Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Dopad GDPR na ERP systémy

Diplomová práce

Autor: Bc. Ladislav Škop
Studijní obor: Informační management

Vedoucí práce: Ing. Pavel Čech, Ph.D.

Hradec Králové 2019

Prohlášení:

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

V Hradci Králové dne 4.8.2019 Ladislav Škop

Poděkování:

Děkuji vedoucímu diplomové práce Ing. Pavlu Čechovi, Ph.D., za metodické vedení práce, věcné připomínky, cenné rady a vstřícnost.

Anotace:

Práce je zaměřena na dopad obecného nařízení GDPR na ERP systémy. Popisuje povinnosti vyplývající z nařízení, jak se vztahují na dodavatele a uživatele ERP systémů a jak je možné dosáhnout splnění těchto povinností. Úspěšná implementace požadavků GDPR s sebou samozřejmě nese různá úskalí, a některá z nich práce vyjmenuje. V závěru práce dojde k popsání obecných postupů pro dosažení souladu s Obecným nařízením.

Klíčová slova: Obecné nařízení o ochraně osobních údajů, zpracování osobních údajů, ERP systémy

Annotation:

Title: Impact of GDPR on ERP systems

The thesis focuses on impact of GDPR on ERP systems. It describes obligations as a consequence of this regulation, how they apply to both developers and customers of ERP systems and how to achieve fulfillments of these obligations. There are many risks and difficulties when fulfilling legal requirements of GDPR and some of them will be named. Finally, universal prucedures will be described and also how they can be used in order to achieve concordance with GDPR.

Keywords: General Data Protection Regulation, processing of personal data, ERP systems

Obsah

1 ÚVOD

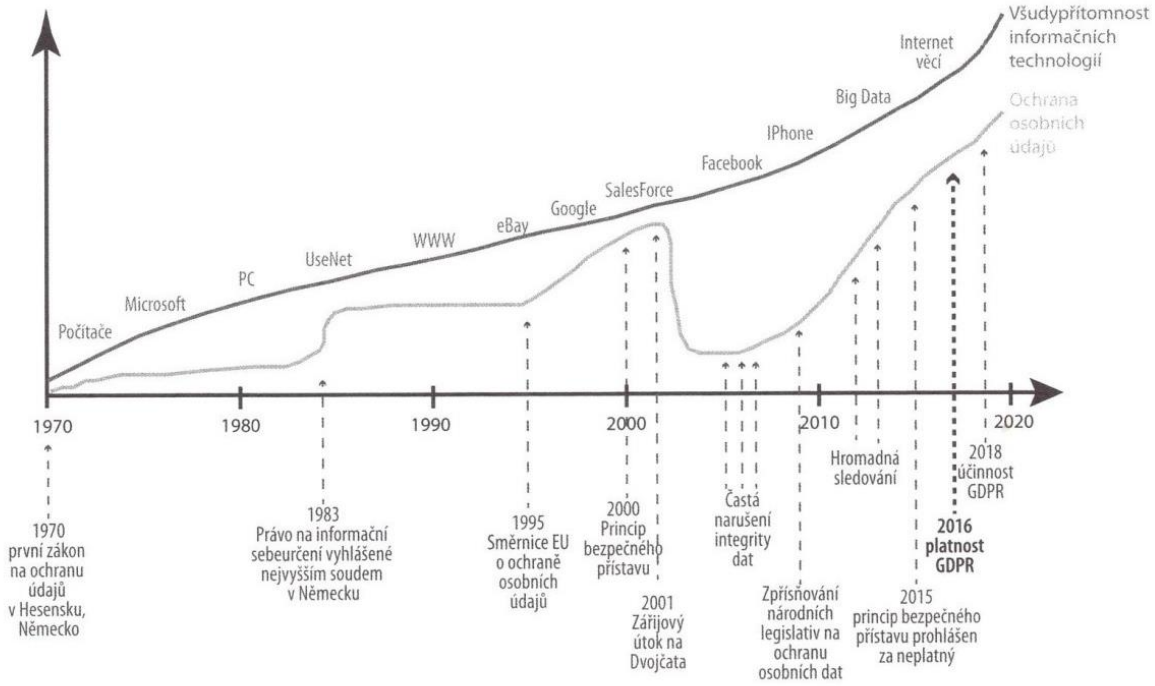
Ochrana osobních údajů je pojem existující již po desetiletí. V České republice začala fungovat přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Dle názvu lze správně usoudit, že se zákon zabýval ochranou osobních údajů pouze v informačních systémech. Zákon byl ale nekomplexní a nedokončený. A to až do roku 2000, kdy vešel v platnost a nabyl účinnosti plnohodnotný zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Též byl zřízen dozorový orgán Úřad pro ochranu osobních údajů. V roce 2004, při vstupu České republiky do Evropské unie, bylo třeba zákon novelizovat tak, aby bylo možné splnit podmínky v oblasti ochrany osobních údajů, resp. Směrnici Evropského parlamentu a Rady 95/46/ES [1].

