**Univerzita Hradec Králové**

**Fakulta informatiky a managementu**

**Katedra informačních technologií**

# Obecné nařízení o ochraně osobních údajů (GDPR) v prostředí České republiky

Diplomová práce

Autor: Bc. Anna Borkovcová

Studijní obor: Informační management

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové duben 2019

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne Anna Borkovcová

**Poděkování**

Ráda bych poděkovala vedoucímu diplomové práce Mgr. Josefu Horálkovi, Ph.D. za odborné vedení a cenné rady, které mi poskytl při vypracování této práce a dále Mgr. Lukáši Lýskovi za obornou konzultaci při řešení problematiky práce.

**Anotace**

BORKOVCOVÁ, Anna. *Obecné nařízení o ochraně osobních údajů (GDPR) v prostředí České republiky.* Hradec Králové: Fakulta informatiky a managementu, Univerzita Hradec Králové, 2019, 123 str. Diplomová práce

**Název:** Obecné nařízení o ochraně osobních údajů (GDPR) v prostředí České republiky.

Předkládaná diplomová práce se zabývá ochranou osobních údajů dle nařízení EU 2016/679 (GDPR) a to jak v kontextu EU, tak i v České republice. Cílem práce je analýza oblasti ochrany osobních údajů, šetření v rámci několika velkých firem působících v ČR a vytvoření vyhodnocení, jehož výstupem je postup pro ověření souladu správy a zpracování osobních údajů s GDPR. V teoretické části se autorka podrobně zaměří na problematiku implementace GDPR v prostředí České republiky s důrazem na objasnění a jednoznačné vysvětlení komplexní problematiky nařízení, a to zejména v oblastech vztahujících se na subjekt údajů a jejich práva ke zpracovateli a správci osobních údajů a jejich zakotvení v připravovaném tzv. adaptačním zákoně. V praktické části autorka provede komparativní analýzu platné legislativy (platné v době zadání) a nařízením GDPR. Dále využije přístupů vybraných významných společností spravujících osobní údaje, na kterých modelově demonstruje komplexní problematiku spojenou s implementací GDPR. V závěru autorka představí návodný postup pro ověření souladu správy a zpracování osobních údajů s nařízením GDPR.

**Klíčová slova:** GDPR, ochrana osobních údajů, subjekt údajů

**Annotation**

BORKOVCOVÁ, Anna. *General Data Protection Regulation (GDPR) in the Czech Republic.* Hradec Králové: Faculty of Informatics and management, University of Hradec Králové, 2019, 123 pp. Diploma Thesis.

**Title**: General Data Protection Regulation (GDPR) in the Czech Republic.

The Diploma Thesis deals with the protection of personal data pursuant to the European General Data Protection Regulation (GDPR) nr. 2016/679. This issue will solve for the Czech environment and in the EU context. The aim of this Thesis is to analyze the area of personal data protection, research within several large companies operating in the Czech Republic. Then create and evaluate the final output, which is the procedure for verifying compliance of the management and processing of personal data with the GDPR. In the first theoretical part, the author focuses on the implementation of GDPR in the Czech Republic. The thesis emphasizes the clarification and clear explanation of the complex issue of the regulation. These are mostly areas related to the data subject and their rights to the processor and the data controller. This will also be described in the Czech Republic's adaptation law. In the practical part, the author performs a comparative analysis of the legislation (valid at the time of the award) and the GDPR. Furthermore, it will use the approaches of selected important companies managing personal data, on which it demonstrates the complex issues associated with the implementation of GDPR. In conclusion, the author introduces a guideline for verification of compliance of the administration and processing of personal data with the GDPR regulation.

**Keywords:** GDPR, personal data protection, data subject

# Obsah

# Seznam zkratek

DPO – pověřenec pro ochranu osobních údajů

DPIA – posouzení vlivu na ochranu osobních údajů

ICT – informační a komunikační technologie

ES – Evropské společenství

EU – Evropská unie

GDPR – Obecné nařízení o ochraně osobních údajů

FO – fyzická osoba

PO – právnická osoba

OÚ – osobní údaj

SÚ – subjekt údajů

OOÚ – ochrana osobních údajů

ZOÚ – zabezpečení osobních údajů

ÚOOÚ – Úřad pro ochranu osobních údajů

# Úvod

Současná informační společnost svojí činností zanechává mnoho datových stop, toto je samozřejmě způsobeno větší dostupností internetu, chytrých zařízení, sociálních sítí, apod. Se stále se zvyšujícím využíváním informačních a komunikačních technologií roste také počet údajů, které aplikace provozované na těchto technologiích zachycují, vytváří či shromažďují. Z datových stop mohou některé instituce či organizace získávat cenná data, na základě kterých mohou následně rozvíjet svoje strategické cíle, ale i profilovat konkrétní marketingové nabídky na daného uživatele. Obecně lze konstatovat, že data získaná z používání různých aplikací či technologií mohou mít kromě pozitivních či neutrálních dopadů, dopad negativní. Tento představuje různé formy zneužití či šíření nepravdivých a poškozujících informací. Důsledkem toho přistoupila Evropská unie k opatření, které má tyto negativní činnosti minimalizovat, v ideálním případě eliminovat. Proto, aby bylo možné stanovit takové obecné nařízení, které cílí na ochranu osobních údajů, je nutné provést právní vymezení této problematiky. Toto bylo stanoveno v Obecném nařízení EU o ochraně osobních údajů, které jsou členské země EU povinné aplikovat ve své legislativě. V České republice vyšlo toto nařízení v účinnost 25.května 2018 a je v povědomí veřejnosti známé pod zkratkou GDPR. Nařízení GDPR je tedy přelomové v tom, že se uplatní na všechny subjekty dotčených států, a to jak aktivně v případě správců či zpracovatelů, tak pasivně v případě subjektů údajů. Vzhledem k medializaci tohoto nařízení dochází ovšem velmi často k chybné interpretaci zásadních či okrajových částí tohoto nařízení. Především pro osoby, které nemají právní povědomí, je často velice složité rozeznat, které formulace či tvrzení jsou správné, a v jakých případech by se mohli kvůli nesprávnému výkladu dostat často i do rozporu s nařízením či jinou většinou tuzemskou právní úpravou.

Tato práce má za cíl uvést čtenáře do problematiky ochrany osobních údajů, představit klíčové aspekty nařízení a adaptačního zákona, který toto nařízení upravuje pro podmínky v České republice. Vzhledem k tomu, že se práce musí zabývat komplexně nařízením GDPR, adaptačním zákonem, zákonem o ochraně osobních údajů a další legislativou byl konzultantem této práce odborník v oblasti práva, specialista pro ochranu osobních údajů, Mgr. Lukáš Lýsek. Další část práce obsahuje komparaci nařízení se zákonem 101/2000 Sb., a to pro lepší orientaci čtenáře ve změnách, které GDPR přináší.

Následovat bude analýza účelů zpracování ve dvou veřejně známých subjektech, a to T-Mobile Czech Republic, a.s. a ČEZ, a.s. Po provedení analýzy u těchto subjektů budou tyto poznatky využity pro hlavní přínos práce, kterým bude návodný postup pro zajištění souladu zpracování osobních údajů s nařízením EU 2016/679 (GDPR). Součástí práce je také identifikace hlavních krizových bodů pro danou organizaci. Práce je tak určena pro čtenáře, které zajímá nejen přehled toho, co nařízení obsahuje, ale i ukázka, jak je řešena jedna z oblastí velkými subjekty a návodná dokumentace pro základní implementaci a přehled povinností, které se mohou jednotlivých ekonomických subjektů týkat.

# Cíle práce a metodika

Hlavním cílem předkládané diplomové práce je analýza z oblasti ochrany osobních údajů, šetření v rámci dvou velkých firem působících v ČR a vytvoření vyhodnocení, jehož výstupem je obecný návodný postup pro dosažení souladu správy a zpracování osobních údajů dle nařízení GDPR. Struktura práce se tak dělí na část teoretickou a praktickou. Pro řádné naplnění hlavního cíle byly určeny i cíle dílčí:

1) Definice základních pojmů ve vztahu k GDPR.
2) Obecný popis nařízení GDPR.
3) Definice struktury nařízení.
4) Popisný rozbor subjektů údajů a jejich práv a problematiky správce a zpracovatele.
5) Představení funkce dozorových úřadů včetně ČR.
6) Pro úplnost doplnění předávání osobních údajů do třetích zemí nebo mezinárodních organizací a stručný popis zvláštních situací při zpracování osobních údajů.
7) Analýza adaptačního zákona a dopady na ochranu osobních údajů v podmínkách České republiky.
8) Komparace legislativy v ČR před účinností nařízení GDPR a samotným nařízením.
9) Analýza dvou významných subjektů v ČR zpracovávající ve velké míře osobní údaje.
10) Návodný postup implementace v souladu s nařízením
11) Stanovení doporučení.

Pro splnění výše vytyčených cílů je nejprve provedena *literární rešerše*, výstupy literární rešerše na základě metody *analýzy* a *deskripce* poskytují teoretická východiska pro řádné vytvoření praktické části práce. *Literární rešerše* zahrnuje definici základních pojmů spojených s tématem, uvádí čtenáře do problematiky ochrany osobních údajů a s tím souvisejících částí nařízení, kterými jsou obecné zásady zpracování. Dále se literární rešerše zaměřuje na samotný subjekt údajů a zároveň zdůrazňuje jeho práva a na druhou stranu uvádí povinnosti správce a zpracovatele. Navazující problematika správce a zpracovatele seznamuje s obecným rámcem s nakládáním s osobními údaji včetně předávání osobních údajů do třetích zemí nebo mezinárodním organizacím. Neméně podstatnou částí *literární rešerše* je základní popis a princip fungování nezávislých dozorových úřadů a pro úplnost je vhodné začlenit i zvláštní situace při zpracování

osobních údajů. Tyto části budou definovány obecně, tak jak je definováno přímo v nařízení GDPR a pro cíle práce je nutné zdůraznit úpravy tohoto nařízení v podmínkách ČR. Diplomová práce vychází z aktuální legislativy, avšak platné a účinné v době psaní této práce.

Praktická část práce pro co nejvhodnější přechod od teoretické části ke konkrétním praktickým ukázkám a řešením charakterizuje stručný rámec odlišností v podobě srovnání zákona 101/2000 Sb. a GDPR. Pro získání ověřených a zavedených výsledků při aplikaci metody *analýzy* byly využity dva dlouhodobě stabilní ekonomické subjekty, a to ČEZ, a.s. a T-Mobile Czech Republic a.s. U těchto právnických osob je práce zaměřena na účely zpracování osobních údajů. Tyto subjekty byly do práce vybrány, jelikož jejich hlavní činnosti jsou významně ovlivněny právě GDPR. Srovnání výsledků šetření v těchto dvou subjektech pomocí metody *komparace* bude možné využít také v návodném postupu pro soulad s nařízením a vytvořit tak použitelný výstup sloužící k ověření implementace GDPR.

Praktická část práce bude mít tak na základě *analýzy* legislativních opatření v Evropské unii a v České republice, výsledků z *komparace* dvou právnických subjektů zabývajícími se pravidelně ochranou osobních údajů a vytvořením přehledu rozdílů pro oblast ochrany osobních údajů platných v tuzemsku oproti obecnému nařízení GDPR dostatečný základ pro využití metody *syntézy* při vytváření návodného postupu, který ověřuje implementaci GDPR do organizace.

Vzhledem k rozsáhlé právní problematice je legislativa uvedená v práci konzultována se specialistou v oblasti ochrany osobních údajů. Zároveň s tím souvisí často opakované formulace, zákonné normy a právní předpisy, kterým se autorka nemůže vyhnout ani je z důvodu zachování významu nemůže změnit.

Některé pojmy, které nemusí být zřejmé všem čtenářům nebo nejsou doplněny jinou vysvětlující skutečností přímo v textu práce, mohou být dále rozšířeny o poznámku pod čarou.

# 1 Základní pojmy spojené s tématem

Nařízení pracuje s následujícími pojmy, pro lepší orientaci v celé problematice a práci jsou tyto základní pojmy vypsané samostatně v této kapitole. Jedná se o výčet nejčastěji využívaných pojmenování se stručným definičním popisem.

- bezpečnostní incident
    - událost ohrožení bezpečnosti informací nebo porušení pravidel bezpečnosti
- biometrické údaje
    - osobní údaj
    - vyplývají z konkrétního zpracování fyzických či fyziologických znaků, či znaků chování FO, umožňují jednoznačnou identifikaci
    - např. zobrazení obličeje, …
- dotčený dozorový úřad
    - dozorový úřad, kterého se zpracování osobních údajů dotýká
    - správce či zpracovatel je usazen na území členského státu tohoto dozorového úřadu nebo subjekty údajů s bydlištěm v příslušném území dozorového úřadu mohou být nebo jsou zpracováním podstatně dotčeny, či u něj byla podána stížnost
- dozorový úřad
    - nezávislý orgán veřejné moci (zřízený členským státem)
- evidence
    - jakýkoli strukturovaný soubor osobních údajů
- genetické údaje
    - osobní údaj
    - zděděné nebo získané genetické znaky FO, které poskytují jedinečné informace (vyplývají zejména z analýzy biologického vzorku dotyčné FO)
- identifikační údaj
    - údaj, jehož prostřednictvím lze zjistit či stanovit totožnost osobu (jméno, rodné číslo, číslo občanského průkazu, …)
- informační společnost
    - společnost, kde proběhlo zavedení informačních a komunikačních technologií do té míry, že jsou zásadně změněné vztahy a procesy v dané společnosti

- kodexy chování
    - definují základní zásady, postupy, přístupy a metody zpracování osobních údajů pro konkrétní odvětví
- mezinárodní organizace
    - podléhají mezinárodnímu právu nebo subjekt zřízený dohodou mezi dvěma či více zeměmi nebo na jejím základě
- ochrana „by design“ – záměrná ochrana
    - ochrana spočívající v návrhu a zavedených vhodných opatření před zahájením vlastního zpracování (pseudonymizace, šifrování, …)
- ochrana „by default“ – standardní ochrana
    - ochrana spočívající v minimalizaci - dodržení doby uchování a likvidace, zpracovávání pouze nutného rozsahu a dostupnosti pouze nutnému počtu osob
- omezené zpracování
    - označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu
- osobní údaj
    - veškeré informace o identifikované nebo identifikovatelné fyzické osobě (subjekt údajů)
    - např. jméno, jeden či více zvláštních prvků identity této fyzické osoby…
- právní úprava
    - souhrn varianty právních předpisů (zákony, nařízení, vyhlášky,…) pro danou problematiku
- právní zásada
    - pravidla tvořící základ určité oblasti práva s vysokou mírou obecnosti
- pověřenec pro ochranu osobních údajů
    - pracovní pozice dle nařízení pro záležitosti zpracování a ochrany osobních údajů
- právní titul / důvod
    - oprávnění ke zpracování osobních údajů
- profilování
    - forma automatizovaného zpracování osobních údajů pro použití k hodnocení některých osobních aspektů
    - např. pracovní výkon, osobní preference, spolehlivost, chování

- pseudonymizace
    - zpracování osobních údajů tak, že již nemůžou být přiřazeny ke konkrétnímu subjektu bez dodatečných informací (které jsou uchovávány odděleně) a je zajištěno, že nebudou přiřazeny ke konkrétní osobě
- příjemce
    - subjekt, kterému jsou osobní údaje poskytnuty
    - za příjemce nejsou považovány orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření (musí být v souladu s právem členského státu a zpracování musí být v souladu s pravidly ochrany osobních údajů pro daný účel/y)
- přeshraniční zpracování
    - zpracování, které probíhá v souvislosti s činnostmi provozoven ve více členských státech nebo zpracování, které probíhá v souvislosti s činnostmi jediné provozovny, ale mohou jim být nebo jsou podstatně dotřeny subjekty údajů ve více členských státech
- porušení zabezpečení osobních údajů
    - porušení, které vede k náhodnému či protiprávnímu zničení, záměně, ztrátě, neoprávněnému poskytnutí či zpřístupnění osobních údajů
- relevantní a odůvodněná námitka
    - námitka vůči návrhu rozhodnutí za účelem posouzení porušení tohoto nařízení, jasný důkaz významnosti rizik, případně volný pohyb osobních údajů v rámci EU
- správní místo
    - místo pro vykonávání správních aktů
- subjekt údajů
    - fyzická osoba, ke které se týkají dané osobní údaje
- správce
    - FO či PO, orgán veřejné moci, či jiný subjekt, který sám či společně s jinými určuje účel a prostředky zpracování osobních údajů
- služba informační společnosti
    - jakákoliv služba, která je poskytovaná elektronickými prostředky, která je vykonávána na základě elektronické individuální žádost
- souhlas
    - jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle ke zpracování osobních údajů daného subjektu

- třetí strana
    - subjekt, který není subjektem údajů, správcem, zpracovatelem, ani osobou jim přímo podléhající, a je oprávněný ke zpracování osobních údajů
- účel zpracování
    - záměr a důvod správce pro zpracování osobních údajů (za jakým účelem chce osobní údaje zpracovávat)
- údaje o zdravotním stavu
    - osobní údaj
    - tělesné či duševní zdraví FO, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o zdravotním stavu
- vymahatelnost práva
    - mechanismus pro vynucení chování dle právních norem
- zákonné normy
    - závazná pravidla chování dané zákonem
- zákonnost zpracování
    - zpracování, které je v souladu se zákonem (hlavním předpokladem je existence právního titulu)
- závazná podniková pravidla
    - koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel
- zpracovávání
    - jakákoliv sofistikovaná operace (soubor operací) s osobními údaji nebo jejich souborem
    - např. zaznamenání, uložení, omezení, výmaz…
- zpracovatel
    - FO či PO, orgán veřejné moci, či jiný subjekt, který zpracovává osobní údaje pro správce

# 2 Úvod do nařízení o ochraně osobních údajů

Ochrana osobních údajů je v současné době velmi skloňované téma. Z hlediska práva je tato problematika stále vnímána jako nová, na území České republiky vznikla právní úprava osobních údajů a jejich ochrany až v první polovině 90.let 20.století. Prvním právním předpisem řešící ochranu osobních údajů byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. O několik let později v Evropě vznikla směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, která vstoupila v platnost v prosinci roku 1995. V souvislosti s touto směrnicí byl tedy zákon č. 256/1992 Sb. neodpovídající, a tak vznikla nová právní úprava – Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který z evropské směrnice vycházel.[1] Nejnovější právní úpravou pracující s ochranou osobních údajů je v tuto chvíli *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)*[1], které je ve vybraných částech upraveno do prostředí České republiky Zákonem č. 110/2019 Sb., o zpracování osobních údajů.

Nařízení je právním aktem Evropské Unie (EU), které bylo vyhlášeno dne 27. dubna 2016 a v celé EU je účinné od 25. května 2018. Je přelomové v tom, že se netýká jen organizací v rámci EU, ale kterékoli instituce či organizace, která pracuje s daty občanů EU. V současné době se jedná o nejkomplexnější zákonnou normu svého druhu, která má za jeden ze stěžejních cílů chránit soukromí svých občanů. Dále je ojedinělé také v případě, kdy organizace a instituce tvoří na základě nařízení analýzu rizik ve vztahu k ochraně osobních údajů, jelikož udává povinnost analyzovat dopady i z pohledu samotného subjektu údajů, kterého se případný únik dat týká. [2]

Toto nařízení stanovuje pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla volného pohybu osobních údajů. Vztahuje se na zcela či

[1] Jedná se o oficiální název, známý pod zkratkou GDPR či zkráceném názvu Obecné nařízení o ochraně osobních údajů (*General Data Protection Regulation*), je v této práci označováno také jako nařízení.

částečně automatizované zpracovávání osobních údajů a neautomatizované zpracovávání těch údajů, které jsou v evidenci nebo do ní mají být zařazeny.

Proč je vůbec důležité právní ochranu osobních údajů řešit? V současné době je společnost z velké části postavena na využívání informačních a komunikačních technologií (ICT) ve všech oblastech života až do takové míry, že značně mění společenské vztahy či procesy a vnímání informací, takovou společnost lze označit termínem „informační společnost“. Již z názvu je patrné, že hlavním prvkem jsou informace, které jsou klíčové pro udržitelný rozvoj společnosti. Zpracování informací, které organizace mohou čerpat z interních systémů, představuje významnou ekonomickou aktivitu, což souvisí i s velkým nárůstem informačních a komunikačních technologií.[2]Nedílnou součástí těchto dat jsou právě i osobní údaje. Je nutné připomenout, že osobním údajem není jen identifikační údaj, jako jméno, příjmení, rodné číslo, ale jedná se o jakoukoli informaci, která se vztahuje ke konkrétní osobě. Takové údaje souvisejí se životem určité osoby, mohou být více či méně soukromé a pro danou osobu mít větší či menší význam. Pokud jsou tedy osobní údaje právně chráněné, je tím pokryta část ochrany osobnosti, obzvlášť ochrany soukromí daného subjektu, jakožto i jeden ze základních prvků současného demokratického systému v evropském pojetí. Instituce či organizace zpracovávající osobní údaje nesmí zapomínat, že ochrana OÚ se netýká pouze osob vystupujících v roli zákazníků, ale také zaměstnanců a všech ostatních osob u kterých k uchovávání dat o nich dochází. Současné právní úpravě tak podléhají všechny informační systémy, evidence, kartotéky, které jakékoli osobní údaje uchovávají či s nimi pracují. [3]

Vždy je nutné, najít rovnovážný bod, který spočívá ve vytvoření takového právního prostředí, ve kterém není ohrožen vývoj a služby plynoucí ze zpracování a vytěžování dat a informací, ale zároveň je dodržena ochrana osobnosti a soukromí, tzn. osobních údajů. Dalším důležitým aspektem je reakční doba právního systému na změny v technologickém prostředí tak, aby právní úprava a předpisy dokázaly reagovat na neustále se vyvíjející technologie. [2]

V prostředí ČR lze identifikovat následující hlavní změny vůči Zákonu 101/2000 Sb., které GDPR ve výčtu přináší a jedná se o:

- Rozšíření působnosti.
- Sjednocení legislativy pro EU (lepší vymahatelnost a přehlednost v zemích mimo EU).
- Spolupráce dozorčích úřadů a působnost a vymahatelnost práva po celé EU.
- Zpřísnění povinností správců a definice nových práv subjektu:
    - právo na portabilitu,
    - právo být zapomenut,
    - právo na informování a přístup k osobním údajům,
    - pro některé subjekty jmenování DPO,
    - posuzování vlivu na soukromí.
- Hlášení bezpečnostních incidentů.
- Ochrana „by design“ a „by default“.
- Stupňování povinností dle rizika,
- Možnost výjimek z práva a úpravy domácí legislativy.
- Zrušení registrační povinnosti.
- Režim jednoho správního místa.

Aplikace těchto změn není potřeba rozsáhleji do právního řádu členského státu transponovat, jako je tomu v případě směrnice, jelikož je nařízení EU právní akt, který je pro členské státy závazný ve všech svých částech a přímo použitelný. Podobá se tedy vnitrostátnímu zákonu a upravuje konkrétní situace. Cílem Obecného nařízení o ochraně osobních údajů [4] je posílení práv subjektů údajů a snaha dosáhnout sjednoceného výkladu. Celý právní rámec je dotvářen adaptačním zákonem, v podmínkách ČR je jim přijetí nového zákona [5], který je specifikován v kapitole *GDPR v podmínkách ČR* této práce.

Je nutné zmínit, že nařízení se nevztahuje na následující situace:

- Na zpracování osobních údajů, které je prováděné, pokud výkon činnosti nespadá do oblasti působnosti EU.
- Na zpracování, které je prováděné fyzickou osobou, které je čistě osobní povahy či v rámci domácnosti (např. korespondenci a vedení adresářů, využívání sociálních sítí a internetu).
    - Pokud ovšem správce nebo zpracovatel pro tyto činnosti nebo činnosti v domácnosti poskytuje prostředky pro zpracování, nařízení se na něj již vztahuje.

## 2.1 Struktura nařízení

V předchozí úvodní kapitole byly obecně popsány klíčové prvky GDPR. Tato kapitola se soustředí na členění nařízení dle legislativy a tak poskytne čtenáři ucelenou přehledovou strukturu nařízení.

Obecné nařízení o ochraně osobní údajů je strukturováno do jedenácti hlavních kapitol, které jsou v některých případech z důvodu rozsáhlosti rozděleny do oddílů. Každá kapitola pak obsahuje několik článků, které již řeší danou problematiku.

Struktura kapitol je následující:

I. Obecná ustanovení (čl. 1-4)
II. Zásady (čl. 5-11)
III. Práva subjektu údajů (čl. 12-23)
IV. Správce a zpracovatel (čl. 24-43)
V. Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím (čl. 44-50)
VI. Nezávislé dozorové úřady (čl. 51-59)
VII. Spolupráce a jednotnost (čl. 60-76)
VIII. Právní ochrana, odpovědnost a sankce (čl. 77-84)
IX. Ustanovení týkající se zvláštních situací, při němž dochází ke zpracování (čl. 85-91)
X. Akty v přenesené pravomoci a prováděcí akty (čl. 92, 93)
XI. Závěrečné ustanovení (č. 94-99)

Hlavními částmi pro tuto diplomovou práci jsou Kapitoly I., II., III., IV., VIII., kdy jsou zpracovány části relevantní pro potřeby a rozsah této práce. Kapitoly V., VI., IX. jsou v práci také zmíněné, ale spíše doplňkově pro úplnost. Kapitola IX je v této práci řešena vzhledem k obsahu v samostatné krátké kapitole *Zvláštní situaci při zpracování*. Kapitoly VII., X. a XI. nejsou v práci popsány vůbec, jelikož tyto kapitoly neodpovídají tematickému zaměření a oblasti řešení této práce.

V jednotlivých Kapitolách nařízení se autorka zaměřuje především na podstatné články a oddíly, které se dotýkají velké skupiny subjektů nebo je na ně kladen největší důraz:

Kapitola II. Zásady (čl. 5-11) je řešena v této práci v kapitole *Obecné zásady zpracování*.

- Článek 5 - Zásady zpracování osobních údajů.
- Článek 6 - Zákonnost zpracování.
- Článek 7 - Podmínky vyjádření souhlasu.
- Článek 9 - Zpracování zvláštních kategorií osobních údajů.
- Článek 10 - Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Kapitola III. Práva subjektu údajů (čl. 12-23) je řešena v této práci v kapitole *Subjekty údajů a jejich práva*.

- Oddíl 2 - Informace a přístup k osobním údajům (čl. 13-15).
- Oddíl 3 - Oprava a výmaz (čl. 16-20).
- Oddíl 4 - Právo vznést námitku a automatizované individuální rozhodování (čl. 21, 22).

Kapitola IV. Správce a zpracovatel (čl. 24-43) je řešena v této práci v kapitole *Problematika správce a zpracovatele*.

- Oddíl 1 - Obecné povinnosti (správce a zpracovatele) (čl. 24-31),
- Oddíl 2 - Zabezpečení osobních údajů (čl. 32-34).
- Oddíl 3 – Posouzení vlivu na ochranu osobních údajů a předchozí konzultace (čl. 35-36)
    - Z tohoto oddílu je v této práci řešen pouze Článek 35 - Posouzení vlivu na ochranu osobních údajů.
- Oddíl 4 - Pověřenec pro ochranu osobních údajů (čl. 37-39).
- Oddíl 5 – Kodexy chování a vydávání osvědčení (čl. 40-43)
    - Z tohoto oddílu je v této práci řešen pouze Článek 40 - Kodexy chování.

Kapitola V. Přidávání osobních údajů do třetích zemí nebo mezinárodním organizacím (čl. 44-50) je řešena v této práci v kapitole *Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím*, z této kapitoly jsou stěžejní následující články:

- Článek 45 - Předání založené na rozhodnutí o odpovídající ochraně.
- Článek 46 - Předávání založené na vhodných zárukách.
- Článek 47 - Závazná podniková pravidla.

Kapitola VIII. Právní ochrana, odpovědnost a sankce (čl. 77-84) je řešena v této práci v kapitole *Nezávislé dozorové úřady*, z této kapitoly jsou řešeny pouze následující články:

- Článek 82 - Právo na náhradu újmy a odpovědnost.
- Článek 83 - Obecné podmínky pro ukládání správních pokut.
- Článek 84 – Sankce.

# 3 Obecné zásady zpracování

Předchozí kapitola byla věnována právním úpravám, které GDPR předcházely, stejně tak o důležitosti ochraně osobních údajů a jejímu významu. Následující kapitola slouží pro uvedení do obecných zásad zpracování a základní pravidla pro operace s osobními údaji, představení podoby zákonného souhlasu se zpracováním osobních údajů, definice zvláštní kategorie těchto údajů, dodržení nutných podmínek v případě subjektu mladšího určité věkové hranice a pravidel pro zpracování osobních údajů související s trestními věcmi subjektů či zpracování, které nevyžaduje identifikaci.

Nařízení stanovuje soubor zásad pro ochranu osobních údajů, které by měly být hlavním návodem toho, jak osobní údaje spravovat a zpracovávat. Zásady jsou tak přehledem nejdůležitějších obecných povinností pro dodržování nařízení a podstatně ovlivňují danou právní oblast a zároveň jsou východiskem pro právní úpravy.

GDPR v Kapitole II, Článek 5 [4] definuje několik zásad pro zpracování osobních údajů a jejich dodržování je pro správce zásadní, jelikož právě správce má odpovědnost za jejich dodržování a schopnost tyto doložit. K takovému prokazování slouží např. záznamy o činnostech zpracování a kodexy.

Zásady zpracování GDPR lze shrnout na:

a) zákonnost, korektnost a transparentnost;
b) účelové omezení;
c) minimalizace údajů;
d) přesnost;
e) omezení uložení;
f) integrita a důvěrnost;
g) odpovědnost;

Osobní údaje musí být ve vztahu k subjektu správcem zpracovávány na základě nejméně jednoho právního titulu a vůči subjektům údajů musí být zpracovány korektně a transparentně. Takové údaje musí být shromažďovány pouze pro určité legitimní účely, které jsou výslovně vyjádřené, a nesmějí být dále zpracovávány v rozporu s těmito účely. Osobní údaje také musí být přiměřené, relevantní a omezené na nezbytný rozsah vzhledem k účelu jejich zpracování. Také musí být přesné a v případě potřeby aktualizované. Takové údaje, které jsou nepřesné (s přihlédnutím k účelům) musí být

bezodkladně vymazány nebo opraveny. Údaje by měly být uloženy jen po nezbytnou dobu pro jejich účel zpracovány v takové formě, která umožňuje identifikaci subjektu údajů. Po delší dobu lze uložit údaje, které jsou zpracovávány výhradně pro účely archivace ve veřejném zájmu, vědeckého či historického výzkumu či pro statistické účely. To za podmínky dodržení zásady minimalizace údajů, což může zahrnovat pseudonymizaci[2], pokud tak lze sledované účely splnit. Způsob zpracování musí zajistit náležité zabezpečení osobních údajů, a to pomocí vhodných technických nebo organizačních opatření, které budou vést k ochraně před náhodnou ztrátou, zničením nebo poškozením. Správce odpovídá za všechny tyto body a musí být schopen toto dodržení doložit.

