovanim-souhlasu-ve-nbsp-skolstvi-pretrvava/d-35989

ÚOOÚ (Úřad pro ochranu osobních údajů) (2019d). *Ze školství.* Cit. 27.02.2020, dostupné z: https://www.uoou.cz/ze-skolstvi/ds-5088/archiv=1&p1=2619

ÚOOÚ (Úřad pro ochranu osobních údajů) (2019e). *Porušení zabezpečení.* Cit. 30.03.2020, dostupné z: https://www.uoou.cz/poruseni-zabezpeceni/ds-5020/p1=5020

ÚOOÚ (Úřad pro ochranu osobních údajů) (2020). *Tisková zpráva: ÚOOÚ ke konzultacím návrhů zákonů v lednu 2020.* Cit. 28.02.2020, dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=40067

Elektronické zdroje – ostatní:

Cloudfare.com (2019). *What Is the Cloud | Cloud Definition*. Cit. 18.10.2019, dostupné z: https://www.cloudflare.com/learning/cloud/what-is-the-cloud/

Collins (2020). *Function creep.* Cit. 27.04.2020, dostupné z: https://www.collinsdictionary.com/dictionary/english/function-creep

ČEZ (2020). *ČEZ.* Cit. 10.04.2020, dostupné z: https://www.cez.cz/

DLA Piper (2020). *DLA Piper GDPR Data Breach Survey 2020.* Cit. 14.04.2020, dostupné z: https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/

GDPR.cz (n. d.). *Proč*. Cit. 16.11.2019, dostupné z: https://www.gdpr.cz/gdpr/proc/

Google (2020a). *Formulář žádosti o odstranění osobních údajů*. Cit. 01.01.2020, dostupné z: https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&hl=cs

Google (2020b). *Jak Google využívá soubory cookies*. Cit. 16.01.2020, dostupné z: https://policies.google.com/technologies/cookies?hl=cs

IAPP (The International Association of Privacy Professionals) (2019). *How the ePrivacy Regulation talks failed again.* Cit. 24.11.2019, dostupné z: https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/

ICZ (2020). *Elektronická spisová služba ICZ e-spis®.* Cit. 24.03.2020, dostupné z: https://www.iczgroup.com/zakaznicka-zona/elektronicka-spisova-sluzba-icz-e-spis/

ICZ (n. d.). *ICZ*. Cit. 24.03.2020, dostupné z: https://share.iczgroup.com/index.php/login?redirect_url=/index.php/apps/files/?dir%3D/Produktova_podpora/e-spis/Dokumentace%2520e-spis%26fileid%3D195596

Information is Beautiful (2020). *World's Biggest Data Breaches & Hacks*. Cit. 14.04.2020, dostupné z: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

ITBiz (2017). *Novela zákona o kybernetické bezpečnosti a GDPR*. Cit. 29.03.2020, dostupné z: https://www.itbiz.cz/clanky/novela-zakona-o-kyberneticke-bezpecnosti-a-gdpr

KeePass (2020). *KeePass Password Safe.* Cit. 18.04.2020, dostupné z: https://keepass.info/

NY Times (2019). *Congress and Trump Agreed They Want a National Privacy Law.* Cit. 14.04.2020, dostupné z: https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html

NY Times (2020). *Personal Data of All 6.5 Million Israeli Voters Is Exposed.* Cit. 14.04.2020, dostupné z: https://www.nytimes.com/2020/02/10/world/middleeast/israeli-voters-leak.html?action=click&module=News&pgtype=Homepage

Passwordmeter.com (n. d.). *The Password Meter.* Cit. 30.03.2020, dostupné z: http://www.passwordmeter.com/

SAP (2019). *Data Protection & Privacy at SAP Cloud Platform*. Cit. 22.02.2020, dostupné z: https://www.sap.com/documents/2019/09/a03f9cb9-6a7d-0010-87a3-c30de2ffd8ff.html

SC Magazine (2020). *Ringing in a new National Privacy Law?* Cit. 14.04.2020, dostupné z: https://www.scmagazine.com/home/security-news/features/ringing-in-a-new-national-privacy-law/

Secure Privacy (2020). *What is the e-Privacy Regulation?* Cit. 16.02.2020, dostupné z: https://secureprivacy.ai/eprivacy-regulation/

Statista (2019). *Annual number of data breaches and exposed records in the United States from 2005 to 2019.* Cit. 17.04.2020, dostupné z: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Svět IT (2019). *Cookies.* Cit. 08.04.2020, dostupné z: https://svetit.cz/cookies

Tenderarena.cz (2020). *Profily*. Cit. 21.02.2020, dostupné z: https://www.tenderarena.cz/profil/detail.jsf?identifikator=Plzen