Nicméně, v současné době jsme na prahu tzv. čtvrté průmyslové revoluce a na nové technologie nebyla stará legislativní nařízení dostatečná. V současném trendu digitalizace se využívá především on-line přístupů. Prvním příkladem jsou cloudová úložiště a s nimi příchozí poskytování různých služeb prostřednictvím internetu. Tyto služby se často označují zkratkou s *aaS na konci (aaS = as a Service = jako služba), typicky například SaaS, což označuje Software as a Service, česky software jako služba.

Dalšími důležitými pojmy jsou Big Data a data mining. Big Data značí velký objem dat, který je velice obtížné a časově náročné zpracovat, a je to téměř nemožné za pomoci běžně užívaných metod a softwaru. Taková data jsou obvykle nestrukturovaná a decentralizovaná. Data mining, neboli dolování z dat, potom představuje činnost, která se využívá k hledání relevantních informací právě z takových veledat. Tento proces se dá přirovnat k příslovečnému hledání jehly v kupce sena.

Umožnění přístupu k síti odkudkoliv, kdykoliv a téměř s čímkoliv dalo vzniknout tzv. Internetu věcí, anglicky Internet of Things (IoT). Už to nejsou jen počítače a mobilní zařízení, které jsou inteligentní, ale i domácí spotřebiče, vozidla, aj. mají vlastní senzory a software a umí komunikovat přes internet.

V neposlední řadě tu máme sociální sítě. Přes ně dnes probíhá většina komunikace, těžce se nachází někdo, kdo nemá účet alespoň na jedné sociální síti. I méně digitálně gramotní jedinci jsou obvykle jejich součástí.



Obrázek 1: Vývoj technologií vzhledem k vývoji legislativy [2]

Charakteristické pro všechny tyto technologie je fakt, že zpracování dat, tedy i osobních údajů, je povětšinou automatizované. Účelem je účinné profilování, díky kterému mohou být následně uživateli například nabízeny personifikované reklamy. Chtě nechtě, tímto je zapříčiněna ztráta soukromí. Téměř děsivá by se poté dala nazvat skutečnost, že přístup k osobním údajům mohou získat i třetí strany, ať je to způsobené nedostatečnou bezpečností dat nebo úmyslným prodejem takových informací. A právě v tomto lze spatřit jeden z mnoha důvodů, které daly vzniknout onu Obecnému nařízení na ochranu osobních údajů neboli GDPR (z anglického General Data Protection Regulation). Tento právní rámec má za cíl hájit práva občanů Evropské unie proti neoprávněnému zacházení s jejich daty. GDPR je účinné jednotně v celé EU od 25. května 2018 a tvoří doposud nejvíce ucelený soubor pravidel pro ochranu dat na světě. V České republice nahradilo právní úpravu ochrany osobních údajů, jímž byl zákon č. 101/2000 Sb., o ochraně osobních údajů.