**Zákonnost zpracování**

Pro každý účel zpracování osobních údajů správce potřebuje právní titul neboli právní důvod. Zpracování osobních údajů se tak vždy váže ke konkrétnímu účelu, na jehož základě se určí právní důvod pro dané zpracování. Nezbytným předpokladem pro zákonné zpracování jsou tedy právní důvody.

Právní důvody přiřazují správci oprávnění osobní údaje zpracovávat, jsou tak nezbytným předpokladem pro legální zpracování. Pokud by správce neměl řádný právní důvod ke zpracování osobních údajů, bylo by takové zpracování nezákonné a musel by je tak odstranit.

Tyto důvody nařízení definuje v Kapitole II, Článek 6 [4]. Není vyloučeno, že stejné osobní údaje (či jejich souhrn) správce bude zpracovávat pro více účelů, které mohou v čase vznikat a zanikat, aniž by vznikala povinnost správce údaje zlikvidovat. Ta nastane až v případě, kdy správci zanikne poslední právní důvod pro zákonné zpracování osobních údajů.

Právními důvody jsou následující podmínky, a pokud je splněna nejméně jedna z následujících podmínek, lze osobní údaje zpracovávat, a to v odpovídajícím rozsahu.

---

[2] Pseudonymizace představuje nahrazení identifikačních údajů osob nesouvisejícím řetězcem dat tak, aby nebylo možné spárovat tyto údaje s konkrétními osobami. [6]

1. Zpracování údajů je nezbytné pro:
   a) Splnění smluvních povinností, kdy subjekt údajů je smluvní stranou, či v souvislosti s provedením opatření přijatých před uzavřením smluvního vztahu, pokud se jedná o žádost subjektu údajů.
   b) Splnění povinností, které správci ukládá právo.
   c) Ochranu zájmů, které jsou pro subjekt údajů či jiné fyzické osoby (FO) životně důležité.
   d) Splnění úkolu, kterým je pověřen správce a který je vykonáván ve veřejném zájmu či při výkonu veřejné moci, rozsah ovšem musí být přiměřený ke sledovanému cíli.
   e) Účely oprávněných zájmů příslušného správce či třetí strany. Takové zájmy ovšem nesmí převažovat nad zájmy či základními právy a svobodami subjektu údajů vyžadující ochranu osobních údajů, a to zejména jestliže je subjektem údajů dítě. Tato podmínka se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.
2. Nebo v případě, že subjekt údajů udělil souhlas se zpracováním pro jeden / více konkrétních účel(ů).

U jiných zvláštních situací, při nichž dochází ke zpracování, nařízení umožňuje členským státům EU provést upřesnění, a to určením konkrétních požadavků na zpracování a jiná opatření. Jedná se o přizpůsobení používání pravidel pro případ 1.b), 1.d) (viz výše). Tyto dvě podmínky musí být stanoveny buď právem EU, nebo právem členského státu EU, a dotýkat se daného zpracování osobních údajů správcem. Pokud jsou osobní údaje zpracovány pro jiný účel, než pro které byly nashromážděny a zpracování není založeno na souhlasu nebo na právu EU či členského státu EU musí správce zohlednit, zda je zpracování pro jiný účel slučitelné s účely, pro které byly osobní údaje původně shromážděny. Jedná se o zohlednění vazby mezi účely, za jakým byly shromážděny a účely zamýšlené pro další zpracování včetně možných důsledků tohoto zpracování pro subjekt údajů, okolnosti shromáždění osobních údajů. Dále se jedná o povahu osobních

údajů[3] či existenci vhodných záruk, např. šifrování či pseudonymizace. Následuje příklad sdělení účelů zpracování osobních údajů v České spořitelně.

***Příklad: Účely zpracování osobních údajů v České spořitelně***

Zpracování osobních údajů probíhá v rozsahu nezbytném pro dané služby, kterou si klient v bance sjednává.

**Zpracování osobních údajů na základě souhlasu:**

- marketingové činnosti,
- nefinanční služby partnerů,
- vzájemné informování oprávněných uživatelů Bankovního a Nebankovního registru klientských informací (BRKI a NRKI),
- alternativní posouzení rizik,
- podpisová biometrie,
- automatizované rozhodování,
- služba informování o vedení účtu (služba Multibanking).

**Zpracování osobních údajů, ke kterým není potřeba souhlas:**

- plnění povinností, které vyplývají z uzavřených smluv,
- splnění povinností, které bance ukládají zvláštní právní předpisy,
- zajištění ochrany práv a právem chráněných zájmů (např. uplatnění nároků u soudů či pojišťoven), rozsah je omezen na osobní údaje nezbytné pro úspěšné uplatnění nároku,
- splnění úkolu prováděného ve veřejném zájmu.

Pokud klient odmítne sdělit osobní údaje pro některý z uvedených důvodů, není možné mu poskytnout příslušný produkt, službu, či jiné plnění, pro které jsou OÚ potřeba.

*Převzato z [7].*

[3] zvláště kategorie specifikované ve článku 9 a osobní údaje spojené s rozsudky v trestních věcech nebo trestních činech – článek 10

**Podmínky vyjádření souhlasu**

Souhlas je jedním z právních důvodů pro zákonné zpracování a je jej využíváno, pokud zpracování nelze zařadit v rámci jiného právního důvodu. Souhlas je podle definice z obecných ustanovení svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává své svolení ke zpracování osobních údajů. Jinými slovy, subjekt údajů k vyslovení souhlasu nesmí být donucen, musí být přesně dané pro jaký konkrétní účel je daný souhlas vysloven, musí být doplněn informacemi o důvodu zpracování, jeho rozsahu apod. Subjekt údajů jeho prostřednictvím dává jednoznačně najevo, že s těmito skutečnostmi souhlasí. Souhlas by měl být posledním způsobem, jak získat právní důvod ke zpracování, jelikož zpracování osobních údajů pouze na základě souhlasu je rizikové. Souhlas je dle nařízení vždy možno odvolat a správce je tak povinen údaje zlikvidovat nebo zpracování odůvodnit jiným právním titulem. Pokud je zpracování založeno na souhlasu, musí ho být správce schopen doložit. Souhlas musí splňovat určité náležitosti, které definuje nařízení v Kapitole II, Článek 7 [4].

Z výše uvedeného vyplývá, že souhlas:

- Poskytuje se vždy k určitému účelu, se kterým je subjekt seznámen.
- Je odvolatelný.
    - Odvoláním souhlasu také není dotčena zákonnost zpracování před jeho odvoláním, o čemž musí být subjekt informován.
    - Odvolání souhlasu musí být stejně snadné jako jeho poskytnutí.
- V případě, se jedná o písemné vyjádření spojené i s jinými skutečnostmi, musí být souhlas od takových skutečností jasně odlišitelný, srozumitelný a snadno přístupný.
    - Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná.

Svoboda souhlasu je posuzována podle toho, jestli není souhlasem podmíněno jiné plnění smlouvy, které zpracováním daných osobních údajů není pro plnění dané smlouvy nutné.

Příkladem souhlasu dle nařízení může být výňatek ze souhlasu se zpracováním osobních údajů e-shopu Mall, který následuje.

***Příklad: Výňatek ze souhlasu se zpracování osobních údajů e-shopu Mall***

…

*„Dále souhlasím, aby společnost HC sdílela se společností O2 Czech Republic a.s., Za Brumlovkou 266/2, 140 22 Praha, IČO 60193336, a členy skupiny PPF, uvedenými na internetových stránkách www.homecredit.cz, Osobní údaje i informace o mé důvěryhodnosti a platební morálce a dále aby je tyto společnosti a členové skupiny PPF samostatně zpracovávali, a to za účelem posouzení Žádosti, vyhodnocování postupu splácení poskytnutého úvěru či jiného závazku vůči společnosti O2 Czech Republic a.s. nebo kterémukoli členovi skupiny PPF, dále pro vyhodnocení mé schopnosti platit cenu nabízeného produktu a pro ochranu práv členů skupiny PPF nebo společnosti O2 Czech Republic a.s.; informacemi o mé důvěryhodnosti a platební morálce se rozumí především informace o výši a důvodu jakýchkoli mých závazků, o postupu jejich plnění, o rozsahu těchto závazků po splatnosti a délce prodlení, jakož i o případných skutečnostech snižujících moji důvěryhodnost, jako jsou exekuce, úpadek či podezření na spáchání trestného činu, a údaje o způsobu využívání produktů, které mi poskytli či poskytnou společnosti HC, O2 Czech Republic a.s. nebo členové skupiny PPF. Tento souhlas uděluji na dobu 1 roku, a v případě, že bude na základě Žádosti uzavřena smlouva o úvěru, uděluji souhlas na dobu do uplynutí deseti (10) kalendářních let následujících po dni, ve kterém došlo k zániku smlouvy nebo ke splacení všech mých závazků, které ze smlouvy vyplývají; přednost má ta z uvedených situací, která nastane později.“*

…

*Převzato z [8].*

**Podmínky získání souhlasu od dítěte**

Nařízení vnímá zranitelnost subjektů mladších určité věkové hranice například v souvislosti se sociálními sítěmi a ukládá správcům přísnější režim získání jejich souhlasu.

Článek 8 nařízení [4] se týká souhlasu dítěte v souvislosti se službami informační společnosti. Jako právní důvod udělení souhlasu v souvislosti s nabídkou služeb informační společnosti přímo dítěti je zákonný, pokud je dítě ve věku nejméně 16 let. Pokud je dítě mladší 16 let je právní důvod zákonný, pouze pokud byl souhlas vyjádřen nebo schválen osobou, která vykonává k dítěti rodičovskou zodpovědnost.

I zde mají možnost členské státy provést úpravu v podobě stanovení nižšího věku pro tento účel, nesmí však být nižší než 13 let. Vymezení pro ČR se nachází v kapitole *GDPR v podmínkách ČR*. Tím ovšem není dotčeno obecné smluvní právo členských států, např. pravidla týkající se platnosti, uzavírání či účinků smlouvy vzhledem k dítěti.

Správce je povinen vyvinout přiměřené úsilí, aby ověřil, že souhlas byl vyjádřen nebo schválen zákonným zástupcem dítěte. Příkladem špatné interpretace nařízení v problematice zpracování osobních údajů dětí může být problematika vystavování výkresů dětí viz níže.

***Příklad špatné praxe – Výkresy dětí bez podpisů***

Jednou z obav spojenou s medializací GDPR byla problematika vystavování výkresů dětí, na kterých je jejich podpis, tzn. jméno a věk. Důvodem pro toto nepochopení nařízení v tomto případě byla špatná interpretace pojmu zpracování osobních údajů. Ten byl mylně chápán jako samotná existence osobního údaje v jakékoli podobě. To způsobilo nepřiměřenou snahu o ochranu soukromí v podobě zákazu podepisování dětských výkresů. Ochrana osobních údajů a zpracování osobních údajů musí být chápáno v širším kontextu celého právního systému. V tomto případě by došlo k upřednostnění práva na ochranu osobních údajů před právem na svobodu slova a na informace, kdy z pohledu práva nemá ani jedno právo přednost před druhým a jedná se tedy o špatnou interpretaci nařízení.

Vystavováním výkresů, na kterých je podpis dítěte tedy v tomto případě není možné označit jako zpracování osobních údajů.

*Převzato z [9].*

**Zpracovávání zvláštních kategorií osobních údajů**

Osobní údaje, které vypovídají o rasovém či etnickém původu, náboženském vyznání, členství v odborech, filozofické přesvědčení či politických názorech je zakázáno zpracovávat, stejně jako zpracování genetických, biometrických údajů za účelem jednoznačné identifikace FO a údajů o zdravotním stavu, sexuálním životě či sexuální orientaci FO.

Výjimku tvoří několik případů, vyjmenované v Kapitole II, Článek 9 [4], mezi které patří:

a) Subjekt udělil výslovný souhlas se zpracováním takových osobních údajů, a to pro jeden či více stanovených účelů, pokud se nejedná o případ, ve kterém právo EU či členského státu zakazuje zrušení zákazu.
b) Zpracovávání je nevyhnutelné pro účely plnění povinností a výkon zvláštních práv, které se mohou týkat pracovního práva, sociálního zabezpečení a ochrany. Dále tak musí být povoleno právem členského státu EU či EU, které zároveň stanovuje vhodné záruky pro základní práva a zájmy subjektu.
c) Zpracování je potřebné pro ochranu životně důležitých zájmů daného subjektu nebo jiné FO, pokud subjekt údajů není schopen udělit souhlas.
d) Zpracování provádí neziskový subjekt[4], jehož cíle jsou politické, náboženské, odborové či filozofické, a to za podmínky, že se takové zpracování vztahuje pouze na členy takového subjektu (jak současné, tak bývalé) nebo na osoby, které s nimi udržují pravidelné styky související s takovými cíli. Tyto osobní údaje mohou být zpřístupňovány mimo tento subjekt pouze se souhlasem subjektu údajů.
e) Jedná se o osobní údaje zjevně zveřejněné subjektem údajů.
f) Zpracování je nezbytné pro právní nároky, a to jejich určení, výkon či obhajobu, či pokud se jedná o zpracování prováděné soudy v rámci jejich pravomocí.
g) Zpracování je nezbytné pro významný veřejný zájem (na základě práva EU nebo členského státu), ovšem musí být přiměřené ke sledovanému cíli, dodržovat podstatu práva a poskytuje vhodné a konkrétní záruky pro ochranu subjektu údajů a jeho základních práv a zájmů.
h) Jedná se o účely lékařství, preventivního nebo pracovního, dále posouzení pracovní schopnosti zaměstnance, diagnostiky lékaře či poskytování zdravotní či sociální péče, řízení systémů a služeb zdravotní či sociální péče (na základě práva EU či členského státu nebo smlouvy se zdravotnickým pracovníkem). Zpracování takových údajů pak může provádět pouze pracovník vázaný služebním tajemstvím nebo na odpovědnost svou či jiné osoby taktéž vázané mlčenlivostí.

[4] např. nadace či sdružení

i) Jedná o účely veřejného zdraví (přeshraniční zdravotní hrozby, přísné normy kvality, bezpečnost zdravotní péče a léčivých přípravků) na základě práva EU či členského státu. Musí být jimi stanoveno odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu.
j) Jedná se o údaje nezbytné pro archivaci ve veřejném zájmu, vědeckého či historického výzkumu nebo statistické účely specifikované v ustanovení týkající se zvláštních situací a v souladu s ním.

Stejně jako u jiných zásad, i zde platí pravidlo, že členské státy EU mohou tyto podmínky zachovat nebo zavést další, včetně omezení, pokud jde o zpracování biometrických a genetických údajů či údajů o zdravotním stavu. Specifikace pro ČR určuje Zákon č. 110 viz kapitola *GDPR v podmínkách ČR* v této práci. To, jak s takovými údaji nakládat specifikuje také např. metodika MŠMT viz níže.

***Příklad: Zvláštní kategorie osobních údajů v prostředí školy – Metodika MŠMT***

Do výše uvedené kategorie spadá celá škála citlivých osobních údajů – zejména pak údaje o zdravotním stavu v oblasti jak fyzického, tak mentálního zdraví, údaje o omezeních ve stravování nebo specifické stravovací plány, a to jak ze souvislosti se zdravotním stavem, tak i filozofickým nebo náboženským přesvědčením. Dalšími citlivými údaji mohou být záznamy o sociální situaci jedince, šikaně nebo údaje spojené se sexualitou člověka. Je třeba dát na minimalizaci rizika zneužití takových údajů a primárně je zpracování těchto údajů zakázáno vyjma případů stanovených nařízením.

*Převzato z [10].*

**Zpracování osobních údajů týkajících se trestních věcí a činů**

Zpracování takových osobních údajů, které se týkají rozsudků v trestních věcech a trestních činů a bezpečnostních opatřeních na základě „Zákonnosti zpracování“ definuje Kapitola II, Článek 10 [4], lze provádět pouze pod dozorem orgánu veřejné moci. Jedná se o státní orgány jako jsou ministerstva, soudy, policii, či orgány samosprávy územní i profesní, například obecní policie či disciplinární komise. Dále lze takové zpracování provádět, pokud je oprávněné dle práva EU či členského státu EU, v případě, že jde o práva a svobody subjektu údajů. Souhrnný rejstřík trestů, a to v jakékoli podobě, může být veden pouze pod dozorem orgánu veřejné moci.

***Příklad: Výpis z rejstříku trestů ve vztahu zaměstnavatele a zaměstnance***

Není nic neobvyklého, že zaměstnavatel po zájemci o zaměstnání či svém zaměstnanci žádá předložení výpisu z rejstříku trestů. Ovšem k tomuto požadavku mají právo zaměstnavatelé pouze v případě, kdy to stanovují právní předpisy. Mezi takové práce lze zařadit například:

- zdravotní sestra,
- policisté,
- učitelé,
- auditoři,
- advokáti.

Dále se jedná také o případy, kdy lze požadovat požadavek bezúhonnosti přiměřený k vykonávané práci.

Informace o bezúhonnosti a trestní minulosti nesmí zaměstnavatel získávat ani prostřednictvím třetích osob.

*Převzato z [11]*

**Zpracování, které nevyžaduje identifikaci**

Nařízení v tomto článku počítá s případem, kdy správce zpracovává takové osobní údaje, se kterými není sám schopen identifikovat subjekt údajů (SÚ). Jelikož se i přesto může jednat o osobní údaje, které mohou subjekt údajů přímo nebo nepřímo identifikovat, převážně na základě informací či prostředků, kterými nemusí disponovat sám správce, ale může k nim mít přístup třetí strana. V případě, že by správce musel vyvinout nepřiměřené úsilí, nařízení neukládá správci povinnost získávat další údaje o subjektech pro jejich identifikaci a následné plnění ostatních povinností GDPR.

Pro takové účely zpracování, které nevyžadují nebo již nevyžadují identifikaci subjektu údajů, správce tedy nemá povinnost uchovávat, získávat či zpracovávat dodatečné informace k identifikaci subjektu výlučně kvůli tomuto nařízení. Pokud je *„… správce s to doložit, že není schopen identifikovat subjekt údajů, informuje o této skutečnosti subjekt údajů, pokud je to možné.“* [4]. V takovém případě pak subjekt nemůže uplatnit právo na přístup ke svým osobním údajům a práva spadající do oddílu „Oprava a výmaz“.

Výjimkou pro takový případ je, pokud subjekt za účelem výkonu svých práv poskytne dodatečné informace umožňující jeho identifikaci.

O takové zpracování se může jednat tehdy, pokud je osobním údajem např. IP adresa jako v příkladu viz níže.

***Příklad: IP adresa***

Správce má k dispozici IP adresy uživatelů, ovšem bez informací od subjektu či třetí strany (poskytovatel připojení) není schopný zjistit, jakému subjektu byla daná IP adresa přiřazena. V takovém případě není správce povinen získávat další údaje o subjektu pouze za účelem jeho identifikace.

*Převzato z [12].*

# 4 Subjekty údajů a jejich práva

Předchozí kapitola obsahovala specifikaci obecných zásad zpracování a základních pravidel pro nakládání s osobními údaji správcem či zpracovatelem. Tato kapitola bude věnována subjektu údajů, konkrétně jeho právům a povinnostem, které k němu má správce. Subjekt údajů nařízení označuje fyzickou osobu, ke které se osobní údaje vztahují. V žádném případě se nemůže jednat o právní osobu, ani o zemřelou fyzickou osobu, jelikož nařízení upravuje zpracování osobních údajů pouze žijících fyzických osob.

Toto obecné nařízení, přiznává subjektům údajů práva, jejichž účelem je vyrovnání vztahu mezi správcem a subjektem údajů. Obecné nařízení v Kapitole III [4] tyto práva oproti zákonu o ochraně osobních údajů posiluje, a to jak aktualizací střetávajících práv, tak také zavedením práv nových.

**Práva subjektů údajů**

Mezi práva subjektu údajů patří právo být informován o zpracování svých osobních údajů, zejména o účelu zpracování, totožnosti správce a o jeho zájmech, také o příjemcích osobních údajů. Aktivitu vůči subjektu, tzn. poskytnutí či zpřístupnění informací, musí vyvinout správce, nikoliv subjekt údajů, čímž se jedná o pasivní právo.

Všechny práva jsou podrobně představena v dalších částech práce a jsou jimi právo:

- na přístup k osobním údajům,
- na opravu či doplnění,
- na výmaz,
- na omezení zpracování,
- na přenositelnost údajů,
- vznést námitku,
- nebýt předmětem automatizovaného individuálního rozhodovaní.

Veškerá sdělení a úkony se zásadně poskytují a činí bezplatně. Pokud jsou žádosti zjevně nedůvodné nebo nepřiměřené, zejména pokud se opakují, může správce uložit přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo odmítnout žádosti vyhovět. Takovou nedůvodnost pak dokládá správce.

### Transparentnost a postupy

Při definování způsobu poskytování informací subjektu údajů, vychází GDPR ze stanovených zásad, především transparentnosti. To znamená, že správce poskytne subjektu údajů veškeré informace o účelech zpracování, právních titulech zpracování, době uložení údajů, kontaktních údajů na správce, kategoriích zpracovávaných údajů a ostatních skutečnostech stanovené nařízením. Pro transparentnost musí být tyto údaje předávané stručně, srozumitelně, musí být snadno přístupné a za použití jasných a jednoduchých jazykových prostředků. Učiní veškerá sdělení o právech subjektu a o oznamování porušení zabezpečení osobních údajů (OÚ), zejména pokud se jedná o informace určené dítěti. Informace jsou poskytnuty písemně či jinými prostředky, a pokud si to subjekt vyžádá, mohou být informace sděleny i ústně, v případě, že identita subjektu je prokázána jinými způsoby. Tyto povinnosti vyplývají z Kapitoly III, Článek 12 [4]. Správce dále usnadňuje subjektu údajů výkon a poskytne mu informace o přijatých opatřeních bez zbytečného odkladu, v každém případě do jednoho měsíce od obdržení žádosti.

### Informace a přístup k osobním údajům

Subjekt údajů má právo na potvrzení, zda jsou zpracovávány jeho osobní údaje (Kapitola III, Oddíl 2 [4]). Pokud jsou jeho osobní údaje zpracovávány, má právo na přístup k informacím o:

- účelu zpracování,
- kategorii osobních údajů, které jsou zpracovány,
- kategorii příjemců,
- plánované době uložení,
- o svých právech:
    - na opravu, výmaz, omezení a práva vznést námitku či podat stížnost u dozorového úřadu,
- zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
- automatizované rozhodování a s tím související informace.

Nařízení rozlišuje, které informace je správce povinen poskytnout, podle toho, jestli jsou zpracovávané údaje získané přímo od subjektu údajů či z jiného zdroje. Vždy však musí poskytnout kontaktní a identifikační údaje své a příslušeného DPO, pokud je jmenován,

informace o účelech zpracování a zákonných titulech, jakéhokoli příjemce či zpracovatele, to jestli jsou údaje předávané do třetích zemí, dobu uchování údajů, existence práv subjektu. Dále v závislosti na zdroji údajů pak poskytne např. pokud se jedná o zpracování na základě souhlasu, tak mimo jiné to, jaké jsou důsledky neposkytnutí osobních údajů a souhlasu.

**Právo na opravu**

Subjekt má právo na opravu nepřesných osobních údajů, které se ho týkají, které vyplývá z Kapitoly III, Článek 16 [4]. Správce tak činí bez zbytečného odkladu. S přihlédnutím k účelu zpracování je zde právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení. Toto právo vyplývá ze zásady přesnosti. Správce ovšem není povinen aktivně vyhledávat a ověřovat údaje**,** což mu ovšem nařízení nezakazuje, ani pravidelně žádat subjekt o aktualizaci jeho údajů. Pokud se subjekt domnívá, že jeho osobní údaje, které správce zpracovává jsou nepřesné, upozorní jej na to a správce má pak povinnost se zabývat žádostí subjektu o doplnění či opravu údajů.

**Právo být zapomenut**

Subjekt údajů má právo na vymazání údajů, které jsou o něm zpracovávány, pokud nastal jeden z těchto důvodů (Kapitola III, Článek 17 [4]):

a) Údaje již nejsou potřebné pro účely, pro které byly zpracovány.
b) Subjekt odvolal souhlas se zpracováním u těch údajů, jejichž zpracování je na souhlasu založené.
c) Subjekt vznesl námitku proti zpracování a neexistují žádné převažující oprávněné důvody pro jejich zpracování.
d) Údaje byly zpracovány protiprávně.
e) Vymazání údajů stanovují platné právní předpisy.

Pokud správce osobní údaje zveřejnil a je povinen (viz výše) je vymazat, provede přiměřené kroky s ohledem na dostupnou technologii a náklady na provedení vymazání veškerých odkazů na tyto osobní údaje, včetně jejich kopií či replikacích.

Předchozí neplatí pouze pro takové osobní údaje, jejichž zpracování je nezbytné pro:

a) Výkon práva v souvislosti se svobodou projevu a informací.
b) Splnění povinností dané právem vztahujícího se na správce, které vyžaduje zpracování.
c) Splnění úkolu uloženého správci, ve veřejném zájmu nebo při výkonu veřejné moci.
d) Veřejný zájem v oblasti veřejného zdraví.
e) Pro vědecké, historické, statistické účely, či účely archivace ve veřejném zájmu, pokud je pravděpodobné, že vymazání údajů by znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování.
f) Právní nároky, a to jejich určení, výkon nebo obhajoba.

**Právo na omezení zpracování**

Pokud má subjekt údajů objektivní právní důvod pro omezení zpracování a jsou splněny podmínky, dojde k omezení zpracování po dobu nezbytně nutnou. Takové osobní údaje, s výjimkou jejich uložení, mohou být zpracovány v případě, že subjekt údajů udělil souhlas, zpracování probíhá v souvislosti s právními nároky či z důvodu ochrany práv jiné fyzické osoby (FO) či právnické osoby (PO) nebo z důvodu důležitého veřejného zájmu EU či některého členského státu EU. Úprava pro podmínky ČR je součástí Zákona č. 110/2019 viz kapitola *GDPR v podmínkách ČR*. Správce je povinen předem subjekt údajů upozornit na zrušení takového omezení zpracování.

Objektivními právními důvody se rozumí:

a) Jeho osobní údaje, které jsou zpracovávané, nejsou přesné a nelze provést opravu podle daných pravidel a je nutné ověřovat přesnost údajů ze strany správce.
b) Zpracování je protiprávní a subjekt si nepřeje provedení výmazu.
c) Údaje mají být smazány, ale subjekt je vyžaduje pro určení, výkon nebo obhajobu právních nároků.
d) Ověření, zda oprávněné zájmy správce, na základě kterých dochází ke zpracování, převažují nad oprávněnými důvody subjektu údajů v případě jeho vznešení námitky proti zpracování.

Právo požadovat omezení zpracování osobních údajů vyplývá z Kapitoly III, Článek 18 [4].

**Právo na přenositelnost údajů**

Subjekt má právo získat takové osobní údaje, které se ho týkají a které poskytl správci, pokud je zpracování OÚ založeno na souhlasu případně na smlouvě, a zároveň se zpracování provádí automatizovaně. Podoba takových údajů by měla být ve formě strukturovaného, běžně používaného formátu, který je strojově tak, jak to definuje Kapitola III, Článek 20 [4].

Subjekt má také právo na předání těchto údajů jinému správci, aniž by tomu původní správce bránil. Je-li to technicky proveditelné má subjekt právo na předání osobních údajů přímo jedním správcem správci druhému.

Výkonem tohoto práva není dotčeno právo na výmaz. Právo na přenositelnost se neuplatní, pokud je zpracování nezbytné pro plnění úkolu, který je prováděn správcem na základě pověření, ve veřejném zájmu či výkonu veřejné moci.

Právem na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob.

**Právo vznést námitku**

Subjekt údajů má právo kdykoli vznést námitku proti zpracování osobních údajů v případě, že se jedná o zpracování na základě právních důvodů, kdy zpracování údajů je nezbytné pro:

- Splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci (kterým je pověřen správce), jehož rozsah ovšem musí být přiměřený ke sledovanému cíli.
- Účely oprávněných zájmů příslušného správce nebo třetí strany. Ty ovšem nesmí převyšovat nad zájmy či základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, a to zejména jestliže je subjektem údajů dítě, což se netýká se zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

Pokud správce neprokáže závažné a oprávněné důvody pro zpracování, které by převažovaly nad zájmy či právy a svobodami subjektu, správce osobní údaje dále nezpracovává.

Subjekt údajů tedy může vznést námitku, pokud se jedná o zpracování za účelem přímého marketingu, a to i profilování, pokud se týká tohoto přímého marketingu. Pokud subjekt v tomto případě vznese námitku proti zpracování, nebudou již osobní údaje pro tyto účely zpracovávány. Na tyto práva je subjekt údajů výslovně upozorněn a toto právo je uvedeno zřetelně a odděleno od jiných informací, a to nejpozději při první komunikaci se subjektem.

Pokud jsou osobní údaje zpracovány pro statistické účely či účely historického či vědeckého výzkumu, má subjekt údajů právo vznést námitku proti zpracování osobních údajů, které se ho týkají. Výjimka je, pokud je zpracování nezbytné pro splnění daného úkolu a pokud je tento úkol prováděn z důvodu veřejného zájmu.

Tato problematika je řešená v Kapitole III, Článek 21 [4].

**Automatizované individuální rozhodování**

Subjekt údajů má právo nebýt předmětem žádného rozhodnutí, které by bylo založené výhradně na automatizovaném zpracováním, to včetně profilování, které by pro subjekt mělo právní účinky nebo se obdobným způsobem významně dotýká. Kapitola III, Článek 22 mimo toto, definuje i případy, kdy toto neplatí, a to pokud je rozhodnutí:

a) nevyhnutelné k uzavření nebo plnění smlouvy,
b) povoleno právem,
c) založené na výslovném souhlasu subjektu údajů.

# 5 Problematika správce a zpracovatele

Tato část práce bude zaměřena na subjekty, které správu a zpracování související s osobními údaji provádějí, a které toto nařízení označuje jako správce a zpracovatele.

Nařízení v Kapitole IV [4] definuje, že v tomto kontextu je správcem subjekt, který určuje účely a prostředky zpracování osobních údajů, a to jak samostatně, tak spolu s jinými subjekty. Zpracovatel je pak subjekt, který osobní údaje zpracovává. Správcem i zpracovatelem může být subjekt jakékoli podoby, tzn. jak fyzická osoba, tak právnická osoba, případně orgán veřejné moci nebo jiný subjekt. Těmto subjektům jsou nařízeny povinnosti, které v souvislosti s osobními údaji musí plnit. Nařízení GDPR respektuje při určování těchto povinností technické možnosti správce a zpracovatele a rozsah či kategorii zpracovaných údajů a na základě toho povinnosti a podmínky mírně upravuje.

## 5.1 Obecné povinnosti správce a zpracovatele

Vzhledem k velké rozsáhlosti druhů a účelů zpracování, různé míry zranitelnosti subjektů údajů i osobních údajů samotných a jiných aspektů zpracování, je i rozsáhlost povinností značná a částečně se různí dle konkrétních případů zpracování OÚ. Obecné nařízení o ochraně osobní údajů tedy definuje obecné povinnosti správce a zpracovatele, které jsou platné v různém rozsahu pro všechny správce a zpracovatele a poté specifické povinnosti dle konkrétních aspektů a náležitostí. Správce má za povinnost zavést taková opatření, aby soulad s nařízením nejenom zajistil, ale byl schopný i doložit, k čemuž má možnost využít několik nástrojů.

Obecné povinnosti jsou blíže specifikovány v Kapitole IV, Oddíl 1 nařízení [4] a patří mezi ně odpovědnost správce, záměrná a standardní ochrana osobních údajů, problematika zpracovatelů či záznamy o zpracování. Dle relevantnosti pro potřeby této práce budou tyto povinnosti dále představeny.

Pro dokládání souladu operací zpracování osobních údajů, mezi které patří právě plnění povinností ukládaných správci či zpracovateli, může správce využít odpovídající dokumentaci např. při kontrole Úřadu pro ochranu osobních údajů (ÚOOÚ) či zpracovatelskou smlouvu. Lze ovšem využít i nových, nutno dodat, že nepovinných nástrojů, které nařízení zavádí, kterými jsou kodexy chování definovány v Kapitole IV, Oddíl 5 nařízení [4].

**Kodexy chování**

Kodexy chování poskytují příležitost subjektům v daném odvětví dohodnout se společně na konkrétních a praktických pravidlech při zpracování OÚ v daném odvětví. Jedná se o samoregulační nástroj, který by měl zohledňovat specifika různých odvětví. Jak bylo zmíněno výše, jedná se o nástroj nepovinný, který se ovšem stává závazný pro instituce, které se k jeho dodržování přihlásí. Kodexy nezpracovává dozorový úřad, pouze poskytuje nezbytné konzultace ve fázi přípravy a následně posoudí předložený kodex a vydá stanovisko, zdali je kodex v souladu s nařízením a poté jej schválí. Musí být ovšem zpracován tak, aby pokryl požadavky upravené nařízením GDPR.

Cílem kodexů chování by mělo být upřesnění uplatňování ustanovení tohoto nařízení, mimo jiné se jedná o:

a) spravedlivé a transparentní zpracování,
b) oprávněné zájmy, jež správci sledují,
c) shromažďování osobních údajů,
d) pseudonymizaci osobních údajů,
e) informace poskytované veřejnosti a subjektu údajů,
f) výkon práv subjektů údajů,
g) informace poskytované dětem, převážně způsob získávání souhlasu apod.,
h) opatření a postupy plynoucí z tohoto nařízení,
i) ohlašování případů porušení zabezpečení OÚ,
j) předávání osobních údajů do třetích zemí či mezinárodním organizacím,
k) mimosoudní vyrovnání a jiné postupy řešení sporů.

Kodexem chování se tedy rozumí jistá forma metodiky pro konkrétní specifické odvětví, kterým může být např. pojišťovnictví či bankovnictví, která shrnuje specifikace daného odvětví a k němu přidružených ostatních zákonů a zajišťuje jednotný výklad nařízení. Kodexy by tak měly zajistit snadnější adaptaci nařízení a zjištění souladu s nařízením, jelikož subjekt je vázán jeho dodržováním. Mimo jiné mohou pro subjekt údaj zjednodušit přechod mezi konkurenčními firmami, jelikož firmy, které přistoupí do kodexu chování jsou vázáné mimo jiné i dodržením formátu osobních údajů při právu na přenositelnost. Žádný kodex v době zpracování diplomové práce zatím nebyl v českém prostředí schválen, byla pouze zveřejněna metodiku náležitostí kodexů.

**Standardní a záměrná ochrana osobních údajů**

Co se týká vnímání ochrany osobních údajů, nařízení nabádá k zavedení přiměřených technických a organizačních opatření, které mají za cíl vytvořit ochranu ve dvou rovinách:

- ochrana standardní, která je v originále označovaná jako *by default*,
- ochrana záměrná, která je v originále označovaná jako *by design*.

Standardní ochrana osobních údajů spočívá v zavedení vhodných opatření k zajištění toho, aby správce využíval pouze ty údaje, které jsou pro daný účel nezbytné, a aby osobní údaje nebyly standardně dostupné neomezenému počtu osob. Příkladem může být sociální síť, na které je výchozí nastavení uzpůsobeno pro co nejvhodnější ochranu soukromí, tzn. že bez aktivity dané osoby nejsou údaje přístupné velkému množství jiných osob.

Záměrná ochrana naproti tomu počítá s tím, že správce zavede vhodné opatření jak v době před zpracováním, tak i v jeho průběhu za účelem zajištění souladu s nařízením od samého začátku. Nástrojem pro takovou ochranu může být pseudonymizace či šifrování.

Všechna tato opatření jsou tvořena s ohledem na technické možnosti, náklady na provedení, rozsah, účel a kontext zpracování.

**Záznamy o činnostech zpracování**

Správce i zpracovatel mají povinnost vést záznamy o činnostech zpracování, za které odpovídají. Důvodem pro vedení těchto záznamů je zajištění důsledného monitorování a transparentnosti zpracování údajů a schopnosti správce či zpracovatele doložit soulad s nařízením. Tato povinnost se vztahuje na takové správce a zpracovatele, kteří splňují alespoň jeden z těchto bodů:

- má více než 250 zaměstnanců,
- provádí zpracování, které pravděpodobně představuje riziko pro práva a svobody subjektů údajů,
- zpracování neprovádí příležitostně,
- zahrnuje zpracování údajů dle článku 9 anebo 10 (zvláštní kategorie údajů a OÚ týkajících se rozsudku v trestních věcech a činech).

Podoba záznamů se pro správce a zpracovatele se v některých bodech liší, a to následovně:

- Správce i zpracovatel musí uvést jméno a kontaktní údaj správce, zpracovatele, pověřence pro ochranu osobních údajů, informace o případném předání údajů do třetí země či mezinárodní organizace a je-li to možné, tak uvést i obecný popis opatřeních (technických i organizačních).
- Správce navíc uvádí účely zpracování, popis kategorií SÚ a kategorií OÚ, kategorie příjemců OÚ a je-li to možné, plánované lhůty pro likvidaci jednotlivých kategorií OÚ.
- Zpracovatel oproti správce udává pouze kategorie zpracování prováděné pro každého ze správců.

Jak správce, tak zpracovatel, tyto záznamy vyhotovují písemnou formou a na požádání umožní dozorovému úřadu přístup k těmto záznamům.

## 5.2 Podmínky využití zpracovatele

Jak již bylo nastíněno v úvodu kapitoly, správce má možnost využít subjekt pro zpracování osobních údajů, který je označován jako zpracovatel. Správce ovšem může využít pouze takové zpracovatele, kteří poskytují dostatečné záruky vhodných technických a organizačních opatření za účelem splnění požadavků tohoto nařízení a zajištění ochrany práv subjektu údajů. Zpracovatel je umožněno zpracování osobních údajů pouze z pověření správce.

Zapojení dalšího zpracovatele je možné jen po předchozím písemném povolení správce, kdy minimální rozsah informování zahrnuje veškeré zamýšlené změny týkající se přijetí dalších zpracovatelů či jejich nahrazení, a poskytne tak správci příležitost se vůči takovým změnám ohradit.

Veškeré zpracování zpracovatelem se řídí smlouvou, či jiným právním aktem dle práva EU nebo členského státu, která zpracovatele vůči správci zavazuje a v nichž jsou stanoveny náležitosti zpracování jako: předmět, doba trvání zpracování, povaha a účel zpracování, kategorie subjektů údajů a osobních údajů, povinnosti a práva správce.

Zpracovatelská smlouva či jiný vhodný právní akt zejména stanovuje, že zpracovatel:

- Osobní údaje zpracovává pouze na základě doložených pokynů správce, a to i v případě otázek předání osobních údajů do třetí země či mezinárodní organizace, pokud toto zpracování nemá základ již v právu EU nebo členského státu.
- Zajišťuje, aby osoby, které zpracovávají osobní údaje, byly zavázány mlčenlivostí, případně aby se na ně vztahovala mlčenlivost zákonná.
- Přijme opatření pro zabezpečení zpracování dle nařízení (článek 32).
- V případě zapojení dalšího zpracovatele dodržuje související podmínky.
- Pokud je to možné, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření pro splnění povinnosti správce reagovat na žádosti související s právy subjektu údajů (Kapitola III nařízení).
- Společně se správcem zajišťuje soulad s povinnosti, které jim ukládá nařízení jako je Zabezpečení osobních údajů, Posouzení vlivu na ochranu osobních údajů a předchozí konzultace (čl. 32-36 nařízení).
- Při rozhodnutí správce všechny osobní údaje buď vymaže, nebo je vrátí správci pokud dojde k ukončení spolupráce nebo zpracování a vymaže existující, pokud to není v rozporu s právem EU nebo členského státu.
- Poskytne správci veškeré informace dokládající splnění povinností a přispěje a umožní audit, včetně inspekcí, prováděné správcem či jiným auditorem pověřeného správcem. Zpracovatel je povinen informovat správce pokud je určitý pokyn v rozporu s nařízením nebo jiným právním předpisem týkající se ochrany osobních údajů (OOÚ).

Konkrétní úpravu pro Českou republiku definuje Zákon č. 110/2019 viz kapitola *GDPR v podmínkách ČR*. V případě, kdy zpracovatel zapojí do určité činnosti zpracování dalšího zpracovatele, musí být i tento zpracovatel zavázán stejnými povinnostmi, zejména by se mělo jednat o poskytnutí dostatečných záruk zavedení vhodných technologických a organizačních opatření pro splnění tohoto nařízení, jaké jsou uvedeny ve smlouvě mezi správcem a původním zpracovatelem.

Pokud neplní uvedený další zpracovatel své povinnosti týkající se ochrany osobních údajů, odpovídá správci za plnění povinností dalšího zpracovatele i nadále původní, tedy prvotní zpracovatel.

Smlouvy nebo jiné právní akty, které definují povinnosti pro zpracovatele, mohou být zcela nebo částečně založené na standardních smluvních doložkách stanovených Komisí či dozorovým úřadem s využitím nástrojů, které nařízení umožňuje (čl. 63, 93). Také jedním z prvků, jimiž lze doložit dostatečné záruky, je skutečnost, že zpracovatel případně dodržuje schválený kodex chování dle článku 40.

## 5.3 Zabezpečení osobních údajů

Zpracování osobních údajů může přinášet rizika, kterými mohou být např. ztráta, zničení, pozměnění, zpřístupnění uložených či jiným způsobem zpracovaných osobních údajů, což může vést k újmě subjektu údajů, a to jak fyzické, hmotné, tak i nehmotné. Z toho důvodu by měl správce zachovávat bezpečnost zpracování i samotných osobních údajů. Při určování úrovně zabezpečení osobních údajů nařízení nahlíží na řadu různých aspektů, mezi které patří stav techniky, náklady na provedení, kategorii osobních údajů či subjektu údajů a možné dopady při porušení zabezpečení.

Dle potřebné úrovně zabezpečení správce i zpracovatel zavede relevantní technická i organizační opatření, jimiž může být:

a) pseudonymizace a šifrování OÚ,
b) schopnost zajistit důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,
c) schopnost obnovit dostupnost OÚ a přístup k nim včas v případě incidentů,
d) pravidelné testování, posuzování, hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Správce i zpracovatel jsou také povinni zajistit, že FO, kterým udělili přístup k osobním údajům, provádí veškeré zpracování pouze na základě jejich pokynu či práva EU nebo členského státu EU, jak je to definováno v Kapitole IV, Oddíl 2 [4].

**Ohlašování dozorovému úřadu**

Pokud přes všechny opatření dojde k jakémukoli porušení zabezpečení OÚ, má správce povinnost bez zbytečného odkladu do 72 hodin, od okamžiku, kdy se takovém porušení dozvěděl, pokud správce nemá oprávněné důvody pro zpoždění, jej ohlásit dozorovému úřadu. Ohlášení správce nemusí učinit pouze v případě, že není pravděpodobný vznik rizika pro práva a svobody fyzické osoby.

Toto ohlášení musí obsahovat minimálně:

a) Popis povahy daného porušení a pokud je to možné, tak včetně kategorií, přibližného počtu dotčených SÚ a záznamů OÚ.
b) Jméno a kontaktní údaje DPO nebo jiného kontaktního místa, které může poskytnout bližší informace.
c) Popis pravděpodobných důsledků.
d) Popis opatření, které správce přijal či přijme pro vyřešení daného porušení, včetně případných opatření ke zmírnění možných dopadů.

V případě, že správce není schopný tyto informace poskytnout současně, lze je poskytnout i postupně, ovšem bez další zbytečné prodlevy.

Další povinností správce vytvoření dokumentace, kde jsou uvedeny všechny případy porušení zabezpečení včetně všech skutečností, jeho účinků a přijatých nápravných opatření. Tato dokumentace pak slouží dozorovému úřadu, v prostředí České republiky ÚOOÚ, k ověření souladu s touto částí nařízení.

Pokud porušení zabezpečení zjistí zpracovatel, je povinen takovou skutečnost bez zbytečného odkladu ohlásit správci, který následovně učiní patřičné kroky.

**Oznamování subjektu údajů**

V případech, kdy je pravděpodobné, že určitý případ porušení zabezpečení OÚ bude mít za následek vysoké dopady na práva a svobody FO, je správce povinen oznámit toto porušení bez zbytečného odkladu také subjektu údajů. Toto oznámení musí obsahovat popis povahy porušení zabezpečení a při nejmenším informace a opatření viz výše v bodech b), c), c)d), které musí být formulováno jasnými a jednoduchými jazykovými prostředky pro snadné pochopení všech skutečností.

Správce ovšem toto oznámení subjektu údajů nemusí vykonat, pokud:

- Zavedl náležitá technická a organizační opatření u dotčených OÚ, zejména např. šifrováním.
- Přijal opatření, díky kterým se vysoké riziko pro práva a svobody SÚ značně snížilo.
- By oznámení vyžadovalo nepřiměřené úsilí. V tomto případě jsou subjekty údajů informováni veřejně či podobně účinným opatřením.

V případě, že správce subjekt údajů doposud neinformoval, může dozorový úřad rozhodnout o tom, jestli je či není vhodné v daném případě subjekt dodatečně informovat.

## 5.4 Pověřenec pro ochranu osobních údajů

Některým správcům a zpracovatelům vzniká Kapitolou IV, Oddíl 4 nařízení [4] povinnost jmenovat pověřence pro ochranu osobních údajů (DPO). Pověřenec je nařízením nově zavedená funkci, která má správci plnit úlohu pomocníka, konzultanta či koordinátora ochrany osobních údajů a zároveň zaštiťovat komunikaci s ÚOOÚ případně jinými dozorovými úřady a všeobecně se dá hovořit o jakési kontaktní místo pro záležitosti spojené s GDPR. Pověřenec má tedy za úkol především poskytování informací a poradenství správci či zpracovateli (včetně zaměstnanců, kteří se na zpracování podílejí) a monitorování souladu zpracování s GDPR a dalšími předpisy. Pokud správce provádí posouzení vlivu na OOÚ, pověřenec může poskytnout pro danou problematiku poradenství a může také vypracovávat záznamy o činnostech zpracování. Pověřenec může také plnit i ostatní úkoly, které mu organizace zadá, ale nikdy se nesmí při jejich plnění dostat do střetu zájmů s funkcí pověřence. To by nastalo především tehdy, pokud by určoval účel zpracování OÚ či při existenci zákona, který by pověřenci v určitých momentech znemožňoval jeho činnost (např. zvláštní mlčenlivost).

Správci, kterých se povinnost jmenovat DPO týká, musí sdělit veřejně i přímo dozorovému úřadu označení pověřence (jméno a příjmení) a jeho kontaktní údaje (telefonní číslo a e-mail). Vždy sdělení o těchto informacích činí správce či zpracovatel. Forma zveřejnění není blíže specifikovaná, nejvhodnější forma je prostřednictvím webových stránek či u některých subjektů prostřednictvím úřední desky.

Povinnost jmenování pověřenec pro ochranu osobních údajů vzniká správci a zpracovateli pokud:

a) Správcem či zpracovatelem je orgán veřejné moci či veřejný subjekt. To se ovšem netýká soudů jednajících v rámci svých soudních pravomocí.
b) Operace zpracování, které správce či zpracovatel provádí jako svou hlavní činnost, vyžadují rozsáhlé pravidelné a systematické monitorování subjektů, a to vzhledem k své povaze, rozsahu nebo účelům.
c) Hlavní činnosti správce či zpracovatele souvisí s rozsáhlým zpracováním zvláštních kategorií údajů a OÚ týkajících se rozsudku v trestních věcech a trestních činech.

Skupina podniků může jmenovat společného DPO, pokud je snadno dosažitelný z každého podniku, či naopak lze jmenovat více pověřenců v případě orgánu veřejné moci či veřejného subjektu s přihlédnutím k organizační struktuře a velikosti. Pověřenec by měl být přímo podřízený vrcholovým řídícím pracovníkům správce nebo zpracovatele. To ovšem neznamená, že pověřence musí řídit přímo vedení organizace, ale že pověřenec musí mít přímý přístup k vedení organizace, tzn. aby mezi DPO a vedením nebyl další mezičlánek.

Žádné požadavky na vzdělání či certifikaci pověřence údajů obecné nařízení nestanovuje, musí se ovšem jednat o osobu, která má dostatečnou odbornou znalost práva, prostředí profese správce, praxe v oblasti OOÚ a musí dostatečně ovládat toto obecné nařízení.

## 5.5 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na OOÚ lze chápat jako analýzu rizik a dopadů, která jednotlivá rizika definuje, přiděluje jim pravděpodobnost výskytu a dopadu (především na subjekt údajů) a dle těchto specifikacích jsou následně rizika rozřazena do jednotlivých kategorií na významná, středně významná a málo významná. Na základě tohoto zhodnocení jsou pak následně eliminována vhodným opatřením. [13] Povinnost provést takové posouzení, které je v originále nazýváno jako *Data Protection Impact Assessment* (DPIA), správci nařízení uděluje v Kapitole IV, Článek 35 [4]. Jedná se tedy o provedení posouzení vlivu zamýšlených operací zpracování na OOÚ před samotným zpracováním, a to především v případě, že je pravděpodobné, že určitý druh zpracování, zejména při použití nových technologií, bude mít za následek vysoké riziko pro práva a svobody FO. Pokud je to vhodné, stačí pro soubor podobných operací zpracování pouze jedno posouzení, ale vždy je vyžadován posudek DPO, v případě, že byl jmenován.

Povinnost správce zpracovat DPIA se týká případů, kdy dochází k:

- ohodnocování nebo bodování FO
- zpracování:
    - velkého rozsahu,
    - systematické a rozsáhlé založené na automatickém rozhodování, včetně profilování
    - zvláštních kategorií údajů,
    - údajů týkající se zranitelných subjektů údajů,
    - údajů týkající se rozsudků v trestních věcech a činech,
    - s obtížně uplatnitelnými právy subjektů údajů (veřejná oblast – procesu se nemohou vyhnout).
- systematické monitorování veřejně přístupných prostor.

U těch druhů operací zpracování, které podléhají požadavku na posouzení vlivu na OOÚ, dozorový úřad sestaví příslušný seznam, který může sestavit i pro druhy operací zpracování, u nichž DPIA nutné není.

Posouzení obsahuje v nejmenším rozsahu alespoň:

a) Systematický popis zamýšlených operací zpracování, účely zpracování, případně včetně zájmů správce.
b) Posouzení, zda jsou operace zpracování nezbytné a přiměřené, a to z hlediska účelů.
c) Posouzení rizik pro práva a svobody subjektu.
d) Plánovaná opatření k takových rizik, včetně záruk, mechanismů a bezpečnostních opatření k zajištění OOÚ a k doložení souladu s tímto nařízením.

V případech, kdy je to vhodné, lze získat stanovisko k plánovanému zpracování i od subjektu údajů či jejich zástupců. Existují také situace, kdy se postup vytvoření DPIA nevyužije, a to v případech, kdy již bylo vytvořeno dostačující obecné posouzení dopadů a zpracování má právní základ v právu EU nebo členského státu EU, které blíže specifikuje nařízení a je součástí kapitoly 8 této práce.

# 6 Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím

Předchozí kapitoly představení zásad zpracování, práv subjektů údajů, povinností správce a o zabezpečení osobních údajů. Tato kapitola v přiměřeném rozsahu nastiňuje pravidla pro předávání osobních údajů do třetích zemí nebo mezinárodním organizacím.

Volný pohyb osobních údajů v EU není v souvislosti s ochranou fyzické osoby a jejich zpracováním ani omezen, ani zakázán. Takové předávání není omezeno z důvodu tzv. institucionálního zabezpečení. Jedná se o to, že v zemích EU platí pro zpracování osobních údajů stejný vysoký standard ochrany a právní rámce, který tyto skutečnosti definuje a není tak potřeba dodatečně zajišťovat institucionální bezpečnost. V kontextu GDPR je nutné jako na součást EU pohlížet i na Island, Norsko a Lichtenštejnsko, kde je nařízení také účinné.

I k takovému předání ovšem musí mít správce či zpracovatel relevantní právní důvod.

Pokud chce správce předat jinému správci OÚ do země, které jsou mimo EU, musí být zajištěna jejich institucionální ochrana. Až na výjimky tedy nelze předávat osobní údaje do zemí, kde není zajištěna dostatečná právní ochrana. Možnosti předávání do třetích zemí jsou tedy následující:

**a) Předání založené na rozhodnutí o odpovídající ochraně.**

- Evropská komise, také označována jako Komise, rozhodne, které konkrétní země zajišťují odpovídající úroveň ochrany osobních údajů, a kdy se tedy nevyžaduje zvláštní povolení a předání nejsou kladeny administrativní překážky.
- Mezi tyto země patří např. Švýcarsko, Kanada, Argentina, Nový Zéland, Izrael, atd.

**b) Předání založené na vhodných zárukách.**

- Pokud neexistuje rozhodnutí Komise o odpovídající úrovni OOÚ v dané zemi, mohou být údaje do takové země předány pouze pokud přijímací správce poskytl vhodné záruky a jsou k dispozici vymahatelná práva subjektů údajů. Mezi vhodné záruky patří:

- **Závazná podniková pravidla**
    - Jedná se o koncepci ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel v jedné nebo více třetích zemí v rámci skupiny podniků. Jde tak o pravidla, která platí uvnitř správců, kteří tvoří skupinu podniků nebo uskupení podniků vykonávající společnou hospodářskou činnost.
- **Standardní smluvní doložky**
    - Na jejich základě lze předávat osobní údaje do třetích zemí. Jedná se o standardizovaný text, kterým se příjemce OÚ zavazuje dodržovat pravidla odpovídajícím pravidlům platící v EU.

**c) Výjimky pro specifické situace, které nezapadají pod předchozí dva body.**

- Předání OÚ do třetí země nebo mezinárodní organizaci je možné ve výjimečných situacích i v případě, že:
    - Subjekt byl informován o možných rizicích, která pro něj vyplývají a k předání dá svůj výslovný souhlas.
    - Předání je nezbytné pro smluvní plnění mezi subjektem a správcem, či pro splnění smlouvy uzavřené v zájmu subjektu mezi správcem a jinou FO či PO.
    - Předání je nezbytné z důležitých důvodů veřejného zájmu nebo pro určení, výkon nebo obhajobu právních nároků, k ochraně životně důležitých zájmů.
- Příkladem časté praxe může být situace, kdy cestovní kancelář předává osobní údaje hotelům do třetích zemí.

# 7 Nezávislé dozorové úřady

Předchozí část práce představila pravidla, okolnosti, práva a povinnosti související se zpracováním osobních údajů. Tato část se věnuje neméně podstatné části, a to monitorování toho, jestli je nařízení řádně plněno a dále se zabývá jednotlivými postupy v případě jeho porušení.

Nařízení GDPR uvádí v Kapitole VI [4], že každý členský stát je povinen stanovit jeden či více nezávislých orgánů veřejné moci, které jsou pověřeny kontrolou uplatňování tohoto nařízení s cílem chránit základní lidská práva a svobody FO v souvislosti se zpracováním osobních údajů a usnadnění volného pohybu osobních údajů uvnitř EU. Každý dozorový úřad přispívá k uplatňování GDPR tak, aby bylo jednotné v celé EU, a to především spoluprací mezi jednotlivými orgány a státy. Pro Českou republiku je stanoven dozorovým úřadem Úřad pro ochranu osobních údajů, který má následující povinnosti:

- Monitoruje a vymáhá uplatňování nařízení.
- Zabývá se stížnostmi podané subjektem údajů či jeho zástupci, což spočívá v prošetření jejich předmětu a v přiměřené lhůtě informuje daný subjekt o vývoji a výsledku šetření.
- Provádí šetření o uplatňování a souladu s nařízením, a to mimo jiné i na základě informací obdržených od jiného dozorového orgánu nebo jiného orgánu veřejné moci.

Podobu a konkrétní činnosti Úřadu pro ochranu osobních údajů, v práci označován také jako Úřad, pak blíže specifikuje česká legislativa. Sídlo Úřadu je umístěno v Praze a jeho činnost je hrazena ze samostatné kapitoly státního rozpočtu České republiky. Do činnosti Úřadu lze zasahovat pouze na základě zákona a Úřad při výkonu své působnosti postupuje zásadně nezávisle a řídí se pouze právními předpisy.

Mezi činnosti Úřadu patří např., že sdělením upozorňuje správce nebo zpracovatele, pokud má podezření na porušení povinností v souvislosti se zpracováním, provádí dozor nad dodržování povinností stanovených zákonem, ověřuje zákonnost zpracování OÚ, projednává přestupky a ukládá pokuty, poskytuje konzultaci v oblasti ochrany osobních údajích, informuje veřejnost o rizicích, pravidel a právech v souvislosti se zpracováním. [14]

## 7.1 Sankce a pokuty

V případě, že dojde k porušení povinností, které nařízení ukládá, umožňuje uložit organizaci nebo instituci správní pokuty, které jsou stanoveny v Kapitole VIII, Článek 84 [4]. Správní pokutou se rozumí finanční trest, který, pokud to legislativa členského státu EU umožňuje, může uložit přímo dozorový úřad, a to z důvodu harmonizace a posílení nařízení a jeho vymáhání napříč státy. Oproti tomu sankce je obecné označení pro trest, který může mít mimo finanční postih i formu nějakého omezení, jimž může být zákaz činnosti či odebrání zisků získaných na základě porušení tohoto nařízení a dále mohou být např. vyústěním soudního sporu. Přesto, že nařízení umožňuje několik možností trestu, připomíná podmínku toho, kdy o jednom činu nemůže být rozhodováno dvakrát[5].

Správní pokuty se pak ukládají podle okolností jednotlivého případu a při rozhodování o uložení a výši se zohledňují tyto:

a) povaha, závažnost, délka trvání porušení, rozsah či účel dotčeného zpracování, počet dotčených subjektů,
b) úmysl či nedbalost,
c) kroky, které správce či zpracovatel podniknul ke zmírnění škod,
d) míra odpovědnosti vzhledem k technickým a organizačním opatřením,
e) předchozí porušení,
f) míra spolupráce s dozorovým úřadem,
g) kategorie osobních údajů,
h) způsob, jakým se úřad dozvěděl o porušení (zejména, zda správce či zpracovatel porušení oznámil),
i) dodržování schválených kodexů chování,
j) jakákoli jiná přitěžující nebo polehčující okolnost.

[5] Právní princip *Ne bis in idem* - ne dvakrát o tomtéž“

Výše správních pokut je rozdělena do dvou skupin, a to následovně:

a) 10 000 000 EUR nebo 2 % celkového ročního celosvětového obratu za předchozí finanční rok, v případě, že se jedná o podnik, podle toho, která částka je vyšší. Tuto výši lze uplatnit v případě porušení povinností v souvislosti s:
    - podmínkami na souhlas dítěte,
    - zpracování, které nevyžaduje identifikaci,
    - povinnostmi správce (Jedná se o obecné povinnosti, zabezpečení osobních údajů, DPIA, DPO, osvědčení o ochraně osobních údajů[6].).
b) 20 000 000 EUR nebo 4 % celkového ročního celosvětového obratu za předchozí finanční rok, v případě, že se jedná o podnik, podle toho, která částka je vyšší. Tato sankce lze uplatnit v případě porušení povinností v souvislosti s:
    - zásadami zpracování osobních údajů, zákonností zpracování, vyjádřením souhlasu,
    - zpracováním zvláštních kategorií osobních údajů,
    - právy subjektu
        - transparentnost, informace a přístup k osobním údajům, oprava a výmaz, právo vznést námitku v souvislosti s automatizovaném rozhodování,
    - předáváním osobních údajů do třetích zemí nebo mezinárodním organizacím,
    - ustanovením týkajících se zvláštních situací, při nichž dochází ke zpracování (v nařízení Kapitola IX, která není součástí této práce),
    - nesplněním příkazu dozorového úřadu a neumožnění kontroly.

Částky z uložených správních pokut putují do státního rozpočtu a nejedná se tak o náhradu újmy pro poškozené subjekty. Problematika náhrady újmy bude řešena v další podkapitole.

[6] Jedná se o osvědčení, které vydává akreditovaný subjekt (v ČR je jím ÚOOÚ), kterým lze dokládat soulad s nařízením a jeho získání je zcela dobrovolným rozhodnutím správce, stejně jako kodexy chování.

Každý členský stát má možnost stanovit, zda a do jaké míry je možné ukládat správní pokuty orgánům veřejné moci a veřejným subjektům na území daného státu. Tyto pravidla nesmí být v rozporu s nařízením, v této práci je jejich úprava součástí kapitoly GDPR v podmínkách ČR. Nařízení také umožňuje členským státům EU stanovit i jiné sankce, které lze uložit za porušení tohoto nařízení, a to zejména pro taková porušení, na která se nevztahují správní pokuty, viz výše.

Při uplatňování pravomocí související s výběrem vhodných nástrojů pro vyřešení neplnění povinností ze strany správce či zpracovatele musí dozorové úřady dodržovat následující zásady:

1. Uložení rovnocenných sankcí:
   - Nařízení vyžaduje soulad při ukládání sankcí napříč členskými státy EU kvůli zajištění jednotného uplatňování a prosazování GDPR, stejný princip platí i při ukládání opatření v podobě pokut.
2. Účinné, přiměřené a odrazující pokuty:
   - Pokyny zohledňují vnitrostátní právní předpisy, které mohou stanovovat doplňující požadavky na vymáhání, což nesmí být v rozporu s účinností, přiměřeností a odrazujícího vlivu sankcí.
3. Individuální posuzování:
   - Dozorový úřad členského státu EU zohlední všechny dané okolnosti, jako je závažnost, povaha a důsledky porušení, dle nařízení.
4. Aktivní účast dozorových úřadů členských států EU:
   - Pro soulad vymáhání napříč EU je nutné, aby dozorové úřady spolupracovaly, jelikož bude možné se odvolat k vnitrostátním soudům daného členského státu EU.

### 7.1.1 Právo na náhradu újmy

Již v předchozích částech práce bylo nastíněno, že hlavním důvodem pro ochranu osobních údajů je ochrana osobnosti a soukromí. Osobní údaje mohou mít velice citlivou povahu či mohou být zneužity třetí stranou a subjekt údajů tak může utrpět značnou újmu, a to jak hmotnou, tak nehmotnou. Nařízení GDPR tedy dává právo na obdržení náhrady takové újmy, která je způsobena zpracováním porušující toto nařízení. Tuto náhradu pak vyplácí správce anebo zpracovatel.

Pokud správce poruší toto nařízení, je zodpovědný za újmu způsobenou protiprávním zpracováním, a to v každém případě. Zpracovatel oproti tomu, je odpovědný za újmu pouze v případě, že nesplnil povinnosti stanovené konkrétně pro zpracovatele nebo pokud jednal nad rámec zákonných pokynů správce či dokonce v rozporu s nimi. Jak správce, tak zpracovatel má možnost prokázat, že za událost, která vedla ke vzniku újmy, nenesou žádným způsobem odpovědnost. Pokud toto prokážou, jsou odpovědnosti zproštěni.

Soudní řízení za účelem výkonu práva na náhradu újmy jsou v kompetenci soudů příslušných podle práva členského státu EU.

# 8 Zvláštní situace při zpracování

Problematika ochrany osobních údajů a jejich zpracování má své opodstatnění v právní úpravě, nicméně může velmi snadno přicházet do kolize s jinými právy a oprávněnými zájmy veřejnosti či ostatních fyzických osob. Nařízení počítá i s takovými situacemi a ustanovuje zvláštní situace, kdy je potřeba podmínky zpracování blíže specifikovat či upravit. Členské státy tak mají možnost v těchto případech upravit specifikace zpracování v dané oblasti, to jak a do jaké míry tuto možnost využila Česká republika, je uvedeno v kapitole *GDPR v podmínkách ČR*.

O těchto zvláštních situacích pojednává Kapitola IX nařízení, a týká se zpracování v souvislosti se svobodou projevu a informací, přístupnosti úředních dokumentů, národních identifikátorů, dále zpracování, které souvisí se zaměstnáním, pro potřeby archivace a vědecké, historické či statistické účely, problematiku mlčenlivosti a církve či náboženských sdružení.

**Svoboda projevu a informací**

Nařízení ukládá členským státům EU uvést jeho znění do souladu i s právem na svobodu projevu a informací. Umožňuje stanovit výjimky a odchylky pro účely spojené s novinářskou, akademickou, uměleckou či literární činností, které se týkají zásad zpracování, práv subjektů údajů, povinností správců a zpracovatelů, a také některých ostatních kapitol, v případech, kdy je to nutné pro zavedení souladu mezi těmito dvěma právy.

**Přístup k úředním dokumentům**

Tato část nařízení umožňuje zpřístupnění osobních údajů ve veřejných dokumentech za účelem plnění úkolu ve veřejném zájmu, a to bez ohledu na držitele těchto dokumentů. Jedná se o způsob zajištění souladu mezi přístupem k úředním dokumentům dle práva EU či členského státu EU a tohoto nařízení.

**Národní identifikátory**

Členské státy EU si mohou dále upravit specifika zpracování národních identifikátorů, jako jsou identifikační čísla, např. rodné číslo, za podmínky vhodných záruk práv a svobod daného subjektu dle tohoto nařízení.

**Zaměstnání**

Vztah zaměstnavatele a zaměstnance může být problémovou oblastí v souvislosti s ochranou osobních údajů, a to především kvůli značné nerovnováze tohoto vztahu. Z tohoto důvodu nařízení umožňuje členským státům EU stanovit konkrétnější pravidla pro. zpracování osobních údajů zaměstnanců, a to ve všech fázích zaměstnání[7], pro zajištění rovnosti či například ochrany majetku.

**Vědecké, historické, statistické účely a archivace**

Za podmínky dostatečných technických a organizačních opatření, což ve vhodných případech může mít např, pseudonymizace, dodržení zásady minimalizování údajů, nařízení umožňuje členským státům EU a právu EU, deklarovat odchylky od některých práv subjektů údajů. Jedná se o právo na přístup k OÚ, opravu, omezení zpracování, přenositelnost údajů a vznést námitku. Nutno dodat, že pokud jsou osobní údaje zpracovávány i pro jiné účely, které nespadají do této kategorie, takové odchylky se jiných účelů týkat nebudou.

**Mlčenlivost**

V případě, kdy správce či zpracovatel získal nebo obdržel osobní údaje podléhající mlčenlivosti, umožňuje nařízení členským státům přijmout taková pravidla, která omezují pravidla pro přístup k takovým osobním údajům dozorovým orgánem.

**Ochrana údajů uplatňována církvemi a náboženskými sdruženími**

Pokud církve nebo náboženské sdružení mají platná a komplexní pravidla týkající se OOÚ, můžou je nadále využívat za předpokladu souladu s nařízením. Na toto dohlíží dozorový orgán.

[7] nábor, plnění pracovní smlouvy, řízení, organizace práce

# 9 GDPR v podmínkách ČR

V předcházejících částech práce byla představena ochrana osobních údajů a důležité aspekty současné legislativy spojené s touto problematikou. Tato část práce navazuje na konkrétní adaptaci pro podmínky České republiky.

V květnu 2018 nabylo nařízení GDPR účinnosti automaticky v plném rozsahu a členské státy EU dostaly možnost některé jeho části zpřesnit či upravit s ohledem na specifické domácí podmínky. Tato možnost se týkala částí nebo celých článků 6, 8, 9, 23, 83-91.

Vysvětlení k jednotlivým článkům se v této práci nachází pro články 6, 8, 9 v kapitole *Obecné zásady zpracování*, pro článek 83, 84 je podstatné vysvětleno v kapitole *Sankce a pokuty*, článkům 85-91 je věnována kapitola *Zvláštní situace při zpracování*. Problematika článku 23 nebyla do práce zakomponována z důvodu úzce specifické problematiky, která není předmětem zaměření této práce. Pro úplnost zde bude krátce představena.

I. **Článek 6 - Zákonnost zpracování odst. 1 písm. c) a e):**
   - Členské státy EU mohou zachovat nebo zavést konkrétnější ustanovení pro přizpůsobení používání pravidel ohledně zpracování tím, že určí konkrétní požadavky na zpracování a jiná opatření. Jedná se o zpracování na základě plnění právní povinnosti správce a zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je správce pověřen.
   - Základ pro zpracování pro tyto případy musí být ustanoven právem EU nebo právem členského státu EU.

II. **Článek 8 - Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti odst. 1:**
   - Členské státy mohou snížit dolní hranici věku, kdy zpracování osobních údajů dítěte je zákonné v případě, že je služba informační společnosti nabídnuta přímo dítěti. Nařízení stanovuje dolní hranici věku dítěte 16 let a dovoluje členským státům EU snížit dolní hranici věku dítěte až na 13 let.

III. **Článek 9 - Zpracování zvláštních kategorií osobních údajů odst. 2 písm. a:**

- Právo členského státu může stanovit případy, kdy i přes výslovný souhlas se zpracováním zvláštních kategorií OÚ subjektu údajů je zpracování takových údajů zakázáno.
- Členské státy mohou zavést další podmínky, a to včetně omezení, ke zpracování genetických anebo biometrických údajů či údajů o zdravotním stavu.

IV. **Článek 23 - Omezení:**

- Právo členského státu může prostřednictvím legislativního opatření omezit rozsah povinností a práv uvedených v článcích 12 až 22[8].
- Jedná se o omezení, které respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření s cílem zajistit národní bezpečnost, obranu, veřejnou bezpečnost, všechny procesy související s trestnými činy či výkonem trestů, ochranu nezávislosti soudnictví, činnosti související s výkonem moci, ochranu subjektu údajů apod.

V. **Článek 83 - Obecné podmínky pro ukládání správních pokut:**

- Každý členský stát má možnost si stanovit pravidla, která se týkají toho, zda a do jaké míry je možné ukládat správní pokuty orgánům veřejné moci a veřejným subjektům na území daného státu. Tyto pravidla nesmí být v rozporu s nařízením[9].
- Na výkon pravomocí dozorového úřadu se vztahují vhodné procesní záruky v souladu s právem členského státu například účinná soudní ochrana, spravedlivý proces, apod.

VI. **Článek 84 – Sankce**

- Pro jiné sankce, které nejsou specifikované v Článku 83 nařízení, členské státy EU stanoví pravidla za porušení tohoto nařízení. Tyto sankce musí být účinné, odrazující a přiměřené. Každý členský stát oznámí do data účinnosti nařízení tyto právní předpisy a bez zbytečného odkladu oznámí jakékoli následné změny.

---

[8] V nařízení se jedná o Kapitolu III – Práva subjektu údajů.

[9] V nařízení toto souvisí s článkem 58 – Pravomoci – Nezávislé dozorové úřady

**VII. Kapitola IX - Ustanovení týkající se zvláštních situací, při nichž dochází ke zpracování**

- Tato část nařízení umožňuje členským státům některé otázky a oblasti zpracování osobních údajů uvést prostřednictvím právních předpisů do souladu s právními úpravami, které mohou být pro daný stát specifické. Jedná se o zpracování v souvislosti s např. svobodou projevu a informací, především zpracování pro novinářské účely, dále přístup veřejnosti k úředním dokumentům, povinnost mlčenlivosti, problematika církví a náboženských sdružení, účely vědeckého či historického významu, či zpracování v souvislosti se zaměstnáním.

## 9.1 Zákon o zpracování osobních údajů

Adaptací do prostředí ČR se s účinností 24.4.2019 stal Zákon č. 110/2019 Sb., o zpracování osobních údajů a Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Tento nově přijatý zákon navazuje na nařízení GDPR a v příslušných částech upravuje práva a povinnosti pro české podmínky.

Nově přijatý zákon o zpracování osobních údajů upravuje zpracování osobních údajů dle nařízení GDPR, zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činech [10], zpracování osobních údajů při zajišťování obranných a bezpečnostních zájmů ČR [11], postavení a pravomoc ÚOOÚ [12]. Dále také upravuje způsobilost dítěte pro souhlas se zpracováním osobních údajů[13], zpracování osobních údajů prováděné pro účely akademického, literárního nebo uměleckého projevu či novinářské účely.

[10] Článek 10 nařízení.

[11] Článek 23 nařízení.

[12] Kapitola VI nařízení.

[13] Článek 8 nařízení.

Česká republika využila možnost adaptace nařízení ve stanovení věkové hranice pro udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti na 15 let věku dítěte.

Jednou ze změn vůči nařízení je také úprava minimálního rozsahu posouzení vlivu na ochranu osobních údajů. V českých podmínkách bude dostačující pouze obecný popis zamýšleného zpracování, posouzení rizika související s neoprávněným zásahem do práv a svobod SÚ a plánované opatření k redukci takového rizika. Toto posouzení správce nemusí provádět, pokud mu dané zpracování ukládá právní předpis.

Dále zákon stanovuje výjimky z povinnosti posuzování slučitelnosti účelů[14] a vlivu na OOÚ, informační a poučovací povinnost, specifická úprava zpracování OÚ, povinnost oznámení porušení zabezpečení OÚ subjektu údajů, a to pro vědecké, statistické, umělecké či novinářské účely. Pro tyto účely je tedy zpracování také umožněno a zákon hovoří o přiměřeném způsobu s přihlédnutím k tomu, zda se zpracovávají osobní údaje uvedené v čl. 9 odst. 1 nebo čl. 10 nařízení.

Aktuální zákon výrazně snižuje pokuty, které je možno udělit za porušení zákazu zveřejnění OÚ stanovený jiným právním předpisem. ÚOOÚ může udělit:

- FO, PO či podnikající FO sankci s horní hranicí 1 000 000 Kč. Pokud jde o přestupek spáchaný tiskem, filmem, televizí či obdobně účinným způsobem pak může ÚOOÚ udělit až 5 000 000 Kč.
- Obci finanční postih s horní hranicí 5 000 Kč, přičemž se nesmí jednat o obci s:
    - přenesenou působnost či dobrovolný svazek obcí,
    - příspěvkovou organizaci,
    - právnickou osobou vykonávající činnost zřizovanou obcí.
    - Pokud jde o přestupek spáchaný tiskem, filmem, televizí či obdobně účinným způsobem, pak může být udělena pokuta ve výši až 15 000 Kč.

[14] Povinnost posouzení slučitelnosti účelů má správce v případě, kdy provádí zpracování pro jiný účel, než pro který byly OÚ původně shromážděny. Správce pak musí zohlednit, jestli je zpracování pro jiný účel slučitelné s původním účelem či účely. Jedná se o posouzení všech vazeb mezi účely původními a zamýšlenými, o vztah správce a subjektu údajů z pohledu okolností shromáždění údajů, povahu osobních údajů, možné důsledky dalšího zamýšleného zpracování a existenci vhodných záruk.

Zákon také nabízí možnost uložení opatření k odstranění nedostatků se stanovením přiměřené lhůty a s možností upustit od správního trestu, pokuty.

Poslední částí nového adaptačního zákona o zpracování osobních údajů [5] je zrušení zákona č. 101/2000 Sb., o ochraně osobních údajů spolu s vybranými ustanoveními některých dalších zákonů týkající se zpracování a ochrany OÚ ve specifických situacích. V současné době je tedy hlavní právní úpravou o zpracování a ochraně osobních údajů nařízení GDPR a nově přijatý zákon o zpracování osobních údajů.

**Pokyny Evropského sboru a Úřadu**

Pro lepší uchopitelnost právní úpravy a s ní spojených pojmů, vydává Evropský sbor pro ochranu osobních údajů[15] pokyny, které mají co nejblíže představit jednotlivé části obecného nařízení a poskytnout upřesnění některých pojmů či povinností. Pro prostředí České republiky jsou k dispozici na webových stránkách Úřadu pro ochranu osobních údajů, který ve vhodných případech vydává také vlastní dokumenty pro specifikaci některých povinností a termínů pro domácí podmínky. Veřejnosti jsou tak k dispozici pokyny týkající se podrobností k povinnosti DPIA, pověřence pro ochranu osobních údajů, správních pokut, podobě souhlasu apod. Je tak konkrétně definováno, co znamená systematické a pravidelné zpracování, zpracování velkého rozsahu, které zpracování představuje vysoké riziko pro práva a svobody fyzických osob, a další termíny a specifikace. [13]

Například co se týče povinnosti DPIA, pro ČR byl Úřadem pro ochranu osobních údajů stanoven demonstrativní seznam osmi takových operací. Patří mezi ně např. zpracování v rámci plnění zákonných povinností vyplývající z vedení účetnictví, agenda související se zaměstnanci (mzdová, personální, sociální a zdravotní pojištění), týkající se obchodní činností, kterým jsou i věrnostní karty, zasílání newsletterů pokud jsou zpracovány pouze nezbytné osobní údaje, které nespadají do kategorie zvláštních. Celý seznam je dostupný na stránkách Úřadu pro ochranu osobních údajů [13].

[15] Dříve Pracovní skupina WP29

# 10 Shrnutí teoretické části

První kapitola teoretické části výčtově definuje často používané pojmy a označení v této práci. Jejím účelem je seznámení čtenáře s dále se vyskytujícími charakteristickými odbornými výrazy pro řešenou problematiku.

Cílem kapitoly *Úvod do nařízení o ochraně osobních údajů* bylo uvedení čtenáře do problematiky ochrany osobních údajů a její významnosti s návazností na ochranu osobnosti a soukromí. Taktéž byly nastíněny hlavní změny, které přináší nařízení GDPR. Tyto změny byly také dány do základního kontextu vůči Zákonu 101/2000 Sb., na ochranu osobních údajů platném v ČR. Pro lepší orientaci čtenáře v následujících kapitolách byla zmíněna struktura nařízení včetně výčtu podstatných a řešených článků v této práci. Tyto články spadají buď přímo do jednotlivých kapitol, případně do oddílů přidružených k rozsáhlejším kapitolám.

Kapitola *Obecné zásady zpracování* popisuje obecné zásady zpracování, tedy zákonnost, korektnost a transparentnost, účelové omezení, minimalizace údajů, přesnost, omezení uložení, integritu a důvěrnost a poslední zásadu, a to odpovědnost. Jednotlivé zásady jsou doplněny příklady dobré a špatné praxe v podmínkách ČR, které jsou graficky zvýrazněny a přibližují čtenáři jednotlivé zásady pro jejich lepší pochopení.

Následující kapitola *Subjekty údajů a jejich práva* uvádí základní práva a povinnosti k subjektům údajů. Zabývá se jednotlivými právy subjektu údajů na přístup k osobním údajům, na opravu či doplnění, na výmaz, na omezení zpracování, na přenositelnost údajů, vznést námitku a nebýt předmětem automatizovaného individuálního rozhodovaní.

Kapitola *Problematika správce a zpracovatele* definuje obecné povinnosti správce včetně kodexů chování, standardní a záměrné ochrany osobních údajů, jakým způsobem je správné provádět záznamy o činnostech zpracování. Dále se tato kapitola zaměřovala na podmínky využití zpracovatele, zabezpečení osobních údajů včetně povinnosti hlášení dozorovému úřadu v případě porušení zabezpečení osobních údajů. Součástí této kapitoly je i podkapitola věnující se pověřenci pro ochranu osobních údajů a v závěru posouzení vlivu na ochranu osobních údajů.

Stručná kapitola *Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím* popisuje způsoby a možnosti při předávání osobních údajů do třetích zemí.

Jelikož je nutné provádět dozor nad plněním povinností plynoucích z nařízení o ochraně osobních údajů je začleněna do práce kapitola *Nezávislé dozorové úřady*. Tato kapitola popisuje, jakým způsobem je monitoring prováděn a v případě nedodržení GDPR, jak jsou stanoveny obecné sankce a pokuty z porušení nařízení plynoucí. Další či upravené hranice sankcí platné v ČR jsou součástí kapitoly *GDPR v podmínkách ČR*.

Kapitola *Zvláštní situace při zpracování* je stručně popsána, jelikož její řešení nesouvisí přímo s hlavními cíli práce. Věnuje se takovým situacím jako je svoboda projevu a informací, přístupům k úředním dokumentům, národním identifikátorům, problematika zaměstnavatele a zaměstnance nebo oblastím zpracování při činnostech vědeckých, historických, statistických či archivace. Zmiňuje i oblast osobních údajů podléhající mlčenlivosti.

Závěrečná kapitola teoretické části *GDPR v podmínkách ČR* popisuje konkrétní adaptaci pro podmínky České republiky, shrnuje články nařízení, které si mohly členské státy EU upravit. Popisuje nově přijatý zákon 110/2019 Sb., o zpracování osobních údajů a Zákon č. 111/2019 Sb., kterým dochází ke změně několika zákonů v prostředí ČR.

# 11 Srovnání zákona 101/2000 Sb. a GDPR

Obecným právním předpisem ochrany osobních údajů je zákon č. 101/2000 Sb., o ochraně osobních údajů (účinné znění), v dalších částech práce označován jako Zákon 101, který je datován ke dni 4. dubna 2000 s účinností 1. června 2000, který byl rozšířen od 25. května 2018 Obecným nařízením EU o ochraně osobních údajů. S nástupem nového adaptačního zákona s účinností od 24.4.2019 byl nakonec Zákon č. 101/2000 Sb. zrušen.

Před účinností obecného nařízení byl tedy zákonem, který upravoval záležitosti ochrany osobních údajů pro Českou republiku. Zákon 101 je v souladu s právem Evropských společenství, s mezinárodními smlouvami, ke kterým je ČR vázána, upravuje práva a povinnosti při zpracování osobních údajů a také stanovuje podmínky, za nichž je možné předávat osobní údaje do jiných států.

V následujících kapitolách bude zákon 101/2000 Sb., [15], představen formou porovnání s GDPR. Tato komparace zákona není komplexní, jedná se o porovnání relevantní pro potřeby této práce.

## 11.1 Působnost

**101/2000 Sb.,**

Jelikož v případě Zákona 101 se jedná o českou legislativu, tento zákon tak upravuje zpracování údajů **pouze na území České republiky**. Vztahuje se jak na zpracování státními orgány, orgány územní samosprávy, jiné orgány veřejné moci, tak i FO a PO.

Zákon 101 se ovšem nevztahuje na zpracování prováděné fyzickou osobou výlučně pro osobní potřebu, ani na nahodilé shromažďování OÚ, pokud nejsou dále zpracovány.

**GDPR**

Místní působnost nařízení sahá **i za hranice EU**. I přes to, že správce nebo zpracovatel **není umístěn v EU**, pokud zpracovává osobní údaje subjektu údajů, které se nacházejí v EU, nařízení se na ně vztahuje, a to, pokud zpracování souvisí s nabídkou služeb nebo zboží takovým subjektům, nebo monitorují jejich chování v rámci EU.

Z tohoto nařízení jsou vyňaty situace, kdy zpracování osobních údajů je prováděné například při výkonu činností nespadajících do oblasti působnosti práva EU, FO pro výlučně osobní či domácí zpracování, nebo příslušnými orgány státní správy za účelem prevence, vyšetřování apod. trestných činů nebo výkonu trestů. Z působnosti GDPR jsou také **vyloučeny údaje, které jsou pouze v anonymní podobě a údaje o zemřelých**.

## 11.2 Zásady

**101/2000 Sb.,**

Oproti GDPR v zákoně **nejsou** zásady zpracování ani ochrany osobních údajů **jasně zpracovány**. Ovšem zákon je koncipován tak, aby ochrana osobních údajů byla vymahatelná a zpracování osobních údajů bylo transparentní vůči subjektu údajů, také je zde specifikována odpovědnost správce za zpracování OÚ.

**GDPR**

Zásada vymahatelnosti je v nařízení **posílena**, předpokládá se s přístupem založeným na riziku a nezávislému dozorovému orgánu jsou přiděleny **nové povinnosti a úkoly**, dozor je také **sjednocený**. Zásada transparentnosti je doplněna o **podrobnější úpravu** a bližší **specifikaci práv a povinností**. Také zásada odpovědnosti správce je zde **výslovně a komplexně upravena**. [16]

## 11.3 Práva a povinnosti

**101/2000 Sb.,**

Zákon 101 umožňuje správci zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Výjimkami je zpracování nezbytné pro dodržení právní povinnosti správce, pro plnění smlouvy, kde je subjekt údajů smluvní stranou, pro zpracování nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo pro ochranu práv jeho či jiné dotčené osoby, nebo se jedná o OÚ zveřejněné v souladu se zvláštním předpisem, zpracování je dále povoleno pro účely archivnictví. Zákon 101 také umožňuje správci zpracovávat osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které souvisí s jeho činností nebo funkčním nebo pracovním zařazením.

Pokud zpracování osobních údajů probíhá za účelem nabízení obchodu nebo služeb subjektu údajů (SÚ), může správce nebo zpracovatel použít pro tento účel jméno, příjmení a adresu subjektu údajů, pokud byly údaje získány z veřejného seznamu nebo v souvislosti se svojí činností. Správce ani zpracovatel ovšem nemůže dále tyto údaje zpracovávat, pokud s tím SÚ vyjádřil nesouhlas. Správce může tyto údaje předat jiném správci, pokud se jedná o zveřejněné osobní údaje, tyto údaje budou využívány pouze k nabízení obchodu a služeb či pokud byl o předání subjekt předem informován a nevyslovil nesouhlas. **Nesouhlas se zpracováním je nutné vyjádřit písemně**. Další údaje nelze k údajům přiřazovat bez získání souhlasu subjektu údajů.

Při udělené souhlasu musí být SÚ informován o účelu zpracování, k jakým osobním údajům souhlas dává, jakému správci a na jaké období. Správce musí být schopný po celou dobu zpracování schopný souhlas prokázat.

Právo na výmaz v jisté podobě bylo i součástí tohoto zákona, ovšem nikoliv tak širokém pojetí, jelikož se vymazání týkalo **pouze správce, kterého subjekt kontaktoval**.

**GDPR**

Nařízení rozlišuje dva způsoby, jak získat oprávnění ke zpracování osobních údajů, a to buď na základě práva EU anebo členského státu (např. pro splnění právní povinnosti správce, splnění úkolu prováděného ve veřejném zájmu) či na základě souhlasu subjektu osobních údajů.

Pokud je to možné, zpracování OÚ by mělo být vždy na základě práva, **souhlas by měl být posledním způsobem získání oprávnění ke zpracování**. GDPR specifikuje okolnosti souhlasu, který musí být **jasně rozeznatelný od ostatních skutečností**, **srozumitelný a snadno přístupný**. Odvolání souhlasu musí být **stejně jednoduché jako jeho poskytnutí.**

Nově zavedené právo „být zapomenut“ ukládá správci, kterého subjekt informuje o exekuci tohoto práva, povinnost **informovat všechny ostatní zpracovatele a správce, kterým údaje předal**. Přehled komparace povinností a práv je naznačen v následující tabulce.

| | 101/2000 Sb., | § | GDPR | čl. |
|---|---|---|---|---|
| **Oznamovací povinnost** | Povinnost registrace na ÚOOÚ[16] | 16 - 19 | ZRUŠENO<br>Povinnost vést záznamy o zpracování | 30 |
| **Likvidace OÚ** | Povinnost likvidace údajů v případě pominutí účelu zpracování nebo na základě žádost FO – pouze u žádaného správce | 20 | Právo být zapomenut – informování i ostatních správců a zpracovatelů | 17 |
| **Chybné/nepřesné údaje** | Při oprávněné žádosti FO správce nebo zpracovatel neprodleně odstraní závadu | 21 | Právo na opravu | 16 |
| **Přenesení OÚ** | --- | | Právo na přenositelnost | 20 |
| **Posuzování vlivu na OOÚ** | --- | | Povinnost posouzení vlivu zpracování s rizikem pro práva a zásady | 35 |
| **DPO** | --- | | Povinnost pro určené organizace | 37 - 39 |
| **Při porušení ochrany dat** | --- | | do 72 hodin obeznámit ÚOOÚ | 34 |

*Tabulka 1: Komparace povinností, zdroj: vlastní zpracování*

## 11.4 Předání do třetích zemí

**101/2000 Sb.,**

Zákon 101 připouští volný pohyb osobních údajů, který nemůže být omezován, pro předávání údajů do členských států EU. Dále zákon hovoří o těch zemích, u kterých zákaz

[16] Pokud správce hodlá zpracovávat OÚ nebo změnit registrované zpracování, je povinen o tom písemně vyrozumět Úřad pro ochranu osobních údajů.

omezení volného pohybu vyplývá z mezinárodní smlouvy, kterou je Česká republika vázána a k jejíž ratifikaci udělil Parlament souhlas či jsou OÚ předány na základě rozhodnutí orgánu EU. V tomto případě zákon předpokládá stejnou úroveň ochrany osobních údajů.

Dále zákon upravuje i předávání do zemí, kde se dá předpokládat nižší úroveň ochrany a předávání je tak možné **pouze na základě předchozího povolení ÚOOÚ**. Zde je určující, zda správce má souhlas subjektu údajů s předáním, případná smlouva o OOÚ mezi správcem a příjemcem či závazná vnitropodniková pravidla o OOÚ v rámci nadnárodní korporace.

**GDPR**

Cílem GDPR je zjednodušit pohyby údajů přes hranice a zajistit vysokou úroveň ochrany osobních údajů při mezinárodním zpracování. Osobní údaje je stále možné volně předávat v rámci zemí EU a nařízení dále popisuje **tři možnosti předávání osobních údajů do třetích zemí,** které jsou obdobné těm, které popisuje Zákon 101.

## 11.5 Nezávislý dozorový orgán

**101/2000 Sb.,**

V zákoně je definován Úřad pro ochranu osobní údajů, který má jasně definované činnosti. Jsou jimi vedení **registru zpracování osobních údajů**, zveřejnění výroční zprávy obsahující zejména informace o provedené kontrolní činnosti, oprávnění a povinnosti při dozoru či uložení opatření k nápravě.

**GDPR**

Každý členský stát je povinen stanovit **jeden či více nezávislých orgánů** veřejné moci pověřených monitorováním uplatňování tohoto nařízení. Jednotlivé dozorové úřady mezi sebou spolupracují pro přispívání **k jednotnému uplatňování nařízení**. Každý dozorový úřad musí jednat nezávisle, jmenován transparentním způsobem a každý člen musí mít zkušenosti, kvalifikaci a dovednosti potřebné pro plnění povinností a výkonu pravomocí. Nařízení stanovuje několik úkolů, které musí každý dozorový úřad na svém území vykonávat. Patří mezi ně monitorování a vymáhání nařízení, zvyšování povědomosti o rizicích, pravidlech, právech a zárukách, poskytování poradenství, zabývání se stížnostmi

od subjektů údajů, schvaluje smluvní doložky a závazná podniková pravidla, navrhuje a zveřejňuje kritéria pro monitorování kodexů chování a plní veškeré další úkoly související s OOÚ. Dozorový úřad také vypracovává výroční zprávy o své činnosti. Dozorovým orgánem pro ČR zůstává ÚOOÚ.

## 11.6 Sankce

**101/2000 Sb.,**

Pokuta do výše 100 000 Kč hrozí FO, která je ke správci či zpracovateli v pracovním nebo obdobném poměru, vykonává pro něj činnost na základě dohody nebo na základě zákona přichází do styku s OÚ, která se dopustí přestupku porušením mlčenlivosti.

Pokuta do výše 1 000 000 Kč hrozí FO / 5 000 000 Kč pro PO, která se dopustí jako správce nebo zpracovatel přestupku tím, že nestanoví účel, prostředky nebo způsob zpracování, zpracovává nepřesné údaje, shromažďování nebo zpracování OÚ neodpovídá rozsahem nebo způsobem účelu, poruší dobu uchování OÚ, neposkytne subjektu informace, na které má subjekt nárok, zpracovává osobní údaje bez souhlasu v případech, kde je zákonem vyžadován, nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování OÚ či nesplní oznamovací povinnost.

Pokuta do výše 5 000 000 Kč hrozí FO / 10 000 000 Kč pro PO za předchozí prohřešky ohrozí větší počet subjektů údajů neoprávněným zasahováním do osobního života nebo poruší povinnost pro zpracování citlivých osobních údajů. Za správní delikt právnická osoba neodpovídá, pokud prokáže, že vynaložila veškeré úsilí, aby porušení zabránila.

**GDPR**

Jsou dané dvě výše sankcí, podrobněji popsané v kapitole *Sankce a pokuty* v této práci, podle míry porušení a zavinění, a to:

a) 10 000 000 EUR nebo 2 % celkového ročního celosvětového obratu za předchozí finanční rok, v případě, že se jedná o podnik, podle toho, která částka je vyšší.
b) 20 000 000 EUR nebo 4 % celkového ročního celosvětového obratu za předchozí finanční rok, v případě, že se jedná o podnik, podle toho, která částka je vyšší.

Dále mohou členské státy využít i jiných sankcí dle konkrétního případu viz kapitola *Sankce a pokuty.*

## 11.7 Slovník

V následující tabulce je uvedena komparace základních pojmů užívaných v rámci Zákona 101 a nařízení GDPR.

| | 101/2000 Sb., | GDPR |
|---|---|---|
| **Osobní údaj** | Jakákoli informace týkající se určeného nebo určitého subjektu údajů. | Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (subjekt údajů). |
| **Citlivý údaj** | Údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofické přesvědčení, odsouzení za trestní čin, zdravotním stavu, sexuálním životě, genetický či biometrický údaj. | Kategorie zvláštních osobních údajů – vypovídají o rasovém či etnickém původu, náboženském vyznání, členství v odborech, filozofické přesvědčení či politických názorech, genetické, biometrické údaje za účelem jednoznačné identifikace FO a údajů o zdravotním stavu, sexuálním životě či sexuální orientaci FO. |
| **Anonymní údaj** | Údaj buď v původním tvaru nebo po provedeném zpracování, který nelze vztáhnout k určené nebo určitelné FO. | GDPR se nevztahuje na údaje, které má správce či zpracovatel již v anonymní podobě. |
| **Pseudonymizace** | --- | Zpracování osobních údajů tak, že již nemůžou být přiřazeny ke konkrétnímu subjektu bez dodatečných informací (které jsou uchovávány odděleně) a je zajištěno, že nebudou přiřazeny ke konkrétní osobě; nevratný proces. |
| **Zpracování** | --- | Jakákoliv operace (soubor operací) s osobními údaji nebo jejich souborem. |
| **Profilování** | --- | Forma automatizovaného zpracování osobních údajů pro použití k hodnocení některých osobních aspektů. |

*Tabulka 2: Slovník pojmů, zdroj: vlastní zpracování*

# 12 Analýza právních titulů ke zpracování v korporátních subjektech

V předchozích částech práce byla analyzována a představena legislativa ohledně zpracování a ochrany osobních údajů. V této části bude provedena analýza jednoho ze stěžejních zásad nařízení následovaná praktickou ukázkou faktické realizace dvou korporátních subjektů a porovnání těchto řešení.

Pro jakékoli legální zpracování musí mít správce zákonný právní důvod. Na této zásadě a tudíž i správné implementaci této části nařízení je založeno veškeré zpracování. V případě, kdy správce pozbude poslední zákonný důvod pro zpracování, musí všechny operace související se zpracování daných údajů ukončit. Zároveň nařízení udává povinnost informovat subjekt údajů o účelech zpracování a na základě kterého právního důvodu zpracování probíhá.

V této části u obou korporátních subjektů dochází k analýze účelů zpracování z veřejně dostupných informací, specifikaci návazností na některé jiné zákony. Všechny tyto získané informace jsou následně na konci analýzy subjektu převedeny do vizuální podoby v kontextu životního cyklu smluvního vztahu.

## 12.1 T-Mobile Czech Republic a.s.

Prvním subjektem, u kterého bude provedena analýza právních titulů a účelů zpracování, je telekomunikační společnost T-Mobile Czech Republic a.s, která provozuje stejnojmennou mobilní síť. Některé zákony, které ovlivňují tento subjekt i z pohledu ochrany osobních údajů jsou uvedeny v následující tabulce. Nejedná se tedy o komplexní výčet všech zákonů, které odvětví definují.

| Zákon č. | Název |
|---|---|
| **563/1991 Sb.** | o účetnictví |
| **235/2004 Sb.** | o dani z přidané hodnoty |
| **480/2004 Sb.** | o některých službách informační společnosti |
| **127/2005 Sb.** | o elektronických komunikacích |
| **182/2006 Sb.** | Insolvenční zákon |
| **262/2006 Sb.** | Zákoník práce |
| **111/2009 Sb.** | o základních registrech |
| **280/2009 Sb.** | daňový řád |
| **468/2011 Sb.** | Zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony |
| **304/2013 Sb.** | o veřejných rejstřících právnických a fyzických osob |
| **297/2016 Sb.** | o službách vytvářejících důvěru pro elektronické transakce |

*Tabulka 3: Přehled některých zákonů ovlivňující toto odvětví, zdroj: vlastní zpracování*

### 12.1.1 Zpracování na základě smluvního vztahu

Prvním právním důvodem pro zpracování, který je v této analýze rozebírán, je zpracování nezbytné pro plnění smluvních podmínek. U těchto zpracování zákazník nemá právo na omezení zpracování nebo na námitku, v případě nesouhlasu se zpracováním by byl klient nucený řešit situaci neuzavřením nebo vypovězením smlouvy či jejích částí.

V této kapitole jsou popsány tyto účely zpracování:

- Poskytování služeb elektronických komunikací, včetně služeb s přidanou hodnotou a platebních transakcí, včetně vyúčtování takových služeb na základě uzavřené smlouvy, včetně jejích změn (dále jen Poskytování služeb elektronických komunikací).
- Poskytování dalších služeb a produktů, včetně jejich doručení (dále jen Poskytování dalších služeb a produktů).
- Zajištění propojení a přístupu k síti, vzájemné vyúčtování (dále jen Zajištění propojení a přístupu k síti).

**Poskytování služeb elektronických komunikací**

Jedná se o poskytování služeb elektronických komunikací a jiných služeb při jejich využívání[17], a dále péče zákazníkům, které vyplývají z uzavřeného smluvního vztahu. Zahrnuje i vystavení vyúčtování a podrobných výpisů, samotné vyúčtování, problematiku reklamací a jejich řešení, či případné změny v uzavřené smlouvě. Údaje jsou zpracovávány po dobu trvání smluvního vztahu.

**Poskytování dalších služeb a produktů**

V tomto případě se jedná zejména o prodej koncových zařízení, kterými mohou být telefony, tablety, modemy, chytré hodinky, notebooky či zařízení pro komunikaci s autem[18]. Zpracování probíhá po dobu, kdy je možné se domáhat právních nároků plynoucích ze smluvního vztahu.

**Zajištění propojení a přístupu k síti**

Toto zajištění propojení představuje zpracování potřebné pro výměnu údajů mezi poskytovali služeb elektronických komunikací. Především se jedná o zajištění připojení, přístupů k síti a vzájemného vyúčtování mezi jednotlivými poskytovateli. Zpracování probíhá po dobu nezbytně nutnou pro poskytnutí služeb a návazných úkonů.

[17] např. IT, doplňkové, s přidanou hodnotou

[18] Chytré auto

### 12.1.2 Zpracování na základě plnění právní povinnosti

V této kapitole jsou uvedeny významné zákonné povinnosti, které vycházejí z platné legislativy, kdy některé jsou specifické pro poskytovatele služeb elektronických komunikací. U tohoto právního důvodu nemá zákazník právo na omezení zpracování nebo námitku.

V této kapitole jsou popsány tyto účely zpracování:

- Zajištění kvality, bezpečnosti a optimalizace sítě/služeb, identifikace zneužívání sítě a služeb (dále jen Zajištění kvality a bezpečnosti).
- Zpracování údajů spojených s trestnou činností.
- Daňové a jiné předpisy.
- Linka tísňového volání.

**Zajištění kvality a bezpečnosti**

Správce je povinen zajistit odpovídající kvalitu sítí elektronických komunikací a poskytovaných služeb pro eliminaci rizika. Správce tak musí konat s ohledem na kybernetické hrozby[19], dále identifikaci subjektů, u kterých má poskytovatel podezření na porušení či zneužití služeb. Součástí je i optimalizace stávajících a vývoj nových služeb vzhledem k technologickém vývoji na trhu.

**Zpracování údajů spojených s trestnou činností**

Týká se povinností vyplývající pro tohoto poskytovatele služeb v rámci uchovávání údajů, které s poskytováním služeb. Jejich účel může být například předcházení, vyhledávání a odhalování trestné činnosti či stíhání trestních činů. Zpracování probíhá v období při trvání smlouvy a maximálně 6 měsíců po ukončení smlouvy.

**Daňové a jiné předpisy**

Toto zpracování osobních údajů souvisí s daňovými a jinými předpisy, které ukládají správci povinnost zpracovávat osobní údaje ve formě dokumentace, například daňové

[19] např. detekci malwaru a spamu

doklady či jiné účetní doklady. Doba zpracování se zde liší podle zákonné úpravy v jednotlivých předpisech, uvedené daňové doklady je nutno uchovávat po dobu 10 let.

**Linka tísňového volání**

Linka tísňového volání[20] je jeden ze základních způsobů ohlášení mimořádné události a následné vyžádání pomoci složkami integrovaného záchranného systému. Volání na tato čísla je bezplatná a je garantován nepřetržitý přístup, a to jak z pevných linek, mobilních telefonů, tak telefonních automatů. Každý poskytovatel veřejné telefonní služby nebo-li operátor je ze zákona[21] povinen svým uživatelům bezplatně umožnit tísňové volání[22]. Lhůta zpracování osobních údajů pro tento účel je nezbytně nutnou pro poskytnutí spojení.

### 12.1.3 Zpracování na základě oprávněných zájmů správce

Tyto účely odpovídají případům, kdy podnikatelský subjekt potřebuje zpracovávat osobní údaje pro úkony spojené s podnikatelkou činností, které ovšem nespadají pod zákonné důvody spojené s právní povinností či plnění smluvních podmínek.

V této kapitole jsou popsány tyto účely zpracování:

- Ověřování bonity – scóring.
- Přímý marketing.
- Určení, výkon nebo obhajoba právních nároků (dále jen Právní nároky).

**Ověřování bonity - scóring**

Ověřování bonity společnost používá pro ověření zákazníka, z důvodu rizika neplnění závazků vyplývající ze smluvního vztahu, a vyhodnocení potencionálního podvodného jednání například zfalšování osobních údajů či použití zcizeného dokladu. Je tedy oprávněným zájmem společnosti si ověřit, zda potencionální sjednání nové služby či

[20] Tísňové volání je služba, kterou je zajišťována ochrana základních lidských práv, a to konkrétně ochrana života a zdraví, dále i životního prostředí a ochrana majetku.

[21] Zákon 127/2005 Sb., o elektronických komunikacích

[22] Telefonní čísla 112, 150, 155, 158, 156

současný klient bude schopný závazky platit, což slouží i jako prevence proti dalšímu zadlužování dané osoby.

Společnost tedy ověřuje správnost osobních údajů, schopnost platit závazky v registru dlužníků, dále vyhodnocení na základě adresy.

Ke zpracování dochází před vstupem a během smluvního vztahu. Zde zákazník nemá právo na omezení či námitku.

**Přímý marketing**

Nařízení stanovuje možnost nabízet svým zákazníkům produkty a služby. Zákazník tímto získává informace o všeobecných výhodách, novinkách a podobně. Nejedná se tedy o nabídky na míru, a správce může zpracovávat pro tyto účely informace o smluvním vztahu. Údaje se zpracovávají po dobu trvání smluvního vztahu až do 3 let od ukončení smlouvy nebo do doby podání námitky. V případě cookies lze provést změnu nastavení.

**Právní nároky**

Právní nárok je možnost domáhat se právní ochrany realizace práva[23]. Správce má tedy oprávněný zájem zpracovávat údaje v případě vedení sporu či řízením před správním orgánem, soudem či jinou institucí k tomu určenou. Zde je subjektu údajů přisouzeno právo na námitku a omezení. Zpracování probíhá po dobu nezbytnou pro vedení příslušného řízení.

### 12.1.4 Zpracování na základě souhlasu

Následující kapitola představuje zpracování osobních údajů, které probíhají pouze na základě udělení souhlasu. Při uzavírání účastnické smlouvy je klient vždy dotázán, zda uděluje souhlas, ten je následně promítnut do relevantní části smlouvy, případně elektronicky v interaktivním formuláři. Některé souhlasy je také možné udělit následně jako při účasti v soutěži či při speciálních marketingových nabídkách. Přehled všech

[23] Například z výpůjčky vzniká právo na vrácení půjčené věci, nárok na vrácení vzniká až skončením stanovené zápůjční doby

souhlasů je účastníkům i uživatelům dostupný v aplikaci organizace, kde je možné je i dále spravovat. Souhlas je vždy odvolatelný a není podmíněný.

V této kapitole jsou popsány tyto účely zpracování:

- Marketingové a obchodní účely, včetně analýzy, T-Mobilu (dále jen Marketing a obchodní účely).
- Marketing třetích stran.
- Obchodní účely třetích stran.
- Ověřování bonity na základě souhlasu.

**Marketing a obchodní účely**

Tyto účely rozšiřují působnost přímého marketingu, kde dochází i ke zpracovávání údajů například na jaké základnové stanici bylo koncové zařízení připojeno. Jelikož se jedná o nabídky relevantní pro daného klienta, toto zpracování zahrnuje i profilování. Obchodní účely zahrnují vypracování anonymizovaných a agregovaných analýz z těchto dat, které společnost využívá k vývoji služeb či pro veřejnoprávní účely jako je plánování parkování či dopravy. Toto zpracování probíhá maximálně po dobu 2 let od ukončení smlouvy či do odvolání souhlasu. V případě metadat, tzv. data o datech, se jedná o maximální dobu zpracování 6 měsíců.

**Marketing třetích stran**

Při tomto zpracování opět dochází k profilování, které využívá osobní údaje jako například věku subjektu údajů a využití jeho služeb. Společnost pak zasílá klientům informace o produktech třetích stran, aniž by samotné třetí strany měly přístup k údajům klienta.

**Obchodní účely třetí strany**

Toto zpracování probíhá pouze na základě výslovného souhlasu subjektu údajů. Pokud subjekt údajů souhlas s tímto účelem zpracování udělí, třetí strany mohou zpracovávat údaje například ve formě analýzy.

**Ověřování bonity na základě souhlasu**

Na rozdíl od předchozího účelu ověřování bonity se zde nejedná o ověření klienta, ale o předávaní jeho údajů do registrů. Lze rozeznávat dva typy registrů, a to negativní a

pozitivní. U těchto registrů se rozlišuje rozsah předávaných údajů, možnost nahlížení do registrů a možnost subjektu údajů vyjádřit nesouhlas s evidencí údajů o své osobě.

Negativní registr

- Obsahuje informace o osobách, které jsou v prodlení s plněním svých závazků. Předávají se údaje jako jméno, příjmení, adresa, rodné číslo, datum vzniku dluhu a jeho výše, typ služby nebo produktu vztaženého k dluhu, výše dlužné částky po splatnosti, počet dlužných vyúčtování apod. U právnických osob se jedná o stejný rozsah předávaných údajů s odpovídající úpravou. K předávání údajů a nahlížení do tohoto registru není potřeba souhlas subjektu údajů.

Pozitivní registr

- Oproti negativnímu registru obsahuje informace o závazcích spotřebitelů, u kterých nedošlo k prodlení. Mezi předávané údaje patří také jméno, příjmení, adresa, ale také navíc datum narození, pohlaví, údaje o dokladech totožnosti, informace o uzavření smlouvy mezi subjektem údajů a společností, údaje o finančních závazcích, které vznikly, vzniknou nebo mohou vzniknout v souvislosti se smlouvou, údaje o zajištění závazků účastníka, údaje vypovídající o bonitě a platební morálce subjektu a další. V případě pozitivního registru je jak k nahlížení, tak k předávání údajů potřeba souhlas subjektu údajů. Subjekt údajů je oprávněn písemně vyjádřit nesouhlas s evidencí jeho údajů v pozitivním registru a provozovatel pak bez zbytečného odkladu odstraní všechny záznamy.

Zpracovávání údajů probíhá po dobu, po kterou závazek trvá, závazky vzniklé ve vztahu ke společnosti jsou zpracovávány dále po dobu 1 roku od uhrazení poslední pohledávky. Pokud závazek zanikl jiným způsobem než splacením či se jedná o promlčený nebo osvobozený závazek, lze informaci zpracovávat nejdéle po dobu 3 let od zániku.

### 12.1.5 Zpracování údajů fyzických osob mimo smluvní vztah

Společnost dále specifikuje případy zpracování osobních údajů fyzických osob, které se společností neuzavřely smlouvu o poskytování služeb. Jedná se o kontaktní osoby, kdy se zpracování zakládá na oprávněných zájmech správce a plnění zákonných povinností,

uživatele služeb a zákazníky s metodou prepaid[24] a ostatní osoby, kde se zpracování zakládá na souhlasu subjektu údajů.

V této kapitole jsou popsány účely zpracování týkající se:

- kontaktních osob,
- uživatelů služeb a zákazníků s metodou prepaid,
- ostatních osob.

**Kontaktní osoby**

Pokud je subjekt údajů uvedený ve smlouvě jako kontaktní osoba, jsou součástí uzavřené smlouvy se zákazníkem nebo dodavatelem i jeho osobní údaje. K takovým údajům je společnost v pozici správce a jsou nadále zpracovávány pro účely uzavírání a plnění smlouvy, vnitřní administrativní potřeby, ochrany majetku a osob, ochrany právních nároků, tvorby statistik a evidencí a plnění zákonných povinností.

**Ostatní osoby**

Do této kategorie spadají osoby, které:

- udělili souhlas se zpracováním v rámci marketingové akce,
- projevili zájem o kontaktování s nabídkou,
- předání kontaktu na subjekt údajů třetí osobou, případně třetím subjektem, který má k předání dalšímu správci za účelem nabídky souhlas.

Subjekt údajů má pak možnost odmítnout posílání nabídek dle instrukcí v poslané nabídce či při telefonické komunikaci. [17]

**Uživatelé služeb a zákazníci s metodou prepaid**

Uživatelé služeb jsou ty osoby, které využívají služby společnosti, ale bez uzavření smlouvy s jejich osobou[25], stejně tak zákazníci s metodou prepaid. Tito uživatelé jsou pro

[24] předplacená dobíjecí karta

[25] Jedná se o uživatele, kteří patří pod tzv. velké zákazníky, většinou se jedná o benefity poskytované zaměstnavatelem.

společnost neidentifikovatelní a svá práva tak mohou vykonávat pouze v omezeném rozsahu dle platných právních předpisů. Data a údaje, které vznikají v rámci poskytování služeb, mají stejnou úroveň ochrany jako data přímých smluvních zákazníků.

I tito uživatelé mají právo spravovat svá oprávnění, jelikož i samotné telefonní číslo či e-mail je kontaktním údajem, na které lze zasílat obchodní sdělení, nabídky apod. Oprávnění lze spravovat přes aplikaci společnosti či ostatními informačními kanály.

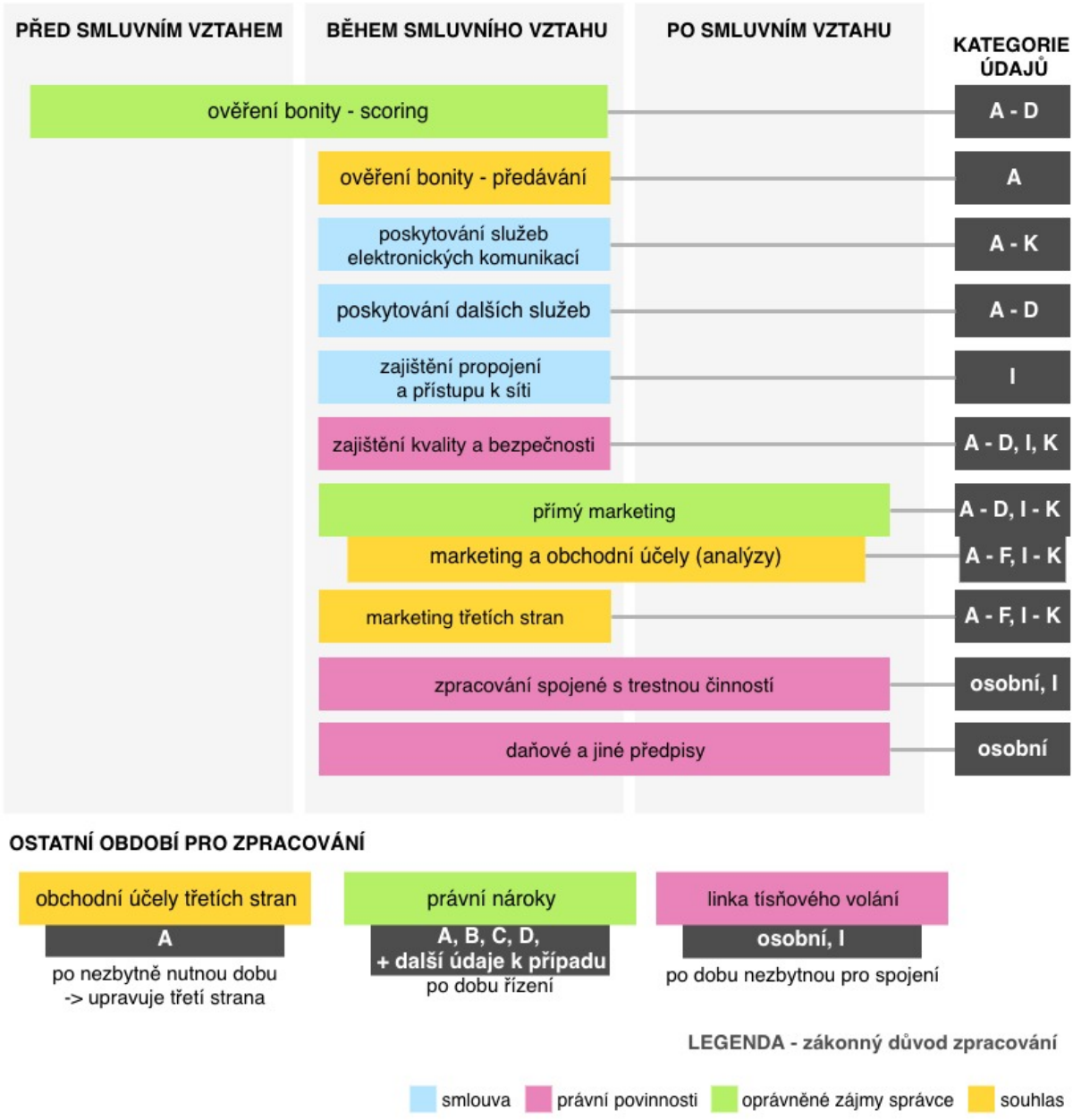
Na základě platných právních předpisů pak společnost zpřístupňuje údaje, které jsou součástí podrobného výpisu v rámci vyúčtování účastníkovi jako součást vyúčtování.

Následuje vizualizace těchto poznatků, která zároveň k jednotlivým účelům zpracování přiřazuje kategorie údajů, legenda viz Tabulka 4, které jsou v rámci tohoto účelu a fáze zpracovávány. Jelikož se jedná o jednotnou legendu pro obě analýzy, údaje, které dané firma nezpracovává jsou v tabulce přeškrtnuté.

| | |
|---|---|
| **A** | identifikační údaje |
| **B** | kontaktní údaje |
| **C** | platební údaje |
| **D** | údaje spojené se službami |
| **E** | vzájemná komunikace a interakce |
| **F** | metadata |
| **G** | cookies |
| **H** | ~~kamerové záznamy~~ |
| **I** | speciální údaje |
| **J** | sociodemografická data |
| **K** | věk, pohlaví, vzdělání, rodinný stav |
| **L** | podpis a dynamický podpis |

*Tabulka 4: Kategorie zpracovávaných údajů, zdroj: vlastní zpracování*

Na následujícím obrázku je grafické vyhodnocení předchozí textové analýzy, které shrnuje zásadní situace v rámci životního cyklu smluvního vztahu i mimo něj. Jednotlivé účely zpracování se tak mohou nacházet v jedné či více fází. Smluvní vztah je rozdělen do třech základních fází, a to před smluvním vztahem, během smluvního vztahu a po smluvním vztahu. Vizualizace je doplněna o barevné rozlišení jednotlivých zákonných důvodů zpracování. Těmito zákonnými důvody zpracování jsou smlouva, právní povinnosti, oprávněné zájmy správce a souhlas. Stejná notace je pak využita i ve vizuálním výsledku analýzy následujícího subjektu.




*Obrázek 1: Vizualizace účelů zpracování T-Mobile, a.s., zdroj: vlastní zpracování*

## 12.2 ČEZ, a.s.

Druhým subjektem, který je předmětem této analýzy, jsou České Energetické Závody, které jsou největším výrobcem elektřiny v České republice a sdružují další desítky společností. I toto odvětví je upravováno řadou zákonů, které mohou udávat povinnosti z hlediska zpracovávat určité osobní údaje. Opět následuje tabulka s výčtem základních zákonů, které odvětví definují.

| Zákon č. | Název |
|---|---|
| **563/1991 Sb.** | o účetnictví |
| **458/2000 Sb.** | Energetický zákon |
| **235/2004 Sb.** | o dani z přidané hodnoty |
| **480/2004 Sb.** | o některých službách informační společnosti |
| **182/2006 Sb.** | Insolvenční zákon |
| **262/2006 Sb.** | Zákoník práce |
| **111/2009 Sb.** | o základních registrech |
| **280/2009 Sb.** | daňový řád |
| **468/2011 Sb.** | Zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony |
| **304/2013 Sb.** | o veřejných rejstřících právnických a fyzických osob |
| **297/2016 Sb.** | o službách vytvářejících důvěru pro elektronické transakce |

*Tabulka 5: Přehled některých zákonů ovlivňující odvětví, zdroj: vlastní zpracování*

Vzhledem k odlišnosti zpracování povinnosti informovat o účelech zpracování je následující struktura analýzy odlišná od předchozí, a to z toho důvodu, že tento subjekt ve většině účelů neurčuje jen jeden jednoznačný právní titul zpracování.

V této kapitole jsou popsány následující účely zpracování:

- Identifikace a autentizace.
- Posouzení obchodního rizika.
- Příprava smlouvy.
- Reporting, řízení informací, optimalizace procesů, školení.
- Využívání služeb a produktů.
- Prevence podvodného jednání.
- Zasílání servisních zpráv.
- Testování softwaru.
- Řízení vztahů se zákazníky a obchodními partnery.
- Účetnictví a daně.
- Využívání webových stránek a on-line prostředí.
- Výkon práv.
- Bezpečnosti.
- Účast na pořádaných akcích.

**Identifikace a autentizace**

Pro uzavření smlouvy a poskytování nebo odebírání produktů či služeb firma potřebuje znát alespoň základní údaje subjektu údajů. Identifikace a autentizace je také vyžadována v případě uplatnění práv v záležitosti ochrany osobních údajů. Údaje jsou v takovém případě zpracovány na základě nezbytnosti plnění smlouvy a právních povinností.

**Posouzení obchodního rizika**

Společnost využívá postupy vnitřního hodnocení pro řízení rizik před uzavřením smluvních vztahů a jejich plnění. Hodnotí rizikovost sjednání určitého produktu nebo služby se zákazníkem nebo obchodním partnerem s využitím externích registrů a interních databází. Toto zpracování probíhá na základě oprávněného zájmu správce.

**Příprava smlouvy**

Pro tento účel jsou využívány pouze údaje nezbytné a potřebné pro návrh smlouvy. Jedná se o jméno a příjmení, datum narození, popřípadě IČO a kontaktní údaje. Dále podle druhu produktu nebo služby případně typu obchodní spolupráce, který je předmětem smlouvy je odvislý další okruh údajů. Právním důvodem zpracování je u tohoto účelu nezbytnost pro plnění právních povinností a smlouvy.

**Reporting, řízení informací, optimalizace procesů, školení**

V každé společnosti Koncernu ČEZ probíhá zpracování osobních údajů, jako jsou základní údaje a údaje o produktech a službách, v rámci plnění interních povinností, jejichž součástí je schvalovací, reportovací systém, plánování, vyhodnocování. Pro vybrané provozní potřeby jsou data ve formě souhrnného čísla, tzn. bez přímé vazby na konkrétní osobu. Do této kategorie zpracování spadají i různé výkazy dle daných právních předpisů, a probíhá na základě plnění právních povinností a oprávněných zájmů správce.

**Využívání služeb a produktů**

Při využívání služeb a produktů, dochází ke zpracování osobních údajů. Jedná se především o základní údaje, údaje o produktech a službách nebo obchodní spolupráci. Je prováděna jejich registrace, správa a aktualizování. Pro usnadnění obsluhy jsou pro klienty na elektronických portálech pro obsluhu produktů zobrazovány a spravovány jejich základní informace a informace o využívaných produktech. Zpracování probíhá na základě plnění smluvních povinností.

**Prevence podvodného jednání**

Tento účel zpracování spočívá v analyzování údajů pro zabránění podvodným jednání, a to jak digitálně tak i fyzicky. Na základě dostupných informací společnost vytváří interní ukazatele, které spolu s jinými informacemi využívá pro relevantní indikaci možných podvodů. Zpracovávanými údaji jsou identifikační údaje, údaje o produktech a službách a způsobu jejich využívání, dále také informace o jednání subjektu údajů v průběhu smluvního vztahu. Tyto údaje jsou zpracovány na základě plnění povinností z právních předpisů a ochranu práv a oprávněných zájmů správce.

**Zasílání servisních zpráv**

Klientovi jsou v rámci poskytování služeb zasílány servisní zprávy pro zvýšení komfortu obsluhy poskytovaného produktu či služby. Pro tento účel jsou zpracovávány kontaktní údaje, a to na základě povinnosti plnění smlouvy.

**Testování softwaru**

Pro interní testování nového softwaru, softwarových změn, případně školení zaměstnanců, jsou v některých nezbytných případech, kdy nejsou testovací data dostatečná, využívána data zákazníků nebo obchodních partnerů. Je kladen důraz na to, aby byla využita data neaktuální a na zabezpečením před případným zneužitím. Zpracování je založeno na základně oprávněných zájmů správce.

**Řízení vztahů se zákazníky a obchodními partnery**

Společnost řeší požadavky, přání a stížnosti, jimiž mohou být i záležitosti týkající se OOÚ, které jsou podané písemně, telefonicky, prostřednictvím internetových stránek, portálových řešeních i dalšími způsoby pro spokojenost zákazníků a zachování přízně. Za tímto účelem společnost shromažďuje, jaké produkty a služby zákazníci využívají a jaké mají přání. Záležitostmi týkající se příslušného produktu nebo služby mohou být jeho nastavení, poskytování informací o jeho využívání, změny a další. Pro tento účel jsou zpracovávány příslušné údaje o produktech a službách či obchodní spolupráci, profilové údaje a údaje ze společné komunikace a interakce, které subjekt údajů sdělí. Tento účel zpracování je prováděn na základě plnění smluvních povinností a pro ochranu práv a oprávněných zájmů správce.

**Účetnictví a daně**

Za účelem plnění účetních a daňových povinností vůči regulačním a státním orgánům společnost shromažďuje a zpracovává identifikační a transakční údaje subjektu. Tyto povinnosti ukládá zákon o účetnictví, zákon o DPH a další české účetní a daňové zákony, stejně tak jako povinné hlášení regulačním orgánům. Toto zpracování je tedy na základě plnění právní povinnosti z právních předpisů.

**Využívání webových stránek a on-line prostředí**

Výstupem tohoto zpracování je pohodlné využívání webových stránek, identifikace jazykového nastavení. Jsou pro to zpracovávány údaje o zařízeních, ze kterých je učiněn přístup, preference nastavení služeb a vyplňované údaje. Zpracování probíhá na základě plnění smlouvy či souhlasu subjektu údajů, a to případě cookies.

**Výkon práv**

V případě potřeby vymáhání pohledávek právní cestou či jiného soudního řízení, které se týká subjektu údajů, jsou použity v nezbytném rozsahu základní údaje, údaje o produktech a službách, údaje ze vzájemné komunikace, případně další údaje nezbytné k ochraně práv. Toto zpracování probíhá na základě plnění povinností z právních předpisů a pro ochranu práv a oprávněných zájmů správce.

**Bezpečnost**

Pro plnění právních předpisů, kterými jsou provozování jaderných elektráren, informační a kybernetická bezpečnost apod., je vyžadováno zpracování některých osobních údajů. Příkladem mohou být kamerové systémy se záznamem či systémy informační a kybernetické bezpečnosti pro prevenci kybernetických rizik. Tyto údaje jsou zpracovávány na základě plnění právních povinností nebo oprávněných zájmů správce.

**Účast na pořádaných akcích**

Skupina ČEZ organizuje velké množství společenských akcí, a to například odborné konference, semináře, kulturní, sportovní, charitativní a další akce. Tyto akce jsou dostupné nejen úzkému okruhu zájemců, a to především odborníkům, ale také široké občanské veřejnosti. Pokud subjekt údajů projeví zájem o takovou společenskou akci, společnost zpracovává jeho osobní údaje, kdy se jedná o registraci, účast a splnění předem oznámených podmínek, kterými je poplatek, závazek aktivního zapojení apod. Základní údaje jsou v tomto případě používány zpravidla pro účely organizačního zabezpečení akce, informování účastníka či zájemce, případně pro vystavení příslušných účetních dokladů a případným vypořádáním souvisejících činností. Právní důvody zpracování se liší podle konkrétního účelu zpracování, kdy např. při potřebě účetních a daňových předpisů se jedná o zpracování na základě plnění právních povinností, dále se jedná o

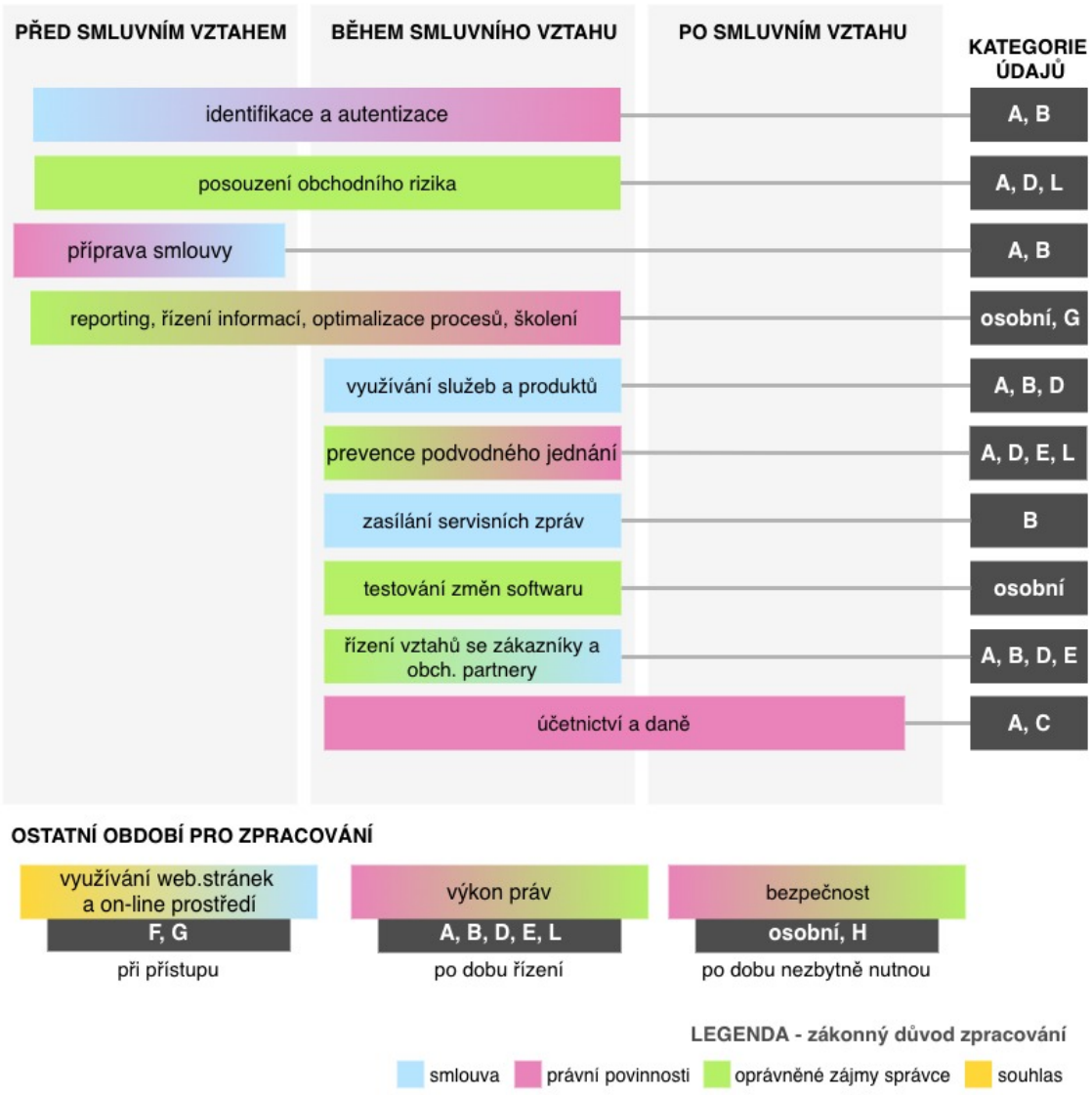
zpracování k uzavření a plnění smlouvy, pro ochranu práv a oprávněných zájmů správce a zpracování na základě souhlasu je např. v případě osobních fotografií.

V následující vizualizaci jsou k účelům zpracování přiřazeny jednotlivé kategorie údajů, legenda viz Tabulka 6, které jsou v rámci tohoto účelu a fáze zpracovávány. Jelikož se jedná o jednotnou legendu pro obě analýzy, údaje, které dané firma nezpracovává, jsou v tabulce přeškrtnuté.

| | |
|---|---|
| **A** | identifikační údaje |
| **B** | kontaktní údaje |
| **C** | platební údaje |
| **D** | údaje spojené se službami |
| **E** | vzájemná komunikace a interakce |
| **F** | metadata |
| **G** | cookies |
| **H** | kamerové záznamy |
| **I** | ~~speciální údaje~~ |
| **J** | ~~sociodemografická data~~ |
| **K** | ~~věk, pohlaví, vzdělání, rodinný stav~~ |
| **L** | podpis a dynamický podpis |

*Tabulka 6: Kategorie zpracovávaných údajů, zdroj: vlastní zpracování*

Jako v analýze předchozího subjektu následuje vizualizace získaných informací do podoby životního cyklu smluvního vztahu. Smluvní vztah je rozdělen do třech základních fází, a to před smluvním vztahem, během smluvního vztahu a po smluvním vztahu. Jednotlivé účely zpracování se tak mohou nacházet v jedné či více fází. Vizualizace viz následující obrázek je doplněna o barevné rozlišení jednotlivých zákonných důvodů zpracování. Těmito zákonnými důvody zpracování jsou smlouva, právní povinnosti, oprávněné zájmy správce a souhlas.




*Obrázek 2: Vizualizace účelů zpracování ČEZ, a.s., zdroj: vlastní zpracování*

## 12.3 Vyhodnocení analýz

Předchozí podkapitoly práce poskytly základ pro analýzu toho, jak dva velké korporátní subjekty specifikují účely zpracování a k nim návazné právní tituly zpracování. V této kapitole proběhne shrnutí zjištěných skutečností.

Jedním z výstupů těchto kapitol jsou dva diagramy účelů zpracování ve dvou různých subjektech. Nutno dodat, že obě tyto implementace jsou v souladu s nařízením, nicméně již na první pohled je patrné, že obě tyto implementace jsou značně odlišné.

| Kategorie údajů – ČEZ, a.s. | Kategorie údajů – T-Mobile, a.s. |
|---|---|
| **A. identifikační údaje** | |
| titul,<br>jméno a příjmení,<br>datum narození,<br>IČO, DIČ,<br>čísla předložených identifikačních dokladů a ostatní informace s nimi spojené. | titul,<br>jméno a příjmení,<br>**rodné číslo,**<br>datum narození,<br>IČO, DIČ,<br>**adresa trvalého pobytu, adresa podnikání, fakturační adresa,**<br>čísla předložených identifikačních dokladů a ostatní informace s nimi spojené. |
| **B. kontaktní údaje** | |
| kontaktní telefonní číslo,<br>**adresa trvalého pobytu, doručovací či jiná kontaktní adresa**<br>e-mailová adresa. | kontaktní telefonní číslo,<br>e-mailová adresa,<br>**adresy na sociálních sítích.** |
| **C. platební údaje** | |
| číslo bankovního účtu. | čísla účtů,<br>**platební metoda,**<br>**údaje o přijatých platbách / dlužných částkách,**<br>**údaje o platební morálce.** |
| **D. údaje spojené se službami** | |
| zákaznické číslo,<br>EAN,<br>číslo obchodního partnera,<br>identifikační číslo osoby dodavatele,<br>číslo přístupové ID karty (pokud je přidělena),<br>přístupové ID a heslo do osobního účtu uživatele (pokud jsou vytvořeny). | číslo SIM karty,<br>smluvní telefonní číslo, aktivní tarif,<br>balíčky, ostatní služby,<br>typ smlouvy,<br>segment zákazníka,<br>doba trvání smlouvy,<br>druh poskytnuté služby,<br>cena za poskytnutou službu,<br>typ používaného koncového zařízení. |
| **H. kamerové systémy** | |
| | **I. speciální údaje**<br>přihlašovací údaje a heslo,<br>PIN, PUK. |
| | **J. sociodemografická data** |
| | **K. věk, pohlaví, vzdělání, rodinný stav.** |

*Tabulka 7: Přehled rozdílů v kategoriích údajů, zdroj: vlastní zpracování*

Co se týče toho, jak jednotlivé společnosti definovaly kategorie osobních údajů. Přesto, že podstata kategorií zpracovaných údajů je podobná, některé osobní údaje jsou zařazené v jiných kategorií či nejsou správcem vůbec zpracovávané. Tyto rozdíly jsou znázorněné v následující tabulce. Přehled všech zpracovávaných kategorií a jejich obsahu je uveden v příloze *19.2 Úplné kategorie údajů pro kapitolu 12*.

Další rozdílnosti lze vyhodnotit ve využití právních titulů zpracování, u společnosti T-Mobile lze konkrétně určit na základě kterého titulu je daný účel zpracován, jelikož specifikace daného účelu je konkrétnější. U společnosti ČEZ je patrný trend prolínání dvou právních důvodů téměř pro každý účel zpracování, což je dané výší mírou variability ve formě specifikace účelu. Dalším rozdílem je využití jednotlivých právních titulů. Zatímco u společnosti T-Mobile lze pozorovat rovnoměrné využití všech přípustných titulů, společnost ČEZ své zpracování zaměřuje především na právní tituly spojené s oprávněnými zájmy správce, právními povinnostmi, zpracování na základě smlouvy a zpracování na základě souhlasu téměř nevyužívá.

Lze najít i několik shodných prvků, a to, že struktura účelů obou společností je ve své podstatě stejná. Ta se dá obecně rozdělit na jednotlivé body:

- Ověření solventnosti klienta před vstupem do smluvního vztahu.
- Zpracování pro poskytnutí smluvené služby či produktu.
- Specifické účely související s oblastí podnikání většinou stanovené zákonem či smluvní povinností.
- Doplňkové služby či zpracování pro interní potřeby správce.
- Povinnosti související s daňovým a účetním zákonem.
- Výkon práv a právní nároky.

Tyto analýzy reprezentovaly jeden z důležitých aspektů nařízení, a to, že se jedná o nařízení obecné, tzn. že poskytuje jistou míru variability v možných způsobech plnění souladu s nařízením, a je již na správci, jestli se, konkrétně v případě obeznámení s účelem zpracování, rozhodne pro konkrétnější a striktnější či volnější specifikování účelů zpracování.

# 13 Návodný postup pro implementaci

Tato část práce čerpá z teoretické části práce a také z oficiálních materiálů ÚOOÚ a Evropského sboru pro ochranu osobních údajů (dříve pracovní skupina W29). Na základě těchto poznatků je vytvořen tento návodný postup, který má organizaci pomoc s identifikací slabých míst či případného nesouladu s nařízením. Je nutné upozornit, že se nejedná o komplexní analýzu pro všechny organizace a pro některé specifické případy může být tento postup nedostatečný a doporučuje se konzultace s právníkem či specialistou. Stejně tak tento postup nezahrnuje specifikace jednotlivých oblastí a s nimi spojené další zákony.

Postup pro implementaci je rozdělen do šesti kroků, viz graf, kdy prvním jsou přípravné kroky, následované zmapováním životního cyklu osobních údajů v organizaci, a Gap analýzou nedostatků. Na základě těchto informací pak může následovat implementace, kterou lze na nejvyšší úrovni rozdělit na vnější a celkovou. Vnější lze rozdělit na implementaci informační povinnosti a výkonu práv, celková pak na právní a technickoorganizační. Všechny tyto kroky budou blíže popsány. Pro tento postup je vytvořen i pomocný dokument, který je přiložen k této práci, a který lze využít pro druhý krok návodu.

## 13.1 Přípravné kroky

Ještě před samotnou implementací GDPR by organizace měla být schopna stanovit, zda se jí vůbec týká zpracovávání osobních údajů, které zahrnuje i samotné nahlížení, shromáždění a uložení. Je nutné podotknout, že subjekty údajů jsou i zaměstnanci, kteří jsou mnohdy opomíjenou skupinou subjektů údajů a na které se také nařízení a ochrana osobních údajů vztahuje. Pokud tedy organizace údaje zpracovává, tak dalším krokem je zmapování toho, v jak velkém rozsahu současně řeší ochranu osobních údajů. Pokud se této problematice věnuje již dlouho a v minulosti byla plně v souladu s předchozí legislativou (především tedy Zákon 101/2000 Sb.), pravděpodobně se jí budou týkat menší změny, případně zavedení nových povinností, ale již dopředu lze očekávat, že implementace GDPR v takové organizaci bude spíše menšího rozsahu. Ovšem v případě, že do této doby problematiku osobních údajů řešila v minimálním či dokonce žádném rozsahu či se jedná o nově založenou organizaci, implementace GDPR bude pro tuto

organizaci či instituci pravděpodobně velmi náročná, především v závislosti na specifikace organizace, zpracovávaných údajů apod.

V závislosti na toto zjištění se musí organizace rozhodnout, v jaké míře a rozsahu bude nařízení implementovat. Zde čeká organizaci rozhodování, o tom, zda je pro ni výhodnější a přístupnější implementovat nařízení v plném rozsahu, anebo nemá dostatečné prostředky a především technické zázemí pro úplný soulad s nařízením. S tím souvisí i rozhodování o tom, zda je schopná přijmout rizika spojená s případným nenaplněním některých částí nařízení a vyplývajících následků. Logickým dalším krokem je tedy finanční plán toho, jak velkou investici je schopna a ochotna organizace na implementaci vyčlenit. V návaznosti na to se pak může rozhodnout, zda využije některé z „krabicových" řešení obdobné tomuto, či využije na část či celou implementaci odborníka či tým odborníků.

Součástí tohoto kroku by měla být příprava na implementaci formou zjištění dotčených osobních údajů a ostatních náležitostí zpracování, toků informací a především účelů zpracování.

Účel zpracování a jeho právní titul určuje vždy správce. Pro každé zpracování musí mít správce účel pevně daný a spolu s právním titulem zaručují zákonnost zpracování.

**Výstupy tohoto kroku**

- zjištění předpokládaného potřebného rozsahu implementace,
- rozhodnutí o aplikovaném rozsahu implementace,
- prvotní informace o zpracování osobních údajů v organizaci, především účely zpracování.

## 13.2 Životní cyklus údajů v organizaci

Pokud má organizace k dispozici všechny potřebné informace a výstupy z předchozího kroku, může přikročit k samotné analýze organizace z hlediska ochrany a zpracování osobních údajů, kterou by organizace měla vyhotovit pro každý účel zpracování pro každou oblast organizace, která jakýmkoli způsobem operuje s osobními údaji. Vznikne ji tak přehled o životním cyklu údajů v organizaci.

Pro tuto analýzu může organizace využít přílohu *19.1 Excel – Nástroj pro analytickou část implementace GDPR*, který je výstupem praktické části této práce. Tento dokument se dělí na list Pokyny, kde je uživateli popsán postup práce s dokumentem, list Analýza, kde vyplňuje potřebné informace, a listy Vyhodnocení a Doporučení pro zabezpečení, kde se na základě vyplnění listu Analýza zvýrazní příslušené informace.

List Analýza obsahuje tabulku, která obsahuje jeden sloupec, kde je nastíněna určitá problematika, čtyři sloupce pro možné odpovědi, sloupec na vyplnění odpovědi a poslední sloupec zobrazuje návaznost na vyplívající povinnosti. Tato tabulka je pak rozdělena na 7 částí dle jednotlivých oblastí dotazů. Jedná se o:

- specifikace ekonomického subjektu,
- uchovávání osobních údajů,
- specifikace subjektů údajů a osobních údajů,
- specifikace zpracování,
- předávání osobních údajů,
- monitorování,
- využitá řešení.

Tuto analýzu by měla organizace pro co nejefektivnější výsledek vypracovat pro každý účel zpracování, který organizace provádí, samostatně. V případě, že chce organizace pouze orientační přehled jejích povinností a rizikových stránek zpracování, lze přílohu *19.1 Excel – Nástroj pro analytickou část implementace GDPR* vyplnit pouze jednou obecně či pouze pro určitou oblast zpracování (zákazníci, zaměstnanci, dodavatelé apod.), což ovšem může zapříčinit zkreslení výsledku či opomenutí důležitých aspektů.

**Specifikace ekonomického subjektu**

Prvním bodem analýzy je rozlišení zainteresovaného subjektu podle kategorizace ekonomického subjektu. Jsou zde rozlišovány fyzické osoby, nekomerční sdružení, podnikající fyzické osoby, právnické osoby či orgány veřejné moci a jiné veřejné subjekty. Tato informace je důležitá pro určení povinnosti jmenovat pověřence pro ochranu osobních údajů. Dalším bodem je počet zaměstnanců, kde jsou organizace rozděleny na ty, které nemají žádné zaměstnance, dále do 249 zaměstnanců a nad 250 zaměstnanců. Toto je jedna z informací, dle které se určuje zjištění povinnosti vytvářet záznamy činností o zpracování.

Posledním bodem k identifikaci organizace je zjištění vztahu organizace k osobním údajům. Je klíčové vědět, jestli organizace zpracovává osobní údaje, zda je pouze přijímá od jiné organizace, tzn. je příjemcem, či provádí zpracování na základě pokynů jiné organizace, tzn. je zpracovatelem, nebo zda určuje účely a prostředky zpracování, což organizaci činí správcem. V případě, kdy organizace nezpracovává žádné osobní údaje a nemá ani zaměstnance, nařízení GDPR se na ni nevztahuje. Na správce a zpracovatele se pak váží případné povinnosti.

**Uchovávání osobních údajů**

Organizace dále zanalyzuje problematiku uchovávání osobních údajů. Konkrétně se jedná o jejich formu, uložení a s tím související přistupování k údajům.

Důležité je, v jaké formě organizace osobní údaje uchovává. Může se jednat o umístění papírové podoby do archivu, či digitální podoby na cloudové řešení či lokální server, které mohou mít různé stupně zabezpečení. V případě listinné podobě se GDPR dokumentů s osobními údaji týká pouze pokud jde o evidenci fyzických osob. Takové dokumenty musí být v uzamčeném prostoru (zásuvka, skříň, místnost), do kterého mají přístup pouze pověřené osoby. Pokud se jedná o elektronickou formu, vztahuje se na úložiště řada bezpečnostních opatření, mezi základní patří např. zabezpečení kvalitním heslem, omezení přístupu a sledování činností v systému pomocí logovacích mechanismů.

Organizace by tedy měla mít přehled pozic v rámci organizační struktury a zároveň seznam rolí a přístupových oprávnění v informačním systému, které mají k osobním údajům přístup.

**Specifikace subjektů údajů a osobních údajů**

Pro tuto část analýzy je podstatné, aby organizace měla dostupné všechny potřebné informace k zodpovězení daných okruhů.

Organizace může osobní údaje získávat z formulářů na webových stránkách, uzavřením dohody nebo smlouvy, objednávky, prostřednictvím kamerového záznamu z prostor sídla firmy, na osobních schůzkách, apod. Organizace také nesmí zapomínat na to, že osobními údaji nejsou jen údaje o zákazníkovi, ale také o zaměstnancích, dodavatelích a ostatních třetích subjektech (pokud se nejedná o PO).

Zvláštní pozornost by měla organizace věnovat zpracování osobních údajů, které jsou definované v článku 9 (zvláštní kategorie OÚ, jako je rasový či etnický původ, sexuální orientace, zdravotní stav, a článku 10 (trestné věci a trestné činy), zpracování OÚ subjektů, kteří jsou zranitelní (děti – čl. 8, zdravotně postižení, sociálně znevýhodněni, pacienti, …), bližší informace k těmto problematikám se nacházejí v kapitole *Obecné zásady zpracování* této práce, a dalšímu zpracování či okolnostem, které vedou k zpřísnění povinností, které nařízení ukládá.

**Specifikace zpracování**

Důležitým aspektem pro identifikaci povinností a jejich rozsahu, dále také rizikovosti zpracování, jsou specifikace zpracování. Jedná se o konkretizaci četnosti zpracování, na kterém základě zpracování probíhá a v jakém rozsahu.

První specifikací zpracování, kterou je nutné zmapovat je tedy četnost zpracování. Zde lze uvažovat příležitostné zpracování, které neprobíhá na základě žádné pravidelnosti, plánování a jedná se tak o zpracování nahodilé. V opačném případě se jedná o zpracování systematické a pravidelné, jelikož se vyskytuje v souladu se systémem, jedná se o zpracování, které je předem naplánované a probíhá opakovaně či dokonce nepřetržitě. Příkladem může být poskytování a provozování telekomunikačních sítí, inteligentních měřičů apod. S tím souvisí i samotný rozsah zpracování. Ten je přímo v nařízení stanoven pouze obecně na rozsáhlé či ostatní, a teprve metodika Úřadu pro ochranu osobních údajů udává konkrétní hodnoty jednotlivých úrovní rozsahu pro tuzemské podmínky. Tyto úrovně jsou tedy tři, a to malý, střední a velký.

- Malý rozsah se týká zpracování osobních údajů méně než 5000 subjektů údajů nebo 0,5 % populace státu, s omezením přístupu k takovým údajům na maximálně dvě osoby anebo maximálně čtyřmi místy zpracování či pobočkami, a zároveň se jedná o zpracování na úrovni obce.
- Střední rozsah zpracování, je většího rozsahu než malý, a to s horní hranicí 10 000 subjektu údajů či 1 % populace státu, do 20 přistupujících osob, maximálně 20 pobočkami či místy zpracování a zároveň se jedná o zpracování na úrovni regionu nebo kraje.
- Velkým rozsahem zpracování se pak rozumí zpracováním nad tyto hranice a na úrovni státu.

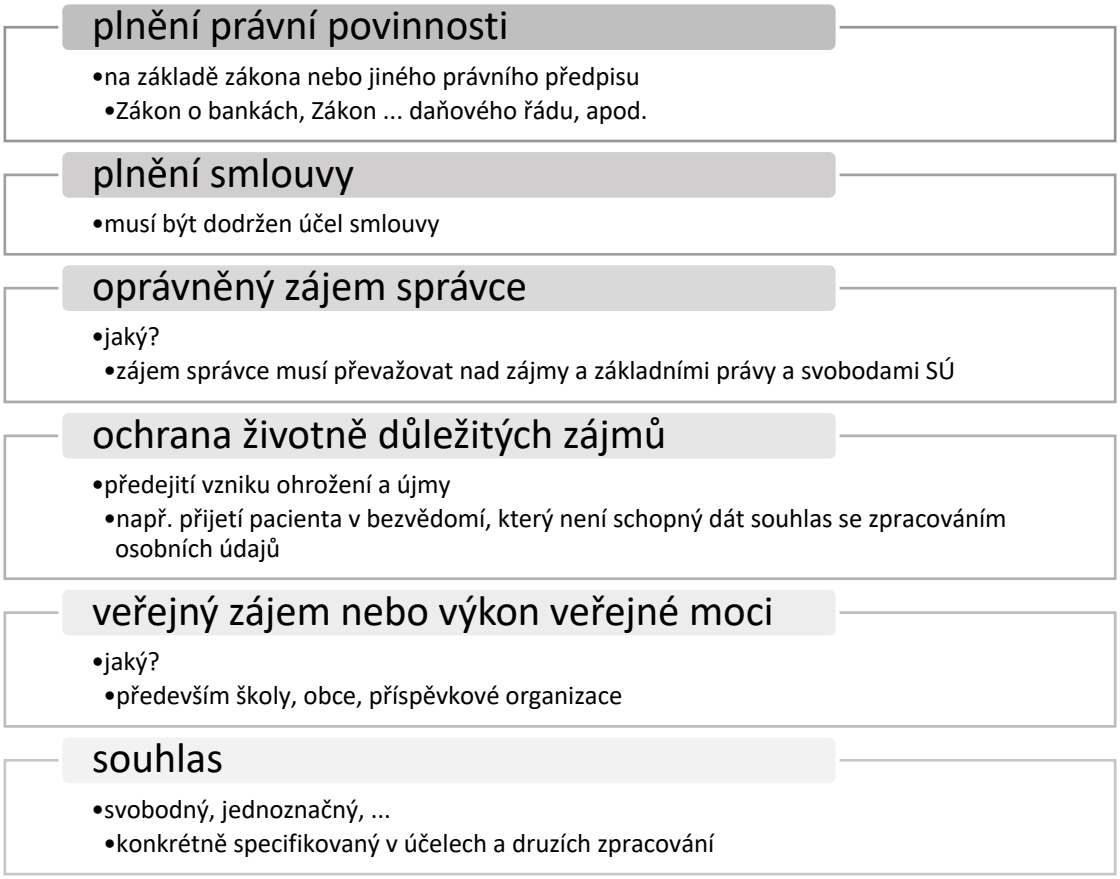
Další důležitou otázkou, je právní titul zpracování, jinak řečeno, na základě čeho zpracování probíhá. Pokud se zpracování resp. zkoumaný účel zpracování uskutečňuje za účelem plnění právní povinnosti, a je tak vyžadováno zákonem, při dodržení všech zásad toto zpracování nebude tak rizikové, jako při ostatních právních důvodech, samozřejmě s ohledem na ostatní aspekty. Správce ovšem musí mít přehled o tom, na základě jakého konkrétního právního předpisu zpracování probíhá. Zpracování na základě plnění smluvních povinností, oprávněného zájmu správce či ochrana životně důležitých zájmů není samo o sobě rizikové, ale má o něco složitější náležitosti. Pokud zpracování probíhá na základě plnění smluvních povinností, nesmí účel zpracování přesáhnout účel smlouvy, pokud se jedná o oprávněný zájem správce, musí být tento oprávněný zájem dobře konkretizován a musí mít větší váhu než zájmy a základní práva a svobody subjektu údajů pro daný případ.

Ochrana životně důležitých zájmů spočívá v předejití vzniku ohrožení a újmy, většiny správců se týkat nebude, příkladem může být přijetí pacienta v bezvědomí, který není schopný dát souhlas se zpracováním.

Dalšími právními tituly, které již jsou pro správce rizikovější, je zpracování pro plnění úkolu prováděného ve veřejném zájmu, který opět musí být přesně specifikovaný a bude se týkat především škol, obcí či příspěvkových organizací.

Dále je tedy zpracování na základě souhlasu subjektu údajů, které by mělo být využíváno v co nejmenším množství a jen pokud nemůže být vykonáno na základě jiného právního titulu. To z toho důvodu, že souhlas je vždy a kdykoli odvolatelný, což by mělo za následek buď ukončení zpracování a likvidaci údajů, případně by správce musel najít jiný právní titul. Souhlas také musí naplňovat všechny náležitosti, které jsou stanovené nařízením, především tedy to, že musí být svobodný, jednoznačný, subjekt údajů musí vědět, za jakým účelem takové zpracování probíhá a musí být informován o následcích případného nesouhlasu.

Následuje přehled právních titulů pro zpracování.




*Obrázek 3: Přehled právních titulů, zdroj: vlastní zpracování*

Dalším neméně důležitým hlediskem je to, jakou mírou může subjekt údajů zpracování ovlivnit, a to především co se týče výkonu práv či předání. I zde jsou rozeznávány tři úrovně ovlivnitelnosti, a to vysoká, omezená a minimální či žádná.

- Při vysoké úrovni ovlivnitelnosti může subjekt údajů bez problému prosazovat všechny své povinnosti, omezení ovlivnitelnosti může být časové anebo za vymezených podmínek, nebo omezení na uplatnění pouze některých práv, což souvisí se zákonným titulem ke zpracování, kdy zpracování může mít částečně vymezeno zákonem a zpracování musí probíhat v minimálním daném rozsahu.
- Neovlivnitelné zpracování či velice omezené, znamená nevymahatelnost některých práv či pouze dílčí vymahatelnost. Jedná se především o zpracování dané přímo právním předpisem, kterým může být např. při činnosti veřejné správy či daňových předpisech.

Poslední oblastí této části analýzy je přístupnost osobních údajů mimo hranice organizace. Zde lze rozeznávat údaje, které nejsou veřejně přístupné a jsou přístupné pouze správci či zpracovateli, případě orgánům veřejné moci ve vybraných případech, dále ty co jsou veřejně přístupné pouze omezené skupině či veřejně přístupné neomezenému počtu subjektů. Poslední dva případy si lze představit na příkladu sociální sítě, kdy určitý příspěvek může být přístupný pouze určitému okruhu uživatelů v rámci uzavřené skupiny či *přátel*, nebo se může jednat o příspěvek, který je viditelný všem.

**Předávání osobních údajů**

Některé povinnosti či specifikace nařízení jsou závislé na předávání údajů. Jedná se o předávání údajů. K předávání údajů dochází při využívání zpracovatele, při využití třetích stran, či při spolupráci se subjekty v zahraničí. Třetí stranou se rozumí ekonomický subjekt, který není správcem či zpracovatelem, ale má k údajům přístup či je přímo oprávněn je zpracovávat. Může se jednat o obchodního partnera, kterému organizace sdílí např. kontaktní údaje ze své databáze. Z pohledu GDPR je vnímáno zahraničí jako země, kde není GDPR účinné. Nejedná se tedy o země EU a další země, které nařízení přijaly viz kapitola *Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím* této práce.

Pro každé zpracování musí organizace vědět, jestli jsou údaje předávané dalším subjektům, kterými mohou být zpracovatelé např. externí účetní, provozovatel SW řešení, dodavatel aplikace pro e-shop nebo příjemci, což jsou organizace, které mají přístup k osobním údajům např. v rámci údržby informačních systémů, ale toto předávání osobních údajů není spojené s jejich zpracováním. Organizaci se pro tuto analýzu vyplatí vytvořit kompletní seznam využívaných služeb, mezi které může patřit cloudové řešení, rozhraní pro rozesílání hromadných mailů, účetní programy, reklamní systémy i např. využívané sociální sítě.

**Monitorování**

Tato část analýzy se věnuje monitorování, a to veřejně přístupných míst, či přímo subjektu údajů. Pro obě tyto činnosti platí, že se organizace vůbec týkat nemusejí, pokud žádné monitorování neuskutečňují.

Monitorování veřejně příslušných prostor pak lze vnímat ve dvou úrovních. Pokud se jedná o monitorování pozemků majitele, bytových domů, prodejen či malému okruhu veřejně přístupného prostranství, které je přilehlé k hlídanému objektu, nejedná se dle nařízení o žádné kritické zpracování. K němu už dochází, pokud se jedná o rozsáhlé monitorování velkého veřejného prostranství, kterým může být například letiště.

Co se týče monitorování subjektů, tak to metodika ÚOOÚ vnímá ve třech stupních, a to že daný subjekt údajů je monitorovaný, rozpoznatelný či lokalizovatelný ve vzestupném pořadí rizikovosti. O monitorované subjekty se jedná v případě např. záznamu životních funkcí pacientů, docházkové systémy či zvukové záznamy a toto monitorování není vnímáno kriticky. Významné už je ovšem monitorování takové, kdy je subjekt rozpoznatelný, a to pokud probíhá ve formě obrazových záznamů při ochraně majetku a zvyšování bezpečnosti, např. při využití běžného kamerového systému. Lokalizovatelný je subjekt, u kterého probíhá monitorování fyzického pohybu či pobytu apod. Toto monitorování již je kritické.

**Využitá řešení**

Další velmi podstatné informace pro implementaci GDPR tkví ve využívaných řešeních. Spadají sem IT systémy, rozsah využívání marketingu, webových stránek a e-shopu.

Tato část analýzy je v přiloženém dokumentu rozebírána spíše okrajově, jelikož se jedná o velmi specifickou oblast, kdy ani samotné nařízení nedefinuje konkrétní kroky či opatření, které má organizace podniknout. Jedná se tedy spíše o analýzu rizik možných kritických míst, na které by se měla organizace podrobněji zaměřit.

Jedná se o tvůrce a správce IT systémů, a to v pojetí interního či externího vývoje a správy. Dále je otázka charakteru využitých řešení v pojetí jejich známosti a vyzkoušení. Pokud se jedná o opětovně nasazené či „krabicové“ řešení, nejedná se o významný aspekt. O ten se jedná, pokud se jedná o nové řešení aplikované na již známé zpracování osobních údajů. Kritické pak je, pokud organizace využívá zcela nové řešení, které nebylo realizované ani mimo hranice organizace a nepojí se s ním tudíž žádné zkušenosti.

Jako další důležitou oblast ÚOOÚ vnímá složitost využívaných systému pro zpracování. Tři úrovně jsou následující, a to jednoduchý či složitý systém bez propojení na jiné zpracování, systém, který je propojený na více rozlišných zpracování, ovšem v rámci jednoho správce, a ostatní systémy, a to především expertní systémy s určitou mírou automatizace.

Další dotazy směřují na využití různých nástrojů, a to webových stránek, marketingu a e-shopu. Vždy se jedná o to, jestli je daný nástroj částečně automatizovaný, sbírá nějaká data, či úplně automatizovaný, který je schopný reagovat na konkrétní subjekt údajů profilovanými nabídkami dle historie chování subjektu, či se jedná o čistě jednoduchý, nedynamický nástroj.

**Výstupy tohoto kroku**

- specifikace práce s údaji,
- zmapování subjektů údajů a zpracovávaných osobních údajů,
- zjištění rizikových aspektů zpracování,
- zjištění nových povinností ukládaných nařízením.

## 13.3 Gap analýza

V zájmu zajištění celkového souladu s GDPR je více než vhodné provést Gap analýzu stávajícího stavu souladu s GDPR. Jedná se o analýzu tržních mezer, která je zaměřena na zjištění chyb, nedostatků či mezer mezi dvěma stavy, a to současným a požadovaným. Nejedná se tedy o nástroj, který by připravil konkrétní kroky pro kompletní implementaci nařízení jako takového, ale o analýzu, která určí chyby v současném zpracování a doporučí jejich řešení.

Předmětem této analýzy by měly být především smlouvy, interní směrnice a jiné právní akty v rámci organizace.

Gap analýza nařízení může být provedena ve dvou rozměrech, a to jako posouzení současného stavu a minima nutného souladu, tak posouzení současného stavu a doporučeného a bezpečného souladu. Poté záleží na organizaci, jaká úroveň souladu je pro ni přijatelná a realizovatelná.

Je nutné, aby tato analýza, především ve fázi doporučení, byla provedena v celkovém hledisku a při znalosti všech aspektů nařízení i okolností zpracování v organizaci. Nejčastější chybou může být to, že Gap analýza zjistí nesoulad s formou použitého souhlasu se zpracováním. Jedna varianta, jak tento nedostatek vyřešit, je vytvoření souhlasu, který je v souladu se zpracováním a od subjektu údajů ho znovu získat. V některých situacích je ovšem na místě, aby zpracování nebylo zaštítěno souhlasem, ale jiným právním důvodem pro zpracování, pokud takový právní důvod existuje. Zpracování na základě souhlasu není doporučené, jelikož takový souhlas je subjekt údajů oprávněn kdykoli odvolat.

Vyřešit zjištěný nesoulad tak nemusí vždy znamenat opravení použitých nástrojů, ale výběr nových, vhodnějších.

**Výstupy tohoto kroku**

- analýza nedostatků,
- doporučení pro jejich řešení.

## 13.4 Zavedení nových povinností

Nařízení mimo jiné definuje také nové povinnosti, jejichž rozsah či existence povinnosti v dané organizace je daná aspekty vyjmenované v nařízení. Výstupem předchozích kroků je mimo jiné identifikace těchto povinností. Jsou jimi posouzení vlivu na ochranu osobních údajů, záznamy o činnostech zpracování a jmenování pověřence pro ochranu osobních údajů.

To, zda se organizace týkají tyto povinnosti, identifikuje vyplnění přiloženého dokumentu.

**Posouzení vlivu na ochranu osobních údajů (DPIA)**

Toto posouzení je povinen správce vykonat před samotným zpracováním, a to především v případě, kdy určitý druh zpracování nese zvýšení rizika pro práva a svobody subjektu údajů či jiných osob. Opět je tato povinnost spojena s kategorií zpracovávaných údajů, dále také kategorií subjektů údajů, přesněji jejich zranitelností, velikosti rozsahu zpracování, monitorování veřejně přístupných prostor, automatizovaným rozhodováním a stupněm obtížnosti při uplatňování práv subjektu vzhledem k povaze zpracování.

Minimální rozsah toho, co posouzení má obsahovat, stanovuje nařízení a je součástí teoretické části, stejně tak přiloženého dokumentu, který obsahuje i ukázku, jak toto posouzení provést.

Toto posouzení je ovšem vhodné provést i v případě, že ho nařízení neudává jako povinnost. Pro organizaci tak vznikne analýza rizik a dopadů, přehled operací, které jsou rizikové a může je případně omezit, pokud zjistí, že dané zpracování pro ni není nezbytné a znamená pro ni významné riziko, které je ovšem snadno vyhnutelné.

**Záznamy o činnostech zpracování (ZČZ)**

Na stav, kdy má organizace povinnost vést záznamy o činnostech zpracování, má vliv několik aspektů, které jsou stanovené v teoretické části této práce. Jedná se o počet zaměstnanců, o kategorii zpracovávaných údajů, jestli zpracování probíhá systematicky a pravidelně, či riziko pro práva a svobody subjektu údajů. Poslední bod ve své podstatě znamená návaznost na povinnost provádět DPIA.

Náležitosti, které mají tyto záznamy splňovat, jsou taktéž součástí teoretické části této práce a liší se v některých bodech s ohledem na to, zda je organizace správcem osobních údajů či jejich zpracovatelem. Ukázka jedné z variant, jak lze tyto záznamy udržovat včetně příkladového vyplnění, je také součástí přiloženého dokumentu.

**Pověřenec pro ochranu osobních údajů (DPO)**

Povinnost jmenovat pověřence pro ochranu osobních údajů se týká všech veřejných subjektů či orgánů veřejné moci, těch správců a zpracovatelů, jejichž hlavní činnosti souvisejí se systematickým a pravidelným monitorováním subjektu, či rozsáhlým zpracováním osobních údajů dle článků 9 a 10.

Pověřenec by měl naplňovat určité profesní kvality především v oblasti ochrany osobních údajů a s tím spojenou legislativou, jak vnitrostátní, tak evropskou. Úroveň těchto znalostí a kvalit by měl být úměrný druhu zpracování, kategorii osobních údajů, kterých se zpracování týká, a také rozsahu zpracování. Pověřenec by se měl také dobře orientovat ve firemních procesech.

Organizace, která má povinnost jmenovat DPO, má možnost zvolit pověřence buď interního nebo externího či společného nebo samostatného. Všechny tyto možnosti mají své přínosy i nevýhody.

Interní pověřenec oproti externímu pověřenci má přínos v možnosti zvolit takového pracovníka, který má již vysokou znalost firemních procesů a způsobu zpracování osobních údajů v dané organizaci. Další výjimkou může být pro některé organizace exkluzivita daného pověřence. Oproti tomu v případě, že se organizace rozhodne využít externí služby zastoupení role pověřence prostřednictvím specializované FO nebo PO, nehrozí střet zájmů a poskytuje lepší zastupitelnost. Z pohledu ekonomického je pravděpodobnost větší výhodnosti interního pověřence, kdy potenciálně představuje nižší pravidelné náklady, ovšem je nutné počítat s počáteční investicí spojenou se vzděláním daného pracovníka v problematice GDPR a samotné ochrany osobních údajů.

Organizace může také využít společného pověřence, který působí ve více subjektech. Výhodou je bezesporu jednotnost dokumentace či procesů a jednotné kontaktní místo, což může být velmi výhodné pro skupinu podniků ve stejném odvětví či vlastněné jedním subjektem. Lze také předpokládat vyšší úroveň specializace a minimalizuje se tak odlišnost přístupů k ochraně. Ovšem společný pověřenec vyžaduje vyšší míru součinnosti ostatních správců a zpracovatelů ve skupině a pro organizaci může představovat riziko úniku interních informací.

Bez ohledu na to, kterou z těchto variant organizace zvolí, pověřenec musí být vždy nezávislý, a z toho důvodu by mě mít přímý přístup k co nejvyššímu vedení organizace, a jeho stanovisku by měl vždy být přidělený značný význam. Dalším podstatným požadavkem na roli pověřence je zamezení střetů zájmů. K tomu může dojít v případě, že osoba v roli pověřence by byla zároveň v některé vedoucí funkci či by přímo byla v pozici, kdy by mohla určovat účely a prostředky zpracování, či byla jiným zákonem vázána mlčenlivostí v záležitostech podstatných pro výkon pověřence.

Povinnostmi pověřence jsou pak vedení a poradenství v souvislosti s OOÚ, monitorování souladu s nařízením a jinými právními normami související s OOÚ, vedení záznamů činností, komunikace s dozorovým úřadem a subjekty údajů, vyjádření v případě tvorby DPIA. Další méně specifikovanou náplní práce pověřence je rozšiřování povědomosti o ochraně osobních údajů v organizaci, a to prostřednictvím zajišťování vzdělávání a

školení zaměstnanců, které by mělo zahrnovat také povědomí o informační bezpečnosti a dalších aspektech souvisejícími s ochranou dat a údajů, především z pohledu rizika lidského faktoru.

Podstatnou informací pro organizace je také to, že pokud je pověřenec firmou jmenován a je tato skutečnost oznámena i Úřadu pro ochranu osobních údajů, musí plnit všechny povinnosti dané nařízením.

**Výstupy tohoto kroku**

- posouzení vlivu na ochranu osobních údajů,
- záznamy o činnosti zpracování,
- jmenování pověřence.

## 13.5 Implementace navenek

Při samotné implementaci by organizace měla postupovat z vnějšku směrem dovnitř. V praxi to znamená, nejdříve splnit povinnosti nařízení, jejichž výstupy jsou veřejně dostupné, jako je informování o účelech zpracování, o existenci práv subjektů aj., a pak také následný výkon práv v případě požadavku subjektu údajů. Vzhledem k tomu, že se jedná o veřejně dostupné informace, případně informace, ke kterým má dle nařízení přístup každý subjekt údajů, a proto je případný nesoulad s touto částí nařízení snadno odhalitelný a tudíž pro organizaci nejrizikovější. Je tak klíčové, aby soulad s těmito povinnostmi, zajistila co nejdříve.

### 13.5.1 Informační povinnost

Jedním z práv, které je aplikováno automaticky a bez žádosti subjektu údajů, je právo na informace o zpracování údajů. Tuto povinnost může organizace plnit prostřednictvím webových stránek, textem souhlasu se zpracováním uvedeného ve smlouvě, všeobecných podmínek či jinou vhodnou formou. Ta by ovšem měla být především jednoduchá, srozumitelná a přehledná.

Nařízení tak dává subjektu údajů možnost snadno zjistit nesoulad zpracování svých osobních údajů, na který může danou organizaci upozornit. Přehled povinných informací, které musí správce poskytnout subjektu údajů je v následující tabulce.

| Informace, které musí organizace sdělit subjektu údajů | |
|---|---|
| **bez ohledu na zdroj** | Identifikační a kontaktní údaje na správce (a DPO) |
| | Účely zpracování a zákonné tituly |
| | Každý příjemce nebo kategorie příjemců |
| | Přesun dat do třetích zemí a poskytnuté záruky |
| | Doba uchování |
| | Existence práv subjektu údajů |
| | Právo na odstoupení od smlouvy kdykoli je to relevantní |
| | Právo na podání stížnosti dozorovému orgánu |
| | Informace o existenci automatizovaného rozhodování včetně možných důsledků |
| **od subjektu údajů** | zákonný nebo smluvní závazek, důsledek neposkytnutí osobních údajů |
| **jiný zdroj** | oprávněné zájmy správce nebo případné třetí strany |
| | kategorie osobních údajů |
| | zdroj (veřejně přístupný?) |

*Tabulka 8: Přehled informací sdělované subjektům údajů, zdroj: vlastní zpracování*

### 13.5.2 Výkon práv

Organizace by měla dále být schopna v odpovídající lhůtě vyřešit požadavky subjektu údajů související s výkonem jejich práv, jako je žádost o výmaz, přenos či úpravu, či informace o zpracovávaných údajích a účelech zpracování, a měla by mít pro tyto činnosti nastavené funkční opatření a procesy. Výkon těchto práv musí organizace uskutečnit bezodkladně, nejdéle však do jednoho měsíce. Tuto lhůta lze prodloužit o další dva měsíce, kdy o prodloužení a jeho důvodu musí být subjekt údajů informován.

Organizace by tedy měla mít jasně stanovené postupy a procesy, ideální je i využití formulářů pro žádost o výkon práv. Žádosti tak budou jednoznačně strukturalizované a jednodušeji vykonavatelné a zároveň tím splní povinnost subjektům výkon práv usnadnit. Ovšem je důležité, aby organizace našla rovnováhu mezi ulehčením výkonu práv a zároveň dostatečného zabezpečení, aby nedošlo k žádosti jinou osobou než subjektem

údajů. To je vždy přiměřeno k uchovávaným údajům a ostatním specifikacím zpracování. Pokud se jedná o zasílání newsletterů, stačí pro potvrzení identity přístup z dotčeného e-mailu, jedná-li se ovšem o údaje citlivé povahy, je vhodné využít např. dvoufaktorového ověření pomocí kódu zaslaného do SMS zprávy, prokázáním dokladem totožnosti při osobní návštěvě apod. Zároveň by výkon práv měl být umožněn obdobným způsobem jako např. samotné uzavření smlouvy[26].

**Výstupy tohoto kroku**

- informování subjektu údajů – především o účelech zpracování a právech subjektu,
- příprava procesů a případně rozhraní pro výkon práv.

## 13.6 Implementace celková

Pokud jsou splněny předchozí kroky, a organizace se rozhodla nařízení implementovat v širším či úplném rozsahu, může již přejít k dalším krokům. Těmi by měly být příslušné právní a technickoorganizační kroky.

### 13.6.1 Právní implementace

Pro soulad s nařízením GDPR je nutné aplikovat změny, ve větším či menším rozsahu i ve smluvních vztazích a jiných právních dokumentech. Jedná se především o smlouvy spojené se zaměstnanci, zákazníky, formulace souhlasů se zpracováním, s externími organizacemi, a také interní předpisy. Takové dokumenty jde tedy základně rozdělit na interní, které regulují vztahy a povinnosti uvnitř organizace, a na externí, které regulují vztahy mezi organizacemi či ostatními subjekty mimo organizaci.

#### Interní

Jak již bylo nastíněno, interní právní dokumenty lze rozdělit na ty, které upravují vztahy se zaměstnanci, dále upravující vztahy se zákazníky a v neposlední řadě na předpisy stanovující specifikace firemních procesů.

[26] Není přiměřené po subjektu údajů požadovat zaslání žádosti oficiálním dopisem, pokud uzavření smlouvy proběhlo on-line či přes telefon.

**Zaměstnanci**

Velké části organizací se bude týkat nařízení minimálně z důvodu ochrany osob v pracovním poměru. Ten totiž automaticky znamená, že organizace zpracovává osobní údaje. Ve většině případů ovšem není nutné zahrnutí účelů zpracování do smluv, jelikož se velmi často jedná o zpracování, které probíhá na základě právní povinnosti vyplývající ze vztahu zaměstnanec a zaměstnavatel.

Pokud ovšem organizace potřebuje zpracovávat osobní údaje zaměstnancům i pro účely, které nejdou zahrnout pod tento právní titul, je vhodné využít dodatků ke smlouvě či jiného způsobu rozšíření smluvních ujednání. Zaměstnavatel by se ale měl vyvarovat využívání souhlasu se zpracováním jako právního důvodu již z povahy vztahu zaměstnanec a zaměstnavatel. Velmi často by totiž takový souhlas byl v rozporu s nařízením, které definuje souhlas jako svobodný projev vůle, a to v případě, kdy případný nesouhlas může vést k újmě subjektu údajů. Pro většinu případů, tak správce musí mít jiný právní důvod než právě souhlas.

Dalším rizikem může být zpracování v souvislosti s využíváním ICT na pracovišti, kdy některá monitorování související s bezpečností jako je např. prevence kybernetických rizik, sice mohou být oprávněnými zájmy správce, ty ale nebudou převažovat nad soukromím zaměstnance.

Neopomenutelnou částí této problematiky je také zpracování údajů potenciálních zaměstnanců, zde se ovšem spíše jedná o organizační opatření než právní ošetření. Souhlas by zde mohl správce využít při zájmu kontaktovat osobu i s profilovanou nabídkou na jinou pozici.

Organizace by měla věnovat zvláštní pozornost případům, kdy zaměstnanci práci vykonávají v zahraničí. Zde platí obecné zásady pro předávání osobních údajů do zahraničí, kdy v případě zemí, kde platí nařízení GDPR, se jedná o minimální komplikaci, ovšem v případě třetích zemí musí být zaměstnavatelé obezřetní. Pokud země či organizace zajišťuje institucionální ochranu, nevyžaduje předání žádné větší opatření, pro ostatní platí značná omezení. Celou tuto problematiku lze najít v Kapitole V nařízení a její základní přehled v kapitole *Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím* této práce. Zaměstnavatel tuto problematiku také může

konzultovat s pověřencem pro ochranu osobních údajů, pokud byl jmenován, či přímo Úřadem pro ochranu osobní údajů.

### Interní směrnice

Je vhodné, aby organizace vydala či upravila interní směrnice či metodické postupy, které upravují zásady pro práci s osobními údaji, a to přímo či nepřímo. Pro zaměstnance jsou tak jasně dané zásady zpracování, a organizace má základ pro přípravu či úpravu firemních procesů pro další krok implementace.

## Externí

Problematika externích vztahů může být také velice rozsáhlá. V základním rozdělení lze rozlišovat dva druhy takových vztahů, a to vztahy s dodavateli a odběrateli, neboli zákazníky. U obou subjektů musí organizace zajišťovat jiné povinnosti. Zde lze opět zmínit, že se ochrana osobních údajů v rámci GDPR týká fyzických osob, tudíž organizace upravuje smlouvy a ostatní právní akty pouze jejich, ne právnických osob.

### Dodavatelé

Dodavateli budou především mzdové organizace, externí účetní, personalisté či smluvní lékaři. S těmito subjekty je nutné provést aktualizaci stávajících či zavedení nových smluv. Ty musí odpovídat požadavkům na zpracovatelské smlouvy, kdy je nutné, aby byla jasně daná odpovědnost za zabezpečení osobních údajů a pokyny pro práci s takovými údaji. Za zpracování osobních údajů je primárně zodpovědný správce, proto by měl velice pečlivě volit organizace, které pro jeho potřeby budou zpracování vykonávat.

### Zákazníci

Odběratelé jsou po zaměstnancích další skupinou subjektů údajů. Zde je důležité naplnit všechny povinnosti stanovené nařízením a změny promítnout i do smluvních dokumentů a prohlášeních. Organizace je povinna subjekt údajů informovat o jeho právech, kterými jsou získání potvrzení o zpracování, přístup k údajům, právo na přenos, omezení a vznesení námitky. Také je nutné subjekty informovat o účelech zpracování.

Podstatnou částí, která se aktualizace smluvních a jiných dokumentů týká je především revize souhlasu. Ten musí být mimo jiné především jednoznačně oddělený od ostatních

ustanovení a informací, nesmí k němu být donucen a jeho odvolání musí být stejně snadné jako jeho poskytnutí.

### 13.6.2 Technická a organizační implementace

Nezbytnou součástí zajištění souladu s nařízením, a také posledním krokem této implementace, jsou technická a organizační opatření. Je nutné zavést procesy, které budou v souladu se zásadami nařízení, které jsou definovány v kapitole *Obecné zásady zpracování* této práce. Implementace nařízení se týká také přizpůsobení použitých technologií, a to jak nástrojů a technologií, tak celých systémů.

## Procesy

V rámci organizace je mnoho procesů, které se přímo nebo nepřímo dotýkají zpracování osobních údajů. K zajištění toho, aby byly v souladu s nařízením, budou sloužit především organizační opatření a jejich správná úprava či zavedení pro organizaci znamená pokrytí standardní ochrany osobních údajů, tzv. *by default*. Ta se konkrétně týká interních procesů zpracování osobních údajů, a to minimalizace údajů využívaných pro daný účel, omezení přístupnosti údajů a nastavení a dodržování lhůt pro likvidaci údajů. Dále se jedná o organizaci vyřizování výkonů práv a požadavků subjektů údajů, zavedení či aktualizace procesů spojených s informační bezpečností či předávání OÚ třetím subjektům.

Organizace je také povinna zavést taková organizační opatření, aby pro dané účely byly využívány pouze ty osobní údaje, které jsou k jeho naplnění nezbytně nutné. V případě, že tento účel pomine, organizace musí podniknout kroky k likvidaci osobních údajů, pro jejíž zpracování nemá zákonný důvod. Interní předpisy by také měly stanovit, jak se budou osobní údaje likvidovat, a to jak v případě listinných dokumentů, tak těch elektronických.

#### Ohlašovací povinnost

Organizace musí být také procesně připravena na ohlašovací povinnost v případě porušení zabezpečení, a to jak subjektu údajů, tak dozorovému úřadu. Pokud správce zjistí či je informován o určitém bezpečnostním incidentu, v prvním kroku zjistí, zda došlo k porušení zabezpečení osobních údajů. Pokud ano, tak provede vyhodnocení rizika

pro fyzické osoby. V případě, že je pravděpodobné riziko pro práva a svobody fyzických osob, je nutné vyrozumět dozorový úřad. Pokud je toto riziko značné, a dozorový úřad neurčí jinak, je nutné vyrozumět i dotčené fyzické osoby. Každé porušení zabezpečení, i v případě kdy nehrozí riziko fyzickým osobám, správce zaeviduje.

Při posuzování rizika musí brát správce ohled na typ porušení, a to jestli se jedná např. o ztrátu či porušení důvěrnosti, kategorie a rozsah dotčených osobních údajů, pravděpodobnost identifikace totožnosti, počet dotčených osob, či všechny ostatní aspekty, které rizika mohou v daném případě ovlivnit.

**Informační bezpečnost**

Ohlašovací povinnost již spadá do procesu informační bezpečnosti, a to detekce a reakce na bezpečnostní incident. Problematika informační bezpečnosti je velice rozsáhlá a pro některé organizace vzhledem k rozsahu zpracování a povaze osobních údajů bude znamenat vhodné vyřešení této problematiky v souladu s některými normami, jako např. ISO 2700x. Zajištění základu informační bezpečnosti je zároveň nutný pro zajištění souladu s nařízením. Jedná se o zajištění důvěrnosti, integrity a dostupnosti. Osobní údaje by tak měly být dostupné pouze autorizovaným osobám, které mají k přístupu oprávnění, měla by být zajištěna ochrana před zničením či úpravou dat bez oprávnění, a údaje by měly být ochráněné před záměrně poškozujícím omezením přístupu. Dalšími základními principy informační bezpečnosti je politika prázdného stolu, kdy by zaměstnanec či jiná odpovědná osoba neměl opouštět své pracovní místo bez jeho zabezpečením odhlášením od systémů a zabezpečení listinných dokumentů. Dalším nezbytným procesem je nastavení politiky hesel, a to jejich nucenou obnovou po uplynutí určité lhůty a stanovení pravidel pro jejich tvorbu (malá a velká písmena, použití číslice či speciálního znaku, minimální počet znaků).

Všechny principy by měla organizace využívat i při předávání osobních údajů třetím subjektům, a to především principy minimalizace osobních údajů.

## Zabezpečení informačních systémů

Ve většině organizacích bude velký podíl zpracování osobních údajů probíhat v informačním systému. Je nutné zajistit, aby jejich zabezpečení bylo v souladu s nařízením. Zde lze rozeznávat dvě úrovně, a to externí a interní informační systémy.

Tyto dvě řešení se budou v určitých úrovních prolínat, ovšem u každého je důležité se zaměřit na relevantní problematiky. V obou případech by ovšem měla být zavedena vhodná technická opatření, kterými může být např. anonymizace.

**Externí informační systémy**

Při využívání externích řešeních, kterými je např. využívání cloudu či jakéhokoliv externího informačního systému, je nutné zjistit soulad dodavatele s nařízením. Většina subjektů, které taková řešení nabízí, kterými jsou např. poskytovatele úložiště, bude nutné uzavřít smluvní vztah na úrovní správce a zpracovatele. Jak stanovuje nařízení, nemusí se jednat přímo o zpracovatelskou smlouvu, ale musí být jasně dané podmínky, co je dodavatelská firma povinna dodržovat, za které rozpory s nařízením ponesou odpovědnost a ostatní povinné náležitosti stanovené nařízením.

Co se týká zabezpečení externích informačních systémů, organizaci, která dané systémy využívá, by při zjišťování vhodnosti daného řešení, měla brát v úvahu několik aspektů. Mezi ně patří to, zda daný systém řádně provádí logování, a to jak úspěšných, tak neúspěšných pokusů a jakékoliv činnosti spojené s osobními údaji. V případě určitého počtu neúspěšných pokusů o přihlášení by měla nastávat blokace. Další zkoumanou oblastí by mělo být šifrování a zálohování. Dodavatel by také měl zajistit řešení problémů v přiměřené reakční době a instrukce pro případ napadení systému.

**Interní informační systémy**

Pokud si organizace IT systémy řeší sama, nebude se jí týkat problematika zpracovatelské smlouvy či obdobného právního dokumentu. Zároveň to ale znamená rozšíření odpovědnosti o zabezpečení daného systému. Zvláštní pozornost je nutné věnovat pokud organizace využívá vlastního firemního serveru. Ten by měl splňovat také otázku fyzické bezpečnosti, kdy by jeho umístění mělo být situováno do uzamykatelné místnosti s omezeným přístupem pro minimalizaci hrozby zničení či poškození. I tohoto řešení se týká problematika šifrování, a to jak dat samotných, tak i jejich přenosu. Dále je ovšem nutné řádně provozovat i antivirovou ochranu či firewall a především pravidelné aktualizace použitého operačního systému. Přibývá také odpovědnost za administrátorské účty, které by měly být poskytnuté jen zodpovědným osobám, kterými můžou být správci ICT či majitel, a jejich řádné oddělení.

**Anonymizace**

Většina organizací se bude potýkat s nutností využití vhodných technických opatření, které mohou souviset především s uložení údajů svých zákazníků a vzhledem k nařízení bude nutné provést opatření tak, aby se k takovým údajům nedostal nikdo nepovolaný. Jedno z možných řešení, je využití anonymizace. Tu lze vykonat třemi základními přístupy:

1. Dynamic Data Masking (DDM),
2. Anonymizační Framework v konkrétní aplikaci (např. SAP),
3. Ničení dat.

Ničení dat je nejúčinnější, co se minimalizace rizika prolomení týče, nicméně v mnoha situacích může být velice nevýhodné v celkovém důsledku. Využití anonymizačního Frameworku bude patrně nejpohodlnější metodou, ovšem je závislé na využití konkrétní aplikace a vhodnosti jejího řešení. Dalším z řešení může být právě Dynamic data masking, a to pro případ, kdy organizace nechce data individuálně anonymizovat, ale pouze skrývat.

Na úrovni databáze lze obsah sloupců, které budou obsahovat osobní údaje, zamaskovat a jejich obsah pak bude zobrazován pouze částečně. Data uvidí pouze ten, komu bude přiřazeno oprávnění UNMASK.

Maska pak je zachována i při obnově databáze, protože maska je definována ve sloupcích tabulky. Masky umožňují příkazy DELETE, UPDATE, INSERT (Smazat, Aktualizovat, Vložit) do tabulky, pokud má uživatel oprávnění provádět tyto změny.

Služba DDM se používá u uživatelů při importu a exportu, takže uživatelé, kteří nemají povoleno vidět nemaskovaná data, je neuvidí ani při těchto operacích (např. při importu do Excelu).

DDM nelze použít pro sloupce, který je vytvořen výpočtem, ale pokud takový vypočítaný sloupec obsahuje operaci s maskovaným sloupec, vypočítaný sloupec bude také maskovaný.

DDM by nemělo být považováno za 100% nerozbitné. Služba DDM má zabránit náhodnému vystavení dat neoprávněným uživatelům. Je pravděpodobné, že útočník by mohl postavit útok na hrubé síle (brutal force attack) tak, aby obešel masku.

Pro konkrétní uživatele (role) je omezen výstup dat například, jak je uvedeno na následujícím obrázku.

| | Emp_ID | Emp_First_Name | Emp_Last_Name | Emp_Date_Of_Birth | Emp_Salary | Emp_Email | Emp_Employment_Date |
|---|---|---|---|---|---|---|---|
| 1 | 1 | Jerome | xxxx | 1981-07-17 01:34:14.000 | 2598 | gXXX@XXXX.com | 1995-08-28 01:22:48.000 |
| 2 | 2 | Roland | xxxx | 1989-10-13 02:02:51.000 | 2036 | qXXX@XXXX.com | 1994-08-13 04:23:04.000 |
| 3 | 3 | Ernest | xxxx | 1980-10-18 17:29:27.000 | 1332 | rXXX@XXXX.com | 2002-07-27 03:34:44.000 |
| 4 | 4 | Jorge | xxxx | 1984-09-09 04:31:38.000 | 1666 | sXXX@XXXX.com | 2002-11-16 15:17:01.000 |
| 5 | 5 | Marvin | xxxx | 1990-08-31 13:00:52.000 | 872 | eXXX@XXXX.com | 1998-01-14 12:19:23.000 |
| 6 | 6 | Stella | xxxx | 1979-10-26 18:11:24.000 | 2046 | sXXX@XXXX.com | 1995-08-17 12:09:45.000 |
| 7 | 7 | Salvador | xxxx | 1982-11-29 06:07:52.000 | 1278 | iXXX@XXXX.com | 1995-08-11 14:02:47.000 |
| 8 | 8 | Aaliyah | xxxx | 1993-06-17 15:00:30.000 | 705 | iXXX@XXXX.com | 2015-11-19 19:12:36.000 |
| 9 | 9 | Lawrence | xxxx | 1984-10-11 15:51:25.000 | 1745 | qXXX@XXXX.com | 1991-07-07 15:07:18.000 |
| 10 | 10 | Nicholas | xxxx | 1983-04-24 18:11:34.000 | 2772 | cXXX@XXXX.com | 1996-07-31 13:25:07.000 |
| 11 | 11 | Alex | xxxx | 1986-01-15 04:45:37.000 | 2090 | vXXX@XXXX.com | 2014-05-05 18:24:51.000 |
| 12 | 12 | Ray | xxxx | 1990-12-06 00:40:41.000 | 1871 | pXXX@XXXX.com | 2007-07-06 16:58:06.000 |
| 13 | 13 | Gilbert | xxxx | 1994-06-22 20:36:18.000 | 2339 | uXXX@XXXX.com | 2007-01-24 00:36:38.000 |
| 14 | 14 | Aria | xxxx | 1996-02-20 15:36:23.000 | 1095 | yXXX@XXXX.com | 2012-10-20 02:46:23.000 |
| 15 | 15 | Edward | xxxx | 1991-12-26 04:01:08.000 | 1569 | kXXX@XXXX.com | 2006-08-14 10:39:27.000 |

*Obrázek 4: Ukázka aplikace DDM, zdroj: vlastní zpracování*

Toto řešení umožňuje např. pro telefonní operátory při kontaktu s klientem pouze částečně ověřovat osobní údaje (email, rodné číslo atp.). Totéž funguje i pro exporty takových dat do Excelu, případně jinam.

Zjištění masek sloupců pro přehled v databázi:

```
SELECT TBLS.name as TableName,MC.NAME ColumnName, MC.is_masked IsMasked,
MC.masking_function MaskFunction
FROM sys.masked_columns AS MC
JOIN sys.tables AS TBLS
ON MC.object_id = TBLS.object_id
WHERE is_masked = 1;
```

| | TableName | ColumnName | IsMasked | MaskFunction |
|---|---|---|---|---|
| 1 | Employee_Financial | Emp_First_Name | 1 | partial(3, "XXXX", 3) |
| 2 | Employee_Financial | Emp_Last_Name | 1 | default() |
| 3 | Employee_Financial | Emp_Salary | 1 | random(1, 9) |
| 4 | Employee_Financial | Emp_Email | 1 | email() |

*Obrázek 5: Výstup při zjištění masek sloupců v databázi, zdroj: vlastní zpracování*

# 14 Shrnutí výsledků

Srovnání zákona 101/200 Sb. a GDPR shrnuje hlavní změny na posílení působnosti, informační povinnosti správce vůči subjektům údajům, existence nových práv, jako je právo být zapomenut či přenositelnost údajů, posílení bezpečnosti a vznik nových povinností, mezi které patří jmenování pověřence pro ochranu osobních údajů a posouzení vlivu na ochranu osobních údajů, které je výjimečné v tom, že nutí správce zkoumat rozsah dopadů pro samotný subjekt údajů nikoli jeho samotného či celou společnost. Další neopomenutelným rozdílem je sjednocení legislativy pro EU, spolupráci dozorových orgánů a zvýšení sankcí. Oproti tomu nařízení přejímá většinu hlavních definic, zásad, práv a povinností, omezení předávání osobních údajů do třetích zemí a důležitost výjimek pro specifická zpracování, které jsou prováděna za účelem archivnictví, statistiky, vědy či historie.

Analýza právních titulů ke zpracování v korporátních subjektech ukázala, že oba ekonomické subjektu provedli implementaci v souladu s GDPR, ale rozdílným způsobem. Společnost T-Mobile má pro každý účel zpracování konkrétní titul, oproti tomu ČEZ má několik titulů sloučených pro jeden účel. Výstupy této analýzy ovšem poskytly přínosný základ a nové poznatky pro tvorbu návodného postupu pro implementaci. Obě implementace potvrdily, že nařízení je obecné a umožňuje vlastní zpracování samozřejmě v mezích nařízení, jak je uvedeno v kapitole *Vyhodnocení analýz*.

Návodný postup pro implementaci byl tvořen několika fázemi a při jeho tvorbě byly využity různé znalosti z teorie a zároveň vycházel z analýzy nad společností T-Mobile a ČEZ. Pro správný postup implementace nařízení do současných procesů organizace nelze konstatovat, že je některá z fází méně či více podstatná. Je důležité dodržet předem stanovený postup, který může být samozřejmě v jednotlivých organizacích modifikován a nemusí být dodrženy navrhované fáze. Fáze slouží jako vodítko pro implementaci a jsou právě návodné. Pro jednodušší orientaci je součástí této kapitoly i příloha *19.1 Excel – Nástroj pro analytickou část implementace GDPR*, který je součástí druhé fáze zavádění Životní cyklus údajů v organizaci a při implementaci může být v této fázi použit.

# 15 Závěry a doporučení

Cíl nařízení GDPR je orientován na zvýšení práva na ochranu občanů (EU) s důrazem na větší vymahatelnost těchto práv. V kontextu informační společnosti se tak jedná o velmi přínosné nařízení jak z pohledu jednotlivce (subjektu údajů), tak z pohledu celé informační společnosti, které jednoznačně určuje pravidla pro využívání a nakládání s osobními údaji občanů, klientů apod. Tato z první pohledu komplikace pro jednotlivé organizace, však přináší možnost vytvořit jednoznačná pravidla a upravit interní procesy tak, aby odpovídali dnešním standardům z pohledu ochrany osobních údajů, ale i ochrany informací např. dle ISO 27001. Při rozebírání této problematiky je důležité zmínit, že nelze opomíjet roli subjektu údajů, který by měl vystupovat v problematice ochrany svých osobních údajů aktivně a zjištěné nesoulady nahlašovat správci případně dozorovému úřadu.

Cílem této práce bylo uvést čtenáře do problematiky ochrany osobních údajů. To zahrnovalo představení hlavních aspektů nařízení a nového adaptačního zákona, který konkretizuje určité části nařízení a upravuje ho tak pro tuzemské podmínky. Po získání těchto znalostí bylo možné provést komparaci této legislativy se zákonem 101/2000 Sb., a tím tak zmapovat změny, které GDPR přináší.

Pro názornou ukázku implementace řešení byla provedena analýza účelů zpracování ve dvou veřejně známých subjektech, která názorně ukázala možnost rozdílného zpracování jedné části nařízení se současným zajištěním souladu u obou subjektů.

Hlavním výstupem práce je návodný postup pro implementaci nařízení v organizaci. Tento výstup se skládá ze dvou částí, a to návodného postupu v textové podobě, který je doplněný interaktivním dokumentem, který organizace může využít jako pomocný nástroj, který identifikuje případné povinnosti pro organizaci, kterými jsou povinnost jmenovat pověřence pro ochranu osobních údajů, posouzení vlivu na ochranu osobních údajů a vedení záznamů činností o zpracování. Současně organizaci poskytne identifikaci hlavních krizových bodů, na které by se organizace měla zaměřit.

Všechny části této práce byly konzultovány s odborníkem na GDPR pro zajištění správnosti informací a interpretace jednotlivých částí nařízení a pro vytvoření použitelného nástroje, který potenciálně může vybraným organizacím a institucím usnadnit získání přehledu o této problematice a přípravu implementace tohoto nařízení.

# 16 Seznam literatury

[1] MATOUŠOVÁ, Miroslava. *Ochrana osobních údajů v otázkách a odpovědích: 73 otázek a odpovědí*. Vyd. 1. Praha: ASPI, 2004. Otázky a odpovědi z praxe. ISBN 978-80-7357-037-8.

[2] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[3] NEŠČÁKOVÁ, Libuše. *Pracovní právo pro neprávníky: rozbory vybraných ustanovení, praktická aplikace, vzory a příklady*. 1. vyd. Praha: Grada, 2012. Právo pro každého. ISBN 978-80-247-4091-1.

[4] EVROPSKÝ PARLAMENT A RADY EU. *Obecné nařízení o ochraně osobních údajů*. 27. duben 2016

[5] *Zákon č. 110/2019 Sb., o zpracování osobních údajů - EU*. 10. duben 2019

[6] MANAGEMENTMANIA. Pseudonymizace (Pseudonymisation). *ManagementMania.com* [online]. [vid. 2019-04-28]. Dostupné z: https://managementmania.com/cs/pseudonymizace-pseudonymisation

[7] ČESKÁ SPOŘITELNA, A. S. *Zásady zpracování osobních údajů v České spořitelně, a.s.* [online]. [vid. 2018-10-29]. Dostupné z: https://www.csas.cz/cs/zasady-zpracovani-osobnich-udaju

[8] INTERNET MALL, A.S. *Souhlas se zpracováním osobních údajů* [online]. 16. srpen 2018 [vid. 2018-10-29]. Dostupné z: https://www.mall.cz/osobni-udaje-platba-splatky

[9] HEJLÍK, Ladislav. *Mysterium pojmu ‚zpracování'. Nepochopení GDPR přineslo absurdní obavy | Právo a justice | Lidovky.cz* [online]. [vid. 2019-04-14]. Dostupné z: https://www.lidovky.cz/byznys/pravo-a-justice/mysterium-pojmu-zpracovani-nepochopeni-gdpr-prineslo-absurdni-obavy.A181110_192616_ln_byznys_pravo_ssu

[10] MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. *Metodika GDPR* [online]. [vid. 2018-10-29]. Dostupné z: http://www.msmt.cz/file/44569/

[11] GUARD7. *Výpis z rejstříku trestů a GPDR* [online]. [vid. 2019-04-17]. Dostupné

z: http://www.guard7.cz/gdpr/vypis-z-rejstriku-trestu-a-gpdr

[12] BARTÍK, Václav a Lenka SUCHÁNKOVÁ. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 1. vyd. Praha: Leges, nedatováno. Praktická právnická příručka. ISBN 978-80-7502-288-2.

[13] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *GDPR (obecné nařízení)* [online]. [vid. 2019-03-23]. Dostupné z: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

[14] MINISTERSTVO VNITRA. *Návrh zákona o zpracování osobních údajů* [online]. [vid. 2018-10-29]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

[15] *Zákon č. 101/2000 Sb., o ochraně osobních údajů*. 25. duben 2000

[16] ÚOOÚ. *Ochrana osobních údajů jako základní hodnota EU* [online]. [vid. 2018-10-29]. Dostupné z: https://www.uoou.cz/dokumenty-k-gdpr/ds-4720/p1=4720

[17] T-MOBILE CZ, A.S. *Zásady ochrany osobních údajů - T-Mobile CZ* [online]. [vid. 2018-12-05]. Dostupné z: https://www.t-mobile.cz/ochrana-udaju/zasady-ochrany-osobnich-udaju

[18] POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY. *Sněmovní tisk 138* [online]. [vid. 2019-04-24]. Dostupné z: http://www.psp.cz/sqw/historie.sqw?o=8&t=138&snzp=1

# 17 Seznam obrázků

# 18 Seznam tabulek

# 19 Přílohy

## 19.1 Excel – Nástroj pro analytickou část implementace GDPR

Úplná interaktivní podoba této přílohy je přiložena v externích přílohách. Zde je pouze ukázka výstupu.

| Účel zpracování | | | | | | |
|---|---|---|---|---|---|---|
| **Problematika** | **A** | **B** | **C** | **D** | **Odpověď** | **Má vliv na:** |
| **Specifikace ekonomického subjektu** | | | | | | |
| Jedná se o | **FO** | **nekomerční sdružení (zájmové spolky, kluby či ostatní nevýdělečné organizace)** | **podnikající FO nebo PO** | **orgán veřejné moci či veřejný subjekt** | | DPO |
| Počet zaměstnanců | | **0** | **1-249** | **250+** | | ZČZ |
| Organizace | **nezpracovává osobní údaje**<br>v žádné části jakéhokoli procesu organizace nepřijde do styku s osobními údaji, neuchovává je, nenahlíží do nich, ani s nimi nijak nemanipuluje | **přijímá osobní údaje (příjemce)**<br>osobní údaje jsou organizaci poskytnuty, ta ovšem zpracování ani neurčuje, ani neprovádí | **zpracovává osobní údaje jiných organizací (zpracovatel)**<br>osobními údaji shromážděné jinou organizací provádí operace na základě pokynů | **určuje účely a prostředky zpracování (správce)**<br>organizace nakládá s osobními údaji bez nutnosti souhlasu jiné organizace, osobní údaje využívá pro své potřeby, určuje jaké operace s osobními údaji budou prováděné, na základě jakého právního titulu zpracování probíhá a pro jaký účel | | |
| **Uchovávání osobních údajů** | | | | | | |
| Forma osobních údajů | | **listinné** | **elektronické** | **obě varianty** | | |
| Úložiště | | **lokální - PC, mobil, tablet, papírové dokumenty** | **server organizace** | **on-line - služba (externí systém), cloud** | | |
| Přístupy v rámci organizace | | **pouze pro osoby pověřené zpracováním** | **omezenému počtu osob** | **neomezenému počtu osob** | | |
| **Specifikace subjektů údajů a osobních údajů** | | | | | | |
| Zdroj osobních údajů | | **přímo od dané osoby (subjektu údajů)** | **jiný** | **obě varianty** | | |
| Kategorie subjektu údajů | | **běžné osoby**<br>osoby bez zvláštní zranitelnosti | **osoba není identifikována**<br>organizace nemá dostatek osobních údajů k jednoznačené identifikaci subjektu údajů | **zranitelné osoby**<br>osoby, které mohou být zpracováním více poškozené - děti, pacienti, zdravotně postižení, žadatelé o azyl, sociálně slabí apod. | | DPO |
| Kategorie osobních údajů | | **běžné údaje**<br>účast na běžných akcích, úroveň vzdělání, popis praxe, ostatní obecné vzhledové a osobnostní charakteristiky, prosté obrazové záznamy, nejedinečné údaje apod. | **významné údaje**<br>údaje znamenající poškození cti či pověsti v případě úniku, přístupové údaje, pseudonym, zaznamenané přestupky/pokuty, účast na některých specifických akcích, jedinečné identifikační údaje např. jméno, příjmení, RČ, číslo OP apod. | **kritické údaje**<br>údaje spadající do čl 9, 10, vysoce osobní povahy, historie navštívených stránek, finanční údaje, údaje o zařízení, o uskutečněných voláních | | DPIA |
| Zvláštní kategorie osobních údajů - čl. 9 | | **nezpracovány** | **zpracovány** | **rozsáhle zpracovány** | | DPIA, DPO, ZČZ |
| Údaje o trestních věcech - čl. 10 | | **nezpracovány** | **zpracovány** | **rozsáhle zpracovány** | | DPIA, DPO, ZČZ |
| Kategorie subjektu údajů z pohledu zařazení do vymezené skupiny a možné ohrožení z okolního prostředí | | **subjekty nejsou součástí vymezené skupiny** | **subjekty jsou součástí vymezené skupiny s omezenou zranitelností**<br>časově omezená nebo situačně daná - subjekty jsou např. nemocní či staří lidé, děti, mladiství, studenti, či žadatelé vůči veřejné správě, příjemci zdravotních a sociálních služeb, odběratelé specifického zboží | **subjekty jsou součástí vymezené skupiny se stálou zranitelností**<br>zranitelnost se není omezená časem či danou situací, subjekty, které jsou vymezné dle údajů spadajících do čl.9 - sexuální orientace, národnost apod.) či odsouzení pro trestný čin | | DPIA |
| **Specifikace zpracování** | | | | | | |
| Zpracování je: | | **příležitostné** | | **systematické a pravidelné**<br>vyskytující se v souladu se systémem, předem naplánované, organizované nebo metodické, odehrávající se jako součást obecného plánu, provedené jako součást strategie, po určité období v určitých intervalech, opakované, nepřetržité | | DPO |
| Rozsah zpracování | | **malý**<br>méně než 5000 / 0,5% populace<br>do 2 přistupujících<br>1-4 míst zpracování<br>obec | **střední**<br>5 001-10 000/0,5-1% populace<br>2-20 přistupujících<br>5-20 míst zpracování<br>region, kraj | **velký**<br>od 10 001 / 1,0% populace<br>více než 20 přistupujících osob<br>více než 20 míst zpracování<br>státní | | DPIA, DPO |
| Zpracování probíhá na základě | | **plnění právní povinnosti** | **plnění smluvních povinností, oprávněný zájem správce, ochrana životně důležitých zájmů** | **souhlas, plnění úkolu prováděného ve veřejném zájmu** | | |
| Možnost subjektu údajů ovlivnit specifikace zpracování a uplatňování svých práv (právo na výmaz, právo vznést námitku apod.) | | **vysoká**<br>subjekt bez problému prosazuje svá práva daná nařízením | **omezená**<br>svá práva může uplatňovat jen částečně, v omezeném časovém úseku nebo za vymezených podmínek – zpracování k uplatnění práv a povinností vyplývající ze zákona – uzavírání smluvních vztahů | **minimální či žádná**<br>svá práva může uplatňovat jen dílčím způsobem či vůbec nelze ovlivnit prosazení práv daná nařízením | | DPIA |
| Přístupnost osobních údajů mimo hranice organizace | | **nejsou veřejně přístupné - přístupné pouze správci nebo zpracovateli (a orgánům veřejné moci na základě právních předpisů)** | **omezenému počtu subjektů - dostupné pouze předem vymezené skupině** | **neomezenému počtu subjektů - např. na základě právních předpisů** | | DPIA |
| **Předávání osobních údajů** | | | | | | |
| Využívá organizace zpracovatele? | | **ne** | **ano, vazby jsou jednoznačně vymezené** | **ano, vazby nejsou jednoznačně vymezené** | | DPIA |
| Předání třetím stranám | | **ne** | **ano, subjekt údajů je informován** | **ano, subjekt údajů není informován** | | |
| Předání do třetích zemí a mezinárodním organizacím | | **ne** | **ano, do zemí zajišťující institucionální bezpečnost** | **ano, do ostatních zemí** | | |
| **Monitorování** | | | | | | |
| Monitorování veřejně přístupných prostor | | **neprobíhá** | **ano**<br>probíhá na pozemcích majitele, bytových domech, průmyslových objektech, prodejnách, 1-1,5m veřejného prostranství, či těsně přilehlé k monitorovanému objektu | **ano, rozsáhlé**<br>kamerové systémy monitorující ve velkém rozsahu veřejná prostranství, např. letiště | | DPIA |
| Monitorování subjektu údajů | **neprobíhá** | **monitorované**<br>monitorování prostřednictvím jedinečných identifikačních údajů – záznam životních funkcí pacientů, docházkové systémy, zvukové záznamy, záznamy z činnosti subjektů na síti | **rozpoznatelné**<br>monitorování ve formě obrazových záznamů za účelem ochrany majetku a zvýšení bezpečnosti jako běžný kamerový systém | **lokalizovatelné**<br>monitorování fyzického pohybu nebo pobytu identifikovatelných SÚ, lokalizace subjektu, nepatří sem zvukové záznamy pro smluvní účely | | DPIA |
| **Využívaná řešení** | | | | | | |
| Používané IT systémy jsou vyvinuté a spravované: | | **přímo společností** | **externím dodavatelem** | **obě varianty** | | |
| Využití nových technologických nebo organizačních řešení | | **již nasazené řešení známého zpracování** | **nové řešení již známého zpracování** | **zcela nové řešení, doposud nerealizované zpracování** | | DPIA |
| Použitý systém pro zpracování | | **jednoduchý nebo složitý systém bez propojení na jiná zpracování**<br>zřetězení operací s proměnlivými nebo vícenásobnými vazbami | **s propojením na jiná zpracování stejným správcem**<br>zejména zpracování se slučováním/sdružováním údajů získaných za různými účely | **automatizované expertní systémy**<br>analýza, profilování, veškeré automatizované zpracování | | DPIA |
| Využití marketingu | | **ne** | **ano, pasivní** | **ano, aktivní, profilovaný (na míru)** | | |
| Využití webových stránek | **ne** | **pouze informativní webové stránky, bez formulářů či sledování uživatele resp. bez identifikace** | **jednoduché formuláře pro kontaktování pomocí e-mailu, žádné statistiky či cizí scripty, pokud cookies, tak pouze výkonnostní či relační** | **lze se zaregistrovat, použití analytik anebo cizích skriptů, cookies i reklamní a trvalá** | | |
| Využití e-shopu | | **ne** | **ano, bez historie, bez registrace** | **ano, historie - předchozí nákupy, návštěvy, remarketing** | | |

## 19.2Úplné kategorie údajů pro kapitolu 12

| | | T-Mobile | ČEZ |
|---|---|---|---|
| A | identifikační údaje | titul,<br>jméno a příjmení,<br>rodné číslo,<br>datum narození,<br>IČO, DIČ,<br>adresa trvalého pobytu, adresa podnikání, fakturační adresa,<br>čísla předložených identifikačních dokladů a ostatní informace s nimi spojené. | titul,<br>jméno a příjmení,<br>datum narození,<br>IČO, DIČ,<br>čísla předložených identifikačních dokladů a ostatní informace s nimi spojené. |
| B | kontaktní údaje | kontaktní telefonní číslo,<br>e-mailová adresa,<br>adresy na sociálních sítích. | kontaktní telefonní číslo,<br>adresa trvalého pobytu, doručovací či jiná kontaktní adresa<br>e-mailová adresa. |
| C | platební údaje | čísla účtů,<br>platební metoda,<br>údaje o přijatých platbách / dlužných částkách,<br>údaje o platební morálce. | číslo bankovního účtu. |
| D | údaje spojené se službami | číslo SIM karty,<br>smluvní telefonní číslo, aktivní tarif, balíčky, ostatní služby,<br>typ smlouvy,<br>segment zákazníka,<br>doba trvání smlouvy,<br>druh poskytnuté služby, | zákaznické číslo,<br>EAN,<br>číslo obchodního partnera,<br>identifikační číslo osoby dodavatele,<br>číslo přístupové ID karty (pokud je přidělena), |

| | | | |
|---|---|---|---|
| | | cena za poskytnutou službu,<br>typ používaného koncového zařízení. | přístupové ID a heslo do osobního účtu uživatele (pokud jsou vytvořeny). |
| E | vzájemná komunikace a interakce | informace o interakci (zákaznická linka, chatbot, záznamy těchto interakcí). | |
| F | metadata | telefonní číslo volajícího/volaného<br>datum a čas uskutečnění spojení,<br>typ přístupu k internetu,<br>IMEI koncového zařízení,<br>adresa datového spojení – IP adresa, URL adresa, …<br>číslo, název, umístění koncového bodu sítě, údaje o síti. | adresa datového spojení – IP adresa, URL adresa, … |
| G | cookies | | |
| H | kamerové záznamy | | |
| I | speciální údaje | přihlašovací údaje a heslo,<br>PIN, PUK. | |
| J | sociodemografická data | | |
| K | věk, pohlaví, vzdělání, rodinný stav | | |
| L | podpis a dynamický podpis | | |

# 19.3Sumarizace zákonů, které jsou ovlivněny adaptačním zákonem

| | Změna | Předpis | Od |
|---|---|---|---|
| 450/2001 | novelizuje | Zákon, kterým se mění zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů, zákon č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů, zákon č. 131/2000 Sb., o hlavním městě Praze, ve znění pozdějších předpisů, zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění zákona č. 320/2001 Sb., zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů, a zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů | 138/0 |
| 107/2002 | novelizuje | Zákon, kterým se mění zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činností bývalé Státní bezpečnosti, a některé další zákony | 138/0 |
| 310/2002 | novelizuje | Zákon, kterým se mění zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 18/1997 Sb., o mírovém využití jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, ve znění pozdějších předpisů, zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem a o doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, zákon č. 283/1993 Sb., o státním zastupitelství, ve znění pozdějších předpisů, a zákon č. 42/1992 Sb., o úpravě majetkových vztahů a vypořádání majetkových nároků v družstvech, ve znění pozdějších předpisů | 138/0 |
| 517/2002 | novelizuje | Zákon, kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy a mění některé zákony | 138/0 |
| 439/2004 | novelizuje | Zákon, kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů | 138/0 |
| 480/2004 | novelizuje | Zákon o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti) | 138/0 |

| | | | |
|---|---|---|---|
| **626/2004** | novelizuje | Zákon o změně některých zákonů v návaznosti na realizaci reformy veřejných financí v oblasti odměňování | 138/0 |
| **413/2005** | novelizuje | Zákon o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti | 138/0 |
| **109/2006** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o sociálních službách | 138/0 |
| **264/2006** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti s přijetím zákoníku práce | 138/0 |
| **342/2006** | novelizuje | Zákon, kterým se mění některé zákony související s oblastí evidence obyvatel a některé další zákony | 138/0 |
| **170/2007** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru | 138/0 |
| **41/2009** | novelizuje | Zákon o změně některých zákonů v souvislosti s přijetím trestního zákoníku | 138/0 |
| **52/2009** | novelizuje | Zákon, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony | 138/0 |
| **227/2009** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o základních registrech | 138/0 |
| **281/2009** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti s přijetím daňového řádu | 138/0 |
| **375/2011** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zdravotních službách, zákona o specifických zdravotních službách a zákona o zdravotnické záchranné službě | 138/0 |
| **468/2011** | novelizuje | Zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony | 138/0 |
| **64/2014** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti s přijetím kontrolního řádu | 138/0 |
| **250/2014** | novelizuje | Zákon o změně zákonů souvisejících s přijetím zákona o státní službě | 138/0 |

| | | | |
|---|---|---|---|
| **301/2016** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o centrální evidenci účtů | 138/0 |
| **183/2017** | novelizuje | Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích | 138/0 |
| **101/2000** | ruší | Zákon o ochraně osobních údajů a o změně některých zákonů | 138/0 |
| **177/2001** | ruší | Zákon, kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 227/2000 Sb., a zákon č. 65/1965 Sb., zákoník práce, ve znění pozdějších předpisů | 138/0 |
| **277/2011** | ruší | Nařízení vlády o stanovení vzoru průkazu kontrolujícího Úřadu pro ochranu osobních údajů | |

Převzato z [18]

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2017/2018

Studijní program: Systémové inženýrství a informatika
Forma: Prezenční
Obor/komb.: Informační management (im2-p)

**Podklad pro zadání DIPLOMOVÉ práce studenta**

| PŘEDKLÁDÁ: | ADRESA | OSOBNÍ ČÍSLO |
|---|---|---|
| Bc. Borkovcová Anna | Břetislavova 1219, Hradec Králové - Pražské Předměstí | I1700334 |

**TÉMA ČESKY:**

Obecné nařízení o ochraně osobních údajů (GDPR) v prostředí České republiky

**TÉMA ANGLICKY:**

General Data Protection Regulation (GDPR) in the Czech Republic

**VEDOUCÍ PRÁCE:**

Mgr. Josef Horálek, Ph.D. - KIT

**ZÁSADY PRO VYPRACOVÁNÍ:**

Cílem práce je analýza oblasti ochrany osobních údajů v souvislosti s nařízením (EU) 2016/679 (GDPR) s účinností od 25.5.2018 v prostředí České republiky.
V teoretické části se autorka podrobně zaměří na problematiku implementace GDPR v prostředí České republiky s důrazem na objasnění a jednoznačné vysvětlení komplexní problematiky nařízení, a to zejména v oblastech vztahujících se na subjekt údajů a jejich práva ke zpracovateli a správci osobních údajů a jejich zakotvení v připravovaném tzv. adaptačním zákoně.
V praktické části autorka provede komparativní analýzu platné legislativy (platné v době zadání) a nařízením (EU) 2016/679 (GDPR). Dále využije přístupů vybraných významných společností spravujících osobní údaje, na kterým modelově demonstruje komplexní problematiku spojenou s implementací GDPR. V závěru autorka představí návodný postup pro ověření souladu správy a zpracování osobních údajů s nařízením EU 2016/679 (GDPR).

**SEZNAM DOPORUČENÉ LITERATURY:**


NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.
NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.
NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
ŠMÍD, Vladimír. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 227/2000 Sb., zákona č. 177/2001 Sb., zákona č. 450/2001 Sb., zákona č. 107/2002 Sb., zákona č. 310/2002 Sb., zákona č. 517/2002 Sb., zákona č. 439/2004 Sb., zákona č. 480/2004 Sb., zákona č. 626/2004 Sb., zákona č. 413/2005 Sb., zákona č. 444/2005 Sb., zákona č. 109/2006 Sb., zákona č. 112/2006 Sb., zákona č. 342/2006 Sb., zákona č. 170/2007 Sb. a zákona č. 52/2009 Sb. (komentář). Masarykova univerzita v Brně
NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Vyd. 1. Praha: Wolters Kluwer, 2014. 484 s. ISBN 978-80-7478-665-5.
SKULOVÁ, Soňa. Nová právní úprava ochrany osobních údajů a některé její souvislosti a problémy ve veřejné správě. Časopis pro právní vědu a praxi. 2001, roč. 9, č. 2. ISSN 12109126.
KOLMAN, Petr. Správní sankce na úseku ochrany osobních údajů. Bulletin advokacie, 2010, č. 7-8. ISSN 1210-6348.
HROMADA, Martin, Petr HRŮZA, Josef KADERKA, Oldřich LUŇÁČEK, Miroslav NEČAS, Bohumil PTÁČEK, Leopold SKORUŠA a Richard SLOŽIL. Kybernetická bezpečnost: teorie a praxe. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6.
KOTSCHY, Waltraut. The proposal for a new General Data Protection Regulationproblems solved? International Data Privacy Law [online]. 2014, roč. 4, č. 4.

**Podpis studenta:** .....  **Datum:** 16.4.2019

**Podpis vedoucího práce:** .....  **Datum:** 16.4.2019