ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

Dopady dodržování pravidel nastavených GDPR na zvolený ekonomický subjekt

Impacts of compliance with the rules set by the GDPR on the selected economic entity

Bc. Tereza Sedlecká

Plzeň 2022

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma

„Dopady dodržování pravidel nastavených GDPR na zvolený ekonomický subjekt“

vypracoval/a samostatně pod odborným dohledem vedoucí diplomové práce za použití pramenů uvedených v přiložené bibliografii.

Plzeň dne v.r. Tereza Sedlecká

Tímto bych chtěla velmi poděkovat paní Ing. Marii Černé, Ph.D. za vedení této diplomové práce a za její odborné rady a připomínky, a zároveň za její ochotu a zejména čas, který mi věnovala.

Dále bych chtěla poděkovat zaměstnancům společnosti Moneta Money Bank, a.s. za poskytnutí veškerých potřebných informací a materiálů. Dále také za jejich čas a možnost pravidelných konzultací.

Obsah

Úvod

Dříve problematice osobních údajů a jejich ochraně nebyla věnována taková pozornost jako v současnosti. Velký vliv na to má neustále se rozvíjející technologie, kdy také roste riziko zneužití těchto dat. Je tedy velmi důležité, aby měla každá společnost správně nastavená bezpečnostní opatření a neustále prohlubovala znalosti v této problematice.

Stejně jako mají lidé právo na bezpečnost a svobodou, mají také právo na ochranu osobních údajů. Ochrana osobních údajů je velmi důležitá nejen z důvodu ochrany subjektů poskytujících tyto údaje, ale také chrání instituce a společnosti zpracovávající tyto údaje. Mezi negativní důsledky lze zařadit například odcizení dat či jejich zneužití nebo také ztrátu důvěryhodnosti firmy.

Již dříve existovaly některé právní předpisy, které upravovaly ochranu osobních údajů. Velký zlom ale přišel až v roce 2018, kdy bylo vydáno evropské nařízení o GDPR. Pro každou společnost to znamenalo mnoho interních změn, které se projevovaly například ve změnách interních předpisů či interních systémů. Od roku 2018 musela mít každá společnost natavená veškerá opatření tak, aby docházelo k co nejvyššímu zabezpečení osobních údajů a veškerá opatření musela být zároveň v souladu s obecným nařízením. To se v současnosti považuje za nejpodstatnější právní ochranu pro osobní údaje a jejich zpracování.

A právě téma GDPR je zpracováno v rámci této diplomové práce. Konkrétně jsou zde uvedeny hlavní dopady tohoto obecného nařízení na zvolený ekonomický subjekt, kterým je Moneta Money Bank, a.s.

Tato diplomová práce je rozdělena do 7 kapitol.

Úvodní kapitola popisuje hlavní cíle a hlavní postup zpracování.

Druhá kapitola se věnuje základní charakteristice obecného nařízení, popisuje, co je předmětem a hlavními cíli GDPR. Vysvětluje také jeho důležité pojmy a historický vývoj ve světě i v České republice. Zmíněné jsou zde také dva nové přístupy, na kterých je obecné nařízení založeno.

Ve třetí kapitole jsou definována hlavní témata týkající se obecného nařízení.

Praktická část začíná čtvrtou kapitolou, kde jsou uvedeny základní informace o zvoleném subjektu, tedy o Monetě Money Bank. Dále jsou zde popsány hlavní subjekty, se kterými banka spolupracuje v rámci předávání osobních údajů a také jaké využívá interní systém.

Pátá kapitola analyzuje subjekt z pohledu na situaci před zavedením GDPR a následně uvádí hlavní postup při implementaci obecného nařízení do chodu společnosti.

Šestá kapitola je zaměřena na konkrétní dopady zavedení GDPR ve společnosti. Informace týkající se všech uvedených podkapitol vychází z osobních konzultací a také ze zpracování interních či veřejně dostupných dokumentů.

Poslední kapitola je zaměřena na analýzu rizik vyplývající ze zpracování a ochrany osobních údajů a na jejich následné vyhodnocení. Na základně toho jsou v rámci této kapitoly také uvedeny konkrétní návrhy na zlepšení bezpečnosti osobních údajů a zjednodušení zpracování těchto údajů.

1 Cíl a metodika práce

První kapitola napomáhá k pochopení základních cílů práce. Také jsou zde uvedeny postupy zpracování či zdroje, které byly použity pro získání potřebných informací.

1.1 Cíle práce

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

Hlavním cílem práce, jak vyplývá z názvu práce, je identifikace a následné vyhodnocení dopadů GDPR na zvolený ekonomický subjekt. Následně je vypracován návrh na zlepšení v rámci této oblasti u konkrétního podniku.

Pro dosažení stanoveného cíle bude nutné provést analýzu zvoleného subjektu, kterým je v tomto případě Moneta Money Bank, a.s. Analýza bude provedena v rámci několika konzultací s pracovníky z oddělení, které má GDPR na starosti.

Bude tedy na konkrétním příkladu uvedena daná problematika, včetně popisu toho, jaké to bylo před zavedením GDPR, jak zavedení GDPR ovlivnilo podnik a jeho zaměstnance. Dále bude uvedeno, jak proběhla implementace pravidel nastavených GDPR a hodnocení výstupů od doby zavedení GDPR.

Vedlejší cíle práce jsou zejména:

- provést literární rešerši řešené problematiky,
- charakterizovat zvolený ekonomický subjekt – Moneta Money Bank, a.s.,
- provést analýzu zavádění GDPR,
- identifikovat případná rizika spojená s ochranou osobních údajů.

V rámci praktické části budou zodpovězeny předem definované výzkumné otázky.

Jaká byla situace před zavedením GDPR?

Jak probíhala implementace GDPR – tedy jak ovlivnila chod subjektu, co bylo potřeba sestavit a upravit pro zavedení této normy?

Jak bylo zavedení GPRD náročné z hlediska času, administrativy a nákladů?

Jak jsou data s osobními údaji chráněna a jak je vedena papírová a elektronická dokumentace?

Kdo je v podniku pověřenec pro GDPR a jaké jsou jeho hlavní úkoly?

Jak dochází ke kontrole dodržování pravidel GDPR?

Jak subjekt hodnotí současnou situaci po zavedení GDPR?

Jaká rizika jsou spojena s ochranou osobních údajů v podniku?

1.2 Postup zpracování

Diplomová práce využívá několik typů zdrojů.

Prvním ze zdrojů jsou zejména podklady legislativního charakteru, tedy zákon či jiné právní předpisy a dále odborná literatura či odborné články vztahující se k tématu GDPR. Tyto zdroje slouží k vypracování teoretické části.

Pro praktickou část jsou využívány zdroje daného ekonomického subjektu. Konkrétně jsou tím myšleny konzultace se zaměstnanci firmy Moneta Money Bank, a to především s manažerkou oddělení Data Privacy & Digital Compliance, která se oblastí ochrany osobních údajů a také vedením GDPR zabývá. Návrhová část je vypracována na základě informací získaných v rámci konzultací se zaměstnancem z oddělení Operation Risk.

Právní předpisy

Dříve nebyla ochrana osobních údajů příliš legislativně chráněna. Dřívější zákony se týkaly spíše konkrétních oblastí (například informačních systémů). Ochrana osobních údajů tak byla nedostatečná v rámci neustále se rozvíjejících technologii. Více se k rozvoji legislativy týkající se ochrany osobních údajů uvádí v kapitole 2.3 a 2.3.1.

Velmi důležitým současným legislativním nařízením, které nabylo účinnosti až 25. května 2018, je *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)*. V textu je nařízení dále uváděno jako „obecné nařízení“ nebo jen „nařízení“. To nahrazuje předchozí právní úpravu – Směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. V roce 2018, kdy bylo toto nařízení uplatněno, došlo i k nahrazení výše zmiňovaného zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (Nezmar, 2018).

V roce 2019 byl ale v platnost uveden nový zákon – *zákon č. 110/2019 Sb., o zpracování osobních údajů.* Ten tedy nahrazuje původní zákon a zároveň doplňuje současné nařízení.

Původní směrnice byla nedostačující a důvod, proč bylo potřeba směrnici nahradit aktuálnější verzí, byl dán především vlivem nové technologie. Veškeré elektronické obchodování, obrovský rozvoj sociálních sítí, internetové obchody a služby či elektronické bankovnictví znamenají velký přenos osobních dat i napříč Evropskou unií. Nové nařízení si tedy již uvědomuje důležitost ochrany osobních údajů a je nejúplnějším opatřením v rámci nástrojů sbližování práva, který je v EU orgánům k dispozici (Navrátil, 2018).

2 Úvodní teoretická východiska GDPR

Následující kapitola poukazuje na základní informace o náležitostech GDPR. Z počátku je popsána charakteristika ochrany osobních údajů, základní pojmy související s GDPR, co je hlavním cílem a předmětem této problematiky. Následuje zohlednění nových přístupů a povinností vyplývajících z nového nařízení. V poslední části je stručně charakterizován vývoj ochrany osobních údajů jak obecně, tak i v rámci České republiky.

2.1 Charakteristika GDPR

GDPR (angl. General Data Protection Regulation) je novým právním rámcem pro ochranu osobních údajů v rámci Evropy. Hlavním cílem je co největší ochrana občanů EU proti neoprávněnému zacházení s jejich daty včetně osobních údajů. Vztahuje se na všechny firmy a instituce, ale i jednotlivce a online služby, které zpracovávají data uživatelů (GDPR, n.d.).

Již v předchozí kapitole bylo zmiňováno, že obecné nařízení nahradilo původní směrnici, která z hlediska ochrany osobních údajů nebyla dostačující. V rámci tohoto nového nařízení došlo ke změnám některých definic obsažených právě v již neplatné směrnici. Jednalo se například o pojmy zabývající se ochranou osobních údajů dítěte, čemuž se věnuje článek 8 v obecném nařízení. Dále se změny týkají bezpečnosti osobních údajů, genetických údajů, údajů týkajících se zdraví, podnikových pravidel a také provozoven. Důležitou změnou či úpravou byla také definice osobních údajů, jelikož byla rozšířena o konkrétní příklady identifikátorů (např. o poloze nebo IP adresy). Došlo také k definování vícero pojmů, které ve směrnici 95/46/ES zcela chyběly (Docksey, 2020).

Jelikož se jedná právě o nařízení, nikoli o směrnici, tak přímo určuje pravidla pro zpracování osobních údajů ve všech zemích Evropské unie. GDPR je ale považováno za právní základ ochrany osobních údajů v EU, ale zásadně ovlivňuje i evropské země, které nejsou součástí Evropské unie (konkrétně se jedná o Island, Lichtenštejnsko a Norsko). Jedná se tedy o sjednocující právní normu, což je velmi přínosné a důležité pro pohyb informací mezi jednotlivými zeměmi. Zajištění toho, aby byla větší jednotnost pravidel ochrany osobních údajů bylo i jedním z důvodů a cílů, proč GDPR přijmout (Navrátil, 2018).

2.1.1 Důležité pojmy

V rámci obecného ustanovení v článku 4 jsou vysvětleny základní pojmy, které jsou důležité k pochopení dané problematiky. V rámci této práce jsou uvedeny pouze některé z nich, které jsou potřeba pro tuto práci.

Za nejdůležitější pojem by se dal považovat **osobní údaj**. Tím je myšlena každá informace o identifikované fyzické osobě, která se také označuje jako **subjekt údajů**.

Zpracování je jakákoli operace s osobními údaji prováděná buď s nebo bez pomoci automatizovaných postupů. Jedná se například o činnosti jako je shromáždění, zaznamenání, uložení, vyhledání, použití, šíření, omezení či výmaz nebo zničení.

Za **evidenci** se považuje jakýkoliv strukturovaný soubor s osobními údaji.

Správce je fyzická nebo právnická osoba nebo jiný subjekt, který určuje účely a prostředky, podle kterých budou osobní údaje zpracovány.

Zpracovatel má za úkol zpracování osobních údajů pro správce.

Příjemce je fyzická nebo právnická osoba či jiný subjekt, kterému se osobní údaje poskytují. Nespadají sem ale orgány veřejné moci, které mohou údaje získávat v rámci zvláštního šetření.

2.2 Předmět a cíle GDPR

Obecně lze říci, že hlavním důvodem, proč bylo GDPR vytvořeno, bylo to, že předchozí legislativní úprava byla nedostatečná v rámci přizpůsobení se současné době a také snaha, aby došlo ke sjednocení právního rámce ve všech zemích.

Nulíček (2018, str. 60) uvádí: „*Předmětem Nařízení jsou pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla týkající se volného pohybu osobních údajů. Fyzické osoby jsou v Nařízení chráněny jednak tím, že jsou jim přiznána určitá práva, kterými mohou vykonávat kontrolu nad využitím svých osobních údajů, a také tím, že Nařízení stanoví určité podmínky, za kterých je osobní údaje možné zpracovávat, a povinnosti pro ty, kdo osobní údaje zpracovávají.*“

Cíle jsou definovány přímo v obecném ustanovení, ale také je uvádějí ve svých publikacích někteří autoři. Dle Navrátila (2018, str. 60) jsou hlavní cíle GDPR tyto:

- *„přizpůsobení právní regulace ochrany osobních údajů poměrům dnešní doby,*

- *sjednocení práva ochrany osobních údajů ve všech zemích Evropské unie a dalších zemích, na které dopadá,*
- *posílení práv v oblasti ochrany osobních údajů všech osob, které jsou subjekty údajů a dosáhnout sjednoceného výkladu GDPR dozorovými úřady jednotlivých zemí Evropské unie,*
- *posílit důvěryhodnost Evropské unie a jejích členských zemí (i dalších zemí, které pod GDPR spadají) pro jiné země, které mají zájem na rozvoji obchodu s Evropskou unií a s tím souvisícím předáváním osobních údajů mezi zeměmi.*

V obecném nařízení v článku č. 1 jsou uváděny tyto hlavní cíle GDPR:

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

2.3 Nové přístupy a povinnosti

Zavedením obecného nařízení došlo k několika zásadním změnám. Tyto změny se také týkají přístupů a jistých povinností, které z nařízení vyplývají. Zásadní v rámci GDPR jsou dva nové přístupy:

1. princip odpovědnosti správce a
2. princip založený na riziku.

Co vyplývá z odpovědnosti správce, je uvedeno v kapitole o zásadách zpracování osobních údajů. Co se týká principu založeného na riziku, je nutné si uvědomit, že správce musí už od úplného začátku v rámci zpracovávání osobních údajů brát v potaz povahu, rozsah, kontext a účel zpracování a zohlednit veškerá rizika, kterým musí být přizpůsobeno i zabezpečení těchto údajů. Týká se to zejména nové povinnosti v rámci ohlašování bezpečnostního incidentu Úřadu pro ochranu osobních údajů (Nezmar, 2018).

Jelikož je bezpečnost z hlediska GDPR velmi důležitá, je tomuto tématu věnována samostatná kapitola.

Co se týká zásad či klíčových instrumentů, nedošlo k příliš velkým změnám, nýbrž spíše k detailnějšímu věnování se jednotlivým oblastem. Přesto dochází k novým povinnostem, které z GDPR vychází.

Nezmar (2018, str. 30) uvádí tyto nové povinnost:

- *„povinnost vést záznamy o činnostech zpracování,*
- *posouzení vlivu na ochranu osobních údajů,*
- *předchozí konzultace,*
- *ohlašování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů,*
- *oznamování případu porušení zabezpečení osobních údajů subjektu údajů, a*
- *ustanovení pověřence pro ochranu osobních údajů.“*

2.4 Historický vývoj legislativních opatření z oblasti ochrany osobních údajů

Ochrana osobních údajů se dříve objevovala spíše v podobě práva na soukromí. Mělo tedy úplně jinou podobu, a i jiný význam, než jaký má dnes. Právo na soukromí uvedl jako jeden z prvních autorů Thomas Cooley v roce 1888 pod pojetím „práva být nechán o samotě“.

O dva roky později vydali S. D. Warren a L. D. Brandeise článek „The Right of Privacy“, kde bylo komplexně definováno právo na soukromí. Nicméně autoři byli toho názoru, že nevytvářejí nic nového, ale objevují již existující právo a ochrana soukromí je jen přirozený krok ve vývoji práva.

Zlomovým byl až rok 1948 krátce po druhé světové válce, kdy došlo ke zhmotnění vývoje chápání ochrany soukromí a tento vývoj byl zakotven do článku 12 Všeobecné deklarace lidských práv (Nulíček, 2018).

Podle tohoto článku 12 nesměl být žádný občan vystaven zasahování do jeho soukromí a každý měl právo být chráněn proti těmto zásahům. I přesto, jak důležitá Všeobecná deklarace lidských práv byla, právní závaznosti nikdy nenabyla. Tu nabyl až Mezinárodní pakt o občanských a politických právech, který ve svém článku 17 obsahově doslovně převzal již zmiňovaný článek 12.

Důležitým dokumentem byla i Evropská úmluva o ochraně lidských práv a základních svobod z roku 1950 (Navrátil, 2018).

Za období, ve kterém nastaly závazné změny, se uvádí 70. léta 20, století, kdy docházelo k velkému vývoji a pokroku v oblasti technologie, což s sebou neslo proměny zejména v komunikaci, uzavírání smluv či získávání informací. Bylo nutné zajistit větší bezpečí v rámci ochrany soukromí lidí. O to se poprvé pokusila nezávazná směrnice OECD z roku 1980, která jako první definovala základní principy pro ochranu osobních údajů a též se zde už objevují některé základní pojmy, které byly zmiňovány v rámci podkapitoly 2.1.1.

Směrnice OECD však nikdy nebyla právně závazná a měla sloužit spíše k vytvoření legislativy pro ty státy, které ji vůbec neměly. Právě tato směrnice stála za vytvořením Úmluvy č. 108 (Nulíček, 2018).

Úmluva č. 108 neboli *Úmluva o ochraně osob se zřetelem na automatizované zpracování dat* se považuje za první komplexní dokument, který se zajímá o ochranu osobních údajů (Navrátil, 2018).

V rámci Evropské unie byla až v roce 1995 vydána speciální směrnice – *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*. Díky této směrnici došlo především k zajištění fungování trhu a ochrany základních práv a svobod fyzických osob (Nulíček, 2018).

Směrnice č. 95/45/ES umožňovala i snazší pohyb osob v rámci tzv. Schengenského prostoru, protože je potřeba si uvědomit, že volný pohyb osob v určitém prostoru je možný jen tehdy, pokud je umožněn i pohyb osobních údajů. Platnost této směrnice skončila v roce 2018, kdy byla nahrazena GDPR (Navrátil, 2018).

V květnu 2018 tedy nabývá účinnosti GDPR neboli Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Nezmar, 2018).

2.4.1 Vývoj v České republice

V České republice jsou v rámci legislativy o ochraně soukromí uplatňovány poprvé *zákon č. 87/1862 Sb.z.s., o ochraně svobody osobní* a *zákon č. 88/1862 Sb.z.s., na ochranu svobody domovní*. Následně po vzniku samostatného Československa uzákonili *Ústavní*

zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního (podle § 107, 112 a 116 ústavní listiny).

