# Projekt implementace GDPR ve vybrané společnosti

Bc. Lucie Mikelová

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav podnikové ekonomiky
akademický rok: 2017/2018

# ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Lucie Mikelová** |
| Osobní číslo: | **M16397** |
| Studijní program: | **N6208 Ekonomika a management** |
| Studijní obor: | **Podniková ekonomika** |
| Forma studia: | **prezenční** |
| Téma práce: | **Projekt implementace GDPR ve vybrané společnosti** |

Zásady pro vypracování:

**Úvod**

**Definujte cíle práce a použité metody zpracování práce.**

**I. Teoretická část**

- **Proveďte průzkum literárních zdrojů a na základě kritické literární rešerše definujte základní pojmy z oblasti ochrany osobních údajů a formulujte podstatu GDPR.**

**II. Praktická část**

- **Charakterizujte vybranou společnost a analyzujte její současný systém ochrany osobních údajů.**
- **Vypracujte projekt implementace GDPR ve vybrané společnosti.**
- **Vyhodnoťte ekonomickou náročnost, přínosy a rizika tohoto projektu.**

**Závěr**

Rozsah diplomové práce: **cca 70 stran**

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

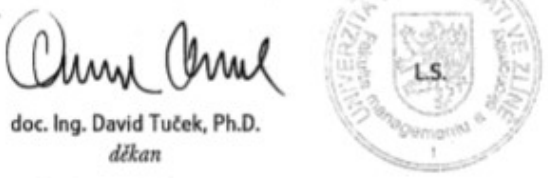
**BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v aplikační praxi (vybrané problémy). 4., aktualiz. vyd. Praha: Wolters Kluwer Česká republika, 2016, 287 s. ISBN 978-80-7552-141-5.**
**CALDER, Alan. EU GDPR: A Pocket Guide. 1st ed. United Kingdom: IT Governance Publishing, 2016, 74 s. ISBN 978-1-84928-833-0.**
**GONZÁLEZ FUSTER, Gloria. The Emergence of Personal Data Protecton as a Fundamental Right of the EU. 1st ed. Switzerland: Springer International Publishing, 2014, 274 s. ISBN 978-3-319-05023-2.**
**MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008, 455 s. ISBN 978-80-7357-322-5.**
**NEZMAR, Luděk. GDPR – Praktický průvodce implementací. 1.vyd. Praha: GRADA Publishing, 2017, 304 s. ISBN 978-80-271-0668-4.**

Vedoucí diplomové práce: **Ing. Zuzana Virglerová, Ph.D.**
Ústav podnikové ekonomiky

Datum zadání diplomové práce: **15. prosince 2017**

Termín odevzdání diplomové práce: **17. dubna 2018**

Ve Zlíně dne 15. prosince 2017




doc. Ing. David Tuček, Ph.D.
*děkan*

Ing. Petr Novák, Ph.D.
*ředitel ústavu*

# PROHLÁŠENÍ AUTORA
# BAKALÁŘSKÉ/DIPLOMOVÉ PRÁCE

**Prohlašuji, že**

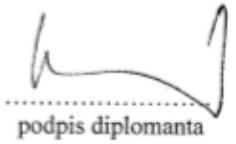
- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen na elektronickém nosiči v příruční knihovně Fakulty managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

1. že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
2. že odevzdaná verze diplomové/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 9.4.2018

Jméno a příjmení: LUCIE MIKELOVÁ



podpis diplomanta

ABSTRAKT

Cílem této diplomové práce je implementace Obecného nařízení o ochraně osobních údajů ve vybrané společnosti. V rámci řešení je analyzován současný stav zpracování a uchovávání osobních údajů ve vybrané společnosti. Na základě zjištěných informací z provedené analýzy je navržen projekt, jehož úkolem je odstranit současné nesoulady s Obecným nařízením a učinit jednotlivé kroky implementace tak, aby proběhla v daném časovém horizontu a došlo tak k zabránění případným sankcím. Výsledky této práce jsou podkladem pro aplikaci dané metody do podnikové praxe.

Klíčová slova: Obecné nařízení o ochraně osobních údajů, osobní údaj, účel zpracování, vnitřní předpis, klienti, zaměstnanci

## ABSTRACT

The main objective of this diploma thesis is the implementation of the General Data Protection Regulation in the selected company. The current state of processing and storage of personal data in the selected company was used within the solution.

On the basis of the information obtained from the analysis a project is designed to remove the current inconsistencies with the General Data Protection Regulation and to do the individual implementation steps in order to proceed in a given time horizon and to prevent potential sanctions. The results of this work are the basis for the application of the method into practice.

Keywords: General Data Protection Regulation, Personal Data, Purpose of Processing, Internal Regulation, Clients, Employees

Ráda bych touto cestou poděkovala vedoucí mé práce, paní Ing. Bc. Zuzaně Virglerové, Ph.D., za veškerou pomoc při zpracování mé práce, za odborné vedení, podnětné a motivující rady, připomínky a vstřícnost.

Dále bych chtěla poděkovat vedení a zaměstnancům vybrané společnosti, za umožnění zpracování diplomové práce a za věnování svého času při poskytování informací.

Největší díky patří mým rodičům, kteří mi umožnili studovat a byli pro mě vždy velkou oporou.

# OBSAH

# ÚVOD

Oblast ochrany osobních údajů se stává v současné době velmi diskutovaným tématem. Je tomu tak z důvodu neustálého rozmachu informačních a telekomunikačních technologií, ale především kvůli novému nařízení GDPR – General Data Protection Regulation. Toto Obecné nařízení o ochraně osobních údajů vstoupí v účinnost v Evropské unii v květnu letošního roku za účelem čelit současným výzvám souvisejícím s ochranou osobních údajů, a zároveň harmonizovat ochranu osobních údajů v rámci celé Evropské unie.

Je nutné si uvědomit, že ochrana osobních údajů je velmi důležitá, neboť každého člověka již od narození doprovází různé údaje, data, které jej svým způsobem identifikují. Jedná se o jméno, datum narození, národnost, či například náboženské vyznání nebo zdravotní stav, kdy některé z údajů mohou být natolik křehké, že jejich zcizení nebo případné zneužití by jedinci mohlo velmi ublížit. Tato diplomová práce je zaměřena právě na Obecné nařízení o ochraně osobních údajů, které má za úkol výrazně zvýšit ochranu osobních dat fyzických osob.

V teoretické části jsou nejdříve definovány základní pojmy vyplývající z problematiky zpracování osobních údajů, jakými jsou mimo jiné informace, data nebo například soukromí, jenž úzce souvisí právě s osobními daty každého jedince. Dále dochází k identifikaci jednotlivých druhů osobních údajů, kdy dochází k jejich rozdělení na reálné a anonymní údaje, identifikační, adresní, popisné a citlivé údaje.

Další kapitola teoretické části je zaměřena na zákon č. 101/2000 Sb., o ochraně osobních údajů. Je zde formulována jeho působnost, základní pojmy z něj vyplývající, dále jaké jsou povinnosti správce a zpracovatele při a během zpracování osobních údajů, také jaké práva smí uplatnit subjekt údajů. Následně dochází ke zmínění postavení a působnosti dozorového orgánu, kterým je pro Českou republiku Úřad pro ochranu osobních údajů.

Kapitola uzavírající teoretickou část je již zaměřena na samotné Obecné nařízení. Popisuje změny v souvislosti s daným nařízením, práva a povinnosti, základní pojmy a sankce.

V praktické části je provedena charakteristika vybrané společnosti, v níž dochází k jejímu představení, shrnutí základních informací a popisu portfolia služeb. Dále je provedena analýza současného systému ochrany osobních údajů, na základě níž byly zjištěny nesoulady s Obecným nařízením.

Poté následuje hlavní část diplomové práce, tedy část projektová, kdy na základě zjištěných nesouladů dochází k tvorbě časového harmonogramu aktivit potřebných k úspěšné implementaci nařízení, tedy především stanovení účelu pro jednotlivé osobní informace nebo například úprava vnitřního předpisu upravujícího pravidla pro ochranu osobních údajů.

V závěru práce je projekt zhodnocen z hlediska rizik, jeho přínosů a nákladů v souvislosti s implementací.

# CÍLE A METODY ZPRACOVÁNÍ PRÁCE

Hlavním cílem této diplomové práce je vypracování projektu implementace Obecného nařízení o ochraně osobních údajů v rámci vybrané společnosti. Hlavním důvodem zpracování projektu je nutnost zavedení tohoto nařízení, neboť vchází v účinnost 25. května 2018 a týká se všech společností, které zpracovávají osobní údaje Evropanů, tedy i společnosti analyzované v rámci této diplomové práci.

Pro splnění daného cíle je nejprve zapotřebí provést průzkum literárních pramenů a na základě tohoto průzkumu zpracovat teoretické poznatky související s problematikou zpracování osobních údajů.

Dalším dílčím cílem je zhodnocení současného, výchozího, stavu společnosti, tedy jaký je její současný systém ochrany osobních údajů, analýzy vnitřních předpisů, identifikaci jednotlivých osobních údajů a naleznutí nesouladů s Obecným nařízením. Toto zhodnocení je v práci provedeno prostřednictvím GAP analýzy.

V rámci analytické části je proveden kvalitativní výzkum sběru informací ve formě analýzy dokumentů. Jsou identifikovány hlavní rozdíly v postupech společnosti v oblasti správy a zpracování osobních údajů a jejich ochrany. Poté je provedena syntéza jednotlivých poznatků a následně ucelená implementace kompletních požadavků Obecného nařízení do společnosti. Pro vytvoření časového harmonogramu je použita metoda CPM (Critical Path Method).

Součástí zhodnocení projektu je riziková analýza provedená prostřednictvím jednoduché polokvantitativní metody PZH.

# I. TEORETICKÁ ČÁST

# 1 VYMEZENÍ ZÁKLADNÍCH POJMŮ

V následující kapitole jsou zpracovány základní pojmy související s problematikou osobních údajů.

## 1.1 Osobní údaj

Jedná se o informace vypovídající o soukromí každého z nás a často mohou prozradit více, než si člověk vůbec přeje. Tyto informace se týkají osob, zálib, zvyklostí, vlastností nebo názorů a majetkových poměrů. Mimo jiné mohou vypovídat o tom, jaké jsou vztahy jednoho člověka k ostatním, o jeho zdravotním stavu a stylu života. Osobním údajem tedy rozumíme jakýkoliv údaj týkající se naší osoby. (Matoušová, Hejlík, 2008, s. 18)

Osobní údaje jsou informace, které přímo nebo nepřímo mohou identifikovat jednotlivce a obsahuje konkrétní on-line identifikátory, jakými jsou například IP adresy, soubory cookies, digitální otisky prstů a údaje, které by mohly identifikovat jednotlivce. (Goddard, 2017, s. 703)

Maštalka (2008, s. 13) osobní údaj znamená každou informaci týkající se identifikované nebo identifikovatelné fyzické osoby. Tato definice je rovněž přebírána zákonem o ochraně osobních údajů. Za identifikovanou či identifikovatelnou se osoba považuje, pokud ji lze přímo nebo nepřímo určit, zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro její fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Pokud se osobní údaje dostanou do nepovolaných rukou, mohou vzniknout osobě, s níž osobní údaje souvisí, patřičné problémy. Podle Matoušové a Hejlíka (2008, s. 20) je jedním z nejvíce nebezpečných příkladů zneužití osobních údajů tzv. „krádež identity“. V tomto případě člověk, který se neoprávněně zmocní dokumentů týkajících se osobních údajů jiné osoby a jejím jménem těchto dokumentů neoprávněně užívá, může způsobit majetkovou újmu nebo také spáchat jinou trestnou činnost, která může mít špatné následky na zneužitou osobu. Dalším nebezpečím mohou být různé formy narušování soukromí. Jedná se o případy méně závažné, přičemž někomu vadí více a někomu méně. Jedná se například o obtěžování nevyžádanou adresnou reklamou, kdy její odesílatel zná kromě kontaktních údajů i další osobní údaje, které odesílateli napoví, o jaký druh zboží či službu bychom mohli mít zájem. V současné době se jedná o velmi rozšířený problém (reklamy na google či na sociálních sítích).

## 1.2 Informace

Za informaci jsou považována přesná a včasná data, jež mají určitou specifikaci a jsou organizována za účelem prezentace v kontextu dávajícím smysl a význam. Cílem informací je zvýšit porozumění a zároveň snížit nejistotu. Každá informace má svoji důležitost, protože je schopná ovlivnit chování, rozhodování a v neposlední řadě i výsledky. Důležité je ovšem mít informaci jako celek, jelikož pouhá její část je bezcenná. (Beneš, 2010, s. 11)

V současné době plné informačních technologií slouží informace ke zpracování, skladování a přenášení dat. V běžném životě jsou informace přenášeny a vyměňovány za účelem získání či sdělení nových skutečností. (Beneš, 2010, s. 12)

Obecně je informace považovaná jako proces vnímání a poznávání vlastností a uspořádání objektů kolem nás. Aby dostála své definici, musí mít následující vlastnosti:

- pravdivost;

- srozumitelnost;

- včasnost;

- relevantnost;

- etičnost – tato vlastnost platí pouze v rámci mezilidských vztahů. (Beneš, 2010, s. 21)

## 1.3 Data

Obecně jsou data výrazem pro údaje, jež se používají pro popis jevu nebo vlastnosti pozorovaného objektu. Jedná se například o číselné hodnoty z tabulky. Data jsou přitom podmnožinou informace, dokonce tvoří jakousi vstupní surovinu pro vytvoření plnohodnotné informace. (Beneš, 2010, s. 11)

Vlastnosti dat:

- nejsou závislá na uživateli, ve většině případů je pro ně typické, že odrážejí současný stav reality;

- vždy slouží pro zjednodušení komplexnosti reality, tzn., že jsou nekompletní, což při rozvoji informačních systémů vede k procesu různých změn a inovací a dochází k dodání dat nových, či zjemnění nebo zpřesnění dat starých;

- obsahují velké množství detailů;

- mění se velkou rychlostí a v poměrně častých intervalech;

- u většiny případů existuje možnost opakovaně a objektivně ověřit správnost a přesnost dat (tzv. verifikovatelnost dat). (Hronek, 2007, s. 20)

Bawden (2017, s. 154) zmiňuje termín *metadata,* neboli data o datech. Jedná se o krátké strukturované popisy informačních zdrojů. Jejich hlavním účelem je identifikace, vyhledání, používání a správa informačních zdrojů. Zahrnuje to vyhledání zdrojů, nalezení konkrétní požadované jednotky prozkoumáním nebo prohlížením, její zobrazení, rozhodnutí pravděpodobné užitečnosti, posouzení právních otázek.

## 1.4 Biometrické data

Osobní údaje vyplývající z konkrétního technického zpracování týkajícího se fyzických, fyziologických nebo behaviorálních vlastností fyzické osoby, umožňující nebo potvrzující jedinečnou identifikaci této fyzické osoby (např. obrazy obličeje, daktyloskopické údaje)

Stále častěji se používají jako metoda autentizace a často i ve spojení s jinými údaji, které by měly být chráněny. (Calder, 2016, s. 10)

## 1.5 Soukromí

Jedním ze základních pojmů je i pojem soukromí, neboť se zde mluví o osobních datech, tedy datech a údajích týkajících se soukromého života jedinců.

Pod pojmem soukromí se skrývá vícero věcí, převážně se jedná o ochranu toho, co je považováno za soukromé (v porovnání s veřejností) a to následujícími způsoby:

- pokud se veřejnost považuje za odkaz na vládní autoritu, obec nebo společnost obecně; soukromé věci jsou poté chápany jako neúčelné nebo takové, které nesouvisí s veřejným pořádkem a to z důvodu toho, že se přímo týkají rodinného života nebo domova.

- nebo je veřejnost brána jako něco, co je společné, exponované, otevřené druhým lidem, a tedy naopak soukromé je to, co patří do uzavřeného prostoru, neexponované, skryté, důvěrné, tajné, obecně nepřístupné jiným lidem. (González Fuster, 2014, s. 22)

Dále lze pojem soukromí chápat jako něco, co se dotýká každého jedince, co je pro něj osobní a jemu vlastní; proto je důležité projevovat úctu k soukromému životu, respektovat to, že každý má právo žít tak, jak si on sám zvolí, na rozdíl od věcí, co jsou kontrolované a odcizené od společnosti. (González Fuster, 2014, s. 22)

# 2 PRÁVNÍ ZAKOTVENÍ OCHRANY OSOBNÍCH ÚDAJŮ

V následující kapitole dochází k vymezení základních pojmů v souvislosti s osobními údaji, konkrétně jsou zde definovány typy osobních údajů, jimiž jsou reálné a anonymní údaje, identifikační údaje, adresní údaje, popisné údaje a citlivé údaje.

## 2.1 Reálné a anonymní údaje

Pro správné pochopení pojmu osobní údaj je potřeba brát v úvahu spojení mezi reálnou fyzickou osobou a hodnotou určitého údaje. Názory, že telefonní číslo nebo e-mailová adresa nejsou osobním údajem, jsou velmi zavádějící, neboť k jejich vzniku dochází v případě, že je opomenuta vazba na reálnou fyzickou osobu. Například určité telefonní číslo můžeme považovat za osobní údaj až v případě, že je uvedeno spojení, z něhož jasně vyplývá, že reálná fyzická osoba vlastní mobilní telefon s daným číslem. (Matoušová, Hejlík, 2008, s. 28)

Anonymní údaje jsou úzce spjaty s termínem „anonymizovat“, přičemž tento proces znamená úpravu osobního údaje do takového stavu, kdy se z něj stane údaj anonymní. Anonymizace může být částečná nebo úplná. O plně anonymním údaji mluvíme tehdy, pokud u něj nikdo není schopen určit subjekt údaje. U částečně anonymního údaje tento subjekt je možno určit, ale pouze za splnění určitých podmínek. (Žůrek, 2017, s. 41)

K anonymizování osobních údajů přitom dochází nejvíce v oblasti statistiky a vědeckého výzkumu. Jako příklad lze uvést zpracování citlivých osobních údajů týkajících se zdravotního stavu v souvislosti s lékařským výzkumem. V tomto případě je však anonymizování nezbytné, a to z důvodu ochrany osobních údajů pacienta. (Matoušová, Hejlík, 2008 s. 33)

## 2.2 Identifikační údaje

Za základní identifikační údaj je považováno *jméno* a *příjmení* dané osoby. Používání těchto základních identifikačních údajů je nejen právem každého z nás, ale zároveň i povinností při vystupování před orgány veřejné moci. Jedná se o osobní údaje v případě, že existuje vazba mezi nimi a reálnou fyzickou osobou. Právo na ochranu těchto údajů vzniká, pokud jsou ve spojení s dalšími osobními údaji. Toto právo však není platné například v zaměstnání, kde tyto údaje slouží pro komunikaci uvnitř kolektivu. Za osobní údaj pak nejsou pokládána jména a příjmení literárních a filmových osob.

Matoušová a Hejlík (2008, s. 54) upozorňují na fakt, že nelze používat jména zkomolená, zdrobnělá a domácká. Muži si nemohou zapsat jména ženská a naopak, rovněž není možné, aby sourozenci, kteří mají společné rodiče, byli pojmenováni stejně.