Kdokoliv nyní zachází s jakoukoliv formou osobních údajů, musí se Obecným nařízením řídit. V praxi se to týká firem, institucí nebo i jednotlivců. Mluvíme-li o firmách, většina z nich využívá ERP systémů pro automatizaci a integraci business procesů. Tyto systémy produkují velké objemy dat a pracují s osobními údaji a je tedy třeba, aby náležitě splňovaly požadavky GDPR.

2 CÍL PRÁCE

Úkolem teoretické části práce je seznámit s důležitými pojmy a povinnostmi dle nařízení GDPR, které jsou relevantní pro oblast aplikace pro ERP systémy. Uživatelé ERP systémů jsou podniky, které se řadí do pozice správců osobních údajů, a je velmi pravděpodobné, že ERP systémy využívají pro operace zpracování osobních údajů.

Některé definice Obecného nařízení se neliší od výkladu z předchozího zákona č. 101/2000 Sb., o ochraně osobních údajů, zatímco jiné ano nebo v něm nebyly vůbec obsaženy. Upozornění na tyto skutečnosti je důležité, neboť podnik a jeho informační systém musely splňovat podmínky stanovené zákonem o ochraně osobních údajů, a díky tomu bude realizace některých povinností Obecného nařízení jednodušší.

Praktická část představí ERP systémy, především jejich obecnou architekturu. Poté dojde k definování oblastí, ve kterých může docházet ke zpracování osobních údajů.

V návaznosti na poznatky z teoretické části budou představeny požadavky vycházející z Obecného nařízení pro dodavatele ERP systémů a i pro podniky, které systémy využívají. Bude vytvořen obecný návod pro dodavatele, pomocí kterého lze úspěšně implementovat řešení do fungujícího ERP systému, a také návod pro podnik, díky kterému lze ověřit připravenost používaného ERP systému plnit GDPR.

V závěru práce dojde také k popsání kritických míst implementace.

3 METODIKA ZPRACOVÁNÍ

Pro splnění cíle teoretické části dojde k vypracování literární rešerše na téma osobních údajů, jejich zpracování a role Obecného nařízení v něm a dalších podstatných okolností vycházejících z Obecného nařízení.

Počáteční část praktické části bude společně s teoretickou částí tvořit přehledovou studii, která se využije pro analýzu problematiky dopadu Obecného nařízení na ERP systémy. Následovat bude návrh obecných postupů a doporučení pro implementaci požadavků Obecného nařízení. Pro využití pro dodavatele systémů budou systematicky zapracovány zásady, povinnosti a další požadavky Obecného nařízení do funkcionality ERP systémů. V případě, kdy to bude možné, budou demonstrovány konkrétní funkce. Kromě popisu této úpravy funkcionality ERP systémů dojde také k vytvoření schématu, který shrne podstatné části tohoto rozšíření i jejich jednotlivé funkce.

Pro použití z pohledu podniku budou opět na základě zásad, povinností a dalších požadavků Obecného nařízení vytvořeny obecné kroky analýzy, které lze rámcově využít pro zjištění souladu používaného ERP systému s Obecným nařízením. Výsledky praktické části budou mimo jiné i graficky znázorněny pomocí diagramů.

V závěru práce budou k celkovému zhodnocení přidána doporučení, která souvisí buď přímo se vztahem ERP systémů a GDPR, nebo se ho částečně týkají a mohly by jej ovlivnit.

4 TEORETICKÁ ČÁST

V této části práce je cílem obeznámení se základními pojmy spojenými s tématikou zpracování osobních údajů a spojitostmi s nařízením GDPR, především s novými povinnostmi z něj vycházejícími. Též budou vysvětleny rozdíly oproti zákonu o ochraně osobních údajů, který byl Obecným nařízením nahrazen.

4.1 OSOBNÍ ÚDAJ

Dle zákona č. 101/2000 Sb., o ochraně osobních údajů, je osobní údaj definován de facto stejně jako v pozdějším GDPR, a to následovně: je to jakýkoliv údaj, který se týká určeného či určitelného subjektu údajů. Subjekt se považuje za určený nebo určitelný tehdy, pokud je na základě alespoň jednoho osobního údaje přímo či nepřímo možné zjistit jeho identitu [3].