Důležitý byl rok 1950, kdy se podepsala *Úmluva o ochraně lidských práv a základních svobod* (neboli Evropská úmluva o lidských právech), která se považuje za základní činitel pro pochopení práva na soukromí.

Až 90. léta 20. století přinesla ochraně osobních údajů větší pozornost. Vešel v platnost zákon *č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech*. Už dle názvu je patrné, že nebyl dostačující, jelikož upravoval ochranu údajů pouze v rámci informatiky. Dále byla vyhlášená Usnesením předsednictva České národní rady č. 2/1993 Sb. *Listina základních práv a svobod*.

Poté byl roku 2000 přijat již *zmiňovaný zákon č. 101/2000 Sb., o ochraně osobních údajů*. Na počátku roku 2009 též nabyla platnost *Lisabonská smlouva* novelizující smlouvu o Evropské unii. Lisabonská smlouva měla stejnou právní sílu jako Listina základních práv Evropské unie a díky tomu se stala její součástí. Stejným způsobem byla do ústavního pořádku České republiky přijata Listina základních práv a svobod (Navrátil, 2018).

Do 90. let 20. století nebyly v ČR zřízeny ani žádné dozorčí orgány. Kontrola byla zřízena pouze v rámci Evropy.

Důležitou součástí české legislativy byla také *Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*, která se oproti zákonu č. 256/1992 Sb., vztahovala již i na zpracování prostřednictvím evidence, nikoli jen na informační systémy.

V roce 2000, kdy vešel v platnost zákon č. 101/2000 Sb., byl také zřízen jako dozorčí orgán Úřad pro ochranu osobních údajů. Tento zákon byl v roce 2004 novelizován v souvislosti s nutností transponovat Směrnici 95/46/ES z toho důvodu, že Česká republika v tom období vstoupila do Evropské unie.

Nejdůležitějším současným nařízením v rámci ochrany osobních údajů je již zmiňované *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)*, platné od roku 2018.

Je ale nutné do legislativního rámce zařadit také *zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.* Právní předpisy zajišťují nejen ochranu osobních údajů, ale částečně i ochranu soukromí. V nejširším slova smyslu je ale soukromí chráněno *zákonem č. 89/2012 Sb., občanský zákoník* (Žůrek, 2018).

Následující tabulka zobrazuje přehled vývoje legislativy na ochranu osobních údajů.

Tabulka 1: Shrnutí vývoje základních dokumentů upravujících soukromí a ochranu osobních údajů

Rok	Legislativní předpis
1948	Všeobecná deklarace lidských práv
1950	Evropská úmluva o ochraně lidských práv a základních svobod
1964	Občanský zákoník
1981	Úmluva o ochraně osob se zřetelem na automatizované zpracování
1992	Počátek výslovné ochrany soukromí v OZ
	Zákon o ochraně osobních údajů v informačních systémech
1995	Směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů
2000	Zákon o ochraně osobních údajů
2002	e-Privacy směrnice
2014	Nový občanský zákoník
2018	Obecné nařízení o ochraně osobních údajů
	Zákon o ochraně osobních údajů (pouze doplňkový)
	Trestněprávní směrnice
	PNR směrnice

Zdroj: Žůrek, 2018

Zpracovala: Tereza Sedlecká, 2022

3 Podstatná témata

V rámci této kapitoly jsou vysvětlena podstatná témata z oblasti ochrany osobních údajů a také některé důležité body vyplývající z obecného nařízení.

3.1 Působnost obecného nařízení

Osobní působnost

Osobní působnost určuje subjekty (adresáty), na které se vztahují právní předpisy. Mezi adresáty se řadí správci, zpracovatelé, subjekty údajů neboli dozorové úřady a Sbor. V rámci obecného nařízení je všem těmto subjektům nařízena povinnost či stanoveno právo, které se na ně vztahují. Za adresáty se však mohou považovat i členské státy, které musí dle nařízení přijímat zákonné předpisy (Žůrek, 2018).

Věcná působnost

V obecném nařízení je tato působnost vymezena v článku 2. Vztahuje se jak na úplně nebo jen z části automatizovaná, tak i na neautomatizovaná zpracování osobních údajů. Tyto údaje jsou uloženy v evidenci nebo do ní budou teprve zařazeny. Příklad automatizovaného zpracování je například pro webový skript, kdy se u žadatele o úvěr posuzují také údaje, podle kterých bude žádost buď schválena, nebo zamítnuta. Neautomatizované neboli manuální zpracování spočívá ve fyzických kopiích dokumentů (např. kartotéky), které musí být uspořádány podle daných kritérií (Nulíček, 2018).

Věcná působnost určuje i pozitivní a negativní vymezení. V rámci pozitivního vymezení určuje, na co se vztahuje a v rámci negativního, na co se nevztahuje. Do negativního vymezení lze zařadit:

- zpracování osobních údajů, které jsou prováděny fyzickou osobou v rámci osobních nebo domácích činností (např. vytváření adresářů, vedení vlastních záznamů, využívání sociálních sítí nesouvisejících s profesní činností), nelze sem ale zařadit například bezdůvodné sledování veřejného prostoru pomocí kamer,
- vše, co provádí příslušné orgány v souvislosti s prevencí, odhalováním, vyšetřováním či stíháním trestných činů nebo výkonů trestů,
- zpracování osobních údajů zesnulých osob, a
- situace u soudu, kdy se neuplatňuje pravomoc dozorových úřadů z důvodu zajištění nezávislosti soudnictví (Žůrek, 2018).

Místní působnost

Místní působnost je vymezena v článku 3 obecného nařízení. Určuje, kde se nařízení použije podle geografického území. K uplatnění dochází v souvislosti s činností správce nebo zpracovatele údajů, kdy je provozovna na území EU, ale i mimo EU.

Nařízení se ale také vztahuje na správce a zpracovatele, kteří nevykonávají činnosti v rámci provozovny, avšak činnosti souvisejí s:

- nabídkou zboží a služeb, které se nacházejí v EU,
- monitorováním chování subjektů z EU.

Monitorování chování probíhá prostřednictvím cookies, IP adres, MAC adres nebo geolokačních údajů (Nulíček, 2018).

Díky tomu, že se nařízení vztahuje jak na činnost provozovny v rámci Evropské unie, tak mimo ni, je zaručeno, že se správci nemohou danému nařízení vyhnout tím, že by svoji činnost prováděli mimo EU.

Časová působnost

Časová působnost se vztahuje na vymezení doby, po kterou je právní předpis považován za součást právního řádu. Je nutné znát rozdíl mezi platností a účinností. Platnost označuje termín, kdy prošel předpis daným legislativním procesem a následně byl vyhlášen v příslušné sbírce a stává se tak součástí právního řádu. Účinnost označuje to, že daný právní předpis je pro všechny adresáty závazný a může dojít k jeho aplikování (Žůrek, 2018).

3.2 Osobní údaje a jeho zvláštní kategorie

I přesto, že nařízení obsahuje řadu novinek a specifičtějších úprav ochrany osobních údajů, definice tohoto pojmu se od původně platného zákona č. 101/2000 Sb. příliš neliší.

Dle zákona č. 101/2000 Sb., je *„osobním údajem jakákoli 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.*

Dle obecného nařízení (článek 4) se za osobní údaj považují *„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"

Dle nařízení v článku 4 jsou za osobní údaje považovány:

- jméno a příjmení,
- datum a místo narození,
- pohlaví,
- místo trvalého pobytu,
- rodinný stav,
- identifikační čísla,
- lokační údaje,
- síťové identifikátory,
- úroveň dosaženého vzdělání.

Dále jsou vymezeny zvláštní (označované také jako citlivé) osobní údaje. Tyto údaje mohou subjekt poškodit ve společnosti, zaměstnání či škole, a proto jim je věnována zvýšená ochrana zpracování. Jedná se o:

- údaje rasového a etnického původu,
- údaje o politických názorech,
- údaje o náboženském vyznání či filozofickém přesvědčení,
- údaje o členství v odborech,
- údaje o zdravotním stavu,
- údaje o sexuálním životě či sexuální orientaci,
- genetické a biometrické údaje (Nezmar, 2018).

Je velmi zásadní uvědomit si, co se dá opravdu za osobní údaj považovat. Ani v rámci nařízení o GDPR nejsou udávány konkrétní příklady těchto údajů. Osobní údaj slouží zejména k identifikaci konkrétního člověka. Pokud by chtěl identifikovat osobu pouze na základě jména či data narození, nebude to dostačující informace, neboť pod takovým údajem může dohledat osob více. Dané jméno musí být spojeno s dalším specifickým údajem (např. rodné číslo) nebo s více údaji, aby se dal údaj považovat dle nařízení za osobní údaj.

3.3 Zásady zpracování osobních údajů

Již v první směrnici upravující ochranu osobních údajů se uvádí základní zásady pro zpracování těchto údajů. Jedná se o směrnici 95/46/ES, podle které členské státy stanoví, že osobní údaje musí být:

- zpracovány spravedlivě a zákonně,
- shromažďovány pro konkrétní účely,
- přiměřené ve vztahu k účelům, za jakými jsou zpracovávány,
- přesné a pokud to situace vyžaduje, i aktualizované,
- uchovávány po dobu ne delší, než je nezbytně nutné (Směrnice 95/46/ES, čl. 6).

V obecném nařízení v článku 5 jsou tyto zásady pro zpracování osobních údajů uvedeny v téměř totožném znění. Navíc obsahuje pouze jednu zásadu, která říká, že údaje musí být zpracovány tak, aby byly řádně zabezpečeny (obecné nařízení, čl. 5).

V obou zmíněných předpisech je dále uvedeno, že za dodržení těchto zásad je odpovědný správce.

Zákonnost je nejdůležitějším principem, jak data ochránit. Stanovuje, že dané zpracování musí vždy probíhat v rámci minimálně jednoho z právních titulů uvedených v článku 6 obecného nařízení (zákonnost zpracování). Dále stanovuje, že zpracovávat osobní údaje nelze nelegálním způsobem, což znamená, že musí být současně i v souladu s občanským zákoníkem.

Korektnost a transparentnost znamená otevřenost a transparentnost v rámci toho, jak je s údaji nakládáno. V podstatě to nařizuje „chovat se fér“. Obě zásady považují za základ informovanost subjektu údajů. Součástí transparentnosti je také povinnost informovat o případech, kdy dojde k závažnému porušení zabezpečení osobních údajů.

Účelové omezení výstižně určuje, k čemu může správce osobní údaje využívat. Může je zpracovávat pouze za tímto účelem až na výjimky, které spadají pod tzv. další zpracování. Účel je velmi důležitý, protože od toho se odvíjí další zásady. Účel musí být určitý (musí z něho být jasné, k jakým zpracováním dojde či nedojde), výslovně vyjádřený (účel musí být sdělen subjektům údajů a jeho formulace musí být i včas dokumentována) a legitimovaný (účel musí být v souladu s právním řádem). Je také možné, aby daný údaj měl více účelů, pro které bude použit.

Další zpracování znamená, že jsou osobní údaje zpracovány za jiným účelem, než pro který byly původně sesbírány. Jedná se o případy, kdy:

- je účelem archivace ve veřejném zájmu, historický výzkum nebo statistický účel,
- k tomu dá subjekt souhlas,
- je založeno na právu členského státu či státu z Evropské unie, nebo
- když bylo správcem provedeno posouzení slučitelnosti.

Zásada **minimalizace údajů** říká, že údaje by se měly shromažďovat nebo zpracovávat jen v takovém množství či rozsahu, který je potřeba pro naplnění účelu. Odráží se to i na principech záměrné a standardní ochrany, což znamená, že správce používá pro volbu prostředků, přes které lze údaje zpracovávat, a pro nastavení parametrů, taková opatření, jež zajišťují nejen minimalizaci údajů, ale i ostatní základní zásady.

Zásada přesnosti udává, že osobní údaje se musí zpracovávat na základě skutečných dat a také musejí být aktualizované. Pokud subjekt poskytne údaje nepravdivé, správce za jejich nepřesnost nenese odpovědnost. Nepřesné údaje se mohou týkat gramatických nebo výpočetních chyb, ale také souvisí s pravdivostí stavu. Dle Úřadu pro ochranu osobních údajů (dále jen jako „ÚOOÚ“) musí každý zpracovatel zajistit opatření, díky kterým nepřesné údaje nebudou zpracovány.

Zásada omezení uložení určuje dobu, kterou mohou být údaje uchovávány. Pokud už jsou data použita v rámci všech účelů, ke kterým byla poskytnuta, musí být poté smazána nebo anonymizována.

Anonymizace je podobný proces jako smazání údajů. Podle údajů, které jsou anonymizovány, nelze identifikovat fyzickou osobu, jelikož anonymizované údaje nelze považovat za osobní údaje. Správce má za úkol pravidelně provádět kontrolu, zda je daná anonymizace dostatečná. O anonymní údaje se jedná tehdy, pokud není možné daný subjekt identifikovat správcem nebo kýmkoli jiným. Pro bezpečnost je vhodnější, aby všechny originální datové soubory byly pro provedení anonymizace vždy mazány.

Zásada integrity a důvěrnosti uvádí, že osobní údaje by měly být zpracovány tak, aby bylo zajištěno řádné zabezpečení před jakýmkoli protiprávním či neoprávněným zpracováním a také před ztrátou nebo poškozením. Tato zásada je velmi důležitá, a proto je také uvedena jako jedna z hlavních v zákoně o ochraně osobních údajů. Bezpečnost údaje je podrobněji rozebrána v samostatné podkapitole.

Ze **zásady odpovědnosti** vyplývají pro správce dvě hlavní povinnosti:

- správce je odpovědný za všechny operace spojené s osobními údaji, které vyplývají z výše popsaných zásad, a
- správce musí být schopen dokázat dodržení souladu.

Druhý bod je novým oproti předchozím legislativním předpisům. Správce je odpovědný za to, že sám zavádí vhodné systémy ochrany a vše musí mít řádně zdokumentováno (Nulíček, 2018).

3.4 Oprava a výmaz osobních údajů

Každý člověk musí mít právo na opravu osobních údajů a také právo na to „být zapomenut“. Pokud poskytne fyzická osoba svoje osobní údaje, určitě je poskytuje za určitým účelem (např. získání úvěru). Jakmile už ale z hlediska účelu nejsou tyto údaje potřeba, měly by být odstraněny, aby nedošlo k jejich zneužití.

Právo na opravu má subjekt údajů kvůli opravě nepřesných osobních údajů či doplnění neúplných osobních údajů (článek 16).

Přesnost osobních údajů spadá pod jednu ze zásad nařízení. Správce by měl zpracovávat přesné a aktuální údaje. Nepřesné údaje by měly být vymazány nebo opraveny. Správce má také za úkol přesnost údajů ověřit a do té doby je zpracování těchto údajů omezeno. Pokud dojde k nějaké změně, musí správce o tom správce informovat subjekty údajů.

Subjekt může využít práva na doplnění neúplnosti osobních údajů. Správce ale musí prověřit, zda tyto údaje bude z hlediska účelu opravdu potřebovat, aby je nezpracovával zbytečně (Nulíček, 2018).

Právo na výmaz (neboli „právo být zapomenut“) dává subjektu údajů možnost požádat o úplné odstranění jeho osobních údajů bez zbytečného odkladu (článek 17).

Vymazat údaje může chtít subjekt z těchto důvodů:

a) z hlediska účelu zpracování už nejsou údaje potřeba,
b) odvolá svůj souhlas,
c) z jeho strany existují námitky se zpracováním
d) došlo k protiprávnímu zpracování osobních údajů,
e) nutnost vymazání kvůli splnění právní povinnosti,

f) údaje byly shromážděny za účelem nabídky služeb informačních služeb (Nulíček, 2018).

3.5 Pověřenec pro ochranu osobních údajů

Pověřenec je specifická funkce, která vznikla při platnosti obecného nařízení. Povinnost jmenovat pověřence nemá ale každý správce. Ty subjekty, které tuto povinnost mají, jsou uvedeny v článku 37 obecného nařízení a jedná se o:

- orgány veřejné moci či veřejný subjekt, jež provádí zpracování (s výjimkou soudů),
- jestliže hlavní činnost správce nebo zpracovatele vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů vzhledem k povaze, rozsahu a účelu zpracování,
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů (ÚOOÚ, 2013a).

Ale pověřence lze správcem či zpracovatelem jmenovat dobrovolně i přesto, že se na něho povinnost nevztahuje. Pokud se tak rozhodne, musí ale veškeré povinnosti a požadavky dle obecného nařízení plnit stejně jako ti, kteří tuto povinnost mají. Výhodou a důvodem, proč se tak rozhodnou může být i to, že tím získají nezávislou osobu, která bude na vše dohlížet a dává tím najevo, že ochranu osobních údajů bere velmi vážně a zodpovědně (Nulíček, 2018).

Hlavní úkoly pověřence

Pověřenec má za úkol dohlížet na soulad zpracování s obecný nařízením a radit správcům ohledně různých skutečností týkajících se ochrany osobních údajů. Považuje se také za kontaktní místo pro subjekty údajů a za dozorový úřad v záležitostech týkajících se zpracování těchto údajů. Pověřen i přesto, že má správcům či zpracovatelům radit v různých opatřeních, nenese za jejich zpracování žádnou odpovědnost.

I přesto, že se považuje za zcela nový pojem, není tomu tak. V některých legislativních předpisech v rámci některých evropských zemí již existoval, ale neexistovala nutnost jmenovat ho správcem.

Člověk, který tuto funkci vykonává, by měl mít v organizaci či společnosti specifické a v mnohých ohledech nezávislé postavení. Nesmí se dostat do střetu zájmů a v rámci jeho úkolů dle nařízení mu nesmějí být ukládány žádné pokyny. Dále je důležité, aby pověřenec fungoval jako samostatný orgán, který nemá povinnost řídit se obchodním či jiným zájmem správce či zpracovatele. Pokud ale přijde pověřenec na to, že správce či zpracovatel porušuje své povinnosti vyplývající z nařízení, musí tuto skutečnost ihned ohlásit (Nulíček, 2018).

Kvalifikace pověřence

Jak je uvedeno v obecném nařízení (článek 37), pověřenec by měl být jmenován na základě jeho odborných znalostí z práva a praxe v oblasti ochrany osobních údajů a také na základě jeho profesních kvalit.

Velmi důležitá je úroveň odbornosti a profesionální kvalita. Pověřencova odbornost by měla odpovídat citlivosti zpracovaných osobních údajů a komplexnosti a rizikovosti procesů zpracování. Čím složitější zpracování bude, tím je vyžádána vyšší odborná úroveň. Zároveň by měl mít pověřenec znalosti ohledně národních i evropských předpisů týkajících se ochrany osobních údajů. Nejdůležitější je sice znát znění obecného nařízení, musí ale ovládat i další předpisy upravující ochranu osobních údajů. Dále by měl znát informační a bezpečnostní opatření správce.