Dalším identifikačním údajem je *datum a místo narození.* Jedná se o údaje, které jsou zjišťovány a zaznamenávány úředně. Jejich součást tvoří číselné hodnoty a zeměpisné názvy. Údaje nemohou být měněny. Den, měsíc a rok narození jsou zapsány do matriční knihy a společně s místem narození se zapisují do rodného listu. Mezi doplňkové údaje se do této skupiny řadí i datum a místo úmrtí, pohřbu a uložení ostatků. (Matoušová, Hejlík, 2008, s. 58)

Následující skupinu identifikačních údajů tvoří identifikační čísla sloužící ke zjištění totožnosti subjektu. Jedná se o rodné číslo, daňové identifikační číslo, číslo účtu v případě finanční instituce a další. Rodné číslo je každému přiděleno při narození a jedná se o konstantní osobní údaj, z něhož je možné vyčíst informaci o datu narození a pohlaví. Platí, že dva lidé nemohou mít stejné rodné číslo. (Matoušová, Hejlík, 2008, s. 60)

Mezi další osobní identifikační čísla patří číslo občanského průkazu, podle něhož lze určit osoby, kterým byl průkaz vydán. Dále se jedná o číslo cestovního dokladu, podle něhož je možné identifikovat jak občany České republiky, tak cizince. Rovněž lze pomocí něj v příslušné evidenci vyhledat pouze osoby, jimž byl cestovní doklad vydán. V neposlední řadě se jedná o číslo služebního průkazu (u policistů a strážníků obecní policie slouží služební identifikační číslo) a osobní číslo zaměstnance. (Matoušová, Hejlík, 2008, s. 68)

## 2.3 Adresní údaje

Mezi další osobní údaje patří údaje adresní. Slouží především ke kontaktování osob pomocí uvedené kontaktní adresy trvalého pobytu či adresy pro doručování, ale také pomocí telefonního kontaktu, pod nímž si můžeme představit například pevnou linku, mobilní telefon, fax, adresu telefonické pošty apod. (Matoušová, Hejlík, 2008, s. 70)

**Místní doručovací adresy**

Mezi tyto se řadí adresa trvalého pobytu, přičemž každý občan může mít pouze jednu adresu trvalého pobytu na území České republiky. Obvykle se jedná o místo, kde daný člověk vyrůstal nebo zde má současnou rodinu, zaměstnání či dům. Dále se uvádí i adresa přechodného bydliště, ze zákona tuto adresu hlásit občan nemusí. Třetí obvyklou adresou

sloužící ke kontaktování a fyzické doručování je adresa zaměstnavatele. (Matoušová, Hejlík, 2008, s. 70)

**Účastnické adresy**

Toto označení není závislé na fyzické podstatě adresy, ale vyjadřuje velmi podstatný znak, jímž se odlišují adresy od předchozích adres. Existence adresy je vázána na účastnický vztah, který vzniká většinou vůči poskytovateli jakékoliv služby. Mezi tyto řadíme telefonní číslo – účastnické telefonní číslo, v tomto případě je však důležité dbát na dodržení telekomunikačního tajemství. Dále se jedná o faxové číslo, volací značku v radiokomunikačním spojení, adresa telekomunikační sítě a služby, adresa elektronické pošty. (Matoušová, Hejlík, 2008, s. 72)

## 2.4 Popisné údaje

Jako popisný údaj je brán každý údaj, který vytváří celkový obraz osoby. Jsou jimi například údaje o dosaženém vzdělání, zaměstnání, o majetkových poměrech, o zvycích a zájmech fyzických osob a další. Je však obtížné určit, co už je osobním údajem. O osobní údaj se jedná tehdy, pokud existuje úmysl používat je k předem stanovenému účelu. (Matoušová, Hejlík, 2008, s. 75)

Popisné údaje jsou rozdělovány jednak na ty, jež se běžně používají k identifikaci, kde jako příklad může být uveden titul před nebo za jménem. Dále na údaje užívané pro hodnocení subjektu údajů, jako je například označení povolání nebo aktuální vykonávané profese. (Matoušová, Hejlík, 2008, s. 76)

## 2.5 Citlivé údaje

Jedná se o skupinu údajů, které jsou považovány vůči subjektu údajů za citlivé a jimž je poskytnuta ještě zvýšená ochrana při jejich zpracování.

Patří sem údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Jsou zde zařazeny i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby. (Česko, 2000, s. 1521-1532)

# 3 ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ

Základním právním předpisem, jenž upravuje ochranu osobních údajů v České republice, je zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů. Tento zákon bude nahrazen tzv. Obecným ustanovením GDPR – General Data Protection Regulation, o němž pojednává jedna z kapitol níže. Toto obecné ustanovení vstoupí v účinnost, a tedy nahradí, či spíše rozšíří, dosavadní zákon o ochraně osobních údajů, dne 25.5.2018. V této části však bude práce zaměřena pouze na dosavadní zákon o ochraně osobních údajů.

Účelem zákona je zajistit ochranu osobních údajů, rovněž také způsob, jakým jsou tyto údaje zpracovávány v České republice a v neposlední řadě předávání osobních údajů do zahraničí a úprava vztahů vznikajících v souvislosti s osobními údaji.

V zákoně č. 101/2000 Sb. je zakotveno vymezení jeho působnosti a pojmů týkajících se dané problematiky, práva a povinnosti související se zpracováním osobních údajů, likvidace osobních údajů, ochrany práv subjektu údajů, nápravy nemajetkové újmy či škody a také předávání osobních údajů do dalších států. Na základě zákona došlo ke zřízení Úřadu pro ochranu osobních údajů, o němž bude také pojednávat jedna z kapitol této práce.

## 3.1 Vymezení pojmů

V rámci tohoto zákona jsou jednak definovány základní pojmy jako osobní údaj, citlivý a anonymní údaj, jejichž definice už v rámci této práce zmíněná je. Dále jsou zde definovány tyto pojmy:

- *subjekt údajů*, jímž je fyzická osoba, k níž se osobní údaje přímo vztahují;

- *zpracování osobních údajů*, kdy se jedná o operaci či soustavu operací prováděných správcem nebo zpracovatelem, ať už automatizovaně, či jinými prostředky;

- *shromažďování osobních údajů*, což je systematický postup či soubor postupů, kdy cílem je získat osobní údaje za účelem jejich dalšího uložení pro jejich další zpracování;

- *uchovávání osobních údajů*, jedná se o udržování údajů v takové podobě, aby mohly být dále zpracovávány;

- *blokování*, tedy operace nebo soustava operací, prostřednictvím kterých dojde k omezení způsobu či prostředků ke zpracování osobních údajů a to po předem stanovenou dobu;

- *likvidace osobních údajů*, čímž se rozumí fyzické zničení nosiče osobních údajů, fyzické vymazání popřípadě přerušení jakéhokoliv dalšího zpracování;

- *správce,* jímž je ten, kdo určí, proč a jakým způsobem se budou osobní údaje zpracovávat, samotné zpracování provádí a odpovídá za něj;

- *zpracovatel*, který je stanoven na základě zvláštního zákona nebo jej pověří správce, aby osobní údaje zpracovával podle tohoto zákona;

- *zveřejněný osobní údaj*, kdy se jedná o takový údaj, jenž byl zpřístupněn prostřednictvím hromadných sdělovacích prostředků či jiným veřejným sdělením;

- *evidence nebo datový soubor osobních údajů*, tedy jakýkoliv soubor osobních údajů, jenž je uspořádán či zpřístupněn na základě společných, popřípadě zvláštních podmínek;

- *souhlas subjektu údajů*, kdy subjekt údajů projeví svobodně a vědomě vůli, že souhlasí se zpracováním svých osobních údajů;

- *příjemce*, přičemž jím je každý ze subjektů, jimž jsou osobní údaje zpřístupněny. (Bartík, Janečková, 2013, s. 159)

## 3.2 Působnost zákona

Zákon o ochraně osobních údajů se vztahuje na ty osobní údaje, které jsou zpracovávány státními orgány, dále orgány územní samosprávy, jiné orgány veřejné moci a fyzické či právnické osoby. Spadá pod něj i veškeré zpracování osobních údajů, jak automatizované zpracování, tak prostřednictvím jiných prostředků. (Bartík, Janečková, 2013 s. 157)

Na druhou stranu se zákon nevztahuje na zpracovávání těch osobních údajů, jež jsou prováděny fyzickými osobami pro jejich vlastní potřeby. Zde se jedná o záležitosti v souvislosti se soukromým a rodinným životem a údaje související s těmito záležitostmi nejsou určeny ke zveřejnění ani pro účely podnikání (např. se může jednat o seznamu různých výročí a jubileí jednotlivých členů rodiny a příbuzných). (Bartík, Janečková, 2013 s. 157)

Dále se zákon netýká nahodilého shromažďování osobních údajů a to za podmínky, že tyto údaje nebudou dále zpracovány. O nahodilé zpracování se jedná v případě, že údaje nejsou nijak tříděny, pokud pro jejich shromažďování nedává podnět správce, ale podnět přichází zvenku. (Bartík, Janečková, 2013 s. 157)

Pro účely statistické a archivní je stanoveno zpracování osobních údajů zvláštními zákony. Nejedná se přitom o odstranění z působnosti zákona o ochraně osobních údajů, ale pouze o řešení otázky obecného a zvláštního zákona. V případě, že součástí zákonu o státní statistické službě nebo zákonu o archivnictví a spisové službě je zvláštní úprava, má přednost před obecnou úpravou, v opačném případě spadají i tyto případy pod zákon č. 101/2000 Sb. Podmínky pro zpracování tohoto typu údajů musejí být stanoveny příslušnými zákony, nestačí zde pouze prohlášení správce (např. o vedení archivu).

Pro vědecké účely není rovněž potřeba souhlasu od subjektu údajů. Ihned, jakmile je to možné, musí se z těchto údajů stát údaje anonymní, tedy musejí být převedeny do takové podoby, kdy je nelze již žádným způsobem spojit se subjektem údajů. Je také potřeba tyto údaje zabezpečit proti potenciálnímu nelegálnímu zneužití. (Bartík, Janečková, 2013 s. 157)

## 3.3 Povinnosti při/během zpracování osobních údajů

Povinnosti týkající se zpracování osobních údajů se týkají správce a zpracovatele, ale také jejich zaměstnanců a jiných osob, které osobní údaje zpracovávají na základě smluvního vztahu se správcem nebo zpracovatelem.

Správce a zpracovatel mají v rámci zpracování osobních údajů stejné povinnosti. Pokud zpracovatel zjistí, že správce porušuje povinnosti, musí jej na tuto skutečnost upozornit a dokončit práci za něj. Pokud to neudělá, odpovídá za vzniklou škodu společně se správcem. U zaměstnanců a jiných osob je povinnost zpracovávat osobní údaje pouze za podmínek a v takovém rozsahu, jaký jim stanovili správce nebo zpracovatel. Velmi důležitou podmínkou je pak zachování mlčenlivosti, a to i poté, co dané osoby své zaměstnání ukončí. (Bartík, Janečková, 2013, s. 160-162)

Zákon o ochraně osobních údajů konkrétně vymezuje povinnosti jak správce, tak zpracovatele.

## 3.4 Práva subjektu údajů

Tyto práva jsou rovněž vymezena v rámci Zákona o ochraně osobních údajů.

Jako jedno z nejzásadnějších práv je považováno právo subjektu údajů obrátit se na ÚOOÚ s žádostí o přijetí nápravy. S takovouto žádostí přichází subjekt v okamžiku, kdy zjistí nebo se domnívá, že správce či zpracovatel zpracovávají jeho osobní údaje v rozporu

s ochranou osobního a soukromého života, nebo k tomuto zpracovávání dochází v rozporu se zákonem.

Za základní právo se pak považuje právo být informován o tom, kdo zpracovává osobní údaje subjektu a za jakým účelem.

Mezi další práva subjektu údajů patří:

- právo bránit se podle ustanovení občanského zákoníku

- právo na přístup k osobním údajům, které o něm správce či zpracovatel zpracovávají

- právo domáhat se ochrany svých práv vůči správci

- právo obrátit se na ÚOOÚ v případě, že došlo k porušení povinností dle zákona (Česko, 2000, s. 1521-1532)

## 3.5 Sankce

Při nedodržení zákona o ochraně osobních údajů mohou být uděleny sankce, jejichž výše jsou uvedeny v § 44 jako přestupky a v § 45 jako jiné správní delikty.

Správce nebo zpracovatel spáchají přestupek v případě, že u nich dojde k porušení některé z povinností, které jim zákon ukládá. Výše pokuty může být až 1 000 000 Kč a to v případě, kdy správce nebo zpracovatel zpracovává buď nepřesné údaje, údaje, k nimž nedostali souhlas od subjektu údajů nebo nedošlo ke stanovení účelu, prostředků nebo způsobu zpracování. Dále může být uložena pokuta až ve výši 5 000 000 Kč, v případě že dojde k porušení povinností týkajících se zpracování citlivých údajů nebo nastane ohrožení většího počtu osob tím, že správce nebo zpracovatel neoprávněně zasáhne do soukromého a osobního života subjektu údajů. (Česko, 2000, s. 1521-1532)

V případě správních deliktů může pokuta sahat až k 10 000 000 Kč, zde se jedná o fyzické či právnické osoby podnikající na základě zvláštních předpisů. Pokud u takovýchto osob dojde k porušení nebo nedodržení povinností při zpracování osobních údajů, jedná se o správní delikt a je jim udělena výše zmíněná pokuta. (Česko, 2000, s. 1521-1532)

# 4 ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Dle autorů Matoušové a Hejlíka (2008, s. 327) je činnost orgánů ze zákona dohlížejících na dodržování povinností při zpracování osobních údajů jedním ze základních stavebních kamenů. Takovým orgánem, zřízeným v České republice na základě mezinárodních předpisů, je Úřad pro ochranu osobních údajů, jehož sídlo je v Praze.

Smyslem této kapitoly je popsat postavení a působnost Úřadu pro ochranu osobních údajů (ÚOOÚ), jehož činnost je vymezena zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a některými dalšími zákony.

Jedná se o nezávislý orgán, jehož základní činnosti jsou:

- držet dozor nad tím, aby byly plněny povinnosti spojené se zpracováním osobních údajů, stanovené zákonem;

- vedení registru, v němž jsou uvedeny povolené zpracování osobních údajů;

- v případě, že nastane porušení zákona, je jeho úkolem přijímat podněty a stížnosti z řad občanů;

- poskytnutí konzultací týkající se problematiky ochrany osobních údajů (Působnost úřadu, ©2013)

## 4.1 Postavení a působnost

Jak již bylo řečeno, jedná se o nezávislý orgán, což znamená, že ve své činnosti postupuje nezávisle a musí se řídit pouze na základě zákonů nebo jiných právních předpisů. Aby mohlo dojít k zasažení do jakékoliv činnosti ÚOOÚ, musí tomu tak být pouze na základě zákonu. Vysoká důležitost jeho statutu je především z důvodu toho, aby byla zajištěna nezávislost při dozoru nad zpracováním osobních údajů.

Matoušová a Hejlík (2008, s. 331) uvádějí, že postavení a působnost ÚOOÚ je stanovena zákonem o ochraně osobních údajů koncentrovaně v §2 a to následujícím způsobem: „*kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem a další kompetence stanovené zvláštním právním předpisem, mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropských společenství a vykonávání působnosti dozorového úřadu pro oblast ochrany osobních údajů vyplývající z mezinárodních smluv, které jsou součástí právního řádu“.*

## 4.2 Kontrolní činnost

Kontrolní činnost ÚOOÚ je podle zákona prováděna inspektory a pověřenými dalšími zaměstnanci. Do této činnosti je zapojen i samotný předseda.

Před zahájením samotné kontroly musí dojít k oznámení statutárnímu orgánu kontrolovaného. Kontrolovanému musí také být oznámen ještě před zahájením předmět kontroly, který vychází z obsahu stížnosti nebo jiného podnětu, popřípadě ze znění plánu kontrolní činnosti Úřadu. Kontrolovanými jsou poté ústřední a jiné orgány státní správy, ostatní veřejnoprávní subjekty, banky, dopravní podniky provozující městskou hromadnou dopravu, veřejné knihovny, obce a další. (Matoušová, Hejlík, 2008, s. 334)

### 4.2.1 Práva a povinnosti kontrolujících

Povinností kontrolujícího je prokázat totožnost příslušným dokladem, oznámení zahájení kontroly po splnění příslušných, výše uvedených, povinností, chránit přiložené doklady a zabránit jejich případnému odcizení, poškození či zničení a předat je zpět do rukou majiteli ihned, jak to bude možné. V průběhu kontroly je třeba analyzovat skutečný stav a udržovat mlčenlivost. Dále mají kontrolující právo na to, aby vstoupili do jakýchkoliv prostor, které patří zpracovateli osobních údajů.

Je nutné, aby kontrolujícím byly poskytnuty pravdivé a úplné informace týkající se zjišťovaných skutečností a v souvislosti s tím i doložena písemná zpráva, kde jsou uvedeny informace o odstranění případných nedostatků.

Kontrolující musí na konci kontroly sestavit kontrolní protokol, v němž jsou uvedeny výsledky kontroly. Součástí takového protokolu by měl být výčet zjištěných skutečností spolu s uvedenými nedostatky, dále označení porušených právních předpisů a určení lhůt, do nichž musí být uskutečněna náprava. Po sestavení takového předpisu musí dojít k jeho představení kontrolovaným, spolu s předáním stejnopisu. Může nastat i situace, kdy kontrolovaný odmítne seznámení s protokolem a v takovém případě i tato skutečnost musí být zaznačena v protokolu. (Matoušová, Hejlík, 2008, s. 335)

## 4.3 Ostatní činnosti

Matoušová a Hejlík (2008, s. 349) zmiňují i ostatní činnosti ÚOOÚ, mezi něž patří:

- příprava a zveřejňování výroční zprávy, která je následně předložena Poslanecké sněmovně a Senátu Parlamentu České republiky a vládě;

- zpracování Věstníku, v němž je zveřejněná výše zmíněná výroční zpráva a jeho součástí je soupis všech zaregistrovaných povolených zpracování osobních údajů a také těch registrací, které již byly zrušeny;

- tvorba publikace Bulletin Úřadu na ochranu osobních údajů, která vychází čtvrtletně a jejím hlavním úkolem je informovat a přinášet zajímavosti z oblasti problematiky osobních údajů

- ukládání sankcí, přičemž pokuty jsou vymáhány finančním úřadem a vybírány ÚOOÚ.

# 5 GDPR – GENERAL DATA PROTECTION REGULATION

Toto obecné zařízení bude sloužit jednak subjektům, které přímo provádí zpracování osobních údajů (správci osobních údajů) a jednak těm, kteří pro správce tyto osobní údaje zpracovávají (zpracovatelé). Nařízení bude platit jak pro fyzickou osobu, tak i pro dozorové úřady, mj. Úřad pro ochranu osobních údajů.

Autorka González Fuster (2014, s. 111) uvádí, že první kroky Evropské unie k tomu, aby docházelo k regulaci práce s osobními údaji a údaji celkově, spadají již do počátku 70. let. Poté se postupně vykrystalizovala legislativa týkající se problematiky osobních údajů až po přijetí Charty základních práv EU v roce 2000.

Obecné ustanovení je vedeno filozofickým přístupem k ochraně údajů, který je založen na konceptu soukromí jako zásadního lidského práva (stejně jako je zakotveno v Chartě práv EU), nařízení bude mít velký globální dopad. Vztahuje se na osobní údaje všech obyvatel EU bez ohledu na to, kde je umístěno zpracování. (Goddard, 2017, s. 705)

Obecné zařízení je založeno na dvou nových přístupech:

- princip odpovědnosti správce

- přístup založený na riziku

*Princip odpovědnosti* přináší správci odpovědnost za dodržení zásad zpracování uvedených v článku 5 odst. 1 Obecného nařízení. Správce musí být schopen tento soulad i doložit, k čemuž mu mohou sloužit kodexy, osvědčení nebo certifikace, případně záznamy o činnostech zpracování. (Nezmar, 2017, s. 29)

*Princip založený na riziku* znamená to, že správce již od prvopočátku musí brát v potaz povahu, rozsah, kontext a účel zpracování, a zároveň přihlížet k rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů. Jinými slovy je tento princip aplikován v případě, kdy by zpracování osobních údajů či porušení zabezpečení znamenalo riziko, nebo dokonce vysoké riziko pro práva a svobody fyzické osoby. Princip je uplatňován zejména u nových povinností, jimiž jsou např. ohlašování (oznamování) případů porušení zabezpečení osobních údajů ÚOOÚ nebo povinné konzultace s ÚOOÚ, jejichž aplikace je vázána na přítomnost rizika či vysokého rizika pro práva a svobody fyzických osob. (Nezmar, 2017, s. 29)

Obecné ustanovení má být účinné i v oblasti působnosti a přenosů dat přes zahraničí, kdy dochází k aktualizaci právních závazků s některými novými pojmy. Zároveň je ale potřeba

neustálý pokrok v této oblasti, neboť v dalších letech je velmi pravděpodobné to, že společnost bude čelit novým situacím a technologiím, které budou vyžadovat opět nové interpretace zákonů nebo vytváření zákonů nových. (Bu-Pasha, 2017, s. 225)

## 5.1 Osobní údaje podle GDPR (základní pojmy)

V následující podkapitole jsou popsány základní pojmy týkající se problematiky zpracování osobních údajů tak, jak je definuje samo Obecné nařízení.

### 5.1.1 Zpracování osobních údajů

*Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.* (Nezmar, 2017, s. 31)

Zpracování osobních údajů není pouze jakékoli nakládání s osobním údajem, jedná se o mnohem sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a určitého pohledu tak činí systematicky. Pojem zpracování má stejný význam, jako měl v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

### 5.1.2 Osobní údaj

*Každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů).* Tato definice je de facto stejná, jako její znění v zákoně o ochraně osobních údajů a o změně některých zákonů. Identifikovatelnou osobou je myšlena fyzická osoba, která může být přímo či nepřímo identifikována, zejména prostřednictvím odkazu na určitý identifikátor, kterým může být např. jméno, číslo, síťový identifikátor), nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. (Nezmar, 2017, s. 31)

Součástí Obecného nařízení je i definice hlavních pojmů, které jsou obsaženy v článku 4 odst. 1 tohoto nařízení:

**- Subjekt údajů -** fyzická osoba, jíž se osobní údaje týkají (nikoliv právnická osoba). Údaje vztahující se k právnické osobě nejsou osobními údaji.