Varonis (2020). *The World in Data Breaches.* Cit. 09.04.2020, dostupné z: https://www.varonis.com/blog/the-world-in-data-breaches/?fbclid=IwAR3rW1Lg2Ey8TLjcF6cwkgNbNJmftophv9KWTh9YkTgtWa2alqK4dfTSffU

Seznam tabulek a obrázků

Seznam tabulek:

Tabulka č. 1: Definice pojmu osobní údaj 25

Tabulka č. 2: Anonymizované a pseudonymizované údaje 27

Tabulka č. 3: Interní zdroje a kontaktní osoby MMP 37

Tabulka č. 4: Časová náročnost implementace GDPR 47

Tabulka č. 5: Finanční náročnost školení v problematice GDPR 49

Tabulka č. 6: Odhad finanční náročnosti 50

Tabulka č. 7: Číselné hodnocení pravděpodobnosti výskytu rizika 59

Tabulka č. 8: Hodnocení závažnosti dopadů rizika 59

Tabulka č. 9: Lidský faktor 61

Tabulka č. 10: Důsledky rizik lidského faktoru 62

Tabulka č. 11: Technický faktor 63

Tabulka č. 12: Důsledky rizik technického faktoru 63

Tabulka č. 13: Externí faktor 64

Tabulka č. 14: Důsledky rizik externího faktoru 64

Tabulka č. 15: Významnost 66

Tabulka č. 16: Kritická rizika 74

Tabulka č. 17: Vysoká rizika 75

Tabulka č. 18: Střední rizika 77

Seznam obrázků:

Obrázek č. 1: Vývoj legislativy ochrany osobních údajů 18

Obrázek č. 2: Notifikace o sběru cookies 23

Obrázek č. 3: Právo na výmaz 30

Obrázek č. 4: Přihlášení do softwaru e-spis 56

Obrázek č. 5: Přijetí PDF souboru 62

Obrázek č. 6: Zobrazení v matici rizik 66

Obrázek č. 7: Počet oznámených úniků osobních údajů 70

Seznam použitých zkratek

DPO	(Data Protection Officer) – pověřenec pro ochranu osobních údajů
EDPB	(European Data Protection Board) – Evropský sbor pro ochranu osobních údajů
GDPR	(General Data Protection Regulation) – Obecné nařízení o ochraně osobních údajů
IP	(Internet Protocol) – internetový protokol
MAC	Media Access Control
MMP	Magistrát města Plzně
UPS	(Uninterruptible Power Supply/Source) – zdroj nepřerušovaného napájení
PST	Pravděpodobnost
SIT	Správa informačních technologií
ÚOOÚ	Úřad pro ochranu osobních údajů
WP	(Working Party) – pracovní skupina