Není jednotný seznam požadavků a znalostí, které by měl pověřenec mít. Každá země má nároky jiné a je tedy na správci či zpracovateli, koho za svého pověřence zvolí. Pověřenec může své znalosti prokázat i tím, že absolvuje odborné školení, nebo získá certifikaci prokazující jeho odbornost. Důležitá jsou také pravidelná školení.

Z hlediska schopnosti vykonávat úkoly pověřence nemusí ovládat všechny oblasti jako IT, právo a lidské zdroje či bezpečnost, ale měl by mít alespoň základní přehled. Správce má povinnost zajistit pověřenci přístup k odborníkům, kteří se jednotlivým oblastem věnují (Nulíček, 2018).

Interní a externí pověřenec

Pověřencem se může stát jak interní zaměstnanec, tak externí osoba najatá společností.

Interního pověřence si volí spíše větší organizace nebo společnosti, pro které z hlediska nákladů na alokaci a vzdělávání nebude tak náročné zaměstnat zaměstnance. Jelikož musí být pověřenec obeznámen i s veškerými interními předpisy, produkty, interními a

informačními systémy, je mnohem jednodušší pověřit výkonem funkce někoho zevnitř společnosti. Další výhodu lze najít v komunikaci s pověřencem, jelikož pracuje ve stejné provozovně. Nevýhodu lze najít v prevenci proti střetu zájmů a případném zajištění ochrany proti ukončení pracovního poměru.

Externí pověřenec je vhodný spíše pro menší či střední podniky, pro které pověřenec znamená výrazné finanční zatížení. Další výhoda je předcházení střetu zájmů a také to, že úkoly pověřence lze takto vykonávat na velmi vysoké úrovni. Zvolit si externího pověřence mohou firmy i kvůli nedostatku interních zdrojů. Za nevýhodu se považuje to, že externí pověřenec nezná tak konkrétně danou firmu a její vnitřní procesy a interní předpisy (Nulíček, 2018).

3.6 Dozorový úřad

Vzhledem k tomu, jak je nařízení závazné a kolik z něho vyplývá povinností, je důležité zvolit i kontrolní orgán, který bude na dodržování pravidel vyplývajících z nařízení dohlížet.

V České republice vykonává tuto kontrolu dozorový orgán **Úřad pro ochranu osobních údajů**, jak tomu bylo již v době, kdy platil zákon o ochraně osobních údajů.

Nejvyšším dozorovým orgánem je ale **Evropský sbor pro ochranu osobních údajů (EPDB)**, jenž zajišťuje jednotnou aplikaci GDPR v rámci všech zemí EU. Tvoří ho vedoucí úřady za každý členský stát a také evropský inspektor ochrany údajů. Dříve tuto činnost v souladu se směrnicí č 29/46/EC prováděla tzv. **Pracovní skupina 29 (WP29)**, což byl nezávislý evropský poradní orgán na ochranu dat a soukromí (GDPR, n.d.).

Dle nařízení je pravděpodobné, že si každý stát svůj dozorový orgán včetně jeho jmenování a kvalifikace zřídí sám. V České republice toto upravuje adaptační zákon, který stanovuje, že vedení úřadu má na starosti předseda, který je jmenován prezidentem České republiky dle návrhu Senátu Parlamentu ČR.

Každý dozorový úřad vykonává svůj úkol a povinnosti dle platného nařízení. Nesmí tedy přijímat ani vyžadovat pokyny od nikoho jiného. Jednotlivé úkoly dozorového úřadu jsou uvedeny v článku 57 obecného nařízení. Mezi ty nejdůležitější patří (ÚOOÚ, 2013b):

- monitorování a vymáhání uplatňování nařízení,

- zabývání se stížnostmi, které mu podá subjekt údajů nebo subjekt, organizace či sdružení v souladu s nařízením a také provádění šetření předmětu stížnosti a v přiměřené lhůtě informování stěžovatele o vývoji a výsledku šetření,
- provádění šetření o uplatnění nařízení, mimo jiné na základě informací obdržených od jiného dozorového úřadu či jiného orgánu veřejné moci.

Každý dozorový úřad má tyto pravomoci:

1. vyšetřovací pravomoc,
2. nápravná pravomoc, a
3. povolovací a poradní pravomoc.

Vyšetřovací pravomoc spočívá například v ohlašování porušování nařízení správci či zpracovateli, získání přístupů ke všem osobním údajům od správce nebo zpracovatele, povinnosti správců nebo zpracovatelů poskytnout dozorovému úřadu veškeré informace za účelem vykonání jeho úkolu nebo při provádění přezkumu osvědčení.

Do **nápravné pravomoci** patří například udělení napomenutí za porušení nařízení správci nebo zpracovateli, uložení trvalého či dočasného omezení zpracování nebo nařízení opravy či výmazu osobních údajů a ohlašování takových opatření příjemcům, jimž byly údaje zpřístupněny.

V rámci **povolovací a poradní pravomoci** dozorový úřad poskytuje poradenství správci, vydává stanoviska buď z vlastního podnětu nebo na požádání, která jsou určená vnitrostátnímu parlamentu nebo jiným orgánům. Dále například schvaluje návrhy kodexů chování, povoluje smluvní položky, nebo schvaluje závazná podniková pravidla (Janečková, 2018).

Právní předpisy

Legislativní předpisy, kterými se musí dozorový úřad řídit a které se týkají jeho činnosti, jsou:

- nařízení (EU) 2016/679 (obecné nařízení o ochraně osobních údajů),
- zákon č. 110/2019 Sb., o zpracování osobních údajů
- zákon č. 255/2012 Sb., o kontrole (kontrolní řád),
- zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, a
- zákon č. 500/2004 Sb., správní řád.

Konkrétní věcná působnost Úřadu pro ochranu osobních údajů je vymezena hlavně v článku 57 obecného nařízení, který už byl uveden výše. Kromě obecného nařízení a zákona č. 110/2019 podléhá věcná působnost úřadu také těmto právním předpisům:

- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti),
- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích),
- zákon č. 40/1995 Sb., o regulaci reklamy a o změně doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, a
- zákon č. 634/1992 Sb., o ochraně spotřebitele (ÚOOÚ, 2013b).

Za zmínku také stojí pojem **DPIA neboli Data Protection Assesment** (v českém znění Posouzení vlivu na ochranu osobních údajů). Jedná se o nástroj, díky němuž může organizace identifikovat nejefektivnější způsob, kterým lze uvést pravidla na ochranu osobních údajů do souladu s GDPR. Souvisí to s vysoce efektivním softwarovým řízením operací spojených se zpracováním citlivých dat nebo dat založených na automatizovaném zpracování včetně profilování (GDPR, n.d.).

3.7 GDPR z hlediska spisové služby

Nakládání s osobními údaji a zpracovávání osobních údajů souvisí i s jejich dokumentací a uložením. Spisovou službu lze obecně chápat jako soubor činností, při nichž dochází k manipulaci s dokumenty, přičemž se bere v úvahu celý proces, tedy od jejich příjmu až po skartaci či uložení.

Právním předpisem, který upravuje spisovou službu je zákon č. 329/2012 Sb., o archivnictví a spisové službě (původně to byl zákon č. 499/2004 Sb.). V tomto zákoně je uvedeno, jaké subjekty mají povinnost spisové služby provádět a v jakém rozsahu. Mezi subjekty, které tuto povinnost mají, patří organizační složky státu, ozbrojené síly, bezpečnostní sbory, státní příspěvkové organizace, státní podniky, územní samosprávné celky, školy a školská zařízení, vysoké školy, zdravotní pojišťovny, veřejné výzkumné instituce, právnické osoby zřízené zákonem.

Pro správné fungování spisových služeb je potřeba mít dobře nastavené administrativní procesy i z důvodu nízké nákladovosti, hledání odpovědnosti za zpracování dokumentů nebo schopnosti rychlého vyhledávání konkrétních dokumentů.

Dokumentace je vedena buď fyzicky nebo elektronicky. Procesy spojené s přijímáním, ukládáním, skartací či odstraněním dat jsou v obou případech velmi podobné. Hlavní rozdíly jsou popsány níže (Navrátil, 2018).

Fyzická dokumentace

I přesto, že je v dnešní době velmi „moderní“ a zejména jednodušší veškerá data digitalizovat, je papírová verze dokumentů i tak v některých oblastech potřebná.

Přijetí a předávání dokumentů probíhá osobně nebo prostřednictvím poštovního doručení. Většinou se dokumenty přebírají na místě zvaném podatelna, nebo jsou předány pracovníkovi, který je pověřen k převzetí a může na požádání vydat potvrzení o převzetí. Ať se jedná o jakékoli dokumenty (otevření či zavřené v obálce), musí se s nimi zacházet tak, aby nedošlo k jejich ztrátě nebo poškození. Pokud neví, co v dané obálce je, musí s ní pracovat tak, jako kdyby obsahovala osobní údaje. Osoba, která s dokumentem manipuluje, musí dbát na to, aby byla zajištěna ochrana osobních údajů. Neměl by tedy dokumenty ukazovat někomu jinému, pokládat na nebezpečná místa (např. k otevřenému oknu) atd.

Někdy je oběh dokumentů velmi dlouhý, a to i z důvodu, že musí projít rukama několika pracovníků. Čím více lidí s dokumentem manipuluje, tím větší je riziko, že dojde k jeho poškození nebo ztrátě. A kvůli tomu je potřeba, aby byly oběh či vyřizování dokumentů ošetřeny z pohledu GDPR.

Odesílání dokumentů probíhá stejným způsobem jako jejich přijetí. Při odesílání je zejména důležité, aby nedošlo k záměně dokumentů, jelikož by se osobní údaje jedné osoby mohly dostat do rukou někoho cizího. Většinou mají na starosti odesílání pošty asistentky či sekretářky, které si ve fyzické evidenční knize poznamenají, co odesílají a komu. Nesmějí však uvádět přílišné podrobnosti, aby nedošlo k poskytnutí osobních údajů někomu, kdo bude do knihy moct nahlížet.

Každý dokument by měl být v rámci ukládání uložen v nějakém archivu či spisovně, kde by měl být označen takovým způsobem, aby bylo jasné, po jakou dobu je možné dokument uchovávat, tedy k jakému datu se musí skartovat. Spisovna musí samozřejmě také splňovat podmínky bezpečnosti a vybavenosti a měla by být přístupná jen odpovědným zaměstnancům.

Při konečné fázi následně dochází ke skartaci. K té dochází v době, kdy je již dokumentace nepotřebná a končí její doba úschovy. Skartaci mohou provádět subjekty samy nebo mohou využívat externí firmy, které tyto služby nabízejí. Správce by měl správně dohlížet na dokumentaci až do její úplné likvidace, tzn., měl by být přítomen i při nakládání dokumentů do automobilů, při vykonávání skartace apod. Je totiž za tyto úkony též zodpovědný a jeho účast je pak důkazem toho, že vynaložil veškeré úsilí na ochranu osobních údajů (Navrátil, 2018).

Elektronická dokumentace

V podstatě prochází elektronická dokumentace stejnými fázemi jako ta fyzická.

Hlavním rozdílem je, že pro manipulaci s dokumenty se používají jiné nástroje.

Přijetí, ale i odesílání dokumentace probíhá přes datové schránky, e-maily, operační systémy, elektronické formuláře apod. Pomocí e-mailů často putují dokumenty velmi krátkou dobu. Dokumenty přijímané ostatními kanály jsou ale zdlouhavější a jejich oběh je obdobný jako u fyzické dokumentace. Je nutné mít řádně zabezpečený systém elektronické komunikace s ohledem na všechny aktivity spojené s nakládáním s osobními údaji.

Jak při fyzické, tak i při elektronické dokumentaci existují rizika, která mohou bezpečnost osobních údajů ohrozit. Nemusí se vždy jednat o problém na straně technické (například kybernetické útoky na systém nebo výpadek elektřiny), ale může to být právě i lidský faktor, kdo danou chybu způsobí.

Subjekty využívají elektronický systém spisové služby a požadavky na něj určuje národní standard pro elektronické systémy spisové služby, který vydává ministerstvo vnitra.

Doba uložení elektronických dokumentů se vůbec neliší od doby úschovy těch fyzických. Přístup k el. dokumentům v elektronické spisovně mají opět jen odpovědní pracovníci.

Skartace je v tomto případě mnohem jednodušší a většinou funguje jen na bázi tlačítka „DELETE“.

V obou případech dokumentace je velmi důležité mít zavedená bezpečnostní opatření, aby nedocházelo k úniku, poškození nebo i ztrátě osobních údajů. Největší hrozbu představuje lidský faktor a je proto nutné, aby byla rizika spojená s ním pomocí daných nástrojů co nejvíce eliminována.

Doporučuje se také, aby subjekty vydávaly jistý spisový řád nebo interní předpis v souladu s nařízením, kde jsou jasně uváděny podrobnosti, jak nakládat s danými dokumenty (Navrátil, 2018).

3.8 Zabezpečení osobních údajů

Vzhledem k tomu, jak důležitá je v současné době ochrana osobních údajů, vyplývá z toho i důležitost dostatečného zabezpečení těchto údajů. Bezpečnostní povinnosti jsou tedy též podstatnou součástí obecného nařízení (článek 30).

V rámci ustanovení jsou po správcích a zpracovatelích vyžadována vhodná technická a organizační opatření z důvodu zajištění vysoké úrovně zabezpečení odpovídající bezpečnostním rizikům, která zpracování osobních údajů představuje. Tato opatření musejí brát v úvahu zejména povahu, rozsah a účely zpracování, ale také pravděpodobnost a závažnost rizika pro práva a svobody fyzických osob (Docksey, 2020).

Důležitost zabezpečení vyplývá ze zásady o integritě a důvěrnosti. Nelze ale jednotně určit, jaká opatření jsou pro daný subjekt vhodná. Záleží na okolnostech jejího vzniku, působení, pravidel, povaze služeb, náhledu na bezpečnost atd.

V souladu s nařízením ale musí každý subjekt navrhnout bezpečnostní opatření takovým způsobem, aby to odpovídalo povaze osobních údajů a minimalizovat tak případné škody. Dále je jeho povinností určit, kdo za nastavená bezpečnostní opatření odpovídá a také ověřit, zda má správné fyzické a technické zabezpečení včetně řádně vyškoleného personálu.

Každý subjekt by se měl zaměřit zejména na manažerská a organizační opatření, personální gramotnost, fyzickou bezpečnost, kybernetickou bezpečnost, počítačovou bezpečnost či bezpečnost e-mailu a faxu.

Příkladem **manažerského a organizačního opatření** je posouzení vlivu na ochranu osobních údajů. Dále se organizace zaměřují na budování firemní kultury v oblasti bezpečnosti a měly by v rámci celé organizace zvyšovat povědomí a odbornost týkající se ochrany osobních údajů.

Školení zaměstnanců je velmi důležité kvůli dostatečnému povědomí personálu o bezpečnosti osobních údajů. Školit by měli zaměstnance hned při jejich přijetí do zaměstnání a následně v pravidelných intervalech opakovaně. Taková školení se týkají

například povinností pro subjekt vyplývajících z obecného nařízení, odpovědnosti jednotlivých zaměstnanců, omezení týkajících se kybernetické bezpečnosti, nebezpečí plynoucích z falešných identit či pokusech o podvod. Na základě školení by tedy zaměstnanci měli být opatrní vůči lidem, kteří je mohou oklamat, používat silná hesla pro přihlášení, být nedůvěřiví k podezřelým e-mailům či ihned mazat nevyžádanou poštu.

Fyzická bezpečnost zahrnuje nejen opatření proti krádeži či poškození technických zařízení, ale také kvalitu dveří a zámků, alarmy, bezpečnostní osvětlení či kamerový systém. Také se sem zařazuje řízení přístupu do budovy a prostor (například přes zaměstnanecké karty), dohled nad pohybem návštěvníků či způsob nakládání s přenosnými zařízeními.

Počítačová bezpečnost zahrnuje především instalace antivirových kontrol do veškerých počítačových zařízení, ochranu počítače stažením nejnovějších oprav, zajištění přístupu zaměstnanců pouze k informacím týkajícím se jejich výkonu práce, provádění pravidelného zálohování dat a uložení těchto dat na jiná místa jako ochrana před případnou ztrátou zařízení.

Bezpečnost e-mailu se týká především správného zadání adresy příjemce, šifrováni či heslování zpráv a opatrnosti v posílání skupinových zpráv. Důležité je také dávat si pozor na to, když se odesílá e-mail ze zabezpečeného serveru příjemci, který server zabezpečený nemá.

Za velmi podstatnou a možná i nejdůležitější ochranu, kterou by měl mít každý subjekt řádně ošetřenou, je považována **kybernetická bezpečnost**. Ta se týká počítačů, tabletů, mobilů a dalších kybernetických zařízení. V dnešní době je čím dál častější digitalizace všeho, u čeho je to možné a zpracovávání dat a osobních údajů není výjimkou. Je podstatné, aby měla veškerá technická zařízení dostatečnou ochranu, a to pomocí hesel, PIN kódů či čteček. Některé stroje (jako např. tiskárna) mohou být chráněny před únikem dat i pomocí interní zaměstnanecké karty, jelikož mají často společnosti tato zařízení ve společných prostorách a mohlo by se stát, že si tištěné dokumenty může kdokoli přečíst a získat tak data, ke kterým by normálně neměli přístup. Dokumenty se tedy tisknou na daném zařízení až v době, kdy k nim tuto kartu zaměstnanec přiloží.

Kromě obecného nařízení se na bezpečnost vztahují mimo jiné i tyto předpisy (Nezmar, 2018):

- zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti,

- norma ISO 27001,
- norma ISO 27018.

PORUŠENÍ BEZPEČNOSTI

I přes veškerá nastavená interní opatření může dojít k narušení chráněných a uchovávaných dat. V takových případech musí každý subjekt postupovat dle standardního procesu při narušení bezpečnosti. K takovým incidentům může dojít například krádeží, úmyslným útokem na firemní systémy, neoprávněným použitím osobních údajů ze strany zaměstnance, náhodnou ztrátou či selháním daného nařízení. Pokud už k takovým incidentům dojde, musí subjekt řídit celý následný proces. Takový proces se skládá z těchto 4 základních prvků (Nezmar, 2018):

- zachycení a zotavení,
- posouzení rizik,
- oznámení porušení zabezpečení,
- hodnocení a reakce.

Porušení zahrnuje tyto tři kategorie:

1. porušení důvěrnosti,
2. porušení dostupnosti,
3. porušení integrity.

Pokud dojde k jednomu z těchto 3 porušení, měl by správce incident nejen vyřešit, ale musí ho také zařadit do správné kategorie rizik. Lze tedy incidenty zařadit jako porušení nepředstavující riziko, porušení představující riziko a porušení představující vysoké riziko (Janečková, 2018).

Rizika spojená s bezpečností ochrany osobních údajů budou více rozebrána v návrhové části této práce na konkrétních příkladech rizik u zvoleného subjektu.

OHLAŠOVÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

Každý správce či zpracovatel, který přijde na porušení bezpečnosti osobních údajů, musí tuto skutečnost ohlásit bez zbytečného odkladu, a to nejpozději do 72 hodin. Incidenty se ohlašují dozorovému úřadu, kterým je v České republice Úřad pro ochranu osobních údajů a pokud by se jednalo o závažnější riziko pro práva a svobody fyzických osob, musí se tato skutečnost ohlásit i subjektu údajů.

Obsahem daného ohlášení musí být minimálně:

a) popis povahy případu porušení včetně kategorie osobních údajů a počtu dotčených osob,
b) kontaktní údaje o pověřenci či jiném kontaktním místu,
c) popis pravděpodobných důsledků porušení,
d) popis opatření přijatých s cílem vyřešení daného incidentu.

Jestliže by z nějakého důvodu nemohl správce tyto údaje poskytnout najednou, může tak udělat postupně, ale bez zbytečného odkladu (Janečková, 2018).

3.9 Sankce a pokuty

Obecné podmínky pro ukládání správních pokut jsou vyhrazeny v článku 83. Obsahuje nejen podmínky uložení, ale také konkrétní sankce za jejich porušení.

Nové nařízení s sebou přineslo řadu změn a ty se dotýkají i nákladů subjektů. Vysoké pokuty a sankce tedy mají zajistit, že subjekty budou provádět ochranu osobních údajů právě v souladu s tímto nařízením a budou tak plnit všechny povinnosti z něho vyplývající. Dá se říci, že sankce působí i jako donucovací prostředek k plnění činností dle právní normy.

Podle toho, k jakému porušení povinností dojde, jsou nastaveny 2 horní hranice sankcí (Janečková, 2018):

a) maximální pokuta je ve výši 10 000 000 euro nebo 2 % z celosvětového obratu (vybrána je vyšší částka),
b) maximální pokuta ve výši 20 000 000 euro nebo 4 % z celosvětového obratu.

Následující tabulka uvádí přehled povinností, které musejí být porušeny v případě a) a v případě b).

Tabulka 2: Přehled porušení povinností vedoucích k udělení sankcí

10 000 000 euro nebo 2 % z celosvětového obratu za porušení:	**20 000 000 euro nebo 4 % z celosvětového obratu za porušení:**
Povinnosti při zabezpečení ochrany osobních údajů	Zásad a zákonnosti zpracování
Podmínek pro najmutí a spolupráci se zpracovatelem	Podmínek vyjádření souhlasu
Povinnosti vyhotovit záznamy o činnostech zpracování	Podmínek pro zpracování zvláštních kategorií osobních údajů
Povinnosti spolupráce s dozorovým úřadem	Práv subjektů údajů
Povinností při ohlašování případu porušení zabezpečení osobních údajů dozorovému úřadu	Podmínek pro předávání osobních údajů do třetí země
Povinnosti posoudit vliv na ochranu osobních údajů a absolvovat předchozí konzultace	Povinnosti vyplývající z právních předpisů členského státu, která se týká zvláštních situací, při nichž dochází ke zpracování, které nařízení umožňuje upravit na vnitrostátní úrovni
Povinností týkajících se jmenování a podmínek pověřence	Povinnosti splnit příkaz nebo dočasné či trvalé omezení zpracování nebo přerušení toku údajů dozorovaných úřadem
Povinnosti ustanovit zástupce pro správce nebo zpracovatele usídleného mimo Evropskou unii	Nesplnění příkazu dozorového úřadu podle č. 58
Povinnosti týkající se činnosti při získávání osvědčení	

Zdroj: Janečková, 2018

Výše uvedené pokuty jsou na české poměry příliš vysoké, ale je nutné brát v potaz, že nařízení se vztahuje na celou Evropu.

Podmínky ukládání pokut

Kromě toho, že obecné nařízení uvádí, jaké pokuty mohou správci dostat, jsou zde uvedené i mechanismy zajišťující spravedlivé ukládání pokut. Stejně tak umožňuje pokuty vůbec nedávat.

Při rozhodování o tom, zda pokutu uložit a v jaké výši, musí dozorový úřad zohlednit tyto okolnosti:

a) povahu, závažnost a délku trvání porušení s ohledem na povahu, rozsah a účelnost daného zpracování,
b) jakým způsobem k porušení došlo, tedy zda se jednalo o úmyslné jednání nebo nedbalost,
c) kroky podniknuté za účelem zmírnění škod způsobených subjektům údajů,
d) veškerá předchozí porušení,
e) do jaké míry jsou odpovědni správci či zpracovatelé vhledem k technickým a organizačním opatřením,
f) míru spolupráce s dozorovým úřadem s účelem nápravy,
g) kategorie osobních údajů, kterých se porušení dotýká,
h) způsob, jakým byl dozorový úřad informován o daném porušení,
i) dodržování schválených kodexů chování,
j) další přitěžující nebo polehčující okolnosti, jako například finanční prospěch či zamezení ztrát.

Pokuta vůbec nemusí být udělena, pokud se jedná pouze o formální porušení obecného nařízení s minimální společenskou škodlivostí. Může tak postačit pouze některé nápravné opatření nebo pouze informování správce o jeho povinnostech. Pak by od správce bylo očekáváno, že na základě informací uvede zpracování do souladu sám. Tento postup je možný i dle platného *zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení z nich.*

Zmiňovaný zákon upravuje tzv. materiálně-formální definici přestupku. V zákoně je také v § 30 uvedena promlčecí lhůta. Při porušení vyplývající z obecného nařízení je tato lhůta 3 roky. Je to u činů, u kterých se stanovuje horní hranice sankce alespoň 100 000 Kč.

Konkrétní přestupky projednává a zároveň za ně vybírá pokuty Úřad pro ochranu osobních údajů. V případě potřeby může pokuty vybírat i celní úřad (Žůrek, 2018).

4 Moneta Money Bank, a.s.

Pro potřebu analýzy dopadů GDPR byl zvolen subjekt Moneta Money Bank, a.s. (dále také jako „MMB“ nebo jen „Moneta“).

Tento subjekt byl zvolen z toho důvodu, že jako podnikatelský subjekt poskytující finanční služby zpracovává denně velké množství osobních údajů. Jedná se o údaje jak jejich zaměstnanců, tak o údaje o všech klientech či osobách třetích stran spolupracujících s Monetou.

Veškerá tato data musí banka správně chránit a mít zabezpečena, aby je mohla používat jen banka a pouze k účelům, ke kterým byla data poskytnuta. Moneta Money Bank je proto vhodným subjektem pro zpracování této práce.

4.1 Základní charakteristika subjektu

MONETA Money Bank, a.s. je akciová společnost, která vznikla a byla zapsána do obchodního rejstříku dne 9. června 1998 s hlavním sídlem na adrese Vyskočilova 1442/1b, Praha Michle 140 000.

Skupina Moneta je koncern, jenž se skládá z mateřské řídící společnosti a jejich dceřiných společností. Mateřská společnost je Moneta Money Bank, a.s. a dceřiné společnosti jsou Moneta Auto, s.r.o., Moneta Leasing, s.r.o, Moneta Stavební spořitelna a.s. a Wüstenrot hypoteční banka a.s.

Obrázek 1: Logo společnosti

Zdroj: moneta.cz, 2022a

Předmětem podnikání této společnosti je:

- poskytování úvěrů,
- finanční makléřství,
- platební styk a zúčtování,
- přijímání vkladů veřejnosti,
- investování do cenných papírů na vlastní účet,
- finanční pronájem (leasing),
- poskytování záruk,
- otevírání akreditivů,
- obstarávání inkasa,
- poskytování bankovních informací,
- výkon funkce depozitáře,
- směnárenská činnost,
- pronájem bezpečnostních schránek,
- vydávání a správa platebních prostředků,
- obchodování na vlastní účet nebo na účet klienta s devizovými hodnotami a se zlatem v rozsahu:
    - obchodování na vlastní účet s devizovými hodnotami a se zlatem,
    - obchodování na účet klienta s peněžními prostředky v cizí měně a se zlatem,
- činnosti, které přímo souvisejí s činnostmi uvedenými v bankovní licenci gecb,
- poskytování investičních služeb podle zvláštního právního předpisu zahrnující investiční služby.

Společnost se skládá ze statutárního orgánu a dozorčí rady. Statutární orgán má celkem 5 osob: předsedu představenstva, místopředsedu představenstva a 3 členy představenstva. Dozorčí rada se skládá z 9 osob a taktéž má jednoho předsedu a jednoho místopředsedu, zbylých 7 osob jsou členové dozorčí rady (rejstrik-firem.kurzy.cz, 2022).

MONETA Money Bank, a.s. je díky svým úspěchům a počtu klientů čtvrtou největší bankou v České republice. Mají celkem 160 poboček a více než 550 bankomatů. Díky modernizaci také samozřejmě nabízí internetové a mobilní bankovnictví včetně aplikace Smart Banka, díky čemuž mají klienti kdykoli a odkudkoli snazší obsluhu i vyřizování záležitostí týkajících se finančních potřeb (moneta.cz, 2022b).

4.2 Základní legislativa

Na každou banku, nejen na MMB, se vztahuje velké množství zákonů, právních předpisů, vyhlášek a směrnic, kterými se musí společnost řídit. Za nejpodstatnější by se dal považovat zákon č. 21/1992 Sb., o bankách.

Moneta se ale musí řídit zákony upravujících mnoho oblastí. Jedná se například o oběh bankovek a mincí, dluhopisy, směnárenské činnosti, ochranu spotřebitele, platební styk, spotřebitelský úvěr, podnikání na kapitálovém trhu, distribuci pojištění, ochranu fyzických osob, obchodních korporací, účetnictví, kybernetickou bezpečnost a mnoho dalších.

Z hlediska GDPR se musí Moneta Money Bank a.s. řídit dle zákona č. 110/2019 Sb., o zpracování osobních údajů a také nařízením 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).

Za zmínku stojí též *Rámcový výklad některých ustanovení GDPR 2019 v bankovním sektoru*. Jedná se dokument, jehož cílem je stanovení výkladového rámce bankovního sektoru využívaný při aplikaci některých ustanovení GDRP tak, aby byl zajištěn soulad s právní úpravou z oblasti finančních služeb. Také obsahuje výklad jednotlivých ustanovení GDPR a poukazuje na jejich specifika. Tento dokument byl vypracován kvůli komplexní regulaci finančního trhu se zaměřením na bankovní sektor vzhledem k jeho závislosti na zpracování osobních údajů. Veškeré části vycházejí z diskusí s Úřadem pro ochranu osobních údajů a Českou národní bankou. (ČBA, 2019)

Žádná společnost není povinna se tímto výkladem řídit, jedná se spíše o doporučené postupy a každá banka si může zvolit vlastní způsob, jak bude GDPR interpretováno a jakým způsobem bude zajištěna ochrana osobních údajů od subjektů.

Tento rámcový výklad je zde zmiňován zejména proto, že MMB se jím řídí a je na seznamu bank, které k tomuto dokumentu přistoupily.

4.3 Oblast vztahů

Nadřízenou institucí společnosti Moneta Money Bank je Česká národní banka (dále jen jako ČNB).

Poskytovat osobní údaje může banka pouze se souhlasem subjektu údajů (klienta). Zákon č. 21/1992 Sb., o bankách mimo jiné definuje právě záležitosti týkající se klienta, jež jsou předmětem bankovního tajemství (§ 38). ČNB je ale jedním z útvarů, kterým může Moneta osobní údaje poskytnout, aniž by bankovní tajemství porušila. Dále se mohou údaje poskytovat orgánům bankovního dohledu a obdobným orgánům jiných států.

Dle zákona o bankách (§ 38) poskytuje banka údaje těmto orgánům a institucím:

- orgánům činným v trestním řízení,
- správcům daně,
- finančnímu arbitrovi,
- orgánům sociálního zabezpečení,
- zdravotním pojišťovnám,
- soudům a soudním exekutorům,
- úřadům práce,
- zpravodajským službám,
- Úřadu pro dohled nad hospodařením politických stran a politických hnutí,
- Národnímu bezpečnostnímu úřadu,
- Policii ČR,
- Generální inspekci bezpečnostních sborů,
- Ministerstvu financí.

MMB samozřejmě také spolupracuje s mnoha dodavateli a třetími osobami. Všechny tyto osoby mají určitým způsobem přístup i k osobním údajům různých subjektů. V těchto případech jsou veškeré oblasti včetně GDPR a ochrany osobních údajů, jejich zpracování a možnost nakládání s nimi upraveny ve smlouvách, které mezi sebou uzavřeli (interní zdroje MMB, 2022).

4.4 Interní systémy

V Monetě Money Bank existuje několik systémů či databází, se kterými jednotliví zaměstnanci pracují. Společnost využívá přes 200 systémů, z nichž většina je mezinárodních a jen malá část interních. Níže v textu budou uvedeny jen některé z nich.

Z těch mezinárodních lze zmínit například SAP, AMAZON (respektive AVS), Microsoft či systém Moody's.

SAP je program, který využívá mnoho společností, a to zejména pro mzdové a finanční účetnictví. Všechna data jsou umístěna na jedné platformě a díky tomu může firma zmapovat každý proces (sap.com, 2022).

Moody's systém poskytuje software pro řízení rizik finančních institucí. Umožňuje i přístup na dluhové trhy a investoři mohou i díky tomu porovnávat úvěrová či jiná rizika, například kybernetická rizika (moodys.io, 2022).

Náhled na určitá data má každé oddělení v rámci databáze, ale přístupy už se liší. Ve firmě nemá většinou každé oddělení své specifické systémy – existují, ale je jich velmi málo (např. zaměstnanecké systémy). Systémy v Monetě jsou spíše sdílené a propojené. To znamená, že základní údaje vidí všichni napříč celou firmou, ale mají trochu jiný náhled.

To, že má každé oddělení jiné přístupy, je odvozeno od toho, jakou funkci či roli ve firmě má. Každá role má totiž jasně definované, jaké údaje může vidět a jak je zpracovávat. Závisí to zejména na náplni práce. Důvodem je potřeba zajistit, aby nedocházelo k tomu, že se k jakýmkoli datům může dostat každý, i když je pro svoji práci nepotřebuje.

Příkladem je **UFO BANKA**, kde každý může vidět v podstatě jen náhled dat, která jsou stažena z databáze. Bankéř ale do větších detailů k údajům přístup nemá.

Existuje také **AML systém**, který provádí tzv. transakční monitoring. Pomocí toho kontrolují, zda se například neprovádí transakce do zemí či organizací, kde existuje možnost ohrožení z hlediska například teroristických útoků apod.

Dále mají **UFO banku nebo UFO OPS**, což jsou systémy pro pobočkovou síť, kam sice nemá přístup každý, ale pokud by ho potřeboval, může si o něj zažádat. Například, pokud by pověřenec z oddělení Compliance, který do tohoto systému běžně přístup nemá, potřeboval prověřit případnou stížnost v rámci GDPR či problém, může si zažádat o přístup k těmto údajům, aby mohl vše řádně prověřit (interní zdroje MMB, 2022).

Je také podstatné zmínit, že kvůli GDPR nebylo nutné pořizovat systémy nové, ale došlo pouze k úpravě či doplnění těch stávajících.

5 Analýza subjektu

Tato kapitola poukazuje na situaci, jakým způsobem byla data chráněna před zavedením GDPR, jakými právními předpisy se banka řídila a také, kdo měl na starosti veškeré aktivity spojené se zpracováním osobních údajů a jejich ochranu.

Dále je popsán proces implementace, tedy jakým způsobem se banka na zavedení GDPR připravovala, kdo byl za aktivity spojené s implementací zodpovědný, jak dlouho implementace trvala, jaké konkrétní činnosti zahrnovala a co bylo jejím výsledkem.

5.1 Situace před zavedením GDPR

Je zřejmé, že Moneta Money Bank, jakožto bankovní instituce, využívá denně obrovské množství osobních údajů. Pracuje s údaji nejen svých klientů, ale také zaměstnanců, partnerů či osob třetích stran. Ochrana těchto údajů je proto nezbytnou součástí veškerých aktivit a činností, které s tím souvisejí.

Situace před zavedením nového nařízení ohledně GDPR nebyla příliš rozdílná oproti současnému stavu. Jelikož existovaly právní předpisy týkající se ochrany osobních údajů již před zavedením GDPR, banka musela už před tímto nařízením chránit tyto údaje dle dříve platného zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

MMB tedy dbala na ochranu veškerých osobních údajů už dlouho před rokem 2018, kdy vešlo v platnost obecné nařízení. Základní povinnosti byly stanoveny už před GDPR, nicméně ne v takové míře a do detailnějších podrobností jako nyní. I přesto, že už ochrana údajů podléhala výše zmiňovanému zákonu, nebyla tomu věnována taková pozornost, jako nyní. Jedním z důvodů může být také to, že se výrazně navyšovaly sankce a pokuty za nedodržení pravidel nastavených dle nařízení.

Už dříve existoval interní předpis, který obsahoval hlavní povinnosti a pravomoci, různé pojmy atd., které určovaly zaměstnancům, jak s osobními údaji nakládat.

Kontrolu nad všemi událostmi týkajícími se ochrany dat mělo na starosti oddělení Compliance (interní zdroje MMB, 2022).

Pro firmy ale i tak představovala náročnost z hlediska implementace GDPR, které je věnována následující kapitola.

5.2 Implementace GDPR ve firmě

V rámci implementace musela společnost udělat několik interních úprav a změn. Z počátku byl sestaven postup, jak v Monetě GDPR implementovat. Příprava na toto zavedení byla zdlouhavá a náročná, i přesto, že už se banka ochranou osobních údajů zabývala předtím. Díky dlouhodobé přípravě ale nebyl pro Monetu květen 2018 tak zásadní, jelikož byli na vše připraveni.

GDPR ale přineslo do firmy změny a mělo samozřejmě jistý dopad, kterému se věnuje samostatná kapitola 4.

Nejprve byl vytvořen **projekt**, který byl veden vybraným projektovým týmem, který byl pod vedením projektového manažera. Ten dohlížel zejména na to, aby se veškerá příprava a změny v rámci GDPR zrealizovaly včas. Tento projektový tým byl tedy zodpovědný za analýzu, která byla prováděna a na základě které došlo k plnohodnotnému zajištění plnění nařízení GDPR.

V rámci GDPR vznikla i nová funkce – **pověřenec**. Pověřencem je osoba, která byla v době implementace součástí projektového týmu. Podrobněji je tomuto tématu věnována samostatná kapitola 5.2.

Zmiňovaná analýza je tzv. **GAP analýza**, během které společnost zanalyzovala současné předpisy v rámci ochrany osobních údajů a zhodnotila, kde je potřeba udělat úpravy. Hlavním smyslem analýzy bylo tedy zkoumání současných pravidel nastavených pro ochranu osobních údajů. Změny se dotýkaly všech procesů jako například v IT oddělení, dokumentace a veškerých interních procesů.

Výsledný předpis tedy uvádí, o jaké osobní údaje se jedná, na jak dlouho a jakým způsobem se uchovávají a také způsob jejich zpracování. Klasifikuje údaje podle toho, o jaké informace se jedná a poté jsou rozděleny na dané úrovně (veřejné, interní, důvěrné, tajné). Ukládat data lze buď elektronicky nebo v tištěné podobě (více v kapitole 6.5). Zpracovávat data lze v případě, že byl subjektem udělen souhlas ohledně nakládání s jeho osobními daty, dále podle legislativních nařízení nebo pokud je tak uvedeno ve smlouvě.

Dále se předpis věnuje oblasti bezpečnosti osobních údajů, což souvisí jak s formou ukládání dat, tak s tím, jak je možné s daty pracovat, jak je lze využívat a kdo má k jakým datům přístup a se způsobem jeho schvalování. Důležitou součástí předpisu je také určení odpovědnosti.

Výsledkem analýzy bylo stanovení nových pravidel interním předpisem tak, aby korespondovala s novým nařízením GDPR.

Poté došlo k **realizaci**, kdy bylo kromě vytvoření nového předpisu, také potřeba stanovit opatření, aby nedocházelo k porušování těchto pravidel. A dále bylo nutné určit, jak postupovat při odhalení určitých rizik ohrožujících bezpečnost osobních údajů.

Poslední činností je pravidelná **revize**, na základě které lze odhalit případné nedostatky (interní zdroje MMB, 2022).

6 Dopady GDPR na vybraný ekonomický subjekt

Pátá kapitola poukazuje na důležité dopady GDPR na Monetu Money Bank. Za hlavní cíl této kapitoly se považuje zodpovězení otázky týkající se změn, které musely být provedeny. Patří sem zejména oblasti zaměřující se na dopady implementace z hlediska času a nákladů, bezpečnosti a ochrany osobních údajů a také důležitých interních změn.

Z velké části jsou podkapitoly zpracovány dle interních zdrojů Monety (interní zdroje MMB, 2022). Informace jsou získány na základě pravidelných konzultací a rozhovorů se zaměstnankyní Monety Money Bank.

6.1 Ochrana osobních údajů po GDPR

Během implementace docházelo k různým komplikacím. Některé záležitosti byly složitější nebo i dražší (např. při přeprogramování systémů docházelo velmi často ke komplikacím). Ale i v současné době se stává, že přijde Moneta v rámci kontrol na to, že v některých oblastech existují nedostatky, které je potřeba odstranit.

Ve velkých organizacích či firmách jako je Moneta může docházet k tomu, že se něco může přehlédnout a až po skončení daného projektu najdou nesrovnalosti. I po skončení projektu implementace GDPR se nyní setkávají s dokumenty, kde se odkazují na starý zákon a nejsou stále pozměněny podle nového nařízení. Většinou se ale jedná o velmi malé úpravy a dá se říci, že jsou „nepodstatné“. Ty hlavní či nejdůležitější stanovy byly upraveny okamžitě a jsou v souladu s obecným nařízením.

Nový interní předpis

Jak již bylo zmíněno, Moneta Money Bank měla interní předpis už dávno před rokem 2018, kdy vešlo v platnost obecné nařízení. Tento předpis ale musel být upraven tak, aby byl v souladu s uvedeným nařízením.

Tento dokument se jmenuje *Zpracování osobních údajů* a je platný od stejného data, kdy nabylo účinnosti obecné nařízení, tedy 28. května 2018. Stanovuje základní povinnosti v rámci celého koncernu, kde jsou uvedena pravidla, jak s osobními údaji nakládat. Jsou tam také uvedeny požadavky na smlouvy s dodavateli, kteří se dostávají k osobním údajům či interní povinnosti týkající se vedení záznamů o činnostech zpracování včetně odpovědnosti jednotlivých osob za tato zpracování.

Předpis je pro všechny zaměstnance závazný a veškeré povinnosti plynoucí z něho musí každý zaměstnanec řádně plnit. Obsahuje zejména tyto položky:

- pojmy a zkratky včetně jejich vysvětlení,
- veškeré pravomoci a odpovědnosti,
- povinnosti týkající se záznamů o činnostech zpracování osobních údajů,
- nakládání s osobními údaji dle účelu jejich zpracování,
- stanovení doby, po jakou budou údaje uchovány (doba se odvíjí od účelu zpracování),
- zpracovatelé,
- pověřenec pro ochranu osobních údajů,
- kontrola dodržování osobních údajů,
- související dokumentace,
- závěrečná ustanovení.

Tento interní předpis v podstatě shrnuje základní údaje a povinnosti vyplývající z obecného nařízení, které jsou pro banku a její zaměstnance velmi důležité a závazné. V případě potřeby bývá tento dokument aktualizován tak, aby bylo vše v souladu s platnou legislativou.

Kromě tohoto interního dokumentu má MMB i mnoho dalších, které se týkají klientů, dodavatelů či uchazečů o zaměstnání. Ty jsou na rozdíl od výše zmiňovaného interního dokumentu veřejně dostupné na jejich webových stránkách.

Situace nyní

Banka musí neustále sledovat případné změny v legislativách a předpisech, a podle toho také upravovat či nahrazovat stávající dokumenty a systémy tak, aby byly vždy v souladu s nejnovějším a platným nařízením. Banka se samozřejmě snaží provádět veškeré důležité změny vždy s dostatečným předstihem, aby byl zajištěn maximální soulad mezi platnými nařízeními a chodem společnosti. V některých oblastech je to ale složitější, a tak se i v současné době může stát, že dojde k odhalení „mezery“ v nějaké oblasti, kterou musí společnost doplnit. Většinou se ale jedná o nepatrné změny.

Moneta však musí samozřejmě reagovat na všechny změny, které se v okolí dějí. Jako řadu společností a různých institucí, i Monetu ovlivnila pandemie Covid, a to právě i z hlediska GDPR. V rámci mimořádných opatření byla totiž mimo jiné bankám stanovena

povinnost poskytnout údaje o místě a době použití elektronických platebních prostředků klientů bank. Díky tomu byla bankami poskytována data a docházelo k lepšímu mapování pohybu osob napadaných Covidem 19. A právě i kvůli tomuto mimořádnému opatření musela banka vydat nový dokument, který se na toto opatření odkazoval a obsahoval informace o tom, jaké údaje mohou být poskytnuty a proč, kdo je správcem poskytovaných údajů, jaká jsou bezpečnostní opatření a práva subjektů poskytujících údaje.

6.2 Funkce pověřence

Každá velká firma či instituce pracuje s osobními údaji, které smějí interně využívat pouze za konkrétními účely.

GDPR pro některé správce nebo zpracovatele stanovuje, že musí zřídit nezávislou kontrolní funkci DPO (angl. Data Protection Officer) neboli pověřence pro ochranu osobních údajů (GDPR, n.d.).

Zavedení nového nařízení přineslo do chodu firmy několik změn. Jednou z nich je také vznik nové pozice – pověřenec pro ochranu osobních údajů. Již před zavedením GDPR ale v Monetě docházelo ke kontrolám zpracování osobních údajů a veškerých aktivit s tím spojených, a také k zajišťování maximální bezpečnosti těchto údajů. Než došlo ke jmenování pověřence, staralo se o tyto záležitosti oddělení Compliance. V první fázi implementace bylo tedy potřeba si vhodně zvolit odpovědnou osobu, která bude moci tuto funkci vykonávat. Každá společnost si pověřence vybírá buď z vlastních interních zdrojů, nebo využije zdroj externí. Externím člověkem bývá většinou osoba z právního prostředí či někdo, kdo má s touto oblastí zkušenosti. Pověřencem každopádně musí být vždy někdo, kdo dobře zná problematiku GDPR a má už nějaké zkušenosti z hlediska zpracování osobních údajů.

V Monetě tuto pozici prvotně obsadil vedoucí oddělení Compliance a v současnosti je touto osobou Michaela Skácelová, která je k dispozici jak zaměstnancům, tak klientům. Díky tomu, že prvotně tuto funkci obsadila osoba, která měla mnohaleté zkušenosti s osobními údaji, jelikož pracoval na Úřadě pro ochranu osobních údajů, nebylo potřeba zajišťovat speciální školení ani přípravu na tuto pozici. Paní Skácelová pracovala v Monetě již předtím, a jelikož pracovala na oddělení Compliance, měla též dostatečné zkušenosti k tomu, aby mohla tuto funkci řádně vykonávat.

Podstata této funkce vyplývá z GDPR a spočívá zejména v tom, být nezávislým poradním orgánem. Hlavní činnost tedy spočívá v konzultacích jak s klienty, tak se zaměstnanci společnosti. Nevstupuje přímo do nastavování procesů a služeb, které používají, ale spíše radí, co je správně či co je třeba změnit a upravit. Jedná se mimo jiné o kontaktní místo pro subjekty osobních údajů a v rámci funkce pověřenci přísluší také monitorování společností koncernu MONETA s legislativou ochrany osobních údajů. Monitorování neboli kontrolní činnost, spočívá v tom, že na konci každého roku se definují rizikové oblasti v rámci ochrany osobních údajů a následně na to navážou konkrétní kontroly. Tyto kontroly nespadají pod audit, ale vážou se k procesům a službám, kterých se dané riziko týkalo. Určí se například čtvrtletí daného období a provádí se revize procesů. Výstupem jsou nálezy, které se regulují dle jejich závažnosti a zavádí se ochrana či opatření, aby se těmto rizikům do budoucna předcházelo.

6.3 Administrativní, finanční a časová náročnost

Celková implementace trvala přibližně dva roky. Prvotní příprava na implementaci GDPR do firmy začala již dva roky před samotným uplatněním nařízení, tedy v roce 2016. Banka si uvědomovala, že nové nařízení s sebou přinese mnoho změn a chtěla tak mít dostatek času, aby bylo vše nastaveno správně a dostatečně včas.

Zaškolení a příprava na funkci pověřence nepředstavovala pro Monetu příliš velkou náročnost, neboť prvotně tuto funkci obsadila osoba, která několik let před uvedením do této pozice pracovala na Úřadu pro ochranu osobních údajů. Až následně tuto funkci převzala paní Skácelová, která je na této pozici doteď a dříve pracovala pro oddělení Compliance, kde měla na starosti i záležitosti týkající se GDPR a měla tak potřebné zkušenosti pro výkon funkce pověřence. I proto nebylo potřeba žádných speciálních školení a příprav pro obě tyto osoby.

Jak již bylo zmiňováno, prvotní fáze začala již v roce 2016 a začala GAP analýzou. Úvodní GAP analýza trvala zhruba 2 měsíce, ale i poté postupně docházelo k odhalení nedostatků v mnoha procesech a oblastech, které bylo ještě potřeba upravit.

Implementaci měl na starosti projektový tým, který se skládal z jednoho hlavního manažera a několika hlavních členů. Nicméně tento proces šel napříč celou společností a dotkl se v konečném důsledku mnoha osob.

Jedenkrát za týden se projektový tým sešel, aby se provedl update či shrnutí toho, v jakých oblastech a jakým způsobem se v rámci implementace Moneta posunula a kde je potřeba ještě provést změny. Tyto aktivity spojené s implementací koordinoval právě projektový manažer a byl také za tyto aktivity odpovědný.

Za hlavní změny by se daly považovat:

- úprava interních dokumentů,
- úprava interních i externích systémů,
- zaškolení zaměstnanců do nových povinností,
- úpravy či dodatky u stávajících smluv (zaměstnaneckých, klientských i dodavatelských.

Z hlediska finanční náročnosti, vynaložila firma náklady zejména na interní i externí zaměstnance a také na úpravy svých systémů. Na některé změny stačilo využít interních zaměstnanců, na některé využila Moneta externí zdroje. Externími zdroji jsou například analytici provádějící analýzu, IT specialisté a také již zmiňovaný projektový manažer.

Ke speciálnímu školení prováděnému od externích zdrojů nedošlo. Moneta má každoročně daný rozpočet, který na všechna školení využívá a musela tak pouze vyhradit určitou část i na proškolení v rámci GDPR. Došlo a stále tedy dochází pouze k internímu proškolení zaměstnanců.

6.4 Uchovávání a bezpečnost dat

Vzhledem k tomu, kolik Moneta denně zpracovává osobních údajů, je velmi důležité, aby měla zajištěnou dostatečnou bezpečnost těchto dat. Samozřejmě i před zavedením GDPR bylo nutné klást velký důraz na kvalitní a dostatečné zabezpečení, nyní ale musí být zaměstnanci z hlediska této oblasti mnohem více opatrní, zaškolení a musejí velmi dbát na dodržování veškerých pravidel. Pokud by došlo k porušení či nedodržení těchto pravidel, hrozí nejen zaměstnancům, ale také celé společnosti vysoká sankce či ztráta dobrého jména firmy.

Za porušení bezpečnostních opatření se považují taková porušení, která vedou k náhodnému či protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí osobních údajů. Veškerá pochybení, na která správce přijde, by se měla hlásit dozorovému úřadu, resp. subjektu údajů. Toto se však hlásí zejména v případě vysokého rizika z hlediska práva a svobody fyzických osob (ÚOOÚ, 2019).

I přesto, že v současné době dochází čím dál častěji k digitalizaci a velkému omezení tištěné dokumentace, je nutné mít nastavená pravidla jak pro tištěnou, tak i pro elektronickou dokumentaci. V Monetě existují stále oblasti, kde se tištěná dokumentace vede i nyní.

TIŠTĚNÁ (PAPÍROVÁ) DOKUMENTACE

Již před zavedením GDPR dbala Moneta na vysokou úroveň zabezpečení veškeré dokumentace. Nicméně v momentě, kdy vešlo v platnost nové nařízení, musela banka nastavit nová pravidla a opatření tak, aby docházelo k poctivějšímu dodržování veškerých pravidel. Tato pravidla jsou součástí interního dokumentu Zásady zpracování osobních údajů. Firma však musí dbát na to, aby se veškerá opatření poctivě dodržovala a nedocházelo k odcizení či zneužití dat.

Mezi ta nejdůležitější opatření, která chrání bezpečnost papírové dokumentace, patří:

- uzavírání a uzamykání všech prostor, kde se papírová dokumentace dočasně ukládá,
- zákaz vynášení veškerých dokumentů obsahujících osobní údaje mimo pracoviště,
- mlčenlivost v souvislosti s osobními údaji jak ze strany zaměstnanců, tak i dodavatelů,
- dodržování povinností ohledně průběžné likvidace veškerých kopií dokumentů,
- dodržování povinnosti ohledně informování o neoprávněném zpracování osobních údajů či jakémukoli podezření týkajícímu se zneužití či ztráty osobních údajů.

K pohybu veškeré papírové dokumentace dochází buď osobním předáním, nebo zasíláním dokumentů poštou. Pokud ale k takovým pohybům dojde, musí být vše řádně zaevidováno.

Pro úschovu této dokumentace využívá Moneta externí archiv. Po dobu maximálně jednoho roku jsou dokumenty uchovávány na centrále banky, kde ale z důvodu vysokého počtu dokumentace nemohou být uchovány tak dlouho, jak je pro účely zpracování osobních údajů potřeba. Moneta proto využívá externí archiv, který je umístěn na území České republiky, aby k němu měla banka v případě potřeby snadnější přístup. Veškerá opatření včetně správné manipulace s dokumenty, jejich způsobu a délky uchování nebo

likvidace jsou součástí smlouvy mezi bankou a dodavatelem poskytujícím daný archiv. V této smlouvě jsou také mimo jiné i opatření pro mimořádné události, jako jsou například záplavy.

Pro likvidaci neboli skartaci papírové dokumentace využívá společnost též externích zdrojů, tedy dodavatelů. Na každé pobočce jsou umístěny kontejnery, kam se dávají veškeré kopie dokumentů určené k likvidaci. Dodavatel tedy zajišťuje hlavně odvoz a fyzickou likvidaci veškerých dokumentů, které jsou v daných kontejnerech. Všechny tyto kontejnery jsou opatřeny zámkem a klíč k němu má buď likvidační firma nebo vedení oddělení. Je ale velmi důležité, aby k dokumentům obsahujícím citlivé údaje o subjektech, neměl přístup kdokoli, kdo danou pobočku navštíví. V tomto ohledu má tedy banka zabezpečení dostatečné.

I přesto, že se v dnešní době většina dokumentů ukládá spíše elektronicky, existují v bance oblasti, kde je i nyní papírová dokumentace v plné míře, a to například u dokumentace týkající se zaměstnaneckých smluv.

Je také potřeba si uvědomit, že žádné z vedoucích oddělení nemá šanci kontrolovat každého zaměstnance, zda tato opatření opravdu dodržuje. Vše je tedy zcela závislé na zodpovědnosti každého takového zaměstnance.

V rámci práce s fyzickými dokumenty musí každý zaměstnanec dodržovat *zásadu čistého stolu.* Ta má za cíl snižovat riziko krádeže nebo úniku informací zevnitř společnosti. Tato zásada říká, že zaměstnanci nesmějí nechávat volně klasifikované dokumenty na stole, v případě vzdálení se od počítače musí uzamknout obrazovku a na konci pracovního dne nenechávat na stole důležité dokumenty. Dále musí mít zaměstnanci pečlivě zabezpečené veškeré složky a pracovní zařízení a důvěrné a tajné dokumenty nesmějí pouze vyhazovat, ale musí je skartovat (interní dokument MMB, 2022).

ELEKTRONICKÁ DOKUMENTACE

Stejně tak jako bezpečnost papírové dokumentace, je velmi důležitá i bezpečnost elektronické dokumentace. Moneta se tak musí řídit i několika legislativními předpisy, které tuto bezpečnosti právně upravují. Za ty nejdůležitější lze považovat:

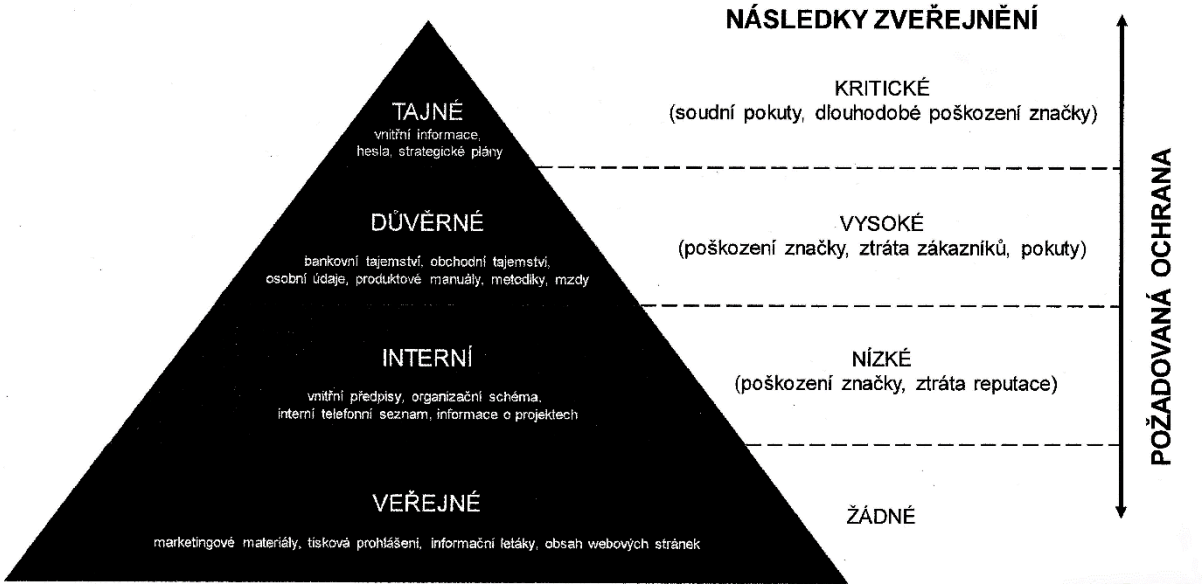
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti,

- směrnice Evropského parlamentu a Rady (EU) 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systému v Unii.

Zákon č. 181/2014 Sb. transponuje výše uvedenou směrnici. Hlavní cíle tohoto zákona jsou stanovení základní úrovně bezpečnostních opatření, zlepšení detekce a zavedení hlášení kybernetických bezpečnostních incidentů a zavedení systému opatření k reakci na tyto incidenty. Zákon byl v roce 2017 novelizován a jsou v něm nyní definované nové pojmy a povinnosti, které musí subjekt plnit (NÚKIB, 2022a)

Pro elektronickou dokumentaci existuje ve společnosti i tzv. podpisová základna, což je dokument, který obsahuje zejména informace o klasifikaci interních dat. Týká se to veškerých dat včetně osobních údajů. Dle tohoto dokumentu lze klasifikovat informace do 4 úrovní dle úrovně jejich důvěrnosti. Tuto klasifikaci zobrazuje následující obrázek:

Obrázek 2: Úroveň důvěrnosti informací společnosti MMB



Zdroj: Interní dokument MMB, 2022

Na výše uvedeném obrázku lze vidět kromě úrovní důvěrnosti informací také následky jejich zveřejnění. U každé úrovně jsou také uvedeny příklady, o jaké informace se může jednat. Za veřejné informace se považují taková data, která nejsou pro společnost Monetu citlivá a mohou být zveřejněna zaměstnancům i veřejnosti. Jejich zveřejnění tedy nemá žádné nepříznivé důsledky. Interní informace se považují za citlivé pouze mimo společnost Moneta a jejich zveřejnění může mít jen omezené nepříznivé důsledky. Důvěrné informace jsou citlivé i v rámci společnosti a mají k nim přístup pouze ti

zaměstnanci, kteří je potřebují k vykonávání své práce. Zveřejnění těchto údajů může mít nepříznivé důsledky. Poslední úrovní jsou informace označované jako tajné. Ty se považují za mimořádně citlivé a jsou přístupné pouze jmenovitě určeným osobám. Jejich zveřejnění má velmi nepříznivé důsledky (interní dokument MMB, 2022).

Opatření, kterými se musí v Monetě řídit v rámci elektronické dokumentace, jsou zejména:

- mlčenlivost v souvislosti na osobními údaji,
- uzamykání a odhlašování se z veškerých zařízení v případě opuštění prostoru, kde se nachází,
- neotevírání pochybných zpráv a e-mailů,
- zajištěná dostatečná antivirová ochrana,
- šifrování,
- dodržování pravidelné likvidace elektronických dokumentů,
- přístupová hesla k jednotlivým databázím a systémům,
- zajištění bezpečného uložení veškerých přenosných elektronických zařízení a datových nosičů tak, aby k nim neměla přístup žádná nepovolaná osoba,
- zákaz vynášení osobních údajů přes různá elektronická zařízení (například USB Flash disk)
- dodržování povinnosti ohledně informování o neoprávněném zpracování osobních údajů či jakémukoli podezření týkajícímu se zneužití či ztráty osobních údajů.

Existuje mnoho způsobů, jak elektronická data spravovat a uchovávat. Mezi ty hlavní patří zejména správa pomocí:

- síťových úložišť,
- cloudových úložišť,
- e-mailové schránky,
- databáze,
- softwaru,
- pravidelného zálohování.

Z hlediska elektronické bezpečnosti je na tom MMB velmi dobře. Veškerá tato dokumentace je vedena přes DMS neboli Document Management System. Tam se

nachází každá dokumentace včetně zdigitalizované papírové dokumentace, převedené do digitální formy zejména skenováním. Například klientská dokumentace je ukládána právě v těchto interních DMS.

Kromě toho, ale využívají také cloudová úložiště, datová centra a také SharePoint od firmy Microsoft. Vše, co se ukládá do cloudových úložišť, bývá šifrované. V Sharepointech ukládají mimo jiné i podklady od klientů, se kterými se pak dále pracuje dle jejich účelu použití.

Zálohování provádí společnost pravidelně a také se pravidelně testuje, zda se dají dokumenty obnovit.

Co se týká přístupu k těmto údajům, musí mít každý zaměstnanec udělen přístup k těmto datům. Je samozřejmostí, že každý zaměstnanec má přístup do jiných systémů či databází, což závisí na tom, jakou funkci ve firmě vykonává, tedy jaký přístup je k vykonání jeho pozice potřeba. Každý rok dochází k revidování, pomocí něhož zjišťuje společnost, zda jsou přístupy povolené jednotlivým zaměstnancům stále oprávněné (zjišťují tedy, zda daný zaměstnanec ještě konkrétní přístup ke své práci opravdu potřebuje). Přístupy jsou povolené za základě hesel, která musí splňovat jisté požadavky. Jedná se o podmínky z hlediska délky, kombinace velkých a malých písmen, použití čísel a znaků. V některých oblastech můžou být přístupy zabezpečeny dvojím faktorem, tzn., že svůj přístup nepotvrzují zaměstnanci pouze heslem, ale i jiným způsobem.

Kromě přístupových hesel mohou svůj přístup povolit například použitím své osobní karty. To lze například použít u tiskáren, které bývají často na pobočkách uloženy na chodbách nebo ve společných prostorech, kam má přístup více zaměstnanců. Pokud tedy zaměstnanec odešle jakýkoli dokument k tisku, může tisk dokončit pouze přiložením své karty přímo na daném zařízení. Díky tomu lze zabránit odcizení či zneužití cizích osobních údajů. Také se může stát, že omylem zaměstnanec pošle dokument k tisku na jiné zařízení, než chtěl a díky potvrzení pomocí karty k jeho tisku nedojde.

Samozřejmostí je také kvalitní antivirová ochrana v každém zařízení, které zaměstnanci používají. Každý zaměstnance pro svoji práci využívá pouze firemní počítače, kde už je tato ochrana implementována. Pomocí Security Monitoring také dochází ke sledování veškerých aktivit, které se na daných zařízeních provádí.

Zaměstnanci mají omezený přístup na některé pochybné webové stránky či domény, nemohou se přihlašovat do své soukromé e-mailové schránky apod. Sledovány jsou také

odchozí zaměstnanecké e-maily, které zaměstnanci odesílají. Pokud jsou tyto e-maily příliš velké nebo jsou systémem vyhodnoceny za podezřelé, tak dochází k evidenci těchto zpráv a případně to řeší odpovědné oddělení. Velmi podezřelý e-mail může být i zablokován. Sledování těchto zpráv je jedním ze způsobů, jak ochránit únik dat. Dalším způsobem je také například omezení použití datových nosičů. Konkrétně se jedná o použití USB Flash disků, přičemž systém je nastaven tak, že se tento disk vůbec nedokáže spárovat s daným zařízením. Proto na tento disk nelze nahrát žádný soubor a je tak zamezeno tomu, aby se pomocí něho přenášela data mimo pracoviště.

Likvidace elektronických dat lze provádět zničením hardwaru, na kterém jsou data uložena, nicméně toto se neděje příliš často.

6.5 Školení zaměstnanců v oblasti GDPR

Stejně jako jiné důležité interní normy a předpisy, bylo důležité zaměstnance seznámit a proškolit s novým nařízením týkajícím se ochrany osobních údajů.

Školení se týká všech zaměstnanců, kteří v rámci své funkce s osobními údaji nakládají. Nově příchozí zaměstnanci jsou zaškoleni ihned na začátku (jsou proškoleni zároveň na všechny oblasti, které musí dobře znát a ovládat).

Dříve probíhalo školení vždy v konkrétní den, kdy zaměstnanci naslouchali školiteli osobně v zasedací místnosti. Poslední dva roky je školení prováděno pomocí e-learningu. V systému každého zaměstnance se ukáže, v jakých oblastech se musí proškolit a jak dlouhou dobu na to má. Většinou se jedná o prezentace, které obsahují ty nejdůležitější informace a pravidla, která musejí zaměstnanci bezpodmínečně znát. Po prezentaci pak musí zaměstnanci absolvovat test, aby bylo zřejmé, že prezentaci řádně četli a jsou se vším srozuměni.

Stejně tak absolvují i školení na GDPR. Zaměstnanci, kteří už v Monetě pracují delší dobu, museli absolvovat školení hned po přijetí obecného nařízení a od té doby jsou pravidelně proškolováni každý rok znovu. Většinou se školení realizuje na začátku roku a zaměstnanci mají cca 3 měsíce na jeho absolvování. Jelikož se zaměstnanci školí ve vícero oblastech, nejen v rámci znalostí GDPR, mají delší časový limit na jejich absolvování.

Nemají jen jeden druh školení na téma ochrany osobních údajů. Oddělení Cyber Security požaduje i školení v rámci ochrany osobních údajů v informačních systémech, což je nezbytnou součástí znalostí v rámci GDPR.

V rámci školení na ochranu osobních údajů tedy musí zaměstnanci porozumět tomu, jak s údaji zacházet, jak je chránit a neohrozit, jak se zachovat v případě podezření na podvodné zprávy a na koho se v takovém případě obrátit.

V rámci společnosti však není možné případnému zneužití či úniku osobních údajů úplně zabránit, jelikož kybernetický svět je velmi nebezpečný a napadení se může stát kdekoli.

6.6 Kontrola dodržování pravidel a povinností vyplývajících z GDPR

Každý proces je nutné z hlediska ochrany osobních údajů neustále kontrolovat a zjišťovat tak, zda je vše dodržováno a plněno dle platného obecného nařízení.

Kontrola v Moneta Money Bank týkající se GDPR se koná pravidelně každý rok. V rámci Compliance Risk Assesment probíhá také každoroční schůze na bázi diskuze, kde se projednávají různá rizika.

Ve firmě existují některé oblasti, které jsou rizikovější, a je tedy nutné je pravidelně sledovat. Většinou se pozorují v řádu několika let, dokud si firma nebude jistá, že dané riziko neexistuje nebo alespoň není tak kritické.

Jestliže v rámci kontroly dojdou k závěru, že jsou mezi nálezy i nějaká rizika, musí určit, jak moc jsou závažná. V případě závažnějších rizik dochází k jejich evidenci v systémech, kde je jasně určeno, jak a do jaké doby musí být hrozba odstraněna. Následně dochází ke kontrole, zda došlo k nápravě včas. Pokud se tak nestane, dochází k reportu na vyšší úroveň či k posunutí termínu úkolu.

Analýza možných rizik společnosti Moneta je provedena v kapitole 7.

Cílem těchto schůzí a kontrol je zejména seznámení se s novinkami v oblasti ochrany osobních údajů, kontrola dodržování všech povinností dle GDPR, případné úpravy či doplnění analýzy, předložení případných opatření.

Nelze každého zaměstnance kontrolovat zvlášť, zda zná veškeré své povinnosti a zda si je plní. Proto musí každý zaměstnanec Monety absolvovat pravidelné školení týkající se problematiky GDPR.

7 Návrhová část

Poslední kapitola se věnuje problematice potenciálních rizik, která mohou vzniknout a ohrozit tak bezpečnost dat a osobních údajů. Právě na rizicích je založen jeden ze dvou přístupů z obecného nařízení (již uváděno v kapitole 2.3).

Na základě analýzy rizik budou vyhodnoceny závěry a doporučení, které by mohla společnost využít v rámci zlepšení bezpečnosti a ochrany osobních údajů.

7.1 Analýza rizik

V rámci analýzy rizik je prvním krokem identifikace veškerých možných rizik, která mohou nastat v rámci porušení ochrany osobních údajů ve společnosti Moneta.

Rizika, která mohou nastat, mohou mít různé příčiny. V rámci MMB je lze rozdělit na interní rizika a externí rizika. Interní rizika jsou zapříčiněna většinou chybou zaměstnanců či technickým problémem. Externí rizika vyplývají z vnějších vlivů.

U každého rizika se musí určit faktory, které určují míru rizika. Jedná se o pravděpodobnost vzniku, závažnost následků ohrožení a názor hodnotitelů.

Pravděpodobnost (P) určuje odhad, s jakou pravděpodobností může dané nebezpečí nastat. Stupnice je dána vzestupně od 1 do 5 (Nezmar, 2018).

Slovní popis jednotlivých stupňů zobrazuje následující tabulka:

Tabulka 3: Pravděpodobnost vzniku a existence nebezpečí

Stupeň	Slovní popis
1	Nahodilá
2	Nepravděpodobná
3	Pravděpodobná
4	Velmi pravděpodobná
5	Vysoká

Zdroj: Nezmar, 2018

Zpracovala: Tereza Sedlecká, 2022

Stupnice **závažnosti (Z)** je hodnocena též hodnotami 1 až 5. Určuje stupeň následků, ke kterým dojde v případě výskytu rizika (Nezmar, 2018).

Popis jednotlivých stupňů vyjadřuje následující tabulka:

Tabulka 4: Závažnost možných následků ohrožení

Stupeň	Popis
1	Poškození bez následků
2	Poškození s minimálními následky
3	Poškození dat bez trvalých následků
4	Poškození dat se závažnými následky
5	Poškození dat s fatálními následky

Zdroj: Nezmar, 2018

Zpracovala: Tereza Sedlecká, 2022

V případě **názorů hodnotitelů (H)** se zohledňuje míra závažnosti ohrožení, počet ohrožených subjektů a čas trvání ohrožení, pracovní podmínky, bezpečnostní opatření z hlediska fyzické i kybernetické povahy, možnost zajištění okamžitého zásadu a případně i další vlivy. Opět je stupnice od 1 do 5 (Nezmar, 2018).

Popis jednotlivých stupňů názorů hodnotitelů vyjadřuje následující tabulka.

Tabulka 5: Názor hodnotitelů

Stupeň	Popis
1	Zanedbatelný vliv na míru nebezpečí
2	Malý vliv na míru nebezpečí
3	Větší, nezanedbatelný vliv na míru ohrožení
4	Velký a významný vliv na míru ohrožení
5	Více významných a nepříznivých vlivů na závažnost a následky

Zdroj: Nezmar, 2018

Zpracovala: Tereza Sedlecká, 2022

Veškerá konkrétní rizika uvedená níže jsou sepsána na základě získaných informací z MMB formou pravidelných konzultací. V rámci konzultací byla probrána veškerá podstatná témata obsažená v této práci a vyplývající z rozhovorů se zaměstnankyní Monety. Rizika jsou tedy zpracována dle těchto rozhovorů a také dle subjektivního dojmu autorky. Přiřazení hodnot stupně u jednotlivých faktorů je taktéž zhodnoceno dle vlastního uvážení autorky.

Míra rizika (označována písmenem „R“) je následně vypočítána vynásobením 3 výše popsaných faktorů.

7.1.1 Interní faktor

Existuje mnoho rizik, která mohou negativně ovlivnit bezpečnost osobních údajů ve společnosti. Obecně lze říci, že největší hrozbu pro společnost představuje riziko spojené s únikem dat. K tomu může dojít při mnoha okolnostech.

Rizika pocházející z interního prostředí mohou být způsobena jak selháním člověka, tak technickou chybou.

Rizika zapříčiněná chybou člověka znamenají pro každou společnost, tedy i pro Monetu, obrovské komplikace. K selhání lidského faktoru může dojít zejména kvůli nedostatečné informovanosti o rizicích na pracovišti, neopatrnosti zaměstnanců, bagatelizování důsledků vyplývajících z rizik či úmyslným negativním chováním zaměstnance.

Problémy může mít společnost i v případě, že dojde k selhání v technické oblasti. Technické komplikace se mohou ve společnosti objevit kdykoli a mohou mít i závažnější důsledky. Ne vždy je ale na první pohled možné identifikovat veškeré jejich dopady.

Interní rizika, která mohou nastat ve společnosti Moneta, zobrazuje následující tabulka.

Tabulka 6: Interní faktor

ID	Popis rizika	P	Z	N	R
1	Nedostatečná znalost GDPR z důvodu nízké úrovně proškolení zaměstnanců	3	4	3	36
2	Nedostatečné zabezpečení při zasílání dokumentace přes e-mail (od klientů)	5	4	4	80

3	Pohyb vícero zaměstnanců na jednom zařízení (počítači)	2	2	2	8
4	Nedodržování interních pravidel bezpečnosti (nezamykání dveří, neodhlašování se z počítačů, nezamykání zásuvek u stolu apod.)	4	2	3	24
5	Vynesení údajů mimo pracoviště (chyba při pohybu dokumentace, zaslání dokumentace do „špatných rukou“)	3	2	4	24
6	Ztráta osobní zaměstnanecké karty	1	3	3	9
7	Chybná manipulace s dokumentací (ponechání dokumentů bez dozoru, neevidování zaslané dokumentace, ztráta, poničení)	3	3	4	36
8	Nedostatečná znalost v oblasti bezpečnosti IT (otevírání nebezpečných odkazů či souborů)	5	5	4	100
9	Špatná likvidace dokumentace	3	3	2	18
10	Výpadek systému	2	3	2	12
11	Nedostatečné zabezpečení z hlediska složitosti a obměny hesel	5	4	3	60
12	Nedostatečná antivirová ochrana	3	5	4	60
13	Selhání zálohování	2	5	4	40
14	Klimatické vlivy (např. potíže s elektřinou)	1	3	2	6

Zdroj: Interní zdroje MMB, 2022

Vypracovala: Tereza Sedlecká, 2022

Z výše uvedené tabulky je patrné, že nejvyšší riziko představuje nedostatečná znalost v oblasti IT. Jedná se o případy, kdy může zaměstnanec otevřít nechráněný soubor či odkaz, který obdržel například ve své e-mailové schránce. Velmi vysoké riziko ale také představuje nedostatečné zabezpečení dokumentace obsahující osobní údaje, kterou posílají klienti zaměstnancům společnosti. Tyto e-maily od klientů jsou ve společnosti MMB na určitých odděleních velmi časté. Pro klienty je tato forma jednodušší a

pohodlnější, než chodit s každým dokumentem do banky osobně. Už si ale bohužel často neuvědomují, jaká rizika mohou v takových případech nastat.

Za největší důsledek těchto rizik se dá považovat únik, ztráta či zneužití osobních údajů. Dle toho, jaké riziko nastane a kdo je za něj zodpovědný, můžou nastat další důsledky. V případě pochybení ze strany zaměstnanců mohou být v reakci na tento problém zajištěna další školení týkající se této problematiky, která pomohou zaměstnancům získat dostatečné znalosti týkající se rizik a jejich řízení. Pokud by se jednalo o závažnější riziko, může dojít k uložení sankcí, případně se společnost s daným zaměstnancem musí rozloučit. V případě technického selhání by mohlo být dle závažnosti rizika potřeba oprav technického charakteru či případná aktualizace systémů.

Každý nález rizika a jeho následné řešení s sebou nese také vyšší časovou, případně i finanční zátěž pro společnost. U velmi závažného rizika může také společnost ztratit své dobré jméno.

7.1.2 Externí faktor

Za externí rizika lze považovat veškerá rizika, která jsou způsobena vnějšími vlivy, jež mohou ovlivnit bezpečnost osobních údajů ve společnosti.

Tabulka 7: Externí faktor

ID	Popis rizika	P	Z	N	R
1	Phisingové e-maily	5	4	4	80
2	Voice phising	3	3	3	27
3	Odcizení dat způsobené vloupáním do prostor s dokumentací (archivu)	1	5	4	20
4	Kybernetické útoky	3	3	5	45

Zdroj: Interní zdroj MMB, 2022

Vypracovala: Tereza Sedlecká, 2022

Z tabulky zobrazující externí faktory je patrné, že největším rizikem z této kategorie jsou phisingové e-maily.

Phisingové e-maily jsou v posledních měsících ve společnosti Moneta aktuální téma. Stále častěji chodí zaměstnancům MMB e-maily, které obsahují upozornění na zvýšené

riziko phisingových a podvodných e-mailů. Pomocí těchto e-mailů mohou útočníci infiltrovat interní síť, zašifrovat data, zaznamenávat stisknuté klávesy nebo získat přístup k citlivým informacím a převzít celkovou kontrolu nad daným zařízením.

Tyto podvodné e-maily vypadají velmi podobně jako věrohodný e-mail zaslaný například od zaměstnavatele nebo od správce systémů, kdy požadují změnu hesel či důležitou aktualizaci. Pomocí nich se snaží vzbudit u dané osoby dojem naléhavosti a většinou v nich útočníci chtějí po uživatelích stáhnout soubor či otevřít odkaz.

V Monetě by měly interní e-maily vždy obsahovat adresu končící „@moneta.cz“. V případě phisingu mohou útočníci použít úmyslný překlep „@rnoneta.cz“, což by mohl zaměstnanec přehlédnout a zvýšit tak riziko napadení a úniku dat, což by mohlo mít vážné důsledky.

Obecně by se za důsledky rizik vyplývající z externích vlivů daly opět považovat únik, ztráta či zneužití dat. Dále také může dojít v případě potřeby k obnovení či zakoupení lepší ochrany pro zabezpečení údajů. Stejně jako u interních rizik, mohou i externí rizika přinést časové a finanční zatížení a také ztrátu dobrého jména firmy.

7.2 Shrnutí a vyhodnocení rizik

V předchozí kapitole byla zpracována analýza rizik, která mohou ovlivnit bezpečnost a ochranu dat ve společnosti Moneta.

Rizika byla rozdělena do dvou oblastí, které mohou být příčinou vzniku rizik. Jedná se o interní a externí faktory, přičemž v rámci analýzy bylo identifikováno celkem 14 rizik z interního prostředí a 4 rizika z externího prostředí.

V této kapitole dochází k celkovému shrnutí a vyhodnocení uvedených rizik za pomoci jednoduché metody „PZH“. Míra rizika (R) se tedy určuje dle pravděpodobnosti (P), závažnosti (Z) a názoru hodnotitelů (H) a je dána vynásobením těchto 3 faktorů (Nezmar, 2018).

Míru rizik lze následně rozdělit do 5 kategorií. Tyto kategorie zobrazuje následující tabulka.

Tabulka 8: Míry rizika

Stupeň rizika	Celkové R	Míra rizika
1.	> 100	Nepřijatelné riziko
2.	51 – 100	Nežádoucí riziko
3	11 – 50	Mírné riziko
4	3 – 10	Akceptovatelné riziko
5.	< 3	Bezvýznamné riziko

Zdroj: Nezmar, 2018

Zpracovala: Tereza Sedlecká, 2022

Bezvýznamné riziko nevyžaduje žádné zvláštní opatření. Jeho hodnota je sice velmi nízká, i přesto je ale potřeba na něj upozornit případně realizovat výchovná opatření.

U akceptovatelného rizika už musí společnost zvažovat náklady na zmírnění či odstranění rizika. Pokud u takového rizika nepomohou technická bezpečnostní opatření, je nutné uvažovat i nad změnami organizačními.

Na mírná rizika se vztahují opatření, k jejichž realizaci dochází dle zpracovaného plánu vycházejícího z rozhodnutí vedení společnosti. Veškerá opatření proti mírným rizikům tak musejí být zavedena přesně dle časového plánu a musí být následně provedeno další zhodnocení.

Nežádoucí rizika si žádají velmi rychlé zavedení opatření, aby došlo ke zmírnění rizika na přijatelnou úroveň.

Nepřijatelné riziko znamená pro společnosti, že musí okamžitě zastavit činnosti, dokud nedojde k realizaci opatření a opětovnému vyhodnocení rizik. Veškeré zpracování osobních údajů může pokračovat až po snížení tohoto rizika (Nezmar, 2018).

V rámci analýzy bylo tedy identifikováno dohromady 18 rizik. Následující tabulka zobrazuje počet rizik odpovídající dané míře rizika.

Tabulka 9: Počet identifikovaných rizik dle jejich míry

Míra rizika	Počet identifikovaných rizik
Nepřijatelné riziko	**0**
Nežádoucí riziko	**5**
Mírné riziko	**10**
Akceptovatelné riziko	**3**
Bezvýznamné riziko	**0**

Zdroj: Vlastní zpracování, 2022

Z tabulky je patrné, že v rámci analýzy byla zjištěna 3 akceptovatelná rizika, 10 mírných rizik a 5 nežádoucích. I přesto, že nebylo zjištěno žádné nepřijatelné riziko, nemělo by být ignorováno žádné zhodnocené riziko.

Jako akceptovatelná rizika byla zjištěna tato 3 rizika:

- pohyb vícero zaměstnanců na jednom počítači,
- klimatické vlivy,
- ztráta osobní zaměstnanecké karty.

Nejvíce rizik bylo identifikováno v položce mírná rizika. Jedná se o tato rizika:

- nedostatečná znalost GDPR z důvodu nízké úrovně proškolení zaměstnanců,
- nedodržování interních pravidel bezpečnosti (nezamykání dveří, neodhlašování se z počítačů, nezamykání zásuvek u stolu apod.),
- vynesení údajů mimo pracoviště (chyba při pohybu dokumentace, zaslání dokumentace do „špatných rukou“),
- chybná manipulace s dokumentací (ponechání dokumentů bez dozoru, neevidování zaslané dokumentace, ztráta, poničení),
- špatná likvidace dokumentace,
- výpadek systému,
- selhání zálohování,
- voice phising,
- odcizení dat způsobené vloupáním do prostor s dokumentací (archivu).
- kybernetické útoky.

Jako nežádoucí rizika byla identifikována tato rizika:

- phisingové e-maily,
- nedostatečné zabezpečení při zasílání dokumentace přes e-mail (od klientů),
- nedostatečná znalost v oblasti bezpečnosti IT (otevírání nebezpečných odkazů či souborů),
- nedostatečné zabezpečení z hlediska složitosti a obměny hesel,
- nedostatečná antivirová ochrana.

Shrnutí

Rizika týkající se úniku dat by se neměla brát na lehkou váhu, a to ani v případě, že neznamenají pro společnost příliš velkou hrozbu. Z výše uvedené analýzy je patrné, že největší riziko vyplývá z nedostatečných znalostí zaměstnanců v oblasti IT bezpečnosti.

Vzhledem k tomu, jak se technologie neustále rozvíjí a firma se snaží mnoho věcí digitalizovat, je pro případné útočníky „lákavější“ nabourat se do interních systémů než vymýšlet, jak získat údaje například loupeží ve vnitřních prostorách společnosti. Chybějící znalosti zaměstnanců nejsou jediným vážnějším rizikem. Vyšších hodnot dosahovala také rizik spojená s phisingovými e-maily a nedostatečným zabezpečením v rámci posílání klientských dokumentů přes e-maily.

Je jisté, že nedostatečné znalosti může společnosti napravit tak, že bude provádět častější školení. To ale nemusí být dostačující pro ostatní rizika. Veškerá opatření navržená pro snížení těchto rizik jsou uváděna v kapitole 7.3.

7.2.1 Kybernetické útoky v České republice

Vzhledem k tomu, jak jsou v dnešní době kybernetické útoky a podvody rozsáhlé, je zpracována i tato podkapitola, která poukazuje na kybernetickou bezpečnost v České republice z hlediska statistických dat. Veškeré informace a data jsou platná pro rok 2020 a vycházejí ze zprávy o kybernetické bezpečnosti České republiky za rok 2020 zveřejněné v červenci 2021 Národním úřadem pro kybernetickou a informační bezpečnost (dále jen jako „NÚKIB“).

V roce 2020 ovlivnila kybernetickou bezpečnost i situace týkající pandemie Covid-19, kdy se internet stal v podstatě jediným místem, kde bylo možné se vzdělávat, pracovat a udržovat kontakt s ostatními lidmi.

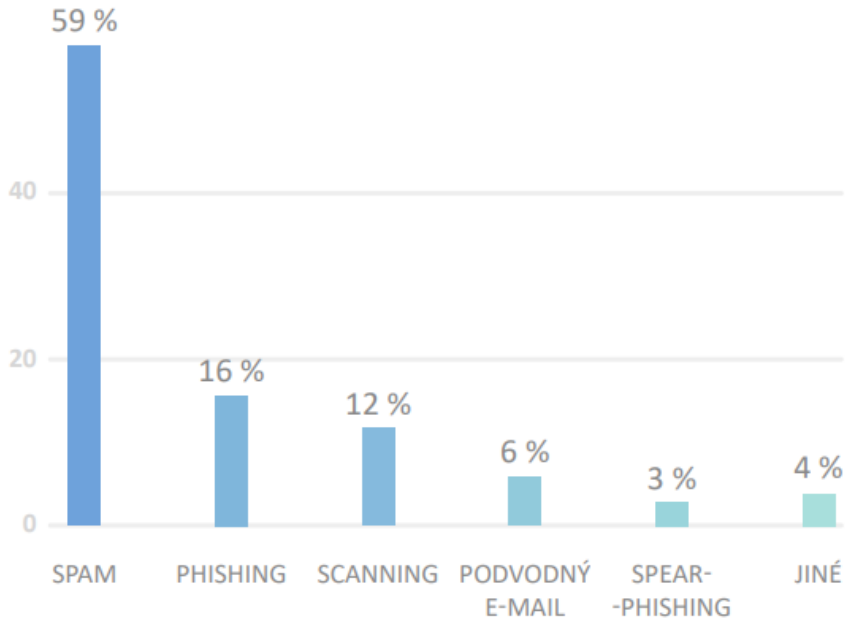
V roce 2020 bylo zaznamenáno v České republice 468 nahlášených incidentů. Oproti roku 2019, kdy bylo těchto nahlášení pouze 217. Došlo tedy k velkému nárůstu. Ze 468 jich NÚKIB řešil 99 a 9 z nich označil za významné incidenty.

Každým rokem se počet incidentů řešených NÚKIB výrazně zvyšuje. Zatímco v roce 2017 jich bylo řešeno 50, v roce 2018 se jejich počet lehce zvýšil na 54. Za rok 2019 už stoupl počet řešených incidentů na 78 a za rok 2020 dokonce dosáhl počtu 99. Nejvíce incidentů bylo řešeno v odvětví státní správy a finanční sektor obsadil 4. místo z 11 uváděných sektorů (státní správa, zdravotnictví, doprava, finanční instituce, obce, digitální infrastruktura, energetika, školství, stavebnictví, kraj, ostatní).

Téměř tři čtvrtiny respondentů z finančního sektoru čelily v roce 2020 pokusům o kybernetický útok a jako nejčastější incident byl zjištěn phishing, který je nyní aktuální i ve společnosti Moneta. Finanční instituce oproti ostatním sektorům vynakládají největší procento ze svého rozpočtu do oblasti kybernetické bezpečnosti a banky se společně s pojišťovnami označují za instituce, které jsou z hlediska této bezpečnosti na dobré úrovni.

V celkovém výzkumu došli k závěrům, že mezi nejčastější útoky za rok 2020 patřily zejména spamové zprávy, phishing a skenování vnějších sítí organizací. Následující obrázek zobrazuje nejčastější typy kybernetických útoků za rok 2020.

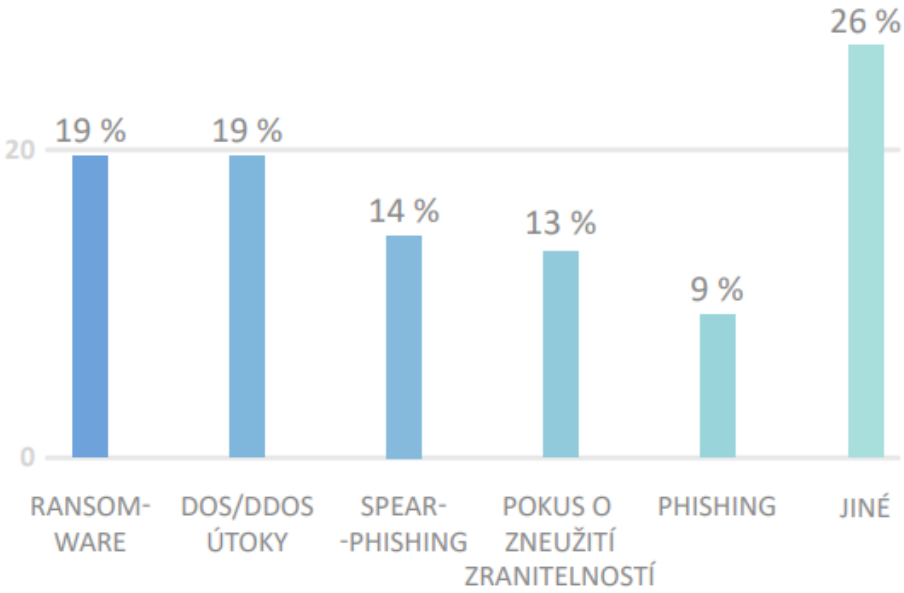
Obrázek 3: Nejčastější kybernetické útoky v roce 2020 (% respondentů)



Zdroj: Zpráva o stavu kybernetické bezpečnosti, NÚKIB, 2020

Na dalším obrázku jsou pak zobrazeny nejzávažnější útoky vyhodnocené za rok 2020.

Obrázek 4: Nejzávažnější kybernetické útoky v roce 2020 (% respondentů)



Zdroj: Zpráva o stavu kybernetické bezpečnosti, NÚKIB, 2020

7.3 Opatření a doporučení navržená pro Monetu Money Bank

Tato kapitola je zaměřena na doporučení opatření k jednotlivým rizikům společnosti Moneta Money Bank.

Navržená opatření čerpají z informací získaných během konzultací, interních dokumentů a jsou sestavena i na základě rad zaměstnankyně společnosti, která byla důležitou konzultantkou pro zpracování této práce.

Následující tabulky podávají stručný a zjednodušený přehled o jednotlivých opatřeních pro každé identifikované riziko. V textu pod tabulkami jsou pak dané návrhy a doporučení blíže specifikována.

Tabulka 10: Opatření k interním rizikům

Riziko	Opatření
Nedostatečná znalost GDPR z důvodu nízké úrovně proškolení zaměstnanců	Pravidelnější proškolení zaměstnanců

Nedostatečné zabezpečení při zasílání dokumentace přes e-mail (od klientů)	Vytvoření bezpečného klientského systému, kam mohou bezpečněji vkládat a posílat dokumenty
Pohyb vícero zaměstnanců na jednom zařízení (počítači)	Zvýšená kontrola na pracovišti, pravidelné školení v dané problematice
Nedodržování interních pravidel bezpečnosti (nezamykání dveří, neodhlašování se z počítačů, nezamykání zásuvek u stolu apod.)	Pravidelné kontroly na pracovišti
Vynesení údajů mimo pracoviště (chyba při pohybu dokumentace, zaslání dokumentace do „špatných rukou“)	Pravidelné školení v problematice
Ztráta osobní zaměstnanecké karty	Pravidelné školení v dané problematice
Chybná manipulace s dokumentací (ponechání dokumentů bez dozoru, neevidování zaslané dokumentace, ztráta, poničení)	Pravidelné kontroly na pracovišti
Nedostatečná znalost v oblasti bezpečnosti IT (otevírání nebezpečných odkazů či souborů)	Pravidelné školení v dané problematice
Špatná likvidace dokumentace	Pravidelné školení v dané problematice
Výpadek systému	Efektivní a rychlé odhalení a následné vyřešení konkrétního problému
Nedostatečné zabezpečení z hlediska složitosti a obměny hesel	Vyšší požadavky na hesla a zabezpečení přístupů
Nedostatečná antivirová ochrana	Aktualizace či přenastavení antivirové ochrany
Selhání zálohování	Vyšší údržba úložišť
Klimatické vlivy (např. potíže s elektřinou)	Využití záložních zdrojů

Zdroj: Vlastní zpracování, 2022

Na rizika, která mají nižší stupeň závažnosti, postačí opatření týkající se větší kontroly na pracovišti nebo pravidelnějšího školení zaměstnanců.

Jestliže dané riziko vyplývá z neznalosti problematiky GDPR nebo z oblasti IT bezpečnosti, považuje se za nejúčinnější nápravu proškolení zaměstnanců. Zaměstnanci mají nyní ve společnosti povinnost absolvovat školení jedenkrát za rok, a to formou on-line prezentace a následného zakončení školení testem, který musí splnit alespoň na 80 %. Vzhledem k tomu, jak vysoké riziko tyto nedostatečné znalosti mohou přinést, je velmi důležité, aby společnost vysoce dbala na **pravidelnější vzdělávání** svých zaměstnanců. Doporučením je v tomto případě školení provádět alespoň dvakrát za rok a poukazovat v něm i na konkrétní dopady, které mohou nastat. Zaměstnanci z důvodu vyšší bezpečnosti musí dbát na to, aby zbytečně nepřehlcovali úložiště dat, aby byl vždy zajištěn dostatek volného místa na disku. Dále by neměli stahovat osobní dokumentaci, měli by spouštěn pravidelné aktualizace na svých zařízeních, a také dbát na odhlašování a vypínání ze svých osobních pracovních počítačů.

Například u rizika spojeného se špatnou likvidací dokumentace je nutno podotknout, že si někteří zaměstnanci ani nemusí uvědomovat, že nezničením či neskartováním nepotřebných dokumentů a kopií můžou umožnit, aby došlo ke zneužití a úniku dat. Stejně tak vynášení dokumentů mimo pracoviště a posílání dokumentů například poštou si žádá, aby zaměstnanec dbal na bezpečnost dokumentů a uvědomoval si důležitost dodržování pravidel bezpečnosti. I v boji těmto rizikům je tedy doporučováno správné zaškolení zaměstnanců.

Díky školení, které by poukazovalo i na tato méně významná rizika, by se úroveň hrozeb mohla podstatně snížit.

Co se týká **kontrol na pracovišti** a sledování dodržování pravidel bezpečnosti, nyní k nim ve společnosti nedochází téměř vůbec. Každý zaměstnanec by měl interní pravidla bezpečnosti dodržovat a zejména dbát na tzv. „zásadu čistého stolu“, která již byla popsána v kapitole 6.4. Pravidelné a předem neohlášené kontroly by mohly zaměstnance více motivovat ke správnému chování na pracovišti. Byla by tak zajištěna maximální možná míra zabezpečení.

V rámci vysokého rizika, týkajícího se zasílání klientské dokumentace přes e-mail, by jako vhodné doporučení, pro bezpečnější přenos údajů, bylo **vytvoření klientského systému**, kam by klient mohl ukládat potřebné dokumenty a bance je tak předat jednoduše

a bezpečně. Tento přenos dokumentů by mu byl umožněn přes internetové bankovnictví. Po přihlášení do svého internetového bankovnictví by měl klient stejný přehled o veškerých svých platbách a údajích týkajících se jeho účtu a klientského portfolia jako doteď. Nově by klientovi vznikla možnost nahrávat dokumentaci potřebnou k vyřízení jeho žádostí, například o poskytnutí úvěru. Klient by v rámci bankovnictví viděl, co vše musí doložit pro vyřízení žádosti a splnění podmínek (nejen v rámci úvěru, ale i v jiných službách) a měl by možnost tyto požadavky splnit z pohodlí domova a být si tak jist, že se k dokumentaci může dostat pouze banka. Velmi často využívají klienti toho, že potřebné dokumenty posílají raději e-mailem přímo zaměstnancům banky, než aby tam zašli odevzdat dokumenty osobně. Je to pro ně snazší a rychlejší, ale tyto soubory a dokumenty většinou nejsou nijak zaheslované či zašifrované a e-mail by tak mohl být snadno napadnutelný a mohlo by dojít například ke zneužití osobních údajů klienta. Proto by vytvoření takového systému bylo v rámci bezpečnosti vhodným řešením, neboť by klient vše vkládal rovnou do systému banky a zamezilo by se tak zbytečné manipulaci s dokumenty a soubory.

Další riziko, které si žádá nápravné opatření, se týká bezpečnosti přístupů založených na složitosti a obnově hesel. Další doporučení pro MMB se tedy týká **politiky heslování**, čímž je myšleno zvýšení požadavků na tvorbu a následnou změnu hesel, pomocí nichž se zaměstnanci přihlašují do interních systémů a databází. V současné době nejsou v Monetě tyto požadavky tak přísné, jak by měly být. Zaměstnanci mohou svá hesla měnit například pouhou úpravou čísla, nikoli celého hesla, dále mohou používat posloupnost znaků (např. jako v číselné řadě). Konkrétním doporučením v této oblasti pro Monetu je tedy zvýšení požadavků na složitost hesel. To znamená vytvářet hesla minimálně o 12 znacích, využívat velká i malá písmena, složitější symboly. Zaměstnanci by také neměla být povolena změna například pouhým přidáním dalšího symbolu, ale systém by měl požadovat celkovou změnu hesla. Dále by zaměstnanec neměl používat podobné či dokonce stejné heslo při přihlašování do interních systémů, jako používá pro přihlášení na konkrétním zařízení. Poslední radou je zamezení možnosti hesla ukládat, aby se k údajům nemohl dostat někdo, kdo k těmto údajům přístup mít nemá.

V případě výpadku systému je potřeba **rychlá a pružná reakce** IT oddělení. Každý zaměstnanec by měl jakoukoli technickou chybu ihned bez prodlení ohlásit na helpdesk. Zaměstnanci z oddělení helpdesk by měli co nejrychleji chybu odstranit a zajistit, aby

k takovým výpadkům nedocházelo častěji a snížit tak riziko, že se mohou nějaká data ztratit.

Na klimatické vlivy se společnost nemůže nikdy předem připravit tak, aby došlo k úplnému odstranění rizika. Pro výpadek elektřiny by měla společnost mít vždy k dispozici **záložní zdroj**, nicméně v současnosti je toto riziko opravdu minimální.

Aby nedocházelo k selhání zálohování, měla by se společnosti soustředit na pravidelnou revizi či **údržbu úložišť,** aby nedocházelo k častému zahlcení systému a bylo zaměstnancům vždy umožněno vykonávat svoji práci.

V případě antivirové ochrany jsou důležité zejména její **aktualizace**. V bance mají nastavenou antivirovou ochranu v každém zařízení, která je chrání před nepříznivými vlivy a také zaměstnance upozorňuje na případné hrozby. Hodně zaměstnanců, po kterých je aktualizace vyžadována, často tuto činnost odkládají, aby mohli řádně dodělat svoji práci. I na toto je ale třeba dbát, aby byla provedena co nejdříve a byla tak zajištěna spolehlivější ochrana.

Následující tabulka už poukazuje na opatření doporučená ke snížení externích rizik.

Tabulka 11: Opatření k externím rizikům

Riziko	Opatření
Phisingové e-maily	Hlubší informovanost zaměstnanců o rizicích a jejich dopadech, proškolení
Voice phising	Hlubší informovanost zaměstnanců o rizicích a jejich dopadech, proškolení
Odcizení dat způsobené vloupáním do prostor s dokumentací (archivu)	Vyšší zabezpečení vnitřních prostor
Kybernetické útoky	Vysoké zabezpečení informačních systémů, přenastavení ochrany

Zdroj: Vlastní zpracování, 2022

Aby došlo ke snížení rizika vyplývajícího z phisingových e-mailů či voice phishingu, je zapotřebí zaměstnance **pravidelně informovat o těchto možných hrozbách** a jejich důsledcích. Voice phishing je forma phisingu, kdy dochází k podvodům prostřednictvím telefonických hovorů. Ve společnosti Moneta už takové pokusy zaregistrovali. V případě

phisingového e-mailu by měl zaměstnanec vždy s odesílatelem e-mailu prověřit, zda je to opravdu jeho e-mailová adresa a také ověřit obsah dané zprávy. Doporučení pro Monetu v tomto ohledu je to, aby pravidelně (ideálně jedenkrát za měsíc) upozorňovala zaměstnance na aktuální nebezpečí a také jim připomněla, jak a kam mají zaměstnanci podezření na tyto podvody nahlásit.

Pro snížení rizika odcizení dat vloupáním na pracovišti lze zamezit pomocí řádného zabezpečení informačních systémů. Společnost by měla dbát na zamykání dveří, používat kamerový systém a uzamykat pracoviště i pomocí alarmového kódu.

I z důvodu vysoké míry digitalizace je v současnosti kybernetické nebezpečí velmi aktuální téma. Proti kybernetickým útokům by měla mít společnost zajištěné vysoké technické zabezpečení. Doporučuje se využívání kvalitních antivirových ochran či systémy, které kontrolují činnosti prováděné v rámci organizací. Zároveň jsou ale důležitá i právní opatření formou interních předpisů, jež upozorňují zaměstnance na veškeré jejich povinnosti. V případě, že by došlo k odhalení, že se útočníci pokusili o kybernetický útok na společnost Moneta, musí své zabezpečení překontrolovat a případně již nastavenou ochranu přenastavit či vyměnit.

Závěr

Hlavním cílem této práce bylo zhodnotit dopady GDPR na Monetu Money Bank a.s. V úvodní kapitole byl čtenář seznámen s hlavními cíli a postupy zpracování této práce. Následovala kapitola definující základní charakteristiku a pojmy obecného nařízení a také historický vývoj v oblasti ochrany osobních údajů. Třetí kapitola byla zaměřena na podstatná témata týkající se obecného nařízení.

Druhá část práce byla zaměřena na subjekt Moneta Money Bank, kde byla zpočátku společnosti představena a zanalyzována z hlediska situace před zavedením GDPR a také jeho implementace. Následovala kapitola popisující konkrétní dopady týkající se zavedení GDPR. Veškeré informace byly zpracovány na základě osobních konzultací se zaměstnanci Moneta Money Bank a také na základě zpracování dat z interních i veřejně dostupných dokumentů.

Jedním z prvních dopadů bylo zavedení funkce pověřence pro ochranu osobních údajů. Pro společnost byla velká výhoda, že prvotně tuto funkci obsadil člověk, který dříve pracoval několik let na Úřadu pro ochranu osobních údajů a nebylo tak potřeba úvodního školení z hlediska této problematiky.

Zavedení GPDR mělo samozřejmě dopad i z hlediska časové, administrativní náročnosti. Moneta se na zavedení GDPR připravovala téměř 2 roky dopředu. Na implementaci pracoval projektový tým, který se skládal z jednoho hlavního manažera a dalších členů. Prvotní fáze spočívala ve vytvoření rozdílové GAP analýzy, která z počátku trvala pouhé dva měsíce, nicméně postupem času se nacházelo i nadále více oblastí, kde bylo potřeba provést změny. Z hlediska finanční náročnosti vzrostly firmě náklady na některé úpravy interních systémů, které musely provádět externí zdroje a dále na některé externí zdroje, mezi které patří například analytik pro provedení analýzy či již zmiňovaný projektový manažer.

Velký dopad mělo zavedení GDPR i na oblast zabezpečení a uchovávání dat. Změny musely být vidět i v interních předpisem o bezpečnosti fyzické i elektronické dokumentace a musela být zavedena vyšší bezpečnostní opatření, kterými se každý zaměstnanec musí řídit. Veškeré vstupy do systémů mají zaměstnanci povoleny na základě nastavených přístupů a jsou zabezpečeny hesly.

Velmi důležitá je také znalost a povědomí zaměstnanců o důležitosti ochrany osobních údajů. Společnost tedy zavedla povinné školení v rámci této problematiky a musí ho absolvovat každý zaměstnanec. Tato školení jsou pak opakována jedenkrát ročně vždy na začátku nového roku. Pro intenzivnější prohloubení znalostí této problematiky napříč společností byl také upraven interní systém, který obsahuje veškeré potřebné informace a povinnosti vyplývající pro zaměstnance a je plně v souladu s obecným nařízením.

K pravidelným kontrolám plnění všech povinností vyplývajících z interních předpisů banky spíše nedochází. Každý rok se koná pouze schůze, kde se seznamují zaměstnanci s novinkami týkajících se ochrany osobních údajů a projednávají případná rizika, která mohou společnost negativně ovlivnit. Pro případné nálezy rizik je pak nutné určit, jak jsou významné a navrhnout plán, kde bude jasně stanoveno, do kdy a jakým způsobem dojde ke snížení rizik.

Celkově lze říci, že nejdůležitější byla doba, kdy se společnost připravovala na zavedení GDPR. Bylo obtížnější upravit některé interní systémy, banka musela upravit stávající interní předpisy a připravit na nové změny i své zaměstnance. Zavedení GDPR s sebou přinášelo z počátku mnoho nových starostí, nicméně z výhledového hlediska by mělo pro společnost působit spíše jako přínos.

V poslední části této práce byla provedena analýza možných rizik ve společnosti MMB. Na základě této analýzy došlo k vyhodnocení těchto rizik a následně jim byla přiřazena opatření, kterými by mohla být rizika snížena.

Největší hrozby představují pro společnost nedostatečná znalost v oblasti IT bezpečnosti, zasílání klientské dokumentace přes e-maily a také nedostatečně vysoké požadavky na složitost a obměnu hesel, na základě kterých se přihlašují zaměstnanci do systémů. Společnost by tedy měla více dbát na vzdělání svých zaměstnanců v oblastní informační technologie a její bezpečnosti. Dále by bylo vhodné upravit politiku heslování, aby docházelo k vytvoření hesel či jejich obměně dle přísnějších požadavků. V neposlední řadě bylo společnosti doporučeno, aby klientům umožnila pomocí internetového bankovnictví nahrávat potřebné dokumenty k vyřízení různých žádostí, jelikož by to bylo snazší a také z hlediska manipulace s danými dokumenty bezpečnější. V současné době také roste počet kybernetických útoků a každým dnem stoupá i jejich agresivita. I přesto, že se útočníci nemusí primárně soustředit jen na odcizení citlivých dat, musí si společnosti nastavit takové zabezpečení, aby těmto rizikům co nejlépe zamezily. U většiny rizik

identifikovaných jako méně závažná postačí zvýšení kvality školení, pravidelné kontrolování na pracovišti či běžná údržba systémů.

Riziko úniku citlivých dat je velkým rizikem pro každou společnosti a pro společnosti Moneta by to mohlo mít fatální důsledky, jelikož zpracovává denně opravdu velké množství osobních údajů. Je proto velmi důležité, aby dbala na maximální bezpečnost a zamezila tak výskytu případných rizikových situací.

Seznam použitých zdrojů

Česká bankovní asociace (2019). *GDPR – Kodexy a standardy.* Dostupné 5. 3. 2022 z https://cbaonline.cz/gdpr

ČESKO. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů*. Sbírka zákonů České republiky. Dostupné 10. 2. 2022 také z https://www.aspi.cz/products/lawText/1/49228/1/2

ČESKO. *Zákon č. 21/1992 Sb., o bankách.* Sbírka zákonů České republiky. Dostupné 1. 4. 2022 z https://www.aspi.cz/products/lawText/1/39677/1/2

Docksey, Ch., & Drechsler, R. (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, UK: Oxford University Press.

Eur-Lex. (2016a). 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. Dostupné 15. 2. 2022 z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

Eur-Lex. (2016b). Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Dostupné 15. 2. 2022 z https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1568638421562&uri=CELEX:32016R0679

GDPR (n.d.). *Co je to GDPR.* Dostupné 1. 2. 2022 z: https://www.gdpr.cz/gdpr/

GDPR (n.d.). *Evropský sbor pro ochranu osobních údajů.* Dostupné 1. 3. 2022 z https://www.gdpr.cz/gdpr/heslo/evropsky-sbor-pro-ochranu-osobnich-udaju/

GDPR (n.d.). *Pracovní skupina 29.* Dostupné 1. 3. 2022 z https://www.gdpr.cz/gdpr/heslo/pracovni-skupina-29/

GDPR (n.d.). *Data Proteciton Impact Assesment.* Dostupné 1. 3. 2022 z https://www.gdpr.cz/gdpr/heslo/data-protection-impact-assessment/

Interní zdroje MMB (2022) – zahrnují informace získané na základě konzultací se zaměstnanci MMB

Interní dokumentace MMB (2022) – zahrnuje informace zpracované z interních dokumentů MMB

Janečková, E. (2018). *GDPR – Praktická příručka implementace.* Praha, Česko: Wolters Kluwer

Kurzy.cz (2022). *Moneta Money bank – obchodní rejstřík firem.* Dostupné 5. 3. 2022 z https://rejstrik-firem.kurzy.cz/25672720/moneta-money-bank-as/

Moody's Better decisions (2022). *Moody's – our capabilities.* Dostupné 26. 3. 2022 z https://about.moodys.io/overview

Moneta Money Bank (2022a). *Moneta – o nás.* Dostupné 15. 3. 2022 z https://www.moneta.cz/o-nas

Moneta Money Bank (2022b). *Loga a fotografie.* Dostupné 15. 3. 2022 z https://www.moneta.cz/servis-pro-media/loga-a-fotografie

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

Nezmar, J. (2018). *Praktický průvodce implementací.* Praha, Česko: Grada Publishing

Nulíček, M. (2018*). GDPR – obecné nařízení o ochraně osobních údajů.* Praha, Česko: Wolters Kluwer

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) (2022a). *NÚKIB – Legislativa KB.* Dostupné 20. 3. 2022 z https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) (2022b). *NÚKIB – Zpráva o stavu kybernetické bezpečnosti 2020.* Dostupné 10. 4. 2022 z https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

SAP (2022). *What is SAP.* Dostupné 5. 3. 2022 z https://www.sap.com/about/company/what-is-sap.html

Úřad pro ochranu osobních údajů (ÚOOÚ) (2013a). *Jmenování a ohlášení pověřence.* Dostupné 20. 2. 2022 z https://www.uoou.cz/jmenovani-a-ohlaseni-poverence/ds-5552/p1=5552

Úřad pro ochranu osobních údajů (ÚOOÚ) (2013b). *Dozorová a rozhodovací činnost.* Dostupné 1. 3. 2022 z https://www.uoou.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277

Úřad pro ochranu osobních údajů (ÚOOÚ) (2019). *Zabezpečení osobních údajů.* Dostupné 10. 3. 2022 z https://www.uoou.cz/8-zabezpe-eni-osobnich-udaj/d-27282

Žůrek, J. (2018). *Praktický průvodce GDPR.* Ostrava, Česko: Nakladatelství ANAG

Seznam tabulek

Seznam obrázků

Seznam zkratek

DMS = Document Management System

GDPR = General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)

EU = Evropská unie

IP = Internet Protocol (internetový protokol)

MAC = Media Access Control

MMB = Moneta Money Bank

resp. = respektive

tzn. = to znamená

ÚOOÚ = Úřad pro ochranu osobních údajů

Abstrakt

Sedlecká, T. (2022). *Dopady dodržování pravidel nastavených GDPR na zvolený ekonomický subjekt* [Diplomová práce, Západočeská univerzita v Plzni].

Klíčová slova: ochrana osobních údajů, GDPR, dopady GDPR, analýza rizik

Tato práce se zabývá tématem ochrany osobních údajů a také dopady GDPR na zvolený ekonomický subjekt – Moneta Money Bank, a.s. Práce uvádí hlavní charakteristiku a cíle obecného nařízení, historický vývoj ochrany osobních údajů a také podstatná témata z GDPR. V praktické části je pak uvedena charakteristika zvoleného subjektu včetně analýzy stavu před zavedením GDPR a po jeho implementaci. Práce se také zaměřuje na hlavní dopady obecného nařízení na vybraný ekonomický subjekt. V poslední části jsou identifikována rizika a následně je shrnuto jejich vyhodnocení. Vyhodnocení probíhalo pomocí zvolené metody a také na základě konzultací se zástupcem sledovaného subjektu. V rámci shrnutí byla zjištěna mírná i významná rizika. Následně byla navržena opatření, která mohou sloužit k jejich zmírnění.

Abstract

Sedlecká, T. (2022). *Impacts of compliance with the rule set by the GDPR on the selected economic entity* [Master's Thesis, University of West Bohemia].

Key words: personal data protection, GDPR, impacts of GDPR, risk analysis

This thesis deals with the topics of personal data protection and also impacts of GDPR on the selected ecnomic entity – Moneta Money Bank, a.s. The thesis presents the main characteristics and objective of the general regulation, the historical development of personal data protection and also essential topic of the GDPR. The practical part then presents the characteristics of the selected entity, including an analysis of the situation before the introduction of GDPR and after its implementation. The thesis also focuses on the main impacts of the general regulation on the selected economic entity. The last part identifies the risks and then summarizes their assesment. The risks were evaluated using the chosen method and also on the basis of data obtained during consultations with the representant of observed subject. The summary identified moderate and significant risks and proposed measures which could help to reduce them.