Mimo běžné osobní údaje, kterými jsou třeba jméno, příjmení, pohlaví, věk, datum a místo narození či rodné číslo, se můžeme setkat i s těmi méně typickými, kterými mohou být například lokační údaje, obrazový záznam, telefonní číslo, číslo platební karty nebo různá další identifikační čísla, nejčastěji vydávaná státem [4]. Zvláštní pozornosti by se mělo dostat, vzhledem k současnému technologickému pokroku, tzv. síťovým identifikátorům. Ty Obecné nařízení dokonce výslovně přidává do výčtu identifikátorů. Mezi ně se řadí především IP adresa, ale i MAC adresa, e-mailová adresa, soubory cookies a jiné údaje, pomocí kterých lze identifikovat subjekt on-line, tedy například přihlašovací jména k různým službám [5].

V případě pochybností v praxi, jestli se jedná o osobní údaj či nikoliv, se vždy doporučuje přistupovat k takovým údajům jako k osobním. Tyto pochybnosti mohou typicky činit právě zmíněné síťové identifikátory.

Subjektem osobních údajů musí být vždy fyzická osoba. Údaje o právnických osobách, tedy například název, forma nebo kontaktní údaje, nejsou osobní. Avšak pokud jde již o údaje řekněme o společnících nebo členech statutárních orgánů, a ti jsou fyzické osoby, jedná se o osobní údaje. Stejně tak je potřeba správně klasifikovat personifikovaný e-mail (např. jmeno.prijmeni@nazevfirmy.cz) jako osobní údaj, ačkoliv může patřit právnické osobě [1].

4.1.1 CITLIVÝ ÚDAJ

„Některé osobní údaje jsou takového charakteru, že mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Z tohoto důvodu je taxativně vymezena skupina údajů, které jsou považovány vůči subjektu údajů za citlivé a jimž je poskytnuta ještě zvýšená ochrana při jejich zpracování.“ [2]

Citlivým údajem se rozumí takový údaj, který vypovídá o rasovém či etnickém původu, politických postojích, členstvích v politických stranách nebo hnutích, členství v odborech, náboženském vyznání, filozofickém přesvědčení, zdravotním stavu, sexuálním životě a sexuální orientaci subjektu údajů [4]. Mezi citlivé údaje se řadí též údaje genetického a biometrického charakteru, ovšem pouze za předpokladu, že jsou zpracovávány za účelem jedinečné identifikace fyzické osoby. Pokud nejsou zpracovávány pro tento účel, pak nejde o zvláštní kategorii osobních údajů. Tím, že jsou zvláštní kategorie citlivých údajů v Obecném nařízení pevně vymezeny, nelze tento výčet libovolně zužovat ani rozšiřovat. Za zmínku stojí fakt, že mezi citlivé údaje nepatří rodné číslo, které tak ale často bývá mylně chápáno. V taxativním výčtu chybí. Zpracování rodných čísel se tedy v rámci GDPR řídí podmínkami pro zpracování osobních údajů, ale dále se podřizuje českému zákonu č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů [1].

Genetické údaje jsou údaje, jež se týkají zděděných nebo získaných genetických znaků, které vyplývají z analýzy biologického vzorku daného subjektu nebo z analýzy jiného prvku, který umožňuje získat ekvivalentní informace. Příkladem takových údajů jsou osobní údaje o zdravotním či duševním stavu minulém, současném i budoucím. Typicky třeba dědičné nemoci [6].

Za biometrický údaj se považuje cokoliv, co vychází z fyzických znaků či chování subjektu a je náležitě technicky zaznamenáno a zpracováno. Zaznamenání fyzických znaků je například scan obličeje nebo oční duhovky, otisk prstu či ruky a nebo samotný profil DNA. Chování je měřeno a zaznamenáváno například formou podpisového vzoru, a to nejen jeho grafickou podobou, ale i důrazem a rychlostí jeho provedení. Dalším možným behaviorálním biometrickým údajem může být rozpoznání hlasu [7].