Seznam příloh

Příloha A: Organizační struktura MMP

Příloha B: Témata a otázky k rozhovoru s vedoucími pracovníky MMP

Příloha C: Analýza

Příloha D: Certifikát

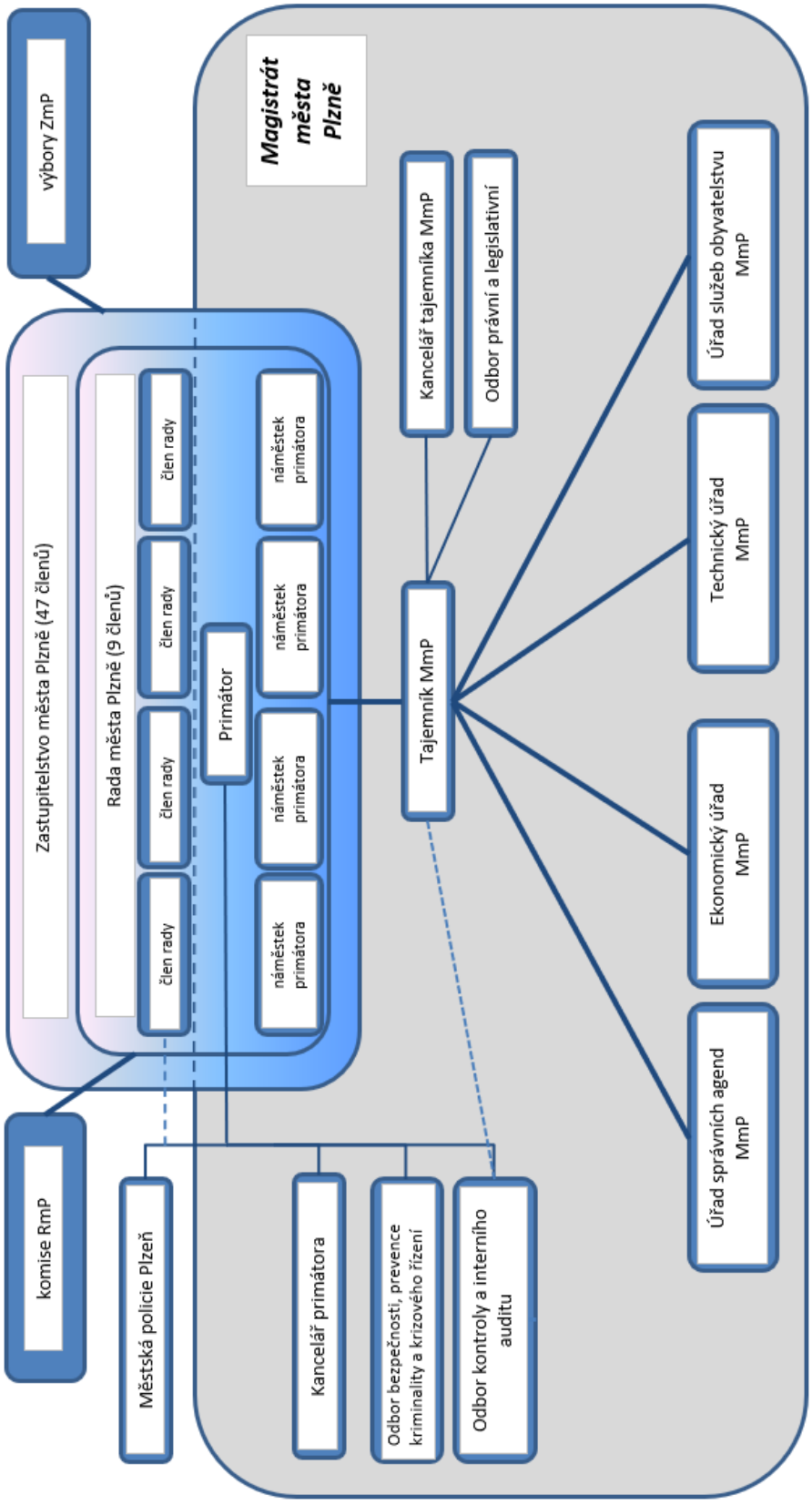
Příloha E: Návod k vyplnění

Příloha F: Úniky dat v letech 2013 až 2019

Příloha G: Grafické zobrazení úniků dat v letech 2017 až 2019

Přílohy

Příloha A: Organizační struktura MMP

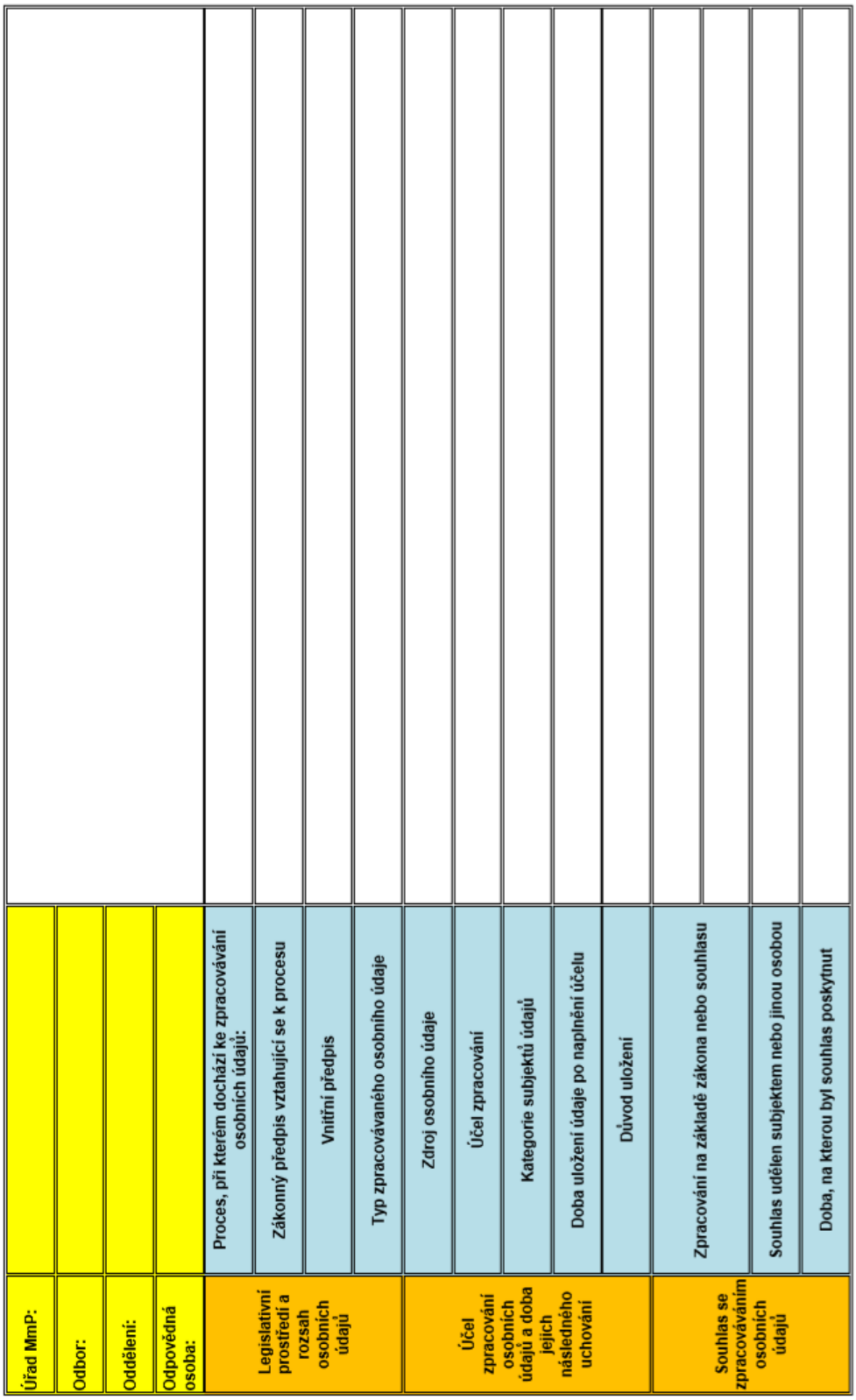


Převzato: Organizační struktura Magistrátu města Plzně, 2019

Příloha B: Témata a otázky k rozhovoru s vedoucími pracovníky MMP

1. Doplňující informace o Magistrátu města Plzně (interní systémy, činnosti atd.).
2. Ochrana osobních údajů před zavedením GDPR (způsob, systém, opatření atd.).
3. Proces implementace GDPR (jednotlivé kroky a postupy) – od přípravy až po zavedení.
4. Proces implementace GDPR v jednotlivých odděleních a odborech a konkrétní dopady.
5. Zpracovávali jste analýzu GDPR za pomoci interních zdrojů či jste volili externí společnost?
6. Aplikovaná metodika ochrany osobních a citlivých údajů a jejich zpracování – jakým způsobem byl vybrán pověřenec pro ochranu osobních údajů, jaké musel mít znalosti, jaká je v současné době náplň jeho práce?
7. Časová a finanční náročnost (náklady na celý proces, časová náročnost, změny pracovní náplně zaměstnanců, zabezpečování archivů, budování nových archivů, technické změny, školení zaměstnanců atd.).
8. Administrativní náročnost.
9. Případné problémy při implementaci GDPR.
10. Problémy v současné době (nejasnosti v původním nařízení, sporné věci, hrozby – pokud jsou).
11. Technické vybavení Magistrátu a bezpečnost online (databáze, internetová úložiště atd.).
12. Návrh zákona o elektronických komunikacích (je zapotřebí?).
13. Přínosy GDPR (došlo k zjednodušení některých procesů?)
14. Zpětný pohled po téměř dvou letech od zavedení.
15. Plány do budoucna (z hlediska ochrany osobních údajů).
16. Další dodatky a zajímavosti z praxe.

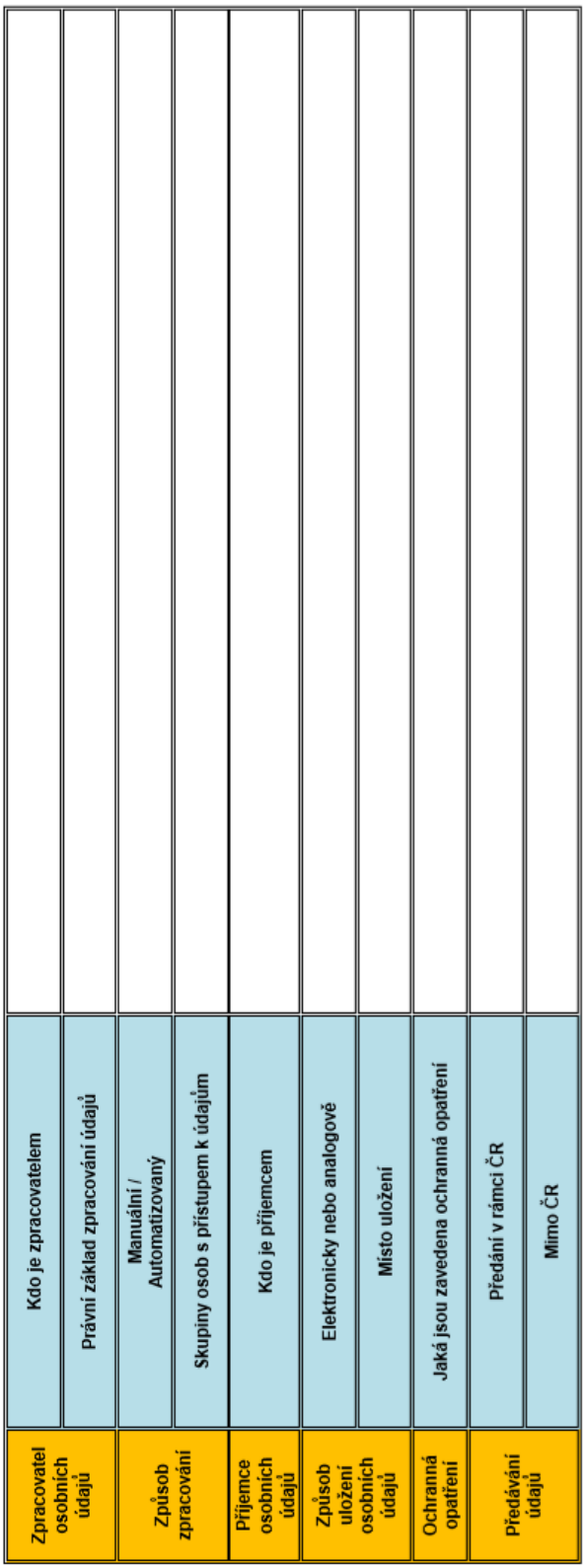
Příloha C: Analýza (část 1)



Úřad MmP:			
Odbor:			
Oddělení:			
Odpovědná osoba:			
Legislativní prostředí a rozsah osobních údajů	Proces, při kterém dochází ke zpracovávání osobních údajů:		
	Zákonný předpis vztahující se k procesu		
	Vnitřní předpis		
	Typ zpracovávaného osobního údaje		
Účel zpracování osobních údajů a doba jejich následného uchování	Zdroj osobního údaje		
	Účel zpracování		
	Kategorie subjektů údajů		
	Doba uložení údaje po naplnění účelu		
	Důvod uložení		
Souhlas se zpracováváním osobních údajů	Zpracování na základě zákona nebo souhlasu		
	Souhlas udělen subjektem nebo jinou osobou		
	Doba, na kterou byl souhlas poskytnut		

Převzato: Interní dokumentace MMP, 2020

Příloha C: Analýza (část 2)



Převzato: Interní dokumentace MMP, 2020

Příloha D: Certifikát

ČESKÁ SPOLEČNOST PRO JAKOST, z.s.

Certifikační orgán pro certifikaci systémů managementu akreditovaný Českým institutem pro akreditaci, o.p.s. a vedený pod registračním číslem 3081

na základě udělené akreditace vydává

CERTIFIKÁT

shody systému managementu hospodaření s energií s požadavky

ČSN EN ISO 50001:2012

organizaci

Statutární město Plzeň

Magistrátu města Plzně

náměstí Republiky 1, 306 32 Plzeň

IČ: 00075370

Předmět certifikace:

Systém managementu hospodaření s energií s ohledem na výkon samostatné působnosti a výkon přenesené působnosti v rámci veřejné správy

Výše uvedené činnosti jsou prováděny na pracovištích uvedených v příloze tohoto certifikátu, která je jeho nedílnou součástí.

Registrační číslo certifikátu: 366/EnMS/2017
Datum prvotní certifikace: 23.03.2017
Certifikační cyklus: 23.03.2017 – 22.03.2020
Platnost od: 15.05.2017
Vedoucí střediska certifikace systémů managementu a produktů:
Ing. Eliška Michálková

CERTIFIKAČNÍ ORGÁN ČSJ č. 3081 ČESKÁ SPOLEČNOST PRO JAKOST

S 3081

Certifikovaná organizace podléhá dozoru České společnosti pro jakost, z.s.
V případě zjištění závažné neshody vůči požadavkům ČSN EN ISO 50001:2012 může být platnost certifikátu pozastavena nebo zrušena.
Místo vydání: Novotného lávka 200/5, Staré Město, 110 00 Praha

Převzato: Interní dokumentace MMP, 2020

Příloha E: Návod k vyplnění (část 1)

Pokyny pro vyplnění formuláře k analýze operací pro implementaci GDPR	
Název položky	Popis
Proces	Uveďte název zpracování, který nejlépe popisuje agendu, ve které jsou osobní údaje zpracovávány.
Odpovědná osoba:	Odpovědná osoba za danou oblast zpracování tohoto formuláře
Zákonný předpis vztahující se k procesu	Uveďte zákonné předpisy, na základě kterých je proces realizován.
Vnitřní předpis	Uveďte vnitřní předpisy MmP, které proces upravují.
Typ zpracovávaného osobního údaje	Uveďte všechny typy osobních údajů, které jsou při procesu zpracovávány: jméno, příjmení, bydliště (trvalý pobyt), doručovací adresa, věk, datum narození, místo narození, rodné číslo, osobní stav, zdravotní znevýhodnění, fotografický záznam, video záznam, audio záznam, e-mailová adresa, telefonní číslo – soukromé i pracovní, identifikační číslo, daňové číslo, číslo občanského průkazu, číslo řidičského průkazu, číslo cestovního pasu, číslo řidičského průkazu, číslo bankovního účtu, vzdělání, příjem ze zaměstnání, příjem z důchodu, zdravotní pojišťovna, počet dětí, mateřská a rodičovská dovolená, nemocenská, údaje o rasovém či etnickém původu (národnost, NE státní občanství), politické názory (NE členství v politické straně nebo hnutí; NE členství v komunistické straně před rokem 1989), náboženské vyznání, členství v odborech, zdravotní stav (- údaje o tělesném nebo dušením zdraví, o poskytnutí zdravotních služeb), trestní delikty, pravomocná odsouzení, otisk prstu, podpis, jméno člena rodiny, příjmení člena rodiny, adresa člena rodiny, pohlaví člena rodiny, věk člena rodiny, datum narození člena rodiny, rodné číslo člena rodiny, zdravotní znevýhodnění člena rodiny, e-mailová adresa člena rodiny, tel. číslo (– soukromé i pracovní člena rodiny), číslo občanského průkazu člena rodiny, číslo řidičského průkazu člena rodiny, číslo cestovního pasu člena rodiny. „osobními údaji“ jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;
Zdroj osobního údaje	Uveďte, z jakých zdrojů osobní údaje shromažďujete: - od subjektu údajů - z veřejných zdrojů (specifikujte z jakých zdrojů) - z jiných zdrojů (specifikujte z jakých zdrojů)

Převzato: Interní dokumentace MMP, 2020

Příloha E: Návod k vyplnění (část 2)

Účel zpracování	Popište k jakému účelu jsou osobní údaje zpracovávány. Osobní údaje musí být: b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely („účelové omezení"); (čl. 5 odst. 1 písm. b) GDPR
Kategorie subjektů údajů	Uveďte jednotlivé kategorie subjektů údajů, které budou předmětem zpracování OÚ (např. vlastní zaměstnanci, zaměstnanci dodavatelů služeb, dlužníci, …)
Doba uložení údaje po naplnění účelu	Uveďte skartační znak dle skartačního řádu.
Důvod uložení	Uveďte právní důvod doby uložení OÚ s odkazem na právní předpis. Pokud takový není, potom vlastní odůvodnění doby uložení.
Zpracování na základě zákona nebo souhlasu	Uveďte příslušná písmena z čl. 6 odst.1 GDPR a vyplývá-li oprávnění z příslušného právního předpisu, potom ustanovení tohoto předpisu, na základě kterého je proces realizován např. **c) - § 36 zák. č. 257/2016.** Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu: **a)** subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů; **b)** zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů; **c)** zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje; **d)** zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby; **e)** zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce; **f)** zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě. První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.
Souhlas udělen subjektem nebo jinou osobou	Uvedte, zda souhlas poskytl přímo subjekt údajů nebo jiná osoba (např. zákonný zástupce)
Doba, na kterou byl souhlas poskytnut	
Kdo je zpracovatelem	
Právní základ zpracování údajů	