**- Správce -** subjekt (nerozhoduje, jaké formy), který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá.

**- Zpracovatel -** subjekt, kterého si najímá správce, aby pro něj prováděl s osobními údaji zpracovatelské operace. Od správce se liší tím, že v rámci činností pro správce může provádět pouze takové zpracovatelské operace, kterými jej správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen. (Nařízení Evropského parlamentu a Rady 2016/679)

## 5.2 Práva a povinnosti

Nulíček a kol. (2017, s. 467) ve svém díle zmiňují, že každý subjekt má právo na to, aby podal stížnost u dozorového úřadu v případě, že se domnívá, že došlo při zpracování jeho osobních údajů k porušení Obecného nařízení (stejně jako tomu bylo doposud v rámci zákona o ochraně osobních údajů). Stejně tak se může subjekt obrátit i na soud s žalobou proti správci či zpracovateli, pokud nastane situace, kdy se poruší práva v důsledku zpracování jeho osobních údajů.

Každý, tedy správce, zpracovatel i subjekt, má právo napadnout závazné rozhodnutí dozorového úřadu, které se ho týká.

### 5.2.1 Zásady Obecného nařízení

Goddard (2017, s. 703) uvádí základní zásady Obecného nařízení:

*Zákonnost, korektnost, transparentnost* – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů dostatečně zřetelně

*Omezení účelu* – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely

*Minimalizace údajů* – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro nějž jsou zpracovávány

*Přesnost*

*Omezení uložení* – uložení ve formě umožňující identifikaci subjektu údajů pouze po nezbytnou dobu pro dané účely, pro něž jsou zpracovávány

*Integrita a důvěrnost* – technické a organizační zabezpečení údajů

Nezmar (2017, s. 33) více rozvádí *přesnost*, kdy podle něj musejí data být přesná a v případě potřeby aktualizovaná. Také musí dojít k přijetí všech rozumných opatření, aby osobní údaje, jež jsou nepřesné v souvislosti s účelem jejich vynaložení, byly co nejdříve možný termín vymazány nebo opraveny. V případě *omezení uložení* dodává, že data musejí být uloženy ve formě, která umožňuje identifikaci subjektu údajů po dobu ne delší, než je nezbytně nutné pro účely jejich zpracovávání. Osobní údaje je přitom možno uložit po delší dobu za předpokladu, že se zpracovávají pouze pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely za předpokladu provedení příslušných technických a organizačních opatření považovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů. Poslední zásadu, *integritu a důvěrnost,* rozvádí tak, že osobní data musejí být zpracovávány takovým způsobem, který by zajistil jejich důsledné zabezpečení, včetně jejich ochrany prostřednictvím vhodných technických nebo organizačních opatření před případným neoprávněným nebo protiprávním zpracováním, dále pak před možnou ztrátou, zničením či jejich poškozením.

Mimo uvedených šesti obecných zásad je nutno dodat, že ochrana dat podle návrhů a výchozího nastavení je jádrem GDPR.

Dodržování těchto zásad je pro správce nejen zásadní, ale znamenají pro něj i povinnost plynoucí z článku 5 odst. 2 Obecného nařízení, v němž je stanovena odpovědnost správce za jejich dodržování a zároveň uvedena i povinnost pro správce, který musí být schopen dodržování těchto zásad doložit. Jedná se o vyjádření tzv. principu odpovědnosti správce. (Obecné nařízení o ochraně osobních údajů prakticky, ©2017)

Aby mohl správce zpracovávat legálně osobní údaje, musí k tomu mít právní důvody zpracování osobních údajů, ty pro něj znamenají oprávnění ke zpracování. Vzhledem k tomu, že osobní údaj může správce zpracovávat pro různé účely, potřebuje právní důvod ke každému z těchto účelů. V případě, že správce pozbude poslední právní důvod ke zpracování osobních údajů, musí dojít k jejich likvidaci. (Goddard, 2017, s. 703)

### 5.2.2 Právní důvody pro zpracování osobních údajů subjektu údajů

Mohou být zpracovávány, pokud je přítomen alespoň jeden z následujících právních důvodů:

- subjekt údajů udělil souhlas pro jeden či více konkrétních účelů;

- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

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

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

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

- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů. (Česko, 2000, 1521-1532)

## 5.3 DPO – Data Protection Officer

Důležitou roli v rámci GDPR bude hrát rovněž DPO neboli v českém jazyce – Pověřenec pro ochranu osobních údajů, který bude důležitým pilířem v rámci prokazování souladu s Obecným nařízením. Jako jeho hlavní úkol bude monitorování souladu zpracování osobních údajů s povinnostmi, jež vyplývají z nařízení, dále bude provádět interní audity, školit pracovníky a v neposlední řadě komplexně řídit agendu interní ochrany dat. (Obecné nařízení o ochraně osobních údajů prakticky, ©2017)

Pověřenec pro ochranu osobních údajů však není nutný ve všech případech. Povinnost jej jmenovat nastává v následujících třech případech:

1. V případě, že zpracování je prováděno orgánem veřejné moci či veřejným subjektem (s výjimkou soudů);

2. Hlavní činnost správce nebo zpracovatele spočívá v operacích zpracování, vyžadující rozsáhlé pravidelné a systematické monitorování občanů;

3. Hlavní činnost správce nebo zpracovatele spočívá v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů. (Žůrek, 2017, s. 103)

V těchto zmíněných třech případech by měla být jak správci, tak zpracovateli nápomocná osoba, která disponuje odbornými znalostmi z oblasti právních předpisů a postupů týkajících se ochrany osobních údajů. Tyto nápomocné osoby (pověřenci), bez ohledu na to, zda se jedná o zaměstnance správce nebo externě poskytovanou službu, musejí být schopni

plnit své povinnosti a úkoly nezávislým způsobem. Může se stát, že některé organizace budou považovat dobrovolné jmenování pověřence za užitečný krok, což bude podporováno dozorovými orgány. (Žůrek, 2017, s. 103)

Úkol ve veřejném zájmu a výkon veřejné moci může být plněn nejenom státním orgánem, ale rovněž jinými fyzickými nebo i právnickými osobami, jimž je tato pravomoc svěřena na základě národních předpisů. Může se jednat například o oblast veřejné dopravy, zásobování vodou a energiemi, silniční infrastrukturu nebo veřejnoprávní vysílání. (Žůrek, 2017, s. 106)

Z nařízení vyplývá, že jeden pověřenec může být jmenován i pro několik státních orgánů, institucí nebo firem, jež mají podobnou organizační strukturu. Součástí jeho odpovědnosti je pak množství různorodých úkolů a je proto důležité zajistit a dohlédnout na to, aby daný pověřenec své úkoly plnil efektivně i přesto, že má odpovědnost za více orgánů. Osobní dostupnost pověřence (fyzická ve stejných prostorách jako zaměstnanci, po horké lince nebo jiným zabezpečeným komunikačním prostředkem) je nezbytná proto, aby měl občan jistotu, že jej bude schopný kontaktovat. Pověřenec je při vykonávání úkolů vázán tajemstvím nebo důvěrností v souladu s právem Unie nebo členských států. (Žůrek, 2017, s. 108)

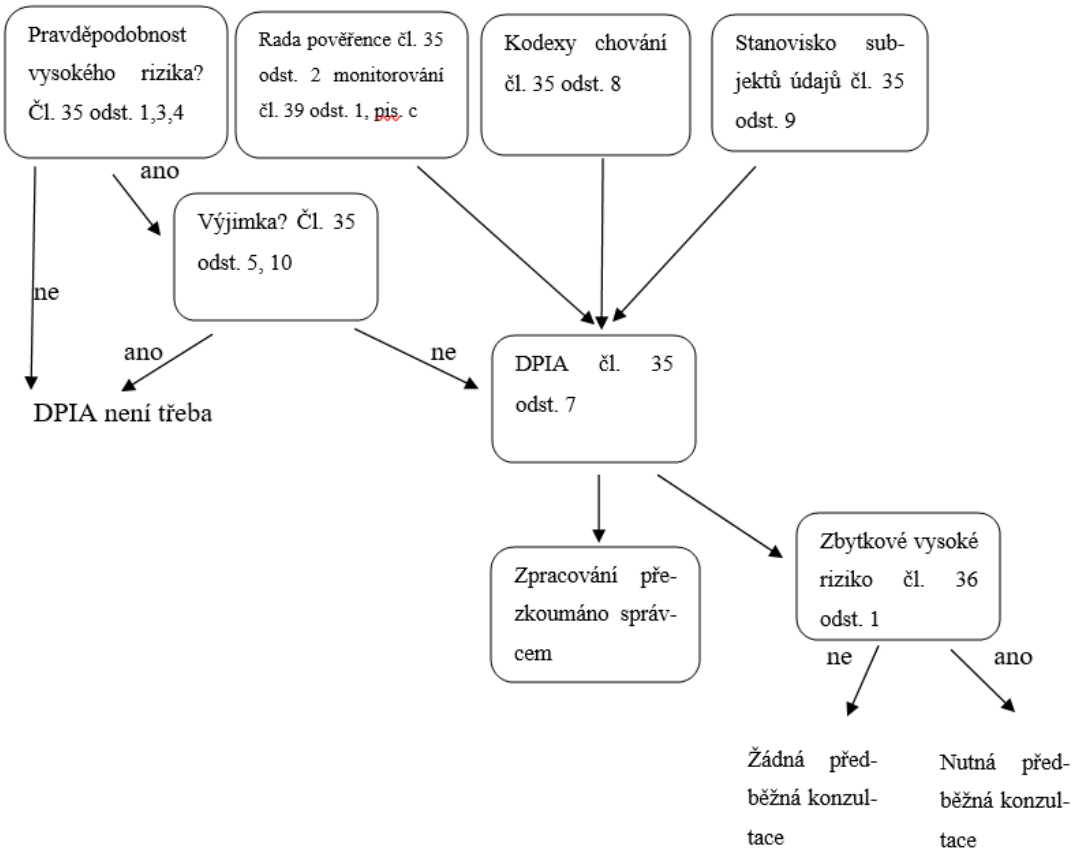
## 5.4 DPIA – Data Protection Impact Assesment

Jedná se o posouzení vlivu na ochranu osobních údajů a vychází ze základních principů Obecného nařízení, tedy vychází přímo z odpovědnosti správce. Na základě DPIA dochází k identifikaci a zhodnocení rizik o hrozby v souvislosti se zpracováním osobních údajů pro klienty, zaměstnance apod. Jeden ze základních principů, minimalizace zpracovávaných dat, s tímto rovněž souvisí, protože na konci této analýzy mohou vyjít najevo některá data, jež jsou pro účel zpracování zbytečná. (Nezmar, 2017, s. 98)

DPIA je možno popsat jako proces, jehož hlavními cíli je nejprve popsat zpracování, dále osoudit, zda je opravdu nezbytné zpracovávat veškerá data, jaká je přiměřenost zpracování a v neposlední řadě tento proces napomáhá zvládnutí rizik pro práva a svobody fyzických osob, jež vyplývají ze zpracování osobních údajů. (Nezmar, 2017, s. 99)

Nutno dodat, že tuto analýzu není potřeba provádět ve všech případech. Je povinná pouze tehdy, pokud existuje pravděpodobnost, že zpracování přinese vysoké riziko a ohrozí tím práva a svobody fyzických osob. Nařízení klade důraz zejména na situaci, kdy se zavádí nová technologie nebo nový způsob zpracování dat. (Nezmar, 2017, s. 102)

Společnosti mohou při rozhodování, zda použít či nepoužít DPIA analýzu, použít následující graf:




Obr. 1 Rozhodováni o realizaci DPIA (Nezmar, 2017, s. 101)

Povinné je DPIA v případě, že zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. (Nezmar, 2017, s. 101)

## 5.5 Změny v souvislosti s GDPR

V rámci Obecného nařízení nedochází k výrazným změnám u základních zásad, principů a klíčových instrumentů. Byly pouze detailněji rozpracovány a zpřesněny (např. byla zavedena nutnost disponovat pro zpracování právním důvodem, zabezpečení osobních údajů, transparentnost vůči subjektu údajů atd.). Obecné nařízení přináší nástavbu, která spočívá v nových povinnostech, které budou pro české správce nové. Jedná se zejména o tyto povinnosti:

- 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;

- ustavení pověřence pro ochranu osobních údajů. (Nezmar, 2017, s. 30)

Záznamy o činnostech zpracování do jisté míry představují náhradu za oznamovací povinnost, která byla zrušena Obecným nařízením. Pokud se na ně nevztahuje výjimka z povinnosti vést záznamy o činnostech zpracování, jsou správce a zpracovatel povinni vést záznamy s určitými informacemi. Těmito záznamy může správce prokázat soulad zpracování s Obecným nařízením. (Nezmar, 2017, s. 31)

Vést záznamy o činnostech zpracování nedoléhá na podnik nebo organizaci zaměstnávající méně, než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektu údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech. (Nezmar, 2017, s. 31)

Tikkinen-Piri shrnul nejpodstatnější změny v rámci Obecného ustanovení do následujících bodů:

*Obecná ustanovení a zásady* - dochází k rozšíření územního rozsahu, kdy ustanovení platí pro kontroléry v EU bez ohledu na to, kde dochází ke zpracování osobních údajů;

- monitoruje se chování subjektů údajů v rámci EU, setkáváme se s novými definicemi výrazů pseudonymizace, genetická data, biometrické údaje, zdravotní údaje;

- upřesněná a lépe specifikovaná ustanovení a principy, jakými jsou minimalizace dat, podmínky pro souhlas, podmínky pro zákonné zpracovávání osobních údajů u dětí

*Transparentnost a způsoby* - v tomto případě upozorňuje na nové povinnosti správců údajů, například u poskytování průhledných a snadno přístupných informací o subjektu údajů.

*Informace a přístup k osobním datům* - vzniká další informační požadavek týkající se údajů samotného subjektu, kdy vzniká právo na přístup k jeho osobním údajům

*Oprava a vymazání* - předepsaná práva na opravu nebo vymazaní údajů, omezení zpracování osobních údajů

- nové právo pro subjekt údajů – možnost přenosu dat z jednoho systému do dalšího

*Vznik práva na námitky a automatizovaného rozhodování jedinců* - právo na námitku musí být jasně a zřetelně odděleno od jakýchkoliv dalších informací

*Obecná povinnost* - vznikají nové povinnosti pro provozovatele – musí dojít k nastavení principů ochrany údajů ve fázi návrhu a výchozím nastavení

- jasné vysvětlení odpovědností a povinností (odpovědnost kontrolních pracovníků, postavení a povinnosti zpracovatelů pod dohledem správců)

- vedení záznamů o zpracovatelských činnostech, které spadají do odpovědnosti správců a zpracovatelů, spolupráce s dozorovým orgánem

- pokud správce a zpracovatel nesídlí v EU, je uložena povinnost určit za daných podmínek zástupce v EU

Autor Bolognini (2017, s. 176) se ve svém článku zaobírá použitím anonymizace, jejím cílem je nezvratně zabránit jakékoliv identifikaci subjektu. Jedná se o proces, který však musí respektovat podmínky stanovené Obecným nařízením, které říká, že konkrétní účely, pro něž jsou zpracovávány osobní údaje, musí být legitimní a určené v době sběru osobních údajů. Techniky anonymizace se používají pro ukládání dat, pro možnost jejich případného zveřejnění či sdělení třetím osobám, dále pro statistické, historické a vědecké účely.

## 5.6 Sankce při nedodržení nařízení

V případě, že dojde k porušení či nezavedení nového zařízení, hrozí subjektům velmi vysoké případy, které by mohly být v některých případech až likvidační.

Maximální výše pokut je 20 000 000 € nebo 4 % z celkového ročního obratu společnosti (záleží na tom, která z částky je vyšší). Výše pokuty se poté odráží od více faktorů, například povaha, závažnost a délka porušování, jaký je počet občanů poškozených tímto porušováním, míra škody, kroky, které podnikli správce či zpracovatel ke zmírnění škod, jaká kategorie osobních údajů byla dotčena tímto porušením apod. (Obecné nařízení o ochraně osobních údajů prakticky, ©2017)

Tato maximální výše pokuty může být udělena jak menší společnosti s pár zaměstnanci, tak velké nadnárodní korporaci, pokud nebudou učiněny kroky potřebné pro uvedení do souladu s principy a povinnostmi v rámci Obecného nařízení. (Působnost úřadu, ©2013)

Kromě těchto výše zmíněných pokut mohou fyzické osoby podat žalobu vůči správci či zpracovateli s tím, že si budou nárokovat náhradu škody v případě hmotné či nehmotné újmy. V neposlední řadě je nutno myslet i na skutečnost, že pokud by nastala některé ze situací, vrhá to na ni velmi špatný dojem, společnost ztrácí důvěru a má zhoršenou reputaci z důvodu špatného zacházení s osobními údaji. (Obecné nařízení o ochraně osobních údajů prakticky, ©2017)

# 6 SHRNUTÍ TEORETICKÉ ČÁSTI

V první kapitole teoretické části této diplomové práce jsou definovány základní pojmy související s danou problematikou. Mezi tyto pojmy řadíme především osobní údaje, informace, dále data, u nichž je zdůrazněno, že tvoří podmnožinu informace, také jaké mají vlastnosti nebo že existují i data poskytující informace o jiných datech. V neposlední řadě dochází i k vysvětlení významu pojmu soukromí, neboť osobní data tvoří velkou část soukromí každého jedince, a tento pojem tedy s problematikou osobních údajů úzce souvisí.

V následující kapitole jsou rozčleněny jednotlivé typy osobních údajů, jako například popisné, identifikační či citlivé. Tato část je velmi důležitá a výchozí pro část praktickou, neboť slouží pro uvědomění si toho, s jakými daty analyzovaná společnost nakládá.

Další část je poté věnována zákonu 101/2000 Sb., o ochraně osobních údajů, tedy jaká je jeho působnost, jednotlivé pojmy vyplývající z tohoto zákona, jaké jsou povinnosti v souvislosti se zpracováním osobních údajů, dále jaké práva může uplatňovat subjekt údajů.

Vzhledem ke skutečnosti, že nedílnou součástí ochrany osobních údajů při jejich zpracování jsou dozorové úřady, je v této diplomové práci zmíněný i Úřad pro ochranu osobních údajů, který tuto roli dozorového úřadu plní v České republice. Nutno dodat, že ji bude plnit i za účinnosti Obecného nařízení a jeho základním úkolem je monitorování uplatňování Obecného nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů.

Poslední kapitola je zaměřená už na samotné Obecné nařízení o ochraně osobních údajů, kdy jsou zde především uvedeny změny vyplývající z tohoto nařízení, dále práva a povinnosti a v neposlední řadě případné sankce hrozící při jeho porušení, nezavedení či nepřipravenosti na něj.

# II. PRAKTICKÁ ČÁST

# 7 CHARAKTERISTIKA VYBRANÉ SPOLEČNOSTI

Následující kapitola pojednává o analyzované společnosti. Je zde uvedeno, jak se společnost v průběhu let vyvíjela, základní informace týkající se organizační struktury a počtu zaměstnanců, dále rozpis nabízených služeb a produktů. V neposlední řadě je provedena analýza nákladů, výnosů a výsledku hospodaření.

## 7.1 Představení a historie společnosti

Analyzovaná společnost XY360 a.s. vznikla v roce 2002. V současné podobě je od roku 2014, kdy se změnil vlastník, a došlo k výrazné změně společnosti. Společnost změnila svůj název a především své cíle. Hlavním cílem se stalo vytvoření nové finanční skupiny, která by místo klasických poboček a statického bankovnictví nabídla chytré algoritmy a FinTech služby nové generace. Společnost rozšířila své licence obchodníka s cennými papíry a získala licenci platební instituce.

V průběhu fungování došlo ve společnosti k sestavení týmu zkušených odborníků corporate finance, kteří poskytují poradentství v oblasti fúzí a akvizic, emisí akcií nebo dluhopisů a v neposlední řadě při restrukturalizaci firem. V roce 2015 došlo k uvedení prvního vlastního FinTech produktu společnosti nazvaného „FX“, prostřednictvím něhož je možná online směna deviz a provádění mezinárodních plateb.

V roce 2016 došlo k představení dalšího FinTech produktu. Jednalo se o investičně-crowdfundingovou platformu „FL“, která slouží k efektivnímu propojování investorů a nadějných růstových projektů. Crowdfunding sám o sobě je způsob financování, při němž přispívá větší počet jednotlivců menším obnosem k cílové částce.

Další změna nastala v letošním roce, kdy 19.2.2018 došlo převzetí původní společnosti další, současnou společností, XY Holding, a.s.. I nadále je její vizí rozšiřovat nabídku FinTech produktů jak pro firmy, tak pro podnikatele a fyzické osoby a stát se tak největší FinTech platformou v České republice.

Cílem minulých let byla stabilizace systémů pro poskytování produktů a služeb s cílem zvýšení komfortu klientů a budování datových struktur k efektivnímu provádění činností. Tento krok byl důležitý pro zlepšení ziskovosti produktů a služeb, zejména pak směny peněz.