Oproti zákonu o ochraně osobních údajů nalezneme v Obecném nařízení několik odchylek ve výčtu skupin citlivých údajů:

- národnostní původ již není citlivý údaj
- údaje o sexuálním životě jsou stále citlivé, nově se však k nim řadí též údaje o sexuální orientaci subjektu
- genetické a biometrické údaje jsou citlivé jen v případech, kdy jsou zpracovávány přímo za účelem jedinečné identifikace
- údaje o trestní činnosti již nejsou citlivé, jejich zpracování nicméně podléhá dozoru orgánu veřejné moci [1]

4.1.2 OSOBNÍ ÚDAJ OSOBY ZESNULÉ

Nařízení GDPR se nevztahuje na osobní údaje zesnulých osob. Avšak členské státy mohou stanovit vlastní pravidla, která budou upravovat zpracování osobních údajů zesnulých osob [4]. Důležité je však vzít v úvahu fakt, že osobní údaje o zesnulé osobě mohou představovat též osobní údaje stále žijící osoby [8].

4.2 ANONYMNÍ ÚDAJ

Existují takové údaje, které nelze ani nepřímo spojit se subjektem a nemohou tak pomoci při identifikaci. Nejčastěji je jejich využití k vidění ve výzkumech, ve kterých se operuje s velkým množstvím dat a kde obvykle nejde o jednotlivce, ale o obecné trendy či statistiky [4].

Na rozdíl od zákona o ochraně osobních údajů, který obsahoval jasnou definici anonymního údaje, GDPR anonymní údaje pouze zmiňuje, nikoliv definuje. Dle § 4 písm. c) zákona č. 101/2000 Sb. je anonymní údaj takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů. Chybějící definice anonymního údaje v Obecném nařízení však netvoří žádnou překážku [1].

Anonymní údaj není osobním údajem a jeho zpracování tak není regulováno Obecným nařízením. Z tohoto tedy vyplývá, že s anonymními údaji může být nakládáno v podstatě bez omezení.

4.2.1 ANONYMIZACE

Proces anonymizace je nevratný a spočívá v úpravě dat do takové podoby, že je není možné použít ke zpětné identifikaci osoby. Neexistuje žádný dodatečný soubor dat, který by se mohl použít k obnově do původní formy, a tudíž je zajištěna kompletní anonymita. Takto upravená data představují anonymní údaje a lze je volně využít, nezávisle na regulích Obecného nařízení.

4.2.2 PSEUDONYMIZACE

Údaje pseudonymizované nelze v žádném případě považovat za anonymní. Je třeba na ně stále pohlížet jako na osobní údaje. Pseudonymizace se velmi často výstižně nazývá jako zdánlivá či nepravá anonymizace [1]. GDPR definuje pseudonymizaci jako zpracování osobních údajů způsobem, že nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, jsou-li takové dodatečné informace uchovány odděleně a jsou-li přijata taková technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované nebo identifikovatelné fyzické osobě [4]. Zde je tedy vidět jasný rozdíl od anonymních údajů, a to, že je možné pseudonymizované údaje navrátit do původní podoby. Stále zde existuje vazba mezi subjektem údajů a údaji, která je však u anonymizace nevratně odstraněna.

Využití pseudonymizace údajů je silně doporučována například při předávání údajů z výzkumu dalšímu subjektu, který s nimi bude pracovat. Díky pseudonymizaci je možné přiřadit dané údaje konkrétní osobě, nelze však již zpětně tyto osoby ztotožnit. Celkově představuje metoda pseudonymizace výhodu při zpracování osobních údajů, jelikož podstatně snižuje riziko. Samotné Obecné nařízení navrhuje aktivní využívání pseudonymizace jako opatření při zabezpečení osobních údajů. Její využití může konečně vyústit i ve vyvinění se správce z povinnosti oznamovat případy porušení zabezpečení osobních údajů dozorovému úřadu, resp. subjektu údajů [1].