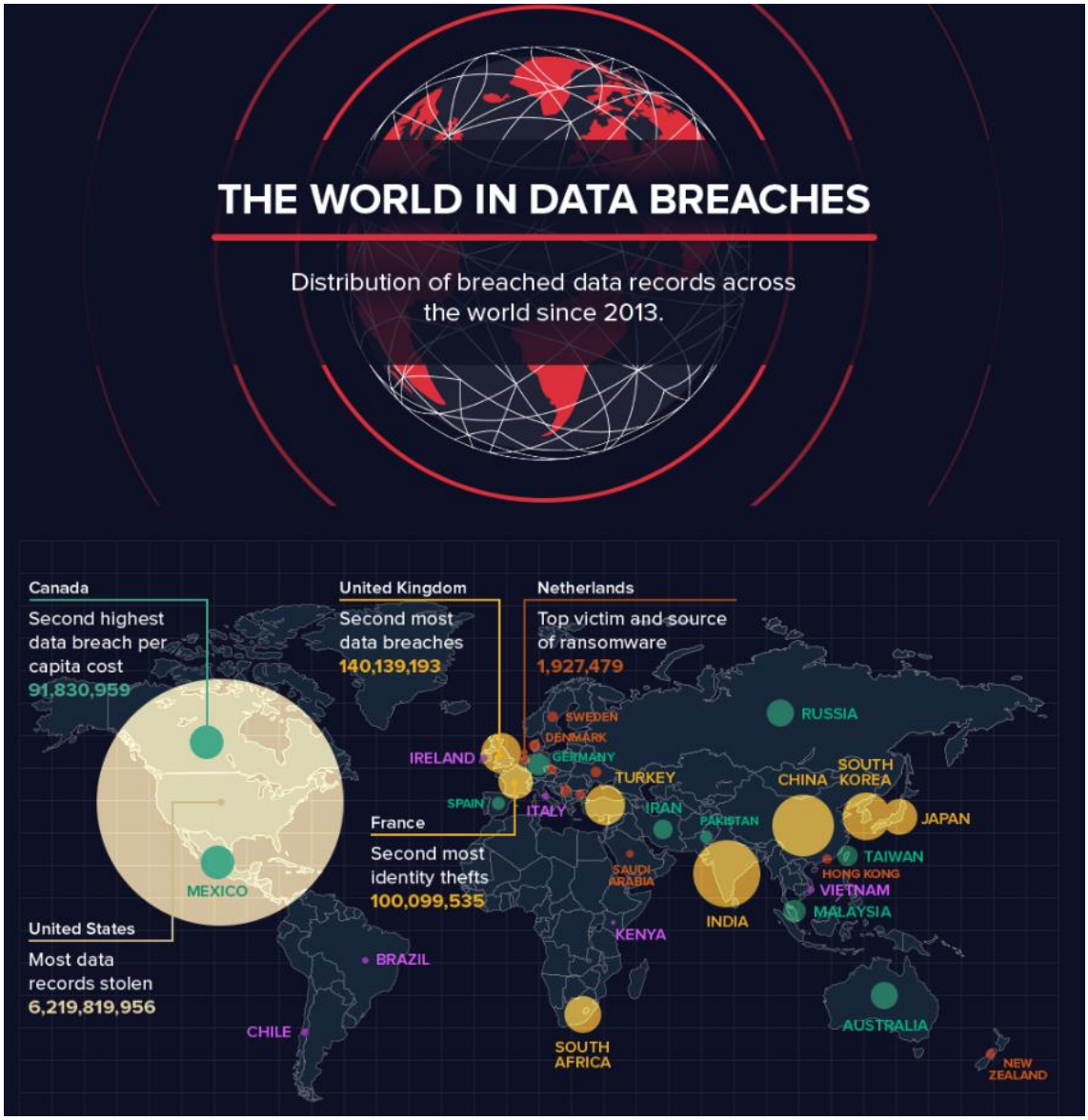
Převzato: Interní dokumentace MMP, 2020

Příloha E: Návod k vyplnění (část 3)

Způsob zpracování	Vyberte variantu z nabízených. V případě automatizovaného zpracování by se s osobními údaji neměly provádět další operace, aby nemohly být měněny. Manulním zpracováním se rozumí zpracování zejména v listinné podobě.
Skupiny osob s přístupem k údajům	
Kdo je příjemcem	Za příjemce se podle GDPR považuje fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.
Elektronicky nebo analogově	
Místo uložení	PC, server, aplikace, kartotéka apod.
Jaká jsou zavedena ochranná opatření	Uzamčená skříň, trezor, přístupová práva k aplikacím
Předání v rámci ČR	Údaje jsou předávány jiným subjektům (třetí osoby, úřady, orgány veřejné moci) v rámci ČR
Mimo ČR	Pokud dochází k předávání údajů do jiných států, uveďte do jakých.

Převzato: Interní dokumentace MMP, 2020

Příloha F: Úniky dat v letech 2013 až 2019 (část 1)

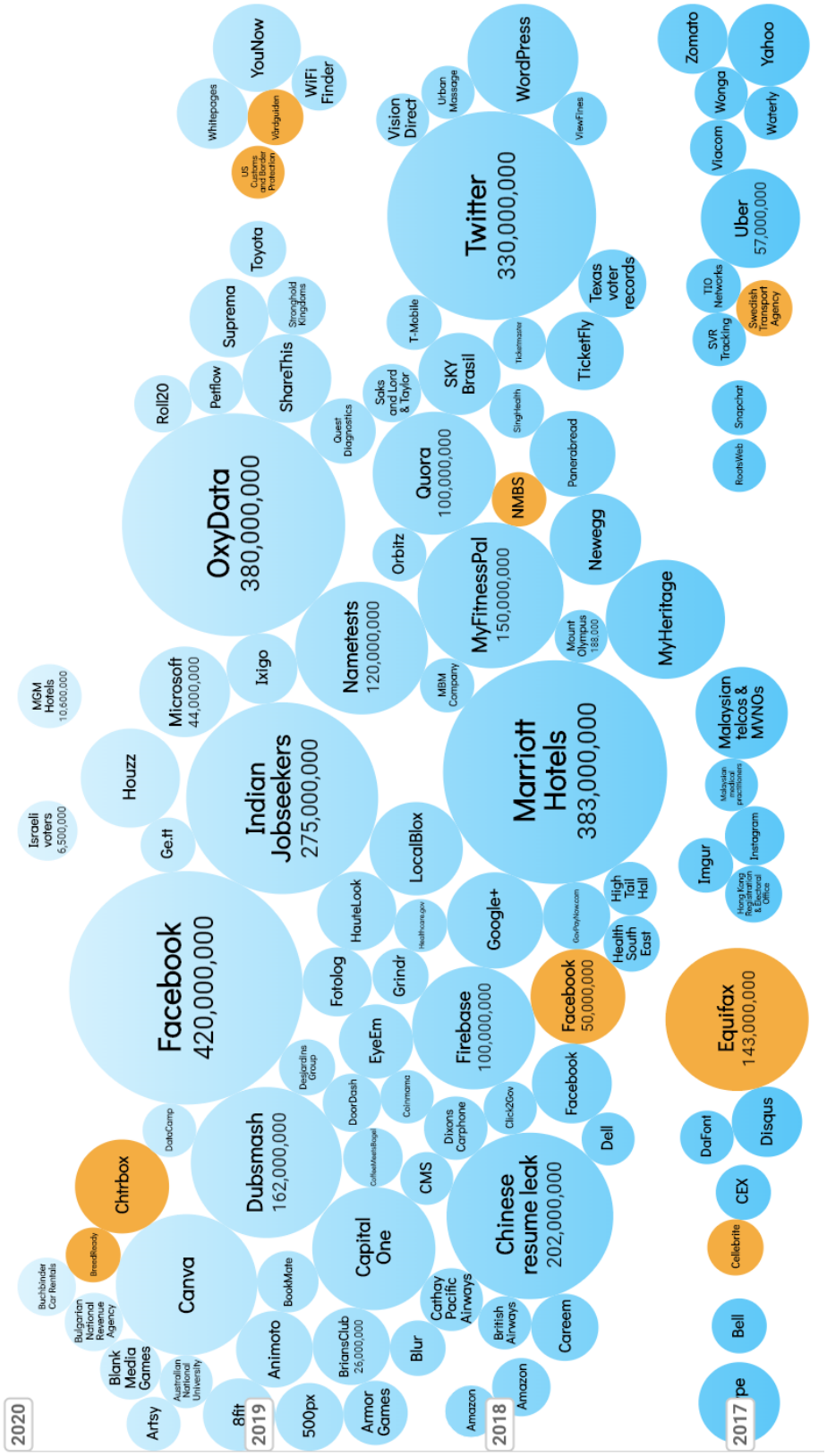


Převzato: Varonis, 2020

Příloha F: Úniky dat v letech 2013 až 2019 (část 2)

Převzato: Varonis, 2020

Příloha G: Grafické zobrazení úniků dat v letech 2017 až 2019



Převzato: Information is beautiful, 2020

Abstrakt

VELKOBORSKÁ, Marie. *Dopady GDPR na zvolený ekonomický subjekt.* Plzeň, 2020. 95 s. Diplomová práce. Západočeská univerzita v Plzni. Fakulta ekonomická.

Klíčová slova: ochrana osobních údajů, GDPR, dopady GDPR, Magistrát města Plzně, analýza rizik

Předložená práce je zaměřena na problematiku ochrany osobních údajů v České republice, konkrétně pak na téma dopadů GDPR na ekonomický subjekt – Magistrát města Plzně. Práce obsahuje hlavní náležitosti tohoto evropského nařízení, jeho historii, související právní předpisy a normy, základní pojmy a důležitá témata obsažená v tomto nařízení. Na teoretickou část práce navazuje představení zvoleného ekonomického subjektu včetně popisu stavu ochrany osobních údajů před i po implementaci GDPR. Dále dochází k identifikaci a vyhodnocení konkrétních dopadů GDPR na tento subjekt, a to prostřednictvím několika výzkumných metod (rozhovorů, diskusí, konzultací a dalších). Na základě zjištěných výstupů je provedena analýza rizik, která odkrývá nejkritičtější rizika v konkrétních kategoriích příčin vzniku. Výsledná matice rizik poté slouží jako podklad pro předložení zlepšujících opatření v této oblasti.

Abstract

VELKOBORSKÁ, Marie. *Impacts of GDPR on chosen economic subject.* Plzeň, 2020. 95 p. Thesis. University of West Bohemia. Faculty of Economics.

Key words: personal data protection, GDPR, impacts of GDPR, The Government Office of Pilsen, risk analysis

This thesis is focused on the issue of personal data protection in the Czech Republic and more specifically, on the impact of GDPR on one particular economic subject – The Government Office of Pilsen. The thesis contains the main requisites of this European regulation, its history, related legal regulations, basic terms and other relevant topics. The theoretical part is followed by the introduction of the economic subject and the description of how the subject managed the personal data protection before and after the GDPR implementation. The following part presents the identification and evaluation of specific impacts using several research methods (interviews, discussions, consultations etc.). Based on the identified outputs, it was possible to perform a risk analysis which revealed the most critical risk factors in specific categories of causes. The resulting risk matrix and its findings could then serve as the basis (starting point) for the submission of the improvement measures in this area.