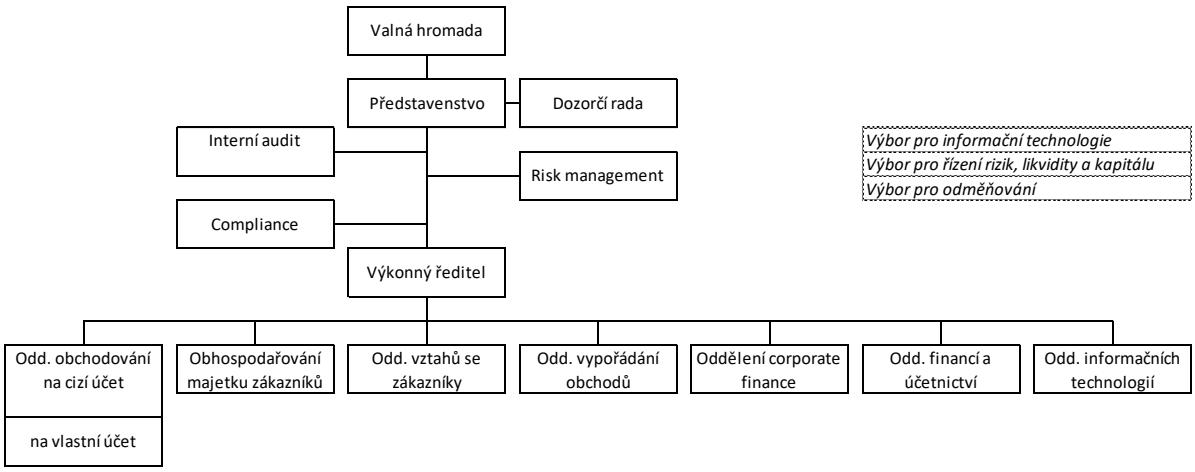
V následujících letech má společnost v plánu investici do nabídky služeb Wealth Managementu, v časovém horizontu 3-5 let, a to prostřednictvím budování služeb ve vlastní režii jako online Asset Management, poradentství při financování a využití aktiv a nabídkou služeb ve spolupráci s třetími stranami jako poskytování úvěrů, pojištění, daňové a právní poradenství a další.

## 7.2 Základní informace

Součástí této kapitoly je popis organizační struktury, jak původní, před jejím převzetím společností XY Holding, a.s., tak té současné. Dále je zde popsán vývoj zaměstnanců.

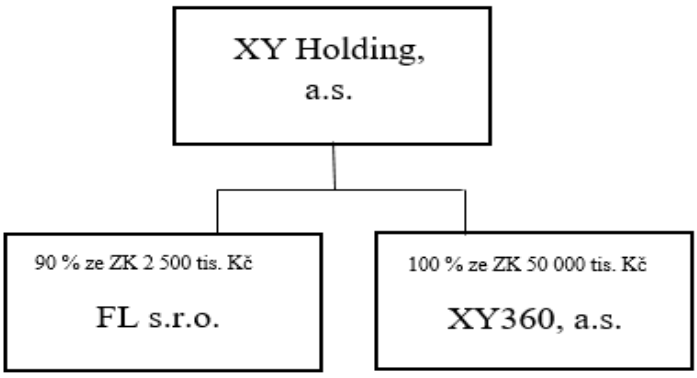
**Organizační struktura**

Původní organizační struktura společnosti, před již zmiňovanou změnou z letošního února, je znázorněna na následujícím obrázku:




Obr. 2 Schéma organizační struktury analyzované společnosti (vlastní zpracování)

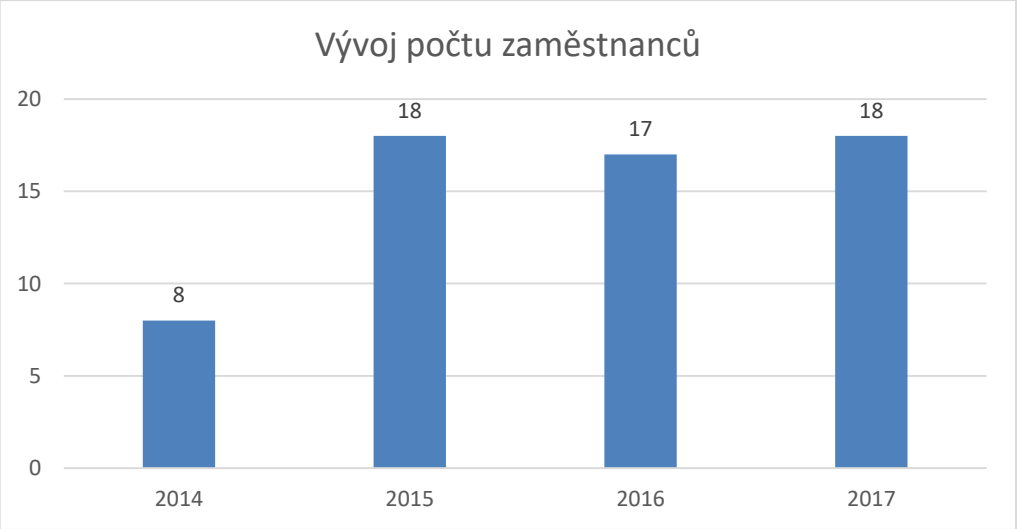
Současná podoba organizační struktury je vyobrazena na obrázku níže. Na vrcholu organizační struktury nachází společnost XY Holding, a.s., pod niž spadají další dvě, a to původní, vzniklá v roce 2014, sídlící ve Zlíně. Druhou společností, je společnost provozující již zmíněnou investment-crowdfundingovou platformu FL.




Obr. 3 Organizační struktura skupiny (vlastní zpracování)

### Vývoj počtu zaměstnanců

Na následujícím obrázku se nachází sloupcový graf představující vývoj počtu zaměstnanců analyzované společnosti v průběhu let 2014 – 2017.




Obr. 4 Vývoj počtu zaměstnanců analyzované společnosti (vlastní zpracování)

Jak vyplývá z grafu, zpočátku společnost měla mnohem méně zaměstnanců, než je tomu v současné době. K nárůstu došlo mezi lety 2014 a 2015 a to o 10 zaměstnanců, což bylo způsobeno významným rozšířením služeb. Bylo zavedeno nové oddělení vztahů se zákazníky a významně posíleno oddělení obchodování. V rámci celé holdingové skupiny je v současnosti celkem 38 zaměstnanců.

## 7.3 Analýza nákladů, výnosů a výsledku hospodaření po zdanění

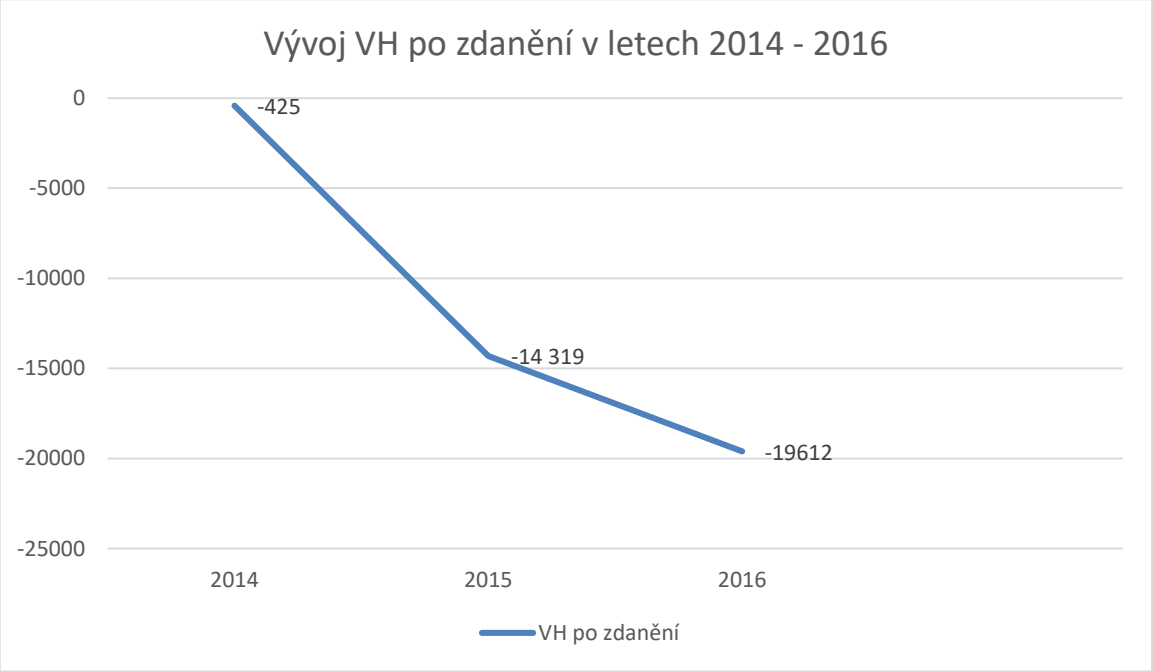
V této části práce jsou porovnány vyprodukované náklady s výnosy společnosti a zachycení vývoje výsledku hospodaření po zdanění v průběhu let 2014 – 2016.

Následující tabulka pojednává o jednotlivých nákladech, výnosech a výsledku hospodaření v průběhu sledovaných let.

Tab. 1 Vývoj výnosů, nákladů a výsledku hospodaření po zdanění (vlastní zpracování)

| V tis. KČ | 2014 | 2015 | 2016 |
|---|---|---|---|
| Výnosy | 4 756 | 6 071 | 4 518 |
| Náklady | 5 183 | 20 390 | 24 130 |
| Výsledek hospodaření po zdanění | - 425 | - 14 319 | - 19 612 |

Na základě tabulky je vytvořen graf, jenž podává přehlednější zobrazení vývoje výsledku hospodaření po zdanění v jednotlivých letech.




Obr. 5 Vývoj výsledku hospodaření po zdanění (vlastní zpracování)

Z tabulky a následně i grafu je patrné, že společnost se dostávala v průběhu let 2014 – 2016 do čím dál větší ztráty. U všech položek nákladů došlo v těchto letech k výraznému nárůstu. Největší skok byl zaznamenán mezi lety 2014 a 2015, kdy například u nákladů na poplatky a provize společnost zaznamenala nárůst o téměř pětinásobek oproti roku přechozímu.

Důvodem, proč v roce 2014 byla o poznání nižší ztráta v porovnání s léty dalšími, je to, že v daném roce byl rozpuštěn nerozdělený zisk z minulých období ve výši 11 mil. Kč, kterým byly pokryty počáteční náklady spojené s rozšířením společnosti a nákupem software.

Vzhledem ke skutečnosti, že společnost v roce 2015 přijala deset dalších zaměstnanců, došlo spolu s tímto k nárůstu správních nákladů, konkrétně položky náklady na zaměstnance, které vzrostly oproti roku 2014 více než čtyřnásobně. Přestože společnost zaznamenala výnosy vyšší, než v roce 2014, enormní nárůst nákladů rovněž měl vliv na propad výsledku hospodaření a prohloubení ztráty společnosti.

V posledním analyzovaném roce pak společnost neprokazovala výrazné změny v oblasti nákladů, pouze jejich mírný nárůst opět ve všech položkách. Nutno zmínit, že tento rok zaznamenala nejnižší výnosy v průběhu analyzovaných tří let, což zapříčinilo další prohloubení ztráty.

## 7.4 Portfolio služeb

Cílem této podkapitoly je popsat, jaké služby může společnost ze zákona poskytovat, dále pak, jaké produkty nabízí.

### 7.4.1 Nabízené služby

Na základě zákona o podnikání na kapitálovém trhu 256/2004 Sb., o podnikání na kapitálovém trhu, je společnost oprávněna k provozování těchto činností:

**Hlavní investiční služby**

a) Přijímání a předávání pokynů týkajících se investičních nástrojů;

b) provádění pokynů týkajících se investičních nástrojů na účet zákazníka;

c) obchodování s investičními nástroji na vlastní účet;

d) obhospodařování majetku zákazníka;

e) investiční poradenství týkající se investičních nástrojů;

f) upisování nebo umísťování investičních nástrojů se závazkem jejich upsání.

**Doplňkové investiční služby**

a) Úschova a správa investičních nástrojů pro zákazníka;

b) poradenská činnost týkající se struktury kapitálu;

c) investiční výzkum a finanční analýza;

d) devizové služby související s poskytováním investičních služeb;

e) služby související s upisováním investičních nástrojů;

**Další oprávnění**

a) Přijímání peněžních prostředků nebo investičních nástrojů od zákazníků;

b) oprávnění k organizování veřejných dražeb CP;

**Platební služby**

Společnost poskytuje platební služby podle zákona č. 370/2017 Sb., o platebním styku. Jedná se o tyto služby:

a) Provedení převodu peněžních prostředků z platebního účtu neposkytnutých jako úvěr, k němuž dává platební příkaz plátce, příjemce nebo plátce prostřednictvím příjemce;

b) vydávání a správa platebních prostředků;

c) předávání platebního příkazu a zpracování platebních transakcí, je-li uživatel příjemcem;

d) provedení převodu peněžních prostředků, při němž plátce ani příjemce nevyužívají platební účet u poskytovatele plátce.

### 7.4.2 Produkty

Společnost poskytuje široké portfolio vzájemně se doplňujících produktů a služeb.

Výčet nabízených produktů:

A. *Produkt FX* - platforma pro směnu deviz a uskutečnění vnitrostátních i mezinárodních plateb, jedná se o směnu online. Klient, který tuto směnu chce provést, musí provést registraci (on-line nebo uzavřením papírové smlouvy) a založit si online účet. Samotná směna poté probíhá ve třech krocích:

1. Zadání částky směny a zjištění současného kurzu, kdy klient ihned uvidí svůj kurz včetně marže. Samotná směna může být provedena online nebo prostřednictvím telefonátu, potvrzení provedeného obchodu přijde vzápětí emailem.

2. Volba, kam chce klient peníze poslat. Peníze mohou být poslány zpět na klientův účet, nebo do více než 200 zemí světa. Pokud by se vyskytl jakýkoliv problém nebo nesrovnalost, je neustále k dispozici makléř společnosti, který je připraven pomoci.

3. Zaslání peněz za směnu. V případě, že klient nedisponuje penězi na daném účtu této služby, musí je zaslat nejpozději do následujícího pracovního dne na jeden z bankovních účtů společnosti, která disponuje účty u osmi českých bank.

Společnost nabízí i službu zajišťování se proti kurzovému riziku prostřednictvím forwardu. Jedná se o druh finančního instrumentu, prostřednictvím něhož je možné zajistit si kurz vybraného měnového páru pro konkrétní den v budoucnu. Je určen pro klienty společnosti, kteří vědí, že budou muset v budoucnu provést nebo přijmout platbu v zahraniční měně a mají zájem se zajistit proti možným kurzovým výkyvům. Měnový forward je možné si sjednat prostřednictvím telefonátu na dealing společnosti, kdy si klient stanoví částku, měnový pár, který chce směnit a spolu s tím i den, kdy chce směnu vypořádat. Zároveň je i potřeba složit vratnou zálohu, která se pohybuje ve výši 5-10 % z hodnoty forwardu. Ta slouží k vyrovnání ztráty v případě pohybu kurzu v neprospěch uzavřeného obchodu. V případě, že dojde ke změně data, je možné forward upravit formou další finanční operace, tzv. swapu, na dřívější či pozdější termín.

Tab. 2 Produkt FX – základní čísla (vlastní zpracování)

| | 2016 | 2017 |
|---|---|---|
| Počet nových klientů | 1 802 | 2 194 |
| Počet klientů celkem | 1 885 | 4 167 |
| Objem transakcí | 3 730 135 | 9 971 338 |

V tabulce jsou uvedeny pro orientaci čísla uvádějící počet nových klientů a počet klientů celkem, dále objem transakcí, a to za období 2016, 2017.

B. *Produkt FL* - investment-crowdfundingová platforma prezentovaná na webovém portálu, jež efektivně propojuje investory a projekty, které mají ambice růst. Firmám s potenciálem růstu poskytuje nový způsob, jak získat financování, napojení na investory a cenný marketingový kanál. Umožňuje investice do společností prostřednictvím koupě konvertibilních investičních certifikátů nebo minibondů. Investování prostřednictvím této platformy je regulovanou aktivitou na kapitálových trzích. Investice jsou realizovány přes obchodníka s cennými papíry a celý tento proces je regulován Českou národní bankou.

Člověk, který se rozhodne investovat do jednoho z projektů, se musí nejdříve zaregistrovat na platformě a musí dojít k ověření jeho totožnosti. Poté už si vybere ze zveřejněných projektů a zašle finanční prostředky a dochází k otevření investičního účtu. V případě neúspěšné kampaně, tedy pokud se kampaň plně nezafinancuje, dochází k návratu veškerých finančních prostředků na účet investora. V případě úspěšné, plně zafinancované kampaně, dochází k převedení finančních prostředků projektu, emisi cenných papírů a jejich vedení v imobilizované formě na účtu u obchodníka s cennými papíry.

V případě zájmu o přidání nového projektu a získání financování pro jeho realizaci emitent v první řadě zasílá základní informace, tedy identifikaci projektu, cílený objem financování a jeho následné využití, a to online nebo na emailovou adresu. Následně dojde k setkání s pracovním týmem a vyhodnocování záměru projektu. Pokud dojde ke schválení kampaně pracovním týmem, začne se s přípravou kampaně, tedy propagačního videa, business plánu a právní dokumentace a poté může dojít ke spuštění samotné kampaně.

Tab. 3 Produkt FL – základní čísla (vlastní zpracování)

| | 2016 | 2017 |
|---|---|---|
| Počet registrovaných uživatelů | 4 024 | 6 866 |
| Počet nově vystavených projektů | 14 | 19 |
| Počet aktivních investorů | 568 | 2 309 |
| Objem pokynů | 64 000 | 101 913 |

C. *Produkt R24* - poskytování aktuálního zpravodajství a dat z domácí i světové ekonomiky, obchodu a finančních trhů. Zde je možné se zaregistrovat a dostávat tak veškerá upozornění.

V rámci tohoto produktu je nabízena služba, tzv. *online valuační kalkulačka*, která slouží pro odhad ocenění firmy metodou DCF (diskontovaných peněžních toků) a násobků. Jinými slovy, je schopná vypočítat, jaká je v současné době tržní cena vybrané společnosti. Pro registrované uživatele je tato služba zdarma.

Jeho součástí je i elitní *studentský klub*, díky němuž se mohou jeho členové mimo jiné setkat například s významnými osobnostmi ze světa financí.

D. *Produkt CF* - zahrnuje tým zkušených odborníků v oblasti korporátních financí, fúzí, akvizic a kapitálových transakcí. Jejich cílem je poskytnout klientům komplexní poradenské služby, a to při prodeji podniků (nebo jejich částí), zvyšování nebo snižování základního kapitálu a v neposlední řadě také poradenství v oblasti finančních restrukturalizací a rekapitalizací.

E. *Produkt R360* – licencované obchodování s cennými papíry. Dále je zaměřen na následující činnosti:

- obchodování cenných papírů pro klienty;

- správa finančních aktiv klientů;

- zprostředkovávání prodeje finančních produktů a služeb třetích stran prostřednictvím webových portálů, například úvěrů.

# 8 ANALÝZA SOUČASNÉHO STAVU ZPRACOVÁNÍ DAT

Společnost v současnosti disponuje osobními údaji a to jak v podobě elektronické, tak tištěné. V této kapitole se práce podrobně věnuje analýze současného stavu osobních údajů, tedy jaké osobní údaje společnost zpracovává, a zároveň jakým způsobem je toto zpracovávání zabezpečeno před únikem osobních údajů.

## 8.1 Analýza vnitřních předpisů

Společnost má za účelem ochrany osobních údajů vytvořeny dva dokumenty.

### 8.1.1 Vnitřní předpis

První z nich je vnitřní předpis upravující tvorbu, zpracování a nakládání s daty a dokumenty a jejich uchovávání. Tento předpis se dotýká jak společnosti samotné, tak především všech jejich zaměstnanců a jedná se o jediný předpis sloužící pro uchování informací a dokumentů.

Součástí vnitřního předpisu je definice základních pojmů, jako jsou data, dokumenty, co je myšleno pod pojmem zpracování, co je pokládáno za písemnosti, dále co je spis, spisová služba a co v sobě všechno zahrnuje, v neposlední řadě pak kdo je to správce. Právě poslední zmíněný pojem je důležitý, neboť se jedná o příslušného zaměstnance či jinou osobu, jež v rámci své činnosti u společnosti data a dokumenty získává a dále je využívá a zpracovává. V dalším článku vnitřního předpisu jsou poté podrobně rozepsány veškeré povinnosti správce osobních údajů.

Další část je poté věnována obecným zásadám tvorby, zpracování dat a dokumentů a nakládání s nimi. Součástí je přesný popis toho, jak správce jednotlivá data a dokumenty získává, kam došlé písemnosti dochází, způsob jejich roztřídění po jejich doručení (písemnosti nesouvisející s činností společnosti, soukromého charakteru a ostatní písemnosti podléhající evidenci). Stejný postup platí i pro elektronickou verzi pošty, pro jejíž příjem je pověřen někdo ze zaměstnanců.

Vnitřní předpis upravuje dále způsob odeslání dat a dokumentů, jejich ukládání a uchovávání a v neposlední řadě i trvalé odstranění dat a skartaci dokumentů.

### 8.1.2 Pravidla pro zpracování osobních údajů

Za účelem úpravy pravidel pro zpracování osobních údajů třetích osob (uživatelů) při využívání webových stránek jednotlivých produktů společnosti byl vytvořen a řídí se jím jak analyzovaná společnost, tak zmiňovaná společnost poskytující produkt FL.

Součástí vnitřního předpisu je jednak účel zpracování osobních údajů. Jednotlivé účely jsou definovány následujícím způsobem:

- realizace práv a povinností společnosti a uživatelů souvisejících s využíváním webových stránek;

- základní identifikace uživatele při jeho registraci

- případná dodatečná identifikace uživatele při zájmu o využití některé ze služeb poskytovaných společností

- komunikace s uživateli včetně zasílání obchodních sdělení.

Ani jedna ze společností nezpracovává žádné osobní údaje uživatelů, které by nebyly poskytnuty dobrovolně přímo od uživatelů s jejich souhlasem. Společnosti jsou oprávněny zpracovávat osobní údaje v souladu s příslušnými právními předpisy.

Dále je v rámci vnitřního předpisu řešen způsob zpracování, kdy jsou zpracovávány osobní údaje ve formě elektronické, přímo prostřednictvím webových stránek. Údaje jsou přitom zpracovávány pouze po nezbytnou dobu podle příslušných právních předpisů v rámci realizace účelů zpracování.

V rámci obou společností dochází ke zpřístupnění údajů třetím stranám a to v těchto případech:

- pokud se jedná o společnosti náležející do skupiny analyzované společnosti

- v rámci třetích stran podílejících se na vývoji, provozu a údržbě webových stránek

- pokud vzniká povinnost podle příslušných právních předpisů tyto osobní údaje příslušné třetí straně zpřístupnit. V tomto případu jsou tyto třetí strany povinny rovněž údaje uchovávat jako důvěrné a bránit je před jejich zneužitím.

Z důvodu zlepšení provozu a údržby webových stránek a v zároveň zlepšení kvality poskytovaných služeb může společnost analyzovat, shromažďovat a zpracovávat některé anonymní statistické údaje uživatelů, k jejichž vzniku dochází během využívání webových

stránek. Za tímto účelem využívá analyzovaná společnost při provozování stránek tzv. cookies.

## 8.2 Identifikace osobních údajů

V této části práce jsou osobní údaje zpracovávané analyzovanou společností rozděleny podle jejich druhů, o nichž pojednává jedna z kapitol teoretické části.

Pokud se jakákoliv osoba chce stát novým klientem společnosti, je potřeba nejprve provést registraci. Tu provádí jak fyzická, tak právnická osoba, ale vzhledem ke skutečnosti, že se Obecné nařízení týká pouze osob fyzických, bude i tato část práce zaměřena pouze na ně.

### 8.2.1 Poskytování služeb v oblasti FX a obchodování s investičními nástroji

Veškeré osobní údaje jsou zavedeny v servisním portálu společnosti. Ten obsahuje všechny klienty (jak fyzické osoby, tak osoby právnické).

Každý nově příchozí klient se může registrovat dvojím způsobem. Buď provede registraci online, kdy sám vyplní příslušné údaje a ty se propíší do servisního portálu, nebo přijde udělat registraci osobně, kdy s ním zaměstnanec vyplní smlouvu o poskytování investičních služeb a smlouvu o poskytování platebních služeb. Veškeré údaje poté zaměstnanec zanese do servisního portálu. Mimo to dochází k naskenování všech dokumentů a jejich uložení na datovém uložišti v počítači. Tištěná verze dokumentů se poté nachází jednak v sídle společnosti v Praze, dále pak i ve zlínské pobočce, kde jsou uchovávány v oddělení back office.

**Adresní a identifikační údaje**

U každého nového klienta společnosti dochází k zanesení následujících údajů do servisního portálu:

- jméno a příjmení;

- datum narození;

- rodné číslo;

- údaj o rezidentství;

- bydliště;

- telefonní kontakt.

Jak vyplývá z definice, v těchto případech se jedná o adresní a identifikační údaje. Mimo jiné je dále povinnost u klienta naskenovat do systému i jeho dva osobní doklady. Ve většině případů se jedná o občanský průkaz, popřípadě pas, jako druhý doklad bývá pak velmi často použit řidičský průkaz. U člověka pocházejícího z jiné země se jedná například i o povolení k pobytu. Z těchto dokladů jsou poté k dispozici další údaje, jako je místo narození, státní příslušnost či rodinný stav.

Přestože se Obecné nařízení, jak již bylo řečeno, netýká právnických osob, může nastat situace, kdy za právnickou osobu bude jednat jiná oprávněná osoba, než například její majitel či jednatel (jehož osobní údaje jsou veřejně dostupné ve veřejných rejstřících). Tato osoba je označena jako disponent a rovněž poskytuje společnosti své adresní a identifikační údaje.

**Citlivé údaje**

Takové osobní údaje společnost nezískává.

**Popisné údaje**

Jedná se o údaje zpracovávané jak u klientů, tak u zaměstnanců společnosti. U zaměstnanců či uchazečů o pracovní pozici se k těmto údajům společnost dostane prostřednictvím životopisu. V tomto případě se jedná zejména o údaje týkající se vzdělání, znalosti cizích jazyků, odborných znalostí a dovedností, údaje o předchozím zaměstnání. Dalším popisným údajem, v souvislosti se zaměstnanci, je i mzda, o jejíž výši si společnost vede záznamy.

U klientů se jedná o údaje, které se nacházejí rovněž v servisním portálu. Vzhledem ke skutečnosti, že nový klient je povinen nahrát dva osobní doklady, má společnost údaj například i o čísle cestovního dokladu. Dále je povinen nahrát i kopii svého bankovního účtu, což je taky jeden z popisných údajů.

**Údaje o jiné osobě**

Stejně jako v případě právnické osoby, i u fyzické osoby může za každého člověka jednat i jím zvolený disponent. Může se jednat o člena rodiny, kdy společnost uchovává v servisním portálu adresní a identifikační údaje i tohoto člověka.

Údaje ze servisního portálu se dále propisují i do databáze IVAN, s níž společnost pracuje. Do konce roku 2017 využívala i CAPITOL, od roku 2018 však tento systém nemá, a tak se v něm údaje za rok 2018 a dále nenacházejí.

Klient má možnost zadat pokyn k obstarání obchodu s cennými papíry, oznámit změnu bankovního účtu nebo podat žádost o převod peněžních prostředků. Ke všem těmto pokynům slouží údaje ze servisního portálu. Pokud klient tento příkaz zadá v papírové podobě, je nutné tento příkaz evidovat.

Kromě smluv, které každý nový klient vyplňuje, dochází i k vyplnění dotazníků. Ty se jednak týkají poskytování investičních služeb, kdy klient vyplňuje dotazník týkající se investování v rámci cenných papírů a také dotazník pro obchodování s měnovými deriváty. V rámci těchto dotazníků klient poskytuje údaje o svém jménu, příjmení, rodném čísle a znalostech a vzdělání v oblasti dané problematiky.

Dále je nutné vyplnit i AML dotazník, který je součástí servisního portálu. Tento dotazník slouží pro tzv. AML kontrolu (dle zákona 253/2008 Sb., zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu), tedy kontrolu rizikovosti klienta dle tohoto zákona. Klient zde uvádí výši svých ročních příjmů, odkud mu příjmy plynou a také v jaké oblasti podniká. Dotazník se nachází jak v elektronické podobě, tak jej může nově příchozí klient vyplnit i v podobě papírové.

### 8.2.2 Ostatní služby

Mezi ostatní služby společnosti patří zaknihování cenných papírů nebo dražby a nabídky převzetí. U těchto služeb jsou sbírány pouze data korporátní, nejsou zde tedy zpracovávány osobní údaje a Obecné nařízení se těchto služeb netýká.

Jak již bylo řečeno, mezi služby společnosti patří i služba zaměřená na poskytování aktuálního zpravodajství a dat z domácí i světové ekonomiky, obchodu a finančních trhů. Pokud má člověk zájem o zasílání informací na jeho emailovou adresu, musí se na stránkách této služby zaregistrovat. Při registraci zde uvede své jméno a příjmení, dále emailovou adresu a uvádí souhlas se zasíláním informací.

### 8.2.3 Údaje o zaměstnancích

Vzhledem k tomu, že společnost má své zaměstnance, pracuje i s jejich osobními údaji. Tyto údaje jsou zaznamenány v pracovní smlouvě, kde se opět jedná o adresní a identifikační údaje. Jak již bylo řečeno, z přiložených životopisů vyplývají i údaje popisné.

### 8.2.4 Výpověď klienta

V případě výpovědi klienta dochází rovněž k jeho identifikaci formou zaslání výpovědi, kdy si společnost ponechává jeho identifikační údaje. Tyto údaje jsou v současné době uchovávány po dobu neurčitou, ale dle Obecného nařízení musí být definována doba, po kterou společnost tyto údaje uchovává.

## 8.3 Analýza cesty osobních údajů

Společnost spolupracuje s řadou partnerů, kteří jí poskytují služby, v rámci nichž dochází k přenášení osobních údajů, s nimiž společnost operuje.

Jak již bylo zmíněno, analyzovaná společnost poskytuje množství produktů. V rámci každého z nich poté spolupracuje s danými partnery a dochází k předávání osobních údajů. Pro představu, odkud kam a v rámci kterého produktu osobní údaje putují, je níže vytvořená tabulka.

Tab. 4 Analýza cest osobních údajů v rámci jednotlivých produktů (vlastní zpracování)

| | FX | FL | Markets | R24 | CF | Z |
|---|---|---|---|---|---|---|
| Servisní portál | x | x | | | | |
| Informační systém IVAN | x | x | | | | |
| Program CAPITOL | x | x | | | | |
| ADC | x | x | | | | x |
| Mobile Net | | x | | | | |
| Currency Cloud | x | | | | | |
| Coolpany | | | | x | | |
| Účetní společnost | | | | | | x |
| Banky | x | x | x | | | |
| AZ Prima | | | | | x | |
| Česká pošta | | | | | x | |
| Správce sítě | x | x | x | | x | x |

| | | | | | | |
|---|---|---|---|---|---|---|
| Insolvenční správci, notáři, dozorové instituce, výzvy datové schránky | x | x | x | | x | x |

Z výše zpracované tabulky je zřejmé, kam putují osobní údaje klientů využívající jednotlivé produkty analyzované společnosti. Například klienti využívající služby v rámci produktů FX a FL své údaje dále poskytují společnostem, které provozují zmiňovaný servisní portál nebo například informační systém IVAN. Tyto dva produkty spolu s dalším produktem Markets navíc pracují s údaji, které se dostanou k bankám, s nimiž společnost spolupracuje. Účetní společnost, jejíž služby jsou využívány, zase získává veškeré údaje o zaměstnancích (v tabulce označeno písmenem Z), stejně jako správce sítě či insolvenční správci. Posledním zmíněným, notářům, dozorovým institucím a pro potřeby výzev datové schránky se propisují údaje téměř ze všech produktů i zaměstnanců.

## 8.4 Současné zabezpečení osobních údajů

Kromě výše zmíněných předpisů se v současné době na analyzovanou společnost vztahují pravidla pro ochranu osobních údajů podle zákona 101/2000 Sb., o ochraně osobních údajů. Společnost je rovněž zaregistrovaná jako správce osobních údajů.

Ke zpracování osobních údajů společnost využívá i externí společnosti, které zajišťují softwarovou podporu evidence.

Společnost uchovává údaje jak v elektronické, tak tištěné podobě a jsou tak přístupné pro všechny zaměstnance. V elektronické podobě se nacházejí na jednotlivých datových uložištích, přičemž ke všem, v nichž se nachází takové údaje, je přístup pouze na heslo jednotlivých uživatelů.

### 8.4.1 IT zabezpečení

Klíčová hardware zařízení, jakými jsou servery, routery, záložní zdroje aj., jsou z důvodu zabránění přístupu neoprávněným osobám, udržení stabilních provozních podmínek a snazší správy a údržby a odolnosti vůči výpadkům napájení umístěny v samostatných místnostech datového centra nebo v uzamykatelných rackových skříních, připojených k záložním zdrojům elektrického napájení.

U zmíněného datového centra se pro společnost nachází slabé místo v podobě závislosti na internetovém připojení. V případě jakékoliv nehody, která bude mít za následek přerušení nebo ztrátu internetového připojení, dochází ke ztrátě přístupu k datovému centru, a tím pádem společnost není schopna dostat se k osobním údajům klientů.

Společnost využívá specializované zařízení NAS (Network Attached Storage), sloužící pro ukládání dat a pro snížení rizika ztráty či poškození klíčových dat. Jedná se o jednoúčelové zařízení, které zajišťuje oddělení serverové části od části datové. V případě selhání některého z pevných disků, budou data obnovena z druhého pevného disku na základě redundantního uložení dat.

V případě, že dojde k výpadku některého ze serverů, ke zprovoznění software zařízení je využíván některý ze zbývajících serverů (jsou využívány celkem 3).

Společnost využívá jeden server v profesionálním datovém centru, kde jsou data ukládána jednak v tzv. primárním uložišti, dále se vytvářejí zálohy na uložišti sekundárním a terciálním. V případě ztráty dat na primárním uložišti dojde k obnově dat z průběžně vytvářených záloh ze sekundárního, popřípadě terciálního uložiště.

Přístup k serverům je uživatelům umožněn přes vzdálenou plochu (tzv. terminálový přístup). Takto se mohou uživatelé přihlašovat do informačního systému IVAN, v němž jsou ukládány osobní údaje zákazníků, dále do programu CAPITOL, v němž jsou údaje zákazníků pouze do konce roku 2017.

Společnost má zaheslovány veškeré přístupy, včetně přístupů do vzdálených ploch. Každý z uživatelů musí být oprávněný k přístupu. Hesla pro jednotlivé přístupy jsou zabezpečovacím prvkem, jelikož musejí splňovat požadavky pro bezpečnost. Každé z hesel se musí skládat z několika znaků, musejí v sobě obsáhnout malá a velká písmena a číslici. Kromě těchto hesel slouží jako další zabezpečovací prvek pro přístup k webovým stránkám provozovaných společností šifrování pomocí „https“, tedy pro zabezpečení dat online. Toto šifrování slouží pro přístup zákazníků k jejich klientským účtům online, kde jsou k dispozici informace o jejich klientském zůstatku, provedených transakcích, případně jejich osobní údaje.

Ve společnosti je používán antivirová a internetová ochrana prostřednictvím lokálního antivirového programu ESET. Jeho úkolem je především chránit společnost proti případným hackerským útokům. U programu dochází k pravidelným a automatickým aktualizacím, které poskytuje výrobce toho software.

## 8.5 Přehled nesouladů – shrnutí GAP analýzy

Na základě analýzy současného stavu zpracování osobních údajů je dalším krokem, a zároveň nejdůležitější částí celé GAP analýzy, popsání nesouladů v souvislosti s nakládáním s osobními údaji. Dále jsou zde uvedeny i kroky potřebné pro odstranění těchto nesouladů. Aby byly plně pokryty potřeby Obecného nařízení, je zapotřebí zapracovat na těchto nedostatcích:

**1. Není stanoven přesný účel zpracování osobních údajů**

Analyzovaná společnost má v současné chvíli uveden účel zpracování osobních údajů, ale není jasně vymezen dle požadavků Obecného nařízení. V rámci projektu implementace Obecného nařízení o ochraně osobních údajů je nutné tyto účely přeformulovat.

**2. Není stanoven rozsah zpracovávaných osobních údajů pro jednotlivé činnosti**

Obecné nařízení klade důraz na minimalizaci zpracovávaných dat. U jednotlivých činností zpracování je nutné specifikovat, v jakém rozsahu budou data zpracovávána v jednotlivých fázích obchodního vztahu, a rovněž po jeho skončení.

**3. Není stanoven rozsah uchovávání osobních údajů po výpovědi smlouvy**

Po ukončení smluvního vztahu se o jednotlivých zákaznících mohou evidovat pouze osobní data, která vyplývají z navazujících zákonných povinností.

**4. Není správně formulován souhlas se zpracováním osobních údajů**

*a. Webové portály* – Služba FL, R24, FX. U těchto služeb je nutné navrhnout souhlasy, včetně jejich platností;

*b. Podpis smluv* - on-line, v tuto chvíli je souhlas se zpracováním osobních údajů napsán obecně, v souladu se zákonem 101/2000 Sb., o ochraně osobních údajů. Souhlas nesmí obsahovat skutečnosti, na které společnost má zákonný základ zpracování – tzn., že tyto údaje jsou potřebné pro samotnou identifikaci klienta a uzavření smlouvy.

- písemná smlouva, kde souhlas se zpracováním osobních údajů musí být součástí smluvní dokumentace.

**5. Souhlas se zpracováním osobních údajů nesmí být podmínkou poskytnutí služby**

Služba musí být poskytnuta i bez podání souhlasu zákazníkem. V rámci interní evidence musí být nově přehled poskytnutých souhlasů jednotlivých klientů (včetně data platnosti souhlasu a možnosti odvolání souhlasu).

**6. U všech současných zákazníků musí být získán souhlas se zpracováním osobních údajů a také musejí být podány informace o zpracovatelích osobních informací.**

Zákazníci musí být osloveni (pravděpodobně v rámci zákaznické webové sekce) s informací o zpracovávání osobních údajů, účelech zpracování osobních údajů, možnostech odvolat souhlas, zpracovatelích osobních údajů, atd.

**7. Nejsou stanovena pravidla přístupů k jednotlivým osobním údajům**

Je nutné nastavit oprávnění jednotlivých osob/skupin osob k osobním údajům a stanovit osoby zodpovědné za uchovávání jednotlivých osobních údajů.

**8. Není vedena evidence zpracovávání osobních údajů**

**9. Chybí pravidla pro případy uplatnění práv subjektů údajů (vyplývající z článků 15-22 Obecného nařízení)**

a. Právo subjektu údajů na přístup k osobním údajům

b. Právo na opravu

c. Právo na výmaz (právo být zapomenut)

d. Právo na omezení zpracování

e. Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

f. Právo na přenositelnost údajů

g. Právo vznést námitku

h. Automatizované individuální rozhodování, včetně profilování

**10. Absence kontrolních mechanismů**

**11. Smlouvy s jednotlivými zpracovateli osobních údajů neobsahují pravidla zpracování dle Obecného nařízení**

Se všemi zpracovateli je nutné upravit smluvní dokumentaci a zahrnout i pravidla pro zpracování osobních údajů včetně specifikace ochrany osobních údajů.

**12. Absence systému ohlašování porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů**

Nutno zapracovat do vnitřního předpisu a nachystat vzorové ohlášení.

**13. Chybí systém ohlašování porušení zabezpečení osobních údajů subjektům údajů**

Rovněž nutnost zapracování do vnitřního předpisu, dále také nachystat vzorovou zprávu subjektům údajů (zákazníci/zaměstnanci)

**14. Chybí vnitřní předpis, který by upravoval všechna pravidla Obecného nařízení**

Je potřeba nachystat nový vnitřní předpis, který bude zahrnovat všechny pravidla pro získávání, správu, ochranu a zpracování osobních údajů.

**15. Chybí systém pro vyhodnocování rizik souvisejících se zpracováváním osobních údajů**

Nutnost navržení systému pro vyhodnocování rizik ke každému způsobu zpracovávání osobních údajů a na jednotlivé druhy činnosti.

**16. Chybí vzorové odpovědi na dotazy subjektů údajů**

Musí se zpracovat vzorové odpovědi na dotazy subjektů údajů o rozsahu zpracovávaných či spravovaných údajů a lhůtě zpracování nebo správy osobních údajů.

**17. Chybí souhlasy se zpracováním osobních údajů v rámci zaměstnaneckého poměru a informace o předávání osobních údajů zpracovatelům**

V rámci pracovních smluv musí být nově informace o správě a zpracování osobních údajů zaměstnanců. Stávající zaměstnanci musí být informování, k čemuž dojde v rámci školení.

**18. Chybí pravidla pro uchovávání osobních údajů zaměstnanců**

Budou součástí vnitřního předpisu.

# 9 PROJEKT IMPLEMENTACE GDPR

Hlavní částí práce je projekt implementace nutných změn v souvislosti s Obecným nařízením analyzované společnosti. V projektové části dojde k odstranění nesouladů zjištěných v rámci analýzy současného stavu zpracování osobních údajů. Projekt je navržen tak, aby byla samotná implementace zvládnuta do doby, než vstoupí Obecné nařízení v účinnost, tedy do 25. května 2018, a tudíž dojde k zabránění případným sankcím.

## 9.1 Cíle projektu

Cílem celého projektu je implementovat Obecné nařízení do vybrané společnosti tak, aby veškeré zpracování osobních údajů, probíhající ve společnosti, bylo v souladu s tímto nařízením a společnost nebyla vystavena nebezpečí v podobě hrozících sankcí. Po stanovení jednotlivých kroků projektu dojde k jejich postupnému plnění. V první řadě je důležité stanovit účel zpracování jednotlivých osobních informací, dále určit rozsah zpracovávaných dat, formulovat souhlas se zpracováním osobních údajů, stanovit pravidla pro přístup k jednotlivým osobním údajům, provést revizi smluv s jednotlivými zpracovateli osobních údajů, upravit vnitřní předpis v souladu s pravidly pro ochranu osobních údajů. V neposlední řadě je důležité projekt celkově zhodnotit, tedy provést kalkulaci nákladů, rizikovou analýzu a zhodnotit jeho přínosy.

## 9.2 Aktivity projektu a časový harmonogram

Na základě přechozích kroků, tedy seznámení s požadavky Obecného nařízení, popsanými v teoretické části této diplomové práce, a provedení vstupní analýzy firemních procesů, při nichž dochází k práci s osobními údaji, byl sestaven časový harmonogram nadcházejících aktivit. Samotná vstupní analýza byla provedena v průběhu 30 pracovních dnů. S jejím provedením se začalo v lednu letošního roku, a to z kapacitních důvodů. V interních pravidlech společnosti bylo zavedeno, že je nejdříve potřeba zavést MiFID II, které začalo platit 3. ledna 2018. Jedná se o směrnici o trzích finančních nástrojů, v českém právním prostředí implementovanou především zákonem o podnikání na kapitálovém trhu. Poté již mohla přijít na řadu implementace Obecného nařízení.

Před uvedením jednotlivých činností bylo nutné posoudit, zda provést DPIA (posouzení vlivu na ochranu osobních údajů) a zda bude potřeba DPO (pověřenec pro ochranu osobních údajů).

Na základě poznatků z teoretické části diplomové práce, kde bylo toto posouzení vlivu na ochranu osobních údajů podrobně rozebráno v podkapitole 5.4 DPIA – Data Protection Impact Assessment, bylo rozhodnuto, že proces DPIA není potřeba provést, jelikož neexistuje pravděpodobnost vysokého rizika. Komplexní riziková analýza je pak rozpracována v poslední kapitole této práce.

DPO rovněž nemusí být jmenován, protože společnosti se netýká ani jeden ze tří případů uvedených v teoretické části v podkapitole 5.3 DPO – Data Protection Officer.

Časový harmonogram projektu je zpracován pomocí metody CPM – Critical Path Method, jež patří mezi základní deterministické metody síťové analýzy. Cílem je stanovení doby trvání projektu na základě délky tzv. kritické cesty. Nejdříve se stanoví jednotlivé činnosti projektu, u nichž se stanoví doba trvání (v tomto případě je doba trvání určena ve dnech), dále se určí předchozí činnosti – tedy u každé z činností musí být jasně dané, které z činností jí musí předcházet.

Samotné činnosti pro časový harmonogram implementace Obecného nařízení jsou:

Tab. 5 Přehled jednotlivých činností implementace (vlastní zpracování)

| Činnost | Popis činnosti | Doba trvání (dny) | Předchozí činnost |
|---|---|---|---|
| A | Stanovení přesného účelu zpracování osobních údajů. | 1 | - |
| B | Stanovení rozsahu zpracovávaných osobních údajů pro jednotlivé činnosti | 1 | A |
| C | Stanovení rozsahu zpracovávaných osobních údajů po výpovědi smlouvy | 1 | A, B |
| D | Vytvoření dokumentu poskytující informace o právech subjektu údajů, dále dokumentu poskytujícímu informace správě o zpracování osobních údajů | 3 | A, B |
| E | Vytvoření souhlasu se zpracováním osobních údajů pro variantu smlouvy i webových stránek | 2 | A, B, D |

| | | | |
|---|---|---|---|
| F | Vytvoření pravidel přístupů k jednotlivým osobním údajům | 3 | A, B, C |
| G | Návrh evidence zpracovávání osobních údajů | 5 | A, B, C, F |
| H | Revize smluv s jednotlivými zpracovateli osobních údajů | 5 | A, B, C, F |
| I | Vytvoření dokumentu pro ohlášení incidentů ÚOOÚ a dokumentu v případě porušení pravidel vůči zákazníkům | 1 | A, B, C |
| J | Vytvoření systému pro vyhodnocování rizik ke každému způsobu zpracování | 5 | A, B, F, G |
| K | Vytvoření vzorových odpovědí na dotazy subjektů údajů | 2 | A, B, C, D |
| L | Revize pracovních smluv, které budou v budoucnu uzavírány | 1 | A, B, C |
| M | Vytvoření pravidel osobních údajů zaměstnanců | 2 | A, B, C, L |
| N | Proškolení všech zaměstnanců o interních pravidlech podle GDPR a o správě jejich osobních údajů | 2 | A, B, C, E, F, G, M |
| O | Vytvoření kontrolních mechanismů uvnitř společnosti | 1 | N |

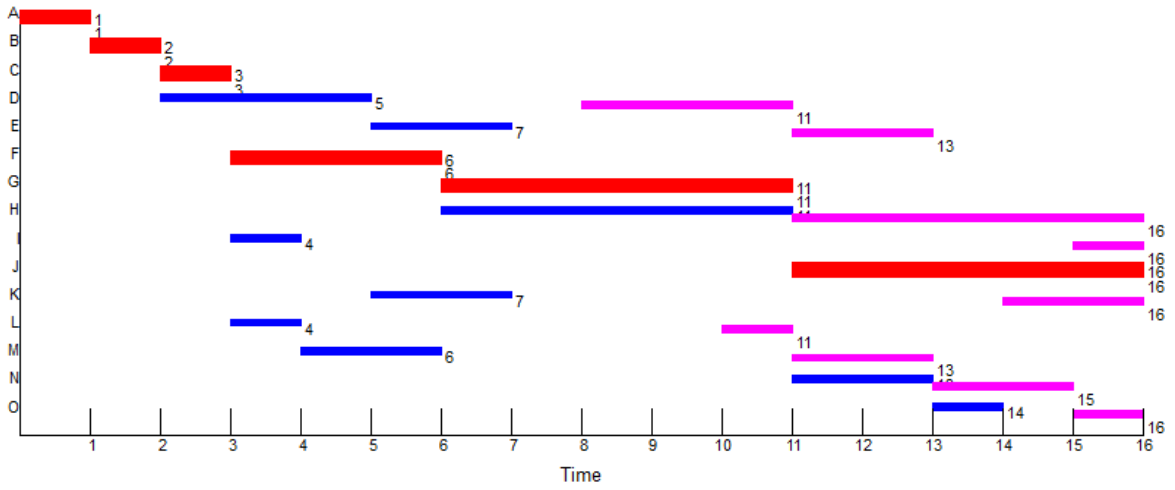
Vstupní data jsou zpracována v programu QM for Windows, který po jejich zadání určí nejkratší možnou dobu, za niž je možné projekt uskutečnit. V případě projektu implementace Obecného nařízení se jedná o 16 dnů, jak vyplývá z tabulky níže. Tabulka rovněž zobrazuje termíny nejdříve možné (Early Start) a termíny nejpozději přípustné (Late Start), tedy kdy se musí nejpozději začít tak, aby byl projekt dokončen v čase.

| Activity | Activity time | Early Start | Early Finish | Late Start | Late Finish | Slack |
|---|---|---|---|---|---|---|
| Project | 16 | | | | | |
| A | 1 | 0 | 1 | 0 | 1 | 0 |
| B | 1 | 1 | 2 | 1 | 2 | 0 |
| C | 1 | 2 | 3 | 2 | 3 | 0 |
| D | 3 | 2 | 5 | 8 | 11 | 6 |
| E | 2 | 5 | 7 | 11 | 13 | 6 |
| F | 3 | 3 | 6 | 3 | 6 | 0 |
| G | 5 | 6 | 11 | 6 | 11 | 0 |
| H | 5 | 6 | 11 | 11 | 16 | 5 |
| I | 1 | 3 | 4 | 15 | 16 | 12 |
| J | 5 | 11 | 16 | 11 | 16 | 0 |
| K | 2 | 5 | 7 | 14 | 16 | 9 |
| L | 1 | 3 | 4 | 10 | 11 | 7 |
| M | 2 | 4 | 6 | 11 | 13 | 7 |
| N | 2 | 11 | 13 | 13 | 15 | 2 |
| O | 1 | 13 | 14 | 15 | 16 | 2 |

Obr. 6 Metoda CPM (vlastní zpracování v programu QM for Windows)

Poslední sloupeček tabulky ukazuje celkovou rezervu (Slack) u jednotlivých činností. Celková rezerva představuje časový interval, v němž lze posunout danou činnost tak, aby tím nedošlo k ovlivnění výsledného plánovaného termínu. Činnosti, které mají nulovou celkovou rezervu, tvoří již zmiňovanou kritickou cestu.

Na obr. 7 je poté vyobrazena kritická cesta (vyobrazena červenou barvou) nacházející se u činností A, B, C, F, G a J. U těchto činností nevzniká žádná časová rezerva, což znamená, že zdržení počátku tohoto úkolu nebo prodloužení doby jeho trvání bude mít vliv na konečné datum projektu. Vytváří nejdelší možnou (z hlediska času) cestu z počátečního bodu do koncového bodu. Na tyto činnosti je tedy potřeba se nejvíce zaměřit, aby došlo k zabezpečení včasného dokončení projektu.




Obr. 7 Metoda CPM – kritická cesta (vlastní zpracování v programu QM for Windows)

Kromě těchto činností, sepsaných v rámci zpracování časového harmonogramu, bylo zapotřebí připravit nový vnitřní předpis, zahrnující všechna pravidla pro získávání, správu, ochranu a zpracování osobních údajů. Ten byl postupně zpracováván spolu s ostatními činnostmi, tedy především spolu s těmi, u nichž byla zjištěna největší časová rezerva. S využitím rezerv a s tvorbou vnitřního předpisu činí tedy skutečná celková doba implementace **32 dní**.

## 9.3 Stanovení účelu pro jednotlivé osobní informace

V rámci projektu implementace Obecného nařízení jsou nově definovány účely zpracování osobních údajů. Veškeré osobní údaje budou zpracovávány z důvodu:

- uzavření smlouvy o poskytování investičních služeb a poskytování těchto služeb (tento účel v sobě zahrnuje i identifikace zákazníka dle zákona 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, tedy identifikaci rizikovosti všech zákazníků). Vzhledem ke skutečnosti, že má tento účel právní základ, není třeba zajišťovat souhlas klienta pro uchovávání jeho osobních údajů.

- uzavření smlouvy o poskytování platebních služeb a poskytování těchto služeb (v tomto případě se rovněž jedná o identifikaci zákazníka dle výše uvedeného zákona, a není tedy potřeba zajistit souhlas)

- oslovování zákazníků s novinkami uskutečňovanými analyzovanou společností

## 9.4 Rozsah zpracovávaných osobních údajů

Dalším krokem je stanovení rozsahu zpracovávaných osobních údajů, a to jak pro jednotlivé činnosti, tak po výpovědi smlouvy.

### 9.4.1 Rozsah zpracovávaných osobních údajů klientů

Jak již bylo zmíněno v jedné z předcházejících kapitol, při provádění analýzy současného stavu zpracování, u klientů, kteří se u společnosti registrují pro využití služeb jednoho z jejich produktů, dochází ke zpracování osobních a adresních osobních údajů, dále údajů jiných osob.

Obecně společnost využívá dvou rozsahů zpracování osobních údajů, a to jednak *zákonného*, na jehož základě dochází k identifikaci klienta pro potřeby uzavření smlouvy o poskytování finančních služeb dle AML zákona. Druhým typem zpracování je *dobrovolné zpracování*, k němuž je potřeba získat souhlas od klienta. Toto dobrovolné zpracování je pouze po dobu trvání smlouvy klienta (po zadání výpovědi se ruší).

Po ukončení smluvního vztahu se o jednotlivých klientech mohou evidovat pouze osobní data vyplývající z navazujících zákonných povinností. Jedná se o dobu 7 let, což je mimo jiné doba, po kterou musí dojít k uchovávání nahrávek hovorů (veškeré hovory s klienty i mezi zaměstnanci v rámci pracovních telefonátů jsou nahrávány).

## 9.5 Dokumenty

V rámci zpracování osobních údajů dle Obecného nařízení je zapotřebí vytvořit dokument, jenž bude poskytovat subjektům údajů informace o jejich právech. Součástí takového dokumentu budou především tyto náležitosti:

- za jakým účelem jsou tyto osobní data zpracovávány

- kdo je zpracovává, tedy ne jenom samotná společnost, ale jakému zpracovateli jsou dále osobní údaje poskytovány (např. zřizovateli servisního portálu apod.)

- poučení o ostatních právech klienta, které jsou uvedeny v kapitole **3.4 Práva subjektu údajů**

Dále se vytvoří dokument, jenž bude poskytovat informace správě o zpracování osobních údajů.

Stručný vzor dokumentu poskytujícího informace o právech subjektů osobních údajů se nachází v příloze této práce.

## 9.6 Souhlas se zpracováním

V rámci osobních údajů, které jsou zpracovávány za určitým účelem bez zákonného titulu (například zpracování osobních údajů za účelem rozesílání newsletterů), je vyžadován svobodný, informovaný a jednoznačný souhlas.

Na webových stránkách bude tento souhlas poskytován prostřednictvím zaškrtnutí políčka „Souhlasím se zasíláním novinek ve formě Newsletteru skupiny …“

Pro papírovou formu uchovávání osobních údajů je vytvořen dodatek ke smlouvě, jenž bude obsahovat souhlas klienta se zpracováváním osobních údajů. Součástí tohoto dodatku budou opět popsána práva klienta spolu s účely zpracování, a bude se zde nacházet věta „Podpisem tohoto dokumentu potvrzuji souhlas se zpracováním osobních údajů pro shora uvedené účely“.

## 9.7 Pravidla přístupů

Přístup ke všem osobním údajům bude rozdílný na základě toho, o jaké osobní údaje se jedná a pro jaký účel. Přístup tedy bude zvlášť pro jednotlivá oddělení a v rámci těchto oddělení bude docházet k rozdílům i mezi jednotlivými uživateli. Vedoucí oddělení (back office, customer care, compliance) budou mít přístup ke všem potřebným údajům, ostatní uživatelé už pak podle aktuální potřeby. Jedná se především o přístupy do servisního portálu, databáze IVAN, ale také přístupy na jednotlivé disky v počítačích. Každý uživatel má přístup pod individuálním jménem a heslem, které musí odpovídat bezpečnostním požadavkům.

## 9.8 Evidence zpracovávání osobních údajů

Evidenci zpracovávání osobních údajů je zapotřebí vytvořit pro případy kontroly Úřadu na ochranu osobních údajů. V případě, že k takovéto kontrole dojde, musí být společnost schopna poskytnout přehled veškerých osobních údajů, které shromažďuje a zpracovává.

Tab. 6 Návrh evidence zpracovávání osobních údajů (vlastní zpracování)

| | |
|---|---|
| Správce | XY, a.s. |
| Zpracovávaný druh osobních údajů | Adresní a identifikační údaje – jméno, příjmení, datum narození, atd.<br>Popisné údaje – vzdělání, odborné znalosti, výše mzdy, atd.<br>Údaje o jiné osobě – adresní a identifikační údaje pověřené osoby (disponenta). |
| Kategorie subjektů, kterých se tyto údaje týkají | Klienti (fyzické osoby), zaměstnanci |
| Účely zpracování | - uzavření smlouvy o poskytování investičních služeb a poskytování těchto služeb<br>- uzavření smlouvy o poskytování platebních služeb a poskytování těchto služeb<br>- oslovování zákazníků s novinkami |
| Zdroj získání osobních údajů | - u registrace nových klientů (online, papírová smlouva obsahující údaje)<br>- pracovní smlouvy se zaměstnanci<br>- životopisy |
| Způsob uložení osobních údajů | - elektronická podoba (servisní portál, databáze IVAN, naskenované smlouvy na místním disku)<br>- papírová podoba (smlouvy) |
| Zpracovatelé osobních údajů | - zřizovatel servisního portálu<br>- banky, atd. |
| Doba uchování | |

V tabulce výše je vyobrazen návrh přehledu evidence osobních údajů. U zpracovávaného druhu osobních údajů budou vypsány veškeré osobní údaje tak, jak jsou uvedeny v rámci analýzy současného systému zpracovávání osobních údajů.

Doba uchování bude vycházet z rozsahu zpracování osobních údajů rozebírané v rámci jedné kapitol výše.

## 9.9 Systém rizik

Dalším krokem implementace je vytvoření systému pro vyhodnocování rizik ke každému způsobu zpracování.

Pro hodnocení rizik je použita jednoduchá polokvantitativní metoda „PZH“. Prostřednictvím této metody dochází k vyhodnocování příslušného rizika ve třech jeho složkách, a to s ohledem na pravděpodobnost vzniku (v tabulce označeno pod písmenem P), závažnost následku (označení Z) a názor hodnotitelů (označení H). U všech tří okruhů byla použita stupnice vzestupně od 1 do 5 na základě odhadu, kde je zjednodušeně zahrnutá míra, úroveň a kritéria nebezpečí a ohrožení. Vynásobením těchto tří hodnot se pak získá hodnota celkového rizika, v tabulce označeného písmenem R. Jednotlivé míry rizika jsou pak následující:

- bezvýznamné riziko s hodnotou celkového rizika < 3

- akceptovatelné riziko s hodnotou celkového rizika v rozmezí 3 – 10

- mírné riziko s hodnotou celkového rizika v rozmezí 11 – 50

- nežádoucí riziko s hodnotnou celkového rizika v rozmezí 51 – 100

- nepřijatelné riziko s hodnotou celkového rizika > 100.

Níže je zpracovaná tabulka, v níž jsou analyzovaná rizika, která se mohou vyskytnout v souvislosti se zpracováváním osobních údajů a to jak v papírové podobě, tak té elektronické.

Tab. 7 Analýza rizik uchovávání dat metodou PZH (vlastní zpracování)

| Druh činnosti | Zdroj rizika | Identifikace nebezpečí | Hodnocení závažnosti rizika | | | | Bezpečností opatření |
|---|---|---|---|---|---|---|---|
| | | | P | Z | H | R | |
| Uchovávání dat v papírové podobě | Zcizení dat outsorcingovou společností | Přístup na server | 3 | 3 | 2 | 18 | Smluvní zajištění o způsobu zpracování |
| | Únik hesel zaměstnanců; jejich předávání; ztráta | Vzájemné prozrazení hesel mezi zaměstnanci; přístupný seznam hesel | 3 | 3 | 3 | 27 | Automatická změna hesla; proškolení zaměstnanců |
| | Ztráta dat zákazníka | IT chyba s následkem selhání systému | 3 | 4 | 3 | 36 | Konfirmační e-mail o přijetí údajů |
| Uchovávání dat v elektronické podobě | Zcizení a následné zneužití dat | Volný přístup k datům v papírové formě | 4 | 3 | 3 | 36 | Uzamykatelné místo, přístup na unikátní kód |
| | Ztráta záznamů | Nepřehlednost v záznamech | 4 | 2 | 2 | 16 | Nastavení systému; archivace; uspořádání dat |
| | Zničení důležitých dokumentů | Chyba zaměstnance | 2 | 3 | 3 | 18 | Školení |
| | Zničení důležitých dokumentů | Nahodilá událost (požár, záplavy) | 2 | 3 | 4 | 24 | Záloha na dvou serverech, každý v jiných prostorách |
| | Ztráta (vybledlnutí) důležitých informací | Opotřebení papíru a inkoustu | 3 | 2 | 2 | 12 | Skenování, tvorba kopií, zálohy |

Na základě provedení rizikové analýzy v souvislosti se zpracováváním dat jak v papírové, tak elektronické podobě, je možno vyhodnotit, že žádné z rizik není nežádoucí, ani nepřijatelné. Celkové riziko se u všech možností pohybuje pod hranicí 50, což je hranice mírného rizika.

Jako nejzávažnější bylo vyhodnoceno riziko ztráty dat zákazníka v důsledku selhání systému kvůli IT chybě. Hodnota celkového rizika činí 36, tedy patří do skupiny mírného rizika, což znamená, že naléhavost opatření sice není tak závažná, jako u rizik nežádoucích a nepřijatelných, ale je nutno realizovat bezpečnostní opatření dle zpracovaného plánu podle rozhodnutí vedení organizace. V případě, že by toto riziko bylo spojeno se značnými nebezpečnými následky, musí se provést další zhodnocení, aby se přesněji stanovila pravděpodobnost vzniku újmy jako podkladu pro stanovení potřeby dosažení zlepšení a snížení rizika. V tomto případě však nebezpečné následky nehrozí. Jako zajištění proti tomuto riziku by mohl fungovat například konfirmační e-mail, který by přišel klientovi po provedení registrace a klient by tak měl potvrzení o tom, že registrace byla provedena a veškerá data jsou uložena. Dále je třeba mít smluvně zajištěný způsob zpracování s outsorcingovou společností, neboť portály a databáze, kam se údaje propisují, jsou provozovány právě externími společnostmi.

Stejná situace je v případě rizika zcizení a následného zneužití dat z důvodu volného přístupu k datům v papírové formě. Ani v tomto případě však nehrozí nebezpečné následky. Zabezpečení proti tomuto riziku by mělo být především v podobě uzamykatelných místností, kde by se data v papírové formě uchovávaly. Tyto místnosti by pak byly přístupné na unikátní kódy, tedy každý zaměstnanec by měl svůj vlastní, a bylo by tak možné zjistit, kdo se k těmto údajům dostal jako poslední.

U ostatních analyzovaných rizik se rovněž jedná o rizika mírná, u nichž je potřeba tyto rizika snížit s tím, že prostředky na snížení rizika musí být implementovány ve stanoveném časovém období. U žádného z nich opět neexistuje hrozba nebezpečných následků.

Důležitým poznatkem u více rizik je to, že je potřeba data zálohovat, pokud možno, tak na více serverech, které se budou nacházet na různých místech. Pokud jsou data v papírové formě, je dobré je skenovat, aby se předešlo jejich zničení z důvodu vyblednutí inkoustu, nepředvídatelných škod v podobě záplav či požárů.

## 9.10 Revize smluv

K revizi smluv musí dojít v rámci všech dalších zpracovatelů osobních údajů, jejichž přehled je vyobrazen v Tab. 5.

S jednotlivými partnery je v rámci smluv uvedena povinnost mlčenlivost a ochrana systému Objednatele, kdy se smluvní strany zavazují zachovávat mlčenlivost o všech skutečnostech, zejména o důvěrných informacích, které se dozvěděly v rámci spolupráce nebo plnění Smlouvy (osobní údaje klientů). Za důvěrné informace se přitom nepovažují:

- ty, které se staly veřejně známými, aniž by to zavinila záměrně či opominutím přijímací strana;

- takové, jež měla přijímací strana právoplatně k dispozici před uzavřením Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací;

- výsledky postupu, při kterém k nim přijímací strana dospěje nezávisle na vůli druhé strany a je to schopna doložit svými záznamy nebo důvěrnými informace třetí strany;

- po uzavření smlouvy poskytnuté přijímací straně třetí osobou, která takové informace nezískala přímo ani nepřímo od strany, jež je jejich vlastníkem.

Poskytovatel se dále zavazuje, že bude dodržovat ochranná a bezpečnostní opatření Objednatele, v případě přístupu k technickým zařízením Objednatele.

Dále dochází mezi partnerem a analyzovanou společností k uzavření *Dohody o mlčenlivosti*. Součástí této dohody je v úvodu popsán předmět dohody, tedy v čem spočívá spolupráce obou stran. Dále jsou zde rozepsány povinnosti obou stran, tedy jak nakládat s danými informacemi – využívat je pouze pro účely zamýšlené spolupráce, neposkytovat je třetím stranám, přistupovat k získaným informacím se stejnou péčí, jako přistupují k vlastním datům.

Další část této dohody je věnována právům, zárukám a závazkům. Součástí je i postup v případě porušení jakéhokoliv závazku určeného v této dohodě, kdy je smluvní straně, která porušila tento závazek dána smluvní pokuta.

Dohoda vstupuje v platnost po řádném podepsání všemi stranami do data ukončení spolupráce a/nebo smluvních vztahů mezi smluvními stranami. Povinnost zachovávat důvěrnost informací končí pět let po ukončení platnosti této dohody.

V neposlední řadě jsou zde uvedeny způsoby řešení sporů, kdy je kladen důraz, aby strany vyvinuly maximální snahu vyřešit případné spory mírně, pokud tomu tak nebude, bude rozhodováno podle práva České republiky u místně příslušného soudu.

Poslední část je věnována přidruženým společnostem, kdy je zde definováno, co je myšleno pod pojmem přidružená společnost, a také za jakých podmínek se přidružené společnosti zapojují do výměny informací.

K této dohodě je potřeba vytvořit dodatek. Jeho návrh je součástí přílohy této diplomové práce.

## 9.11 Dokument pro ohlášení incidentů

V případě, že nastane jakýkoliv incident či dojde k porušení pravidel vůči zákazníkům, je potřeba tuto skutečnost zanést do zadaného formuláře. Formulář bude obsahovat náležitosti uvedené v následující tabulce:

Tab. 8 Vzor formuláře pro ohlášení incidentů (vlastní zpracování)

| **I. Identifikační údaje Správce** | |
|---|---|
| 1. Identifikační údaje společnosti | |
| Název společnosti | |
| Adresa (sídlo společnosti) | |
| 2. Typ oznámení | - úplné oznámení (pole v sekci II. a III. vyplnit do 72 hodin od zjištění incidentu<br>- oznámení ve dvou krocích (pole v sekci II. vyplněno do 72 hodin a v sekci III. postupně bez dalšího zbytečného odkladu) |
| **II. Hlavní údaje k porušení zabezpečení** | |
| 1. Odvětví dotčené strany | (uvedeny jednotlivá odvětví) |
| 2. Počet zaměstnanců | |
| 3. Velikost organizace (roční obrat) | |
| 4. Členský stát, kde došlo k porušení zabezpečení | |

| | |
|---|---|
| 5. Datum a čas porušení zabezpečení | |
| 6. Příčina porušení zabezpečení | Nehoda, nedbalost, škodlivý útok, apod. |
| 7. Pravděpodobné dopady porušení zabezpečení | Krádež osobních údajů, škoda na majetku, přerušení provozu, přímá finanční újma, apod. |
| 8. Stav zašifrování dotčených osobních údajů | Kompletní, částečné, žádné |
| 9. Způsob IT podpory | Interní, externí |
| 10. Technická a organizační opatření přijatá ke snížení následků porušení zabezpečení | Obnovení dat, školení zaměstnanců, posílení bezpečnosti dat, apod. |
| 11. Sjednané pojištění na daný typ incidentu? | |
| **III. Doplňující informace** | |
| 1. Odhadovaná škoda (Kč) | |
| 2. Počet dotčených souborů osobních údajů | |
| 3. Bylo porušení zabezpečení osobních údajů oznámeno subjektu údajů? | |
| 4. Odhadované finanční ztráty (náklady na oznámení, finanční újma) | |
| Bezpečnostní opatření (aby se porušení zabezpečení neopakovalo) | Vylepšení bezpečnostních opatření s ohledem na bezpečnost dat, jiná technická a organizační opatření, apod. |

## 9.12 Formulace odpovědí na dotazy klientů

V rámci implementace je rovněž potřeba vytvořit vzorové odpovědi na možné dotazy klientů týkající se jejich osobních údajů, s nimiž analyzovaná společnost nakládá.

U každé poskytované služby budou vytvořeny možné dotazy (typy dotazů) a k nim vhodně formulovaná odpověď. Například klient využívající službu FX vypověděl smlouvu a jeho dotaz zněl:

„*Jaké mé osobní data bude Vaše společnost uchovávat i po vypovězení smlouvy a po jakou dobu?“*

**Odpověď:**

„Dobrý den, pane/paní …,

V rámci smluvního vztahu navázaného mezi Vámi a naší společností docházelo ke zpracování Vašich osobních údajů. Dobrovolné zpracování sloužící pro marketingové účely vypovězením smlouvy zaniká, nebude tedy již nadále docházet k zasílání novinek na Vámi uvedený e-mail.

Po ukončení smluvního vztahu budeme evidovat Vaše osobní data vyplývající z navazujících zákonných povinností. Jedná se o tyto osobní data, které jsme získali prostřednictvím výpovědi:

- jméno a příjmení

- datum narození

- adresa trvalého pobytu.

Tyto údaje budou uchovávány po dobu 7 let. Po tu samou dobu budou uchovávány i veškeré informace o provedených obchodech a nahrávky hovorů, které proběhly mezi Vámi a naší společností.“

Očekává se, že tento typ dotazu bude patřit mezi nejčastější, ať už se bude jednat o dotazy směřující ke zpracovávání osobních údajů v průběhu trvání smluvního vztahu, či po vypovězení smlouvy. Odpověď bude mít stejnou strukturu u všech služeb, budou se pouze měnit vypsané osobní údaje, kdy například v průběhu trvání smluvního vztahu je těchto dat daleko více.

## 9.13 Revize pracovních smluv

V této části projektu je potřeba provést revizi pracovních smluv, které budou uzavírány v budoucnu. Společnost pracuje se třemi typy smluv a to:

- dohoda o provedení práce

- pracovní smlouva

- smlouva o výkonu funkce člena představenstva.

U dohody o provedení práce a pracovní smlouvy je vytvořen dodatek, v němž je jasně určeno, kdo zpracovává údaje zaměstnanců a po jakou dobu dochází k jejich zpracování.

## 9.14 Pravidla osobních údajů zaměstnanců

Návrh celého projektu je zaměřen jak na klienty společnosti, tak na její zaměstnance, jejichž osobní údaje jsou zde rovněž zpracovávány. Osobní údaje zaměstnanců jsou přitom zpracovány za účelem uzavření pracovní smlouvy / dohody o provedení práce.

Rozsah zpracovávaných osobních údajů již byl zmíněn v přechozích kapitolách.

### 9.14.1 Rozsah zpracovávaných osobních údajů zaměstnanců

U zaměstnanců jsou vedeny dokumenty a písemnosti, které jsou nezbytné pro výkon práce, jakými jsou životopis, případně pracovní posudek od předchozího zaměstnavatele, pracovní smlouva, mzdový výměr, apod.

Každý nový zaměstnanec je povinen vyplnit template (vzor) pro získání potřebných osobních údajů. Původní formulář obsahuje jednak *osobní údaje* (jméno, příjmení, rodné příjmení, trvalé bydliště, tituly, kontaktní adresu, rodinný stav, rodné číslo, datum a místo narození, číslo OP/pasu, státní příslušnost, telefon. Dále *údaje pro výpočet mzdy* (BÚ/kód banky, ostatní srážky, údaje o dětech včetně jejich jmen, rodných čísel, data narození a zda je studující či nikoliv. Následují údaje o *přechozím zaměstnání v daném roce a roce předchozím,* rovněž je zde nutné uvést informace o *vzdělání a dalších kvalifikacích (jazyk, řidičský průkaz apod.).*

Tento formulář je příliš obsáhlý, a proto došlo k jeho redukci pouze na opravdu potřebné údaje. Zůstaly základní osobní údaje (některé původní byly vyčleněny), pro výpočet mzdy poté uvedený bankovní účet, informace o ostatních srážkách a v případě dětí pouze základní informace obsahující počet dětí, případné upozornění na to, zda studují či nikoliv. Údaje o předchozím zaměstnání, vzdělání a další kvalifikaci byly z tohoto formuláře odstraněny vzhledem ke skutečnosti, že jsou již obsaženy v životopisech, které každý zaměstnanec (uchazeč o pracovní pozici) dokládá. Vzor nově vypadajícího formuláře je v tabulce níže.

Tab. 9 Vzor formuláře pro vyplnění osobních údajů zaměstnance (vlastní zpracování)

| **Společnost** | **OSOBNÍ ÚDAJE** | | **IČ** |
|---|---|---|---|
| **Sídlo:** | | | |
| **Osobní údaje zaměstnance** | | | |
| Příjmení | | Jméno | |
| Trvalé bydliště | | Datum narození | |
| Kontaktní adresa (v případě, že se liší od trvalého bydliště) | | Místo narození | |
| Rodné číslo | | Telefon | |
| Číslo OP/pasu | | E-mail | |
| **Údaje pro výpočet mzdy** | | | |
| BÚ/kód banky | | Ostatní srážky | |
| Zdravotní pojišťovna | | Druh/částka | |
| Nařízené srážky | | BÚ/kód banky | |
| Počet dětí | | Var. symbol/ks | |
| Počet dětí – studentů | | Specifický symbol | |

Po skončení pracovního poměru může zaměstnavatel zpracovávat osobní údaje zaměstnance pouze v omezeném rozsahu. Bez souhlasu zaměstnance mohou být uchovávány takové údaje, u nichž je to stanoveno platnými právními předpisy (např. pro účely důchodového a sociálního pojištění). Osobní údaje mohou být uchovávány po dobu, po kterou trvá povinnost zaměstnavatele uchovávat osobní údaje, nebo po dobu nezbytnou k vypořádání vzájemných práv a povinností zaměstnavatele a zaměstnance.

**Archivace dokumentů personálních a mzdových dat**

Konkrétně se jedná o uchovávání *těchto dokumentů*:

- evidenční listy důchodového pojištění po dobu 3 let

- účetní doklady po dobu 5 let

- záznamy o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti po dobu 6 let

- mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění po dobu 30 let.

Vzor mzdového listu je součástí příloh této diplomové práce.

Za záznamy o těchto skutečnostech jsou považovány doklady o druhu, vzniku a skončení pracovněprávního vztahu, záznamy o pracovních úrazech a o nemocech z povolání a záznamy o evidenci pracovní doby včetně doby pracovního volna bez náhrady příjmu.

Pro *oblast sociálního pojištění* platí uchovávání:

- účetních záznamů o údajích potřebných pro stanovení a odvod pojistného po dobu 10 let

- stejnopisy evidenčních listů po dobu 3 let

- evidence údajů týkající se poživatelů starobního nebo invalidního důchodu po dobu 10 let

### 9.14.2 Informace o zpracovávání osobních údajů zaměstnanců

Jak již bylo řečeno, součástí příloh této diplomové práce je i vzor dokumentu podávajícího informace o zpracování osobních údajů. Tento dokument slouží k informování klientů, v případě zaměstnanců je potřeba jej poupravit, struktura však zůstává stejná.

U zaměstnanců dochází, stejně jako u klientů, ke zpracování údajů adresních a identifikačních a také popisných. Změna nastává u účelu zpracování, kdy se jedná o uzavření pracovní smlouvy či dohody o provedení práce, a především pak v části „kdo osobní údaje zpracovává“. Kromě společnosti, která je v tomto případě správcem, je zpracovatelem účetní společnost, která má přístup k veškerým údajům zaměstnanců.

Osobní údaje zaměstnanců jsou získávány prostřednictvím uzavíraných smluv, a také z dokládaných životopisů.

I zde je nutné stanovit jasná pravidla pro přístup k osobním údajům zaměstnanců. Kromě zmíněné účetní společnosti k nim bude mít přístup oddělení back office a compliance. Za oddělení back office se bude jednat o jednu osobu, která k nim bude mít zabezpečený přístup.

## 9.15 Proškolení zaměstnanců

Po provedení všech předešlých kroků je nutno proškolit všechny zaměstnance o interních pravidlech podle Obecného nařízení a o správě jejich osobních údajů.

K tomuto školení zároveň dojde až v době, kdy bude kompletně zhotoven vnitřní předpis. Ten se vytváří postupně, v průběhu celé implementace, jelikož se jedná o časově náročnější činnost a u ostatních činností vznikly časové rezervy a tedy prostor pro jeho tvorbu.

Školení proběhne u zaměstnanců jak ve Zlíně, tak v Praze a všichni budou obeznámeni s novým systémem zacházení a uchování veškerých osobních údajů analyzovanou společností. Rovněž jim budou vysvětleny přístupy k jednotlivým údajům a dána přístupová jména a hesla.

Je potřeba, aby zaměstnanci pochopili podstatu Obecného nařízení, a proto bude školení sestaveno tak, že na začátku dojde k seznámení s tím, co Obecné nařízení je, jaké jsou jeho zásady a požadavky a jaké změny s sebou přináší. V další části již pak dojde k samotnému rozebírání změn ve společnosti.

## 9.16 Kontrolní mechanismy

V neposlední řadě je potřeba navrhnout a zavést kontrolní mechanismy uvnitř společnosti, které budou zaměřeny na systém zpracování osobních údajů a budou sloužit pro kontrolu, zda nedochází k chybným krokům v této oblasti.

Kontroly budou na měsíční bázi, bude zapotřebí je provést vždy v průběhu prvního týdne daného měsíce.

Tab. 10 Návrh kontroly systému zpracování osobních údajů (vlastní zpracování)

| Jméno | Příjmení | Množství zpracovávaných dat | Smlouvy | Uložení smluv | Podpis u newsletterů | Datum kontroly |
|---|---|---|---|---|---|---|
| | | | | | | |

V tabulce jsou uvedeny náležitosti, které by měla obsahovat kontrola systému zpracování osobních údajů. Každý měsíc se z databáze vybere 10 náhodných klientů, u nichž se provedou následující kontroly:

- zda společnost nakládá pouze s údaji, které jsou skutečně potřebné pro účely zpracování (minimalizace dat);

- kontrola všech uzavřených smluv (o poskytování investičních služeb, o poskytování platebních služeb), tedy zda byly podepsány oběma stranami;

- dále zda jsou smlouvy naskenovány na místním disku a jejich papírová podoba se nachází na příslušném místě

- v případě dobrovolného zpracování dat, sloužícímu k zasílání novinek klientům, je nutno zkontrolovat podpis klienta sloužící pro souhlas se zasíláním těchto novinek.

# 10 ZHODNOCENÍ PROJEKTU

Cílem projektu byla implementace Obecného nařízení o ochraně osobních údajů ve vybrané společnosti. Toto nařízení vstoupí v účinnost 25.5.2018 a bylo tedy zapotřebí provést celou implementaci tak, aby byla časově zvládnutelná do této doby a došlo k zabránění případným sankcím. Příprava a samotné provedení implementace s sebou nese určitá rizika a nákladové zatížení. Právě z tohoto důvodu je na závěr této diplomové práce, kromě sumarizace přínosů projektu, také provedena nákladová analýza a riziková analýza jak implementace, tak obecně zpracování osobních údajů.

Po provedení analýzy současného zpracování a zacházení s osobními údaji byly následně sepsány nesoulady vyplývající z této analýzy. Po zjištění nesouladů došlo k vytvoření časového harmonogramu projektu, který byl koncipován tak, aby došlo k odstranění všech nesouladů, tedy aby veškeré činnosti, související s osobními údaji, odpovídaly požadavkům Obecného nařízení. Poté již byly provedeny jednotlivé kroky tohoto harmonogramu tak, aby vše bylo zvládnuto do doby, než vejde Obecné nařízení v účinnost.

V následujících podkapitolách je provedena riziková analýza projektu, tedy implementace nařízení, dále nákladová analýza a v neposlední řadě zhodnocení projektových přínosů.

## 10.1 Riziková analýza

Pro zhodnocení projektů je provedena riziková analýza v souvislosti se samotnou implementací Obecného nařízení. Pro tuto analýzu je opět použita metoda PZH.

Bylo zapotřebí vyhodnotit, jaká rizika s sebou implementace přináší. Nejdříve se musel určit zdroj samotného rizika, dále pak identifikace nebezpečí, tedy co přesně k tomuto riziku vede, čím je způsobeno. V neposlední řadě došlo k zjištění celkového rizika a k návrhu bezpečnostních opatření pro jeho redukci či úplné odstranění.

Tab. 10 Analýza rizik implementace Obecného nařízení (vlastní zpracování)

| Druh činnosti | Zdroj rizika | Identifikace nebezpečí | Hodnocení závažnosti rizika | | | | Bezpečností opatření |
|---|---|---|---|---|---|---|---|
| | | | P | Z | H | R | |
| Implementace Obecného nařízení | Sankce | Časové zpoždění | 3 | 5 | 4 | 60 | Vhodně nastavený časový harmonogram |
| | Únik osobních dat | Neproškolení zaměstnanci | 3 | 3 | 3 | 27 | Naplánované školení, kontrola, zda proběhlo u všech |
| | Chybná implementace, sankce | Špatné (nedostatečné) pochopení principů nařízení | 3 | 4 | 4 | 48 | Školení, důkladné nastudování |
| | Chybná implementace | Špatně definovaný účel zpracování | 3 | 4 | 3 | 36 | Důkladné prostudování požadavků |

Rizika související se samotnou implementací Obecného nařízení jsou již závažnější, než ty týkající se obecně zpracování osobních údajů. V případě jakékoliv chyby v implementaci hrozí společnosti sankce, která by pro ni mohla být až likvidační. K tomuto by mohlo dojít v případě časového zpoždění, kdy hodnota celkového rizika vyšla 60, což je označováno jako nežádoucí riziko. To vyžaduje urychlené provedení odpovídajících bezpečnostních opatření snižujících riziko na přijatelnou úroveň, na snížení rizika se musí přidělit potřebné zdroje. Aby došlo ke snížení či odstranění rizika časového zpoždění, je důležité nastavit vhodný časový harmonogram celého projektu a jednotlivé činnosti pak provádět postupně v daném časovém horizontu.

Dalším rizikem je chybná implementace a tedy hrozící sankce v důsledku špatného pochopení principů Obecného nařízení. Je důležité důkladně nastudovat veškeré principy a požadavky, popřípadě absolvovat školení na Obecné nařízení o ochraně osobních údajů.

## 10.2 Kalkulace nákladů projektu

Projekt byl navržen tak, aby náklady na jeho implementaci byly co nejnižší. Implementace byla prováděna jedním zaměstnancem, který je placen podle počtu odpracovaných hodin. Po celou dobu k dispozici další zaměstnanec, který dělal supervizora a na všechny kroky tedy dohlížel, popřípadě byl připraven pomoci. Supervizor byl za tuto práci odměněn na základě počtu odpracovaných hodin.

Vzhledem ke skutečnosti, že má společnost pobočku i v |Praze, bylo nutné provést i služební cesty z důvodu konzultací, a to převážně s oddělením customer care, tedy oddělení vztahů se zákazníky, které nakládá s jejich osobními údaji. Dále bylo nutné uskutečnit pracovní cestu do Prahy z důvodu školení s advokátní kanceláří. Toto školení bylo zdarma, vzhledem k tomu, že advokátní kancelář je partnerem analyzované společnosti, proplacena byla pouze cesta a čas strávený na tomto školení.

Pro podrobnou představu všech nákladů je níže uvedená tabulka.

Tab. 11 Nákladová analýza (vlastní zpracování)

| **Nákladová položka** | **Doba trvání (hod)** | **Náklady celkem** |
|---|---|---|
| Vstupní analýza (zaměstnanec) | 120 | 12 000 Kč |
| Vstupní analýza (supervizor) | 40 | 11 000 Kč |
| Implementace (zaměstnanec) | 120 | 12 800 Kč |
| Vstupní analýza (supervizor) | 70 | 19 250Kč |
| 3x Služební cesta (konzultace) | 12 | 1 200 Kč |
| Školení (zaměstnanec) | 4 | 400 Kč |
| Školení (supervizor) | 4 | 1 100 Kč |
| 5x cestovné | | 2 500 Kč |
| **Náklady celkem** | | **60 250 Kč** |

Vstupní analýza trvala 30 dnů, samotná implementace pak 32 dnů. V tabulce jsou tyto data převedeny na hodiny, a v případě zaměstnance hodinová mzda činí 100 Kč/hod. Pro výpočet nákladů za cestovné bylo počítáno s průměrnou cenou za jízdenku tam i zpět v částce

500 Kč, byly uskutečněny tři služební cesty za účelem konzultace s jednotlivými odděleními v Praze, přičemž na tyto cesty jel jeden zaměstnanec. Na již zmíněné školení jel zaměstnanec i supervizor, jednalo se tedy o další dvě cesty.

Celkové náklady tohoto projektu, zahrnující mzdy zaměstnance a supervizora, cestovné a čas strávený na školení v Praze, jsou vyčísleny na 60 250 Kč.

## 10.3 Přínosy projektu

Vzhledem ke skutečnosti, že se Obecné nařízení o ochraně osobních údajů týká všech společností, které pracují s osobními údaji fyzických osob v rámci Evropské unie, bylo nutné implementovat veškeré požadavky i v rámci analyzované společnosti. Případné přehlížení implementace, či její nesprávné provedení, by pro společnost znamenalo nebezpečí sankcí, jejichž výše by mohla být až likvidační. Hlavním přínosem je tedy nejen ušetření finančních prostředků, ale především zabránění její likvidace, tedy zajištění jejího bezproblémového fungování z pohledu regulace osobních údajů.

Dalším přínosem je i možné zlepšení povědomí jak u klientů, tak u vlastních zaměstnanců, neboť všechny tyto osoby, správci osobních údajů, budou ujištěni, že s jejich údaji je zacházeno zcela v souladu s Obecným nařízením a nemusejí se bát případným unikům dat, a zároveň se dožadovat práv vyplívajících z tohoto nařízení.

V neposlední řadě je nutno podotknout, že implementace Obecného nařízení s sebou nese další přínos pro samotnou společnost, která po provedení celého procesu implementace bude mít kompletní přehled o tom, kde přesně jsou veškeré osobní data uložena a kdo k nim má jaký přístup. V případě, že by došlo k jakémukoliv pochybení u některých dokumentů, bude díky tomuto přehledu ihned jasné, kdo měl k těmto dokumentům přístup a kdo s nimi tedy nakládal. Tento přehled také poslouží jako podklad v případě kontroly z Úřadu na ochranu osobních údajů, což je pro společnost rovněž velkým přínosem.

# ZÁVĚR

Hlavním cílem této diplomové práce bylo navržení projektu implementace Obecného nařízení o ochraně osobních údajů ve vybrané společnosti tak, aby mohl být tento projekt uskutečněn do 25. května letošního roku, kdy nařízení vstupuje v účinnost.

První fází praktické části práce bylo provedení vstupní analýzy současného stavu zpracovávání a uchovávání veškerých dat, jak klientů, tak zaměstnanců. Na základě této analýzy byl stanoven přehled nesouladů v současném systému zpracování dat spolu se stručným popisem jednotlivých kroků, které bylo zapotřebí provést pro odstranění těchto nesouladů.

Součástí samotného projektu bylo stanovení časového harmonogramu pro jednotlivé kroky implementace Obecného nařízení, což bylo provedeno použitím síťové analýzy. Jejím výstupem bylo jednak zjištění, za jakou nejkratší dobu je možné implementaci provést, a také u kterých činností vzniká časová rezerva. Tento krok sloužil především k zabránění časového zpoždění.

Poté již došlo k samotnému provedení všech kroků, tedy ke stanovení účelu a rozsahu zpracovávaných údajů, vytvoření dokumentů poskytujících informace o právech subjektů a dokumentů pro správu ohledně zpracování osobních údajů, také pro hlášení incidentů. Dále byl formulován souhlas se zpracováním veškerých dat pro klienty, stanovena pravidla přístupů, provedena revize smluv jak s dalšími zpracovateli osobních údajů, tak pracovních. V neposlední řadě došlo k návrhu evidence zpracování, pravidel zacházení s osobními údaji zaměstnanců, systému vyhodnocování rizik a kontrolních mechanismů. Následně byla nutnost proškolit veškeré zaměstnance. Celý tento proces se prolínal s tvorbou vnitřního předpisu pro zpracování osobních údajů ve společnosti.

Přínosem návrhu tohoto projektu a jeho následným uskutečněním je především skutečnost, že dojde k zabránění případným sankcím. Dále se očekává, že po jeho implementaci bude společnost v očích klientů, jak stávajících, tak potenciálních budoucích, více důvěryhodná, jelikož veškeré osobní údaje budou chráněny a subjekty těchto údajů budou moci uplatňovat svá práva v souladu s Obecným nařízením.

# SEZNAM POUŽITÉ LITERATURY

BARTÍK, Václav a Eva JANEČKOVÁ, 2013. *Ochrana osobních údajů v životě podnikatele: 103 řešení modelových situací*. Olomouc: ANAG. ISBN 978-80-7263-811-6.

BAWDEN, David a Lyn ROBINSON, 2017. *Úvod do informační vědy*. Doubravník: Flow. ISBN 978-80-88123-10-1.

BENEŠ, Pavel, 2010. *Informace o informaci, aneb, Nový pohled na tento svět.* Praha: BEN - technická literatura. ISBN 978-80-7300-263-3.

BOLOGNINI, Luca, Camilla BISTOLFI, 2017. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review* [online]. Vol. 33, issue 2, s. 171-181 [cit. 2018-03-24]. ISSN: 0267-3649.

BU-PASHA, Shakila, 2017. Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law* [online]. Vol. 26, issue 3, s. 213-228 [cit. 2018-03-15]. ISSN: 1360-0834.

CALDER, Alan, 2016. *EU GDPR: A Pocket Guide.* United Kingdom: IT Governance Publishing. ISBN 978-1-84928-833-0.

GONZÁLEZ FUSTER, Gloria, 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Switzerland: Springer International Publishing. ISBN 978-3-319-05023-2.

GODDARD, Michelle, 2017. The EU Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research* [online]. Vol. 59, issue 6, s. 703-705 [cit. 2018-03-15]. ISSN: 1470-7853.

HRONEK, Jiří, 2009. Informační systémy. Olomouc: Katedra informatiky Přírodovědecká fakulta Univerzita Palackého [cit. 2018-03-24]. Dostupné z: http://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

MAŠTALKA, Jiří, 2008. *Osobní údaje, právo a my*. Praha: Beck. ISBN 978-80-7400-033-1.

MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK, 2008. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI. ISBN 978-80-7357-322-5.

Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník Evropské unie* [online]. L 119/1 [cit. 2018-03-24]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN

NEZMAR, Luděk, 2017. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing. ISBN 978-80-271-0668-4.

NULÍČEK, Michal, 2017. *GDPR - obecné nařízení o ochraně osobních údajů.* Praha: Wolters Kluwer. ISBN 978-80-7552-765-3.

Obecné nařízení o ochraně osobních údajů prakticky, ©2017. *GDPR* [online]. [cit. 2018-03-24]. Dostupné z: https://www.gdpr.cz/gdpr/

PORMEISTER, Kart, 2018. Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law* [online]. Vol. 7, issue 2, s. 137-146 [cit. 2018-03-15]. ISSN 2044-3994.

Působnost úřadu, ©2013. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-03-24]. Dostupné z: https://www.uoou.cz/pusobnost-uradu/ds-1269/archiv=0&p1=1059

TIKKINEN-PIRI, Christina, Anna ROHUNEN and Jouni MARKKULA, 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review* [online]. Vol. 34, issue 1, s. 134-153 [cit. 2018-03-15]. ISSN 0267-3649.

ČESKO, 2000. Zákon č. 101/2000 Sb. ze dne 25.4.2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky* [online]. 2000, částka 32, s. 1521-1532 [cit. 2018-03-18]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=101/2000&typeLaw=zakon&what=Cislo_zakona_smlouvy

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

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| Apod. | A podobně |
| a.s. | Akciová společnost |
| BÚ | Bankovní účet |
| CPM | Critical Path Method |
| ČNB | Česká národní banka |
| DPIA | Data Protection Impact Assesment |
| DPO | Data Protection Officer |
| EU | Evropská unie |
| GDPR | General Data Protection Regulation |
| OP | Občanský průkaz |
| PZH | Jednoduchá bodová polokvantitativní metoda (pravděpodobnost, závažnost, hodnotitelé) |
| NAS | Network Attached Storage |
| Sb. | Sbírka zákonů |
| s.r.o. | Společnost s ručením omezeným |
| ÚOOÚ | Úřad pro ochranu osobních údajů |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

# SEZNAM PŘÍLOH

# PŘÍLOHA P I: INFORMACE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

## INFORMACE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Společnost XY Holding, a.s., IČO: xxx, se sídlem XXX, považuje ochranu osobních údajů za nedílnou součást svých závazků vůči svým klientům. Ochraně osobních údajů věnuje náležitou pozornost a při zajištění ochrany osobních údajů jedná v souladu s právními předpisy.

V tomto dokumentu se nacházejí informace o tom, jaké osobní údaje jsou zpracovávány v rámci smluvních vztahů s klienty. K nalezení jsou zde informace o tom, na jaké právním základu (důvodu) jsou osobní údaje zpracovávány, k jakým účelům společnost údaje zpracovává, komu je může předávat a jaké mají jednotlivé subjekty osobních údajů práva v souvislosti s jejich zpracováním. Tento dokument je tedy důležitým zdrojem informací o tom, jak jsou zpracovávány osobní údaje touto společností.

**A. Jaké osobní údaje jsou zpracovávány?**

Zpracovávány jsou následující údaje:

a) **Adresní a identifikační údaje**, kterými se rozumí zejména jméno, příjmení, rodné číslo, bylo-li přiděleno, datum narození, adresa trvalého pobytu, státní příslušnost, číslo a platnost tohoto průkazu totožnosti, telefonní kontakt

b) **popisné údaje**, kdy se jedná o číslo cestovního dokladu a číslo bankovního účtu

c) citlivé údaje společnost nezískává

d) **údaje o jiné osobě**, kterými se rozumí údaje o osobě, která je určena k tomu, aby jednala za klienta (tzv. disponent). Konkrétně dochází k uchovávání adresních a identifikačních údajů disponenta.

**B. Proč jsou osobní údaje zpracovávány a co k tomu společnost opravňuje?**

Dochází ke zpracovávání osobních údajů pro následující účely:
- uzavření smlouvy o poskytování investičních služeb a poskytování těchto služeb (tento účel v sobě zahrnuje i identifikace zákazníka dle zákona 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, tedy identifikaci rizikovosti všech zákazníků).
- uzavření smlouvy o poskytování platebních služeb a poskytování těchto služeb
- oslovování zákazníků s novinkami uskutečňovanými analyzovanou společností

K tomuto zpracovávání dochází také v různém rozsahu, a to bez souhlasu klienta na základě oprávněného zájmu, z důvodu plnění právní povinnosti na základě nezbytnosti pro určení, výkon nebo obhajobu právních nároků.

Pro tyto účely jsou osobní údaje společností uchovávány po dobu, po kterou je to nezbytné k realizaci práv a povinností plynoucích z poskytování jednotlivých služeb, které společnost nabízí.

Proti tomuto zpracování má klient právo uplatnit námitku. Pokud využije svého práva vznést námitku proti zpracování osobních údajů, je společnost povinna osobní údaje klienta pro daný účel dále nezpracovávat, ledaže v rámci šetření námitky klienta dojde ke zjištění, že k tomuto zpracování má společnost závažné oprávněné důvody.

**C. Kdo osobní údaje zpracovává**

Všechny výše zmíněné osobní údaje zpracovává společnost jako **správce**. To znamená, že společnost stanovuje shora vymezené účely, pro které jsou shromažďovány osobní údaje, určuje prostředky zpracování a odpovídá za jeho řádné provedení.

Pro zpracování osobních údajů společnost rovněž využívá služeb dalších zpracovatelů, kteří osobní údaje zpracovávají na pokyn společnosti. Takovými zpracovateli jsou zejména:
a) zřizovatel servisního portálu
b) zřizovatel informačního systému IVAN
c) zřizovatel programu CAPITOL
d) banky
e) správce sítě
f) insolvenční správci, notáři, dozorové instituce, výzvy datové schránky

**D. Z jakých zdrojů se osobní údaje získávají?**

Ve většině případů se zpracovávají osobní údaje, které byly společnosti poskytnuty přímo od klienta při jeho registraci.

**E. Jaké jsou práva při zpracování osobních údajů?**

Stejně jako společnost má svá práva a povinnosti při zpracování osobních údajů klientů, tak klienti mají při zpracování jejich osobních údajů určitá práva. Mezi tato práva patří:
- právo na přístup
- právo na opravu
- právo na výmaz
- právo na omezení zpracování
- právo na přenositelnost
- právo vznést námitku proti zpracování
- právo podat stížnost.

**F. Jak lze uplatnit jednotlivá práva?**

Ve všech záležitostech souvisejících se zpracováním osobních údajů klientů, ať již jde o dotaz, uplatnění práva, podání stížnosti či cokoliv jiného, se mohou klienti obracet na oddělení back office společnost.

Toto oddělení lze kontaktovat kterýmkoliv z následujících prostředků:
- e-mailem:
- písemně na adrese:
- prostřednictvím telefonního čísla:

Podání stížnosti proti prováděnému zpracování osobních údajů společností je možno podat u Úřadu pro ochranu osobních údajů.

# PŘÍLOHA P II: DODATEK KE SMLOUVĚ SE ZPRACOVATELI OSOBNÍCH ÚDAJŮ

## DODATEK KE SMLOUVĚ SE ZPRACOVATELI OSOBNÍCH ÚDAJŮ

a) Společnost XY, a.s. a *zpracovatel* se zavazují, v souvislosti s touto smlouvou, postupovat v souladu se Směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů. K vyloučení všech pochybností smluvní strany prohlašují, že jsou jim známy účinky platného Obecného nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 (dále jen „Nařízení").

b) *Zpracovatel* bere na vědomí, že se ve smyslu všech výše uvedených právních předpisů považuje a bude považovat za Zpracovatele osobních údajů, se všemi pro něj vyplývajícími důsledky a povinnostmi. Společnost XY, a.s. je a bude nadále považována za Správce osobních údajů, se všemi pro něj vyplývajícími důsledky a povinnostmi.

c) Ustanovení o vzájemných povinnostech Správce a Zpracovatele při zpracování osobních údajů zajišťuje, že nedojde k nezákonnému použití osobních údajů týkajících se Subjektů údajů ani k jejich předání do rukou neoprávněné třetí strany. Smluvní strany se dohodly na podmínkách zajištění odpovídajících opatření k zabezpečení ochrany osobních údajů a základních práv a svobod Subjektů údajů při zpracování osobních údajů Zpracovatelem.

d) Zpracovatel se zavazuje zpracovávat pouze a výlučně jenom ty osobní údaje, které jsou nutné k výkonu jeho činnosti dle této smlouvy.

e) Zpracovatel je oprávněn zpracovávat osobní údaje dle této smlouvy pouze a výlučně po dobu účinnosti této smlouvy.

f) Zpracovatel je oprávněn zpracovávat osobní údaje pouze za účely stanovenými společností XY, a.s.

g) Zpracovatel je povinen se při zpracování osobních údajů řídit výslovnými pokyny Správce, ústní či písemnou formou.

h) Zpracovatel je povinen přijmout, s ohledem na stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku.

j) Zpracovatel je povinen písemně seznámit Správce s jakýmkoliv podezřením na porušení nebo skutečným porušením bezpečnosti zpracování osobních údajů podle ustanovení této smlouvy.

k) Po skončení účinnosti této smlouvy nebo v případě předčasného ukončení je Zpracovatel povinen všechny osobní údaje, které má v držení, vymazat. Pokud je dosud nepředal Správci, musí je Správci předat a dále vymazat všechny existující kopie. Povinnost uvedená v tomto článku neplatí, stanoví-li právní předpis EU, případně vnitrostátní právní předpis Zpracovateli osobní údaje ukládat i po skončení účinnosti této smlouvy.

# PŘÍLOHA P III: VZOR MZDOVÉHO LISTU

**Mzdový list**

Jméno a příjmení: Druh výkonu práce:
Rodné číslo: Zaměstnán od-do:
Datum a místo narození: Pracovní zařazení:
Bydliště: Pracovní úvazek:
Zdravotní pojišťovna: Základní měsíční mzda:

Skutečnosti rozhodné pro zdaňování příjmů:

Daňové prohlášení podepsáno: Zůstatek dovolené k 1.1.:
Uplatňované slevy na dani: Nárok na dovolenou:
- na poplatníka
- daňové zvýhodnění na děti:

| **Položka** | Leden - Prosinec | Celkem |
|---|---|---|
| Fond pracovní doby (hod.) | | |
| Počet odpracovaných hodin | | |
| Počet neodpracovaných hodin | | |
| - z toho (hod.): dočasná PN | | |
| dovolená | | |
| svátek | | |
| placená nepř. | | |
| neplacené volno | | |
| Mzda za odpracovanou dobu (Kč) | | |
| Odměny, prémie, apod. (Kč) | | |
| Příplatky (Kč) | | |
| Náhrady mzdy za dovolenou atd. (Kč) | | |
| Hrubá mzda celkem (Kč) | | |
| - z toho osvobozeno od daně (Kč) | | |
| Vyměřovací základ – ZP (Kč) | | |
| ZP – zaměstnanec (Kč) | | |
| ZP – zaměstnavatel (Kč) | | |
| Vyměřovací základ – SP (Kč) | | |
| SP – zaměstnanec (Kč) | | |
| SP – zaměstnavatel (Kč) | | |
| Zdanitelný příjem (Kč) | | |
| Superhrubá mzda (Kč) | | |
| Základ daně z příjmů (Kč) | | |
| Vypočtená záloha na daň (Kč) | | |
| Slevy na dani (Kč) | | |
| Záloha na dani po slevách (Kč) | | |
| Daňové zvýhodnění na děti (Kč) | | |
| - z toho: sleva na dani | | |
| daňový bonus | | |
| Záloha na dani po slevě (Kč) | | |
| Odvedená záloha na daň (Kč) | | |
| Čistá mzda (Kč) | | |
| Náhrada mzdy při PN (Kč) | | |
| Srážky ze mzdy (Kč) | | |
| Vyplacená záloha (Kč) | | |
| K výplatě (Kč) | | |

Průměrný hodinový výdělek (Kč/hod.)

| | |
|---|---|
| Průměrný výdělek (Kč/hod.) | |

Dovolená

| | |
|---|---|
| Čerpaná dovolená (dny) | |
| Zůstatek dovolené (dny) | |

Přehled náhrad mzdy při dočasné pracovní neschopnosti:

| Druh náhrady | Nepřítomnost | | Celkový počet dnů PN | | Počet hodin pro náhradu mzdy | Průměrný výdělek | Náhrada v Kč |
|---|---|---|---|---|---|---|---|
| | od | do | kalendářních | pracovních | | | |
| Náhrada mzdy při PN | | | | | | | |
| Celkem | | | | | | | |