4.3 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

„Zpracováním osobních údajů se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“ [4]

Ze smyslu výše uvedené definice vychází, že nelze považovat jakékoliv nakládání s osobními údaji za jejich zpracování. Kdyby ano, pak by Obecnému nařízení podléhaly téměř jakékoliv každodenní činnosti, jako například běžná mluva, ve které je velmi často nakládáno s osobními údaji. Nakládání s osobními údaji, které není zpracováním, je upraveno např. zákonem č. 89/2012 Sb., občanský zákoník [2].

Obecným nařízením se musí řídit pouze subjekty, které osobní údaje zpracovávají dle definice zpracování. Za zpracování je považována systematická a sofistikovaná činnost, prováděná za určitým účelem. Systematičnost byla definována doslovně v zákoně č. 101/2000 Sb., a ačkoliv tomu tak v Obecném nařízení již není, neznamená to, že by se pojem zpracování měl interpretovat rozšiřujícím způsobem, protože systematičnost zůstává imanentním znakem zpracování jako takového.

GDPR se vztahuje na zpracování osobních údajů jak zcela či částečně automatizované, tak i na neautomatizované zpracování těch osobních údajů, jež jsou obsaženy v evidenci nebo do ní mají být zařazeny. Ačkoliv automatizace není v Obecném nařízení přímo specifikovaná, z principu lze pochopit, že se jedná o určitou automatizaci postupů zpracování osobních údajů, především za využití výpočetní techniky [1].

Ke zpracování osobních údajů může docházet i mimo území Evropské unie. V takovém případě se zpracování musí také řídit Obecným nařízením, protože to se vztahuje na osobní údaje všech obyvatel EU, bez ohledu na místo, kde ke zpracování dochází. V tomto ohledu zde lze spatřit globální dopad nařízení GDPR na zpracování osobních údajů [5].

4.3.1 EVIDENCE

Jakýkoliv strukturovaný soubor osobních údajů se považuje za evidenci. Ať je centralizovaný či decentralizovaný nebo rozdělený podle funkčního nebo zeměpisného hlediska. Ani záznamy nebo soubory záznamů, ani jejich titulní strany, které nejsou uspořádány dle určených hledisek, by do oblasti působnosti GDPR neměly spadat [4].

4.3.2 PROFILOVÁNÍ

Jakákoliv forma automatizovaného zpracování osobních údajů, která spočívá v jejich využití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, se nazývá profilováním. Jedná se především o rozbor nebo odhad aspektů týkajících se pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, lokality apod. [4]

Přestože je profilování Obecným nařízením definováno jako nový pojem, prakticky se nejedná o žádnou novinku. Profilování není zakázáno a ani se na něj nevztahuje potřeba speciálního souhlasu. Přesto se musí dít za dodržení určitých pravidel a v předvídatelných případech [9].

Profilování bylo dříve hojně využíváno kupříkladu ve finančních službách, kde díky němu bylo možné určit například bonitu klienta žádajícího o hypotéku. V současné době je však profilování jev daleko více rozšířený, především on-line. Historie prohlížení a uložené soubory cookies dovolují internetovým stránkám a sociálním sítím perfektně profilovat daného uživatele. Dojde ke zjištění zájmů, chutí a nákupního chování a následnému zařazení do určitého segmentu. Prostřednictvím tohoto zařazení se pak mohou uživateli zobrazovat cílené a personifikované reklamy, u kterých je několikrát vyšší šance na interakci, protože právě může mít k určité značce nebo produktu vztah.

4.3.3 SPRÁVCE

Správcem je subjekt, který buď sám, nebo společně s jinými subjekty určuje účely a prostředky zpracování osobních údajů. Může to být fyzická či právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt [4]. Správce zpracovává osobní údaje pro účely vyplývající z jeho činnosti, ale smí je zpracovávat i pro vlastní určené účely, pokud však tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob. Správce též nese primární odpovědnost za zpracování osobních údajů.

Pokud existuje fyzická osoba, která zpracovává osobní údaje takovým způsobem, že tento způsob již vylučuje uplatnění výjimky osobní nebo domácí činnosti, resp. pokud se nejedná o nakládání s osobními údaji, které ještě nesplňuje definici jejich zpracování, může se i taková osoba stát správcem [2].

Porovnáme-li pojem správce v Obecném nařízení s definicí v zákoně č. 101/2000 Sb., o ochraně osobních údajů, nedošlo ke změně. Rozšířila se ale odpovědnost správce, jelikož Obecné nařízení, na rozdíl od dřívější úpravy, stanovuje povinnost soulad také doložit [1].

Konkrétně je touto povinností to, aby s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavedl vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s Obecným nařízením. Tato opatření musí být dle potřeby revidována a aktualizována [4].

Toto se nazývá princip odpovědnosti správce. Je však důležité pochopit, že prokázání souladu není jednotlivá, ale kontinuální a komplexní činnost, vycházející z plnění celého Obecného nařízení.

Zajištění a doložení souladu zpracování osobních údajů se zásadami zpracování, resp. s Obecným nařízením, není jednorázovým stavem v minulosti, ale kontinuálním procesem, který zasahuje až do přítomnosti. Tento proces se zakládá na plnění povinností, které Obecné nařízení klade na správce. Mapování zpracování je činnost, která může správci výrazně pomoci se zvládnutím tohoto procesu. Při mapování zpracování správce zjišťuje, co a proč s osobními údaji vlastně dělá, dochází k vyhodnocení rizik, kontrole zabezpečení a v neposlední řadě se získané informace porovnávají s povinnostmi, které Obecné nařízení stanovuje. Dojde-li ke zjištění jakýchkoliv nevyhovujících rozdílů mezi současným a kýženým stavem, použijí se pro uvedení do souladu. Mapování se dá také použít jako podklad pro vypracování záznamů o činnostech zpracování. Tyto záznamy mohou být nápomocny při orientaci ve zpracování [1].

4.3.4 SPOLEČNÍ SPRÁVCI

V praxi je možné se setkat se situací, kdy účely a prostředky stanovují dva nebo více správců. Ti se pak nazývají společnými správci. Vzhledem k takovému vztahu je naprosto nezbytné vymezit vzájemné odpovědnosti a plnění Obecného nařízení, především týkající se výkonu práv subjektu údajů.

Subjekt údajů smí vykonávat svá práva u každého ze správců, a to nezávisle na ujednání, které platí mezi správci. Toto zajišťuje subjektu údajů zvýšenou míru ochrany [1].

Dle Obecného nařízení, je-li do téhož zpracování osobních údajů zapojen více než jeden správce, a nesou-li odpovědnost za jakoukoliv škodu způsobenou daným zpracováním, nese každý správce odpovědnost za celou újmu. Tímto je zajištěna účinná náhrada újmy subjektu údajů [4].

4.3.5 ÚČEL ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

V souvislosti se zpracováním osobních údajů je účel zpracování naprosto esenciální. Každé zpracování je prováděno za určitým účelem, proto se vůbec provádí. Na účel zpracování se vztahují zásady zpracování a další povinnosti vyplývající z Obecného nařízení. Účel zpracování musí být vždy legitimní a nesmí být protiprávní.

Pro stejné osobní údaje může existovat více účelů zpracování, kdy se může uplatnit několik různých právních důvodů pro jejich zpracování, které je klíčové rozlišovat. V tomto smyslu při pozbytí jednoho účelu zpracování určených osobních údajů nemusí být nutná jejich likvidace, jelikož mohou být tyto údaje nadále zpracovávány například i pro jiný účel [1].

4.3.6 ZPRACOVATEL

„Zpracovatel je fyzická či právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.“ [4]

Správce se může rozhodnout využít pro zpracování osobních údajů jiný subjekt. Takový subjekt se nazývá zpracovatel. Ten smí s osobními údaji provádět jen takové zpracovatelské operace, kterými jej správce pověřil nebo vyplývají z činnosti, pro kterou byl zpracovatel pověřen správcem. Zpracovatel je zpracovatelem pouze vůči osobním údajům, které mu poskytl správce, nikoliv vůči osobním údajům, které může zpracovávat pro své účely [2].

Tak jako u správce ani u zpracovatele není rozhodující jeho právní forma. Pojem zpracovatel se ve své definici dle Obecného nařízení nezměnil v porovnání se zákonem č. 101/2000 Sb., o ochraně osobních údajů.

4.3.7 ŘĚTĚZENÍ ZPRACOVATELŮ

Není vyloučena situace, kdy se zpracovatel rozhodne pro zapojení dalšího zpracovatele. Takto může vzniknout i několik úrovní větvení. Ačkoliv tento přístup není Obecným nařízením přímo zakázán, nelze ho aplikovat bez předchozího písemného povolení správcem, ať je obecné či konkrétní. Důvodem je odpovědnost správce za zpracování osobních údajů a musí tak též kontrolovat výběr zpracovatele, popř. zpracovatelů. Znalost všech zapojených zpracovatelů je nezbytná pro eliminaci jakýchkoliv rizik.

Rozhodne-li se zpracovatel zapojit do procesu zpracování osobních údajů dalšího zpracovatele, musí být zajištěny stejné smluvní podmínky jako ty, které jsou platné mezi

správcem a prvním zpracovatelem. Stručně řečeno, zapojení dalšího zpracovatele nesmí v žádném případě snížit standard ochrany osobních údajů.

Jak již bylo řečeno, svolení správce o zapojení dalších zpracovatelů je možné definovat i obecně. V takovém případě je však nutné, aby zpracovatel informoval správce o všech zamýšlených změnách, které se mohou týkat jak zapojení nového zpracovatele, tak i nahrazení některého ze stávajících. Správce musí dostat možnost vyhodnotit takový záměr a případně vyslovit svůj nesouhlas [1].

Vzhledem k předchozímu zákonu č. 101/2000 Sb., o ochraně osobních údajů, nebyl pojem řetězení zpracovatelů nikde upraven.

4.3.8 VZTAH SPRÁVCE A ZPRACOVATELE

Tento vztah je Obecným nařízením velice podrobně řešen, je-li porovnán s předchozím výkladem ze zákona č. 101/2000 Sb., o ochraně osobních údajů.

Správce smí využít pouze takové zpracovatele, kteří poskytují dostatečné záruky pro zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Obecného nařízení a aby byla též zajištěna práva subjektu údajů [4]. Každé zpracování může klást rozdílné požadavky a tím pádem vyžadovat rozdílně kvalitní zpracovatele. Výběr pak záleží například na rozsahu zpracování, kategoriích osobních údajů apod. [1]

Rozhodne-li se správce pro využití zpracovatele, jejich vztah se řídí smlouvou nebo jiným právním aktem dle práva Evropské unie nebo daného členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektu údajů, povinnosti a práva správce.

Tato smlouva či jiný právní akt musí také stanovit následující body o tom, že zpracovatel:

- zpracovává osobní údaje pouze na základě pokynů správce
- zajišťuje, že osoby oprávněné zpracovávat osobní údaje jsou vázány mlčenlivostí, popř. se na ně vztahuje zákonná povinnost mlčenlivosti
- přijme veškerá opatření, jež jsou požadována dle článku 32 Obecného nařízení
    - s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku
    - zohlednění rizik, která představují zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim
    - dodržování schváleného kodexu chování uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42 Obecného nařízení, toto jsou mimo jiné prvky, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 článku 32
    - opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie či členského státu
- dodržuje podmínky pro řetězení zpracovatelů
- zohledňuje povahu zpracování a je správci nápomocen, pokud je to možné, při plnění správcovy povinnosti reagovat na žádost o výkon práv subjektu údajů
- je správci nápomocen při zajišťování souladu s povinnostmi dle článků 32-36 Obecného nařízení, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici
- v souladu s rozhodnutím správce všechny osobní údaje buď smaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže také všechny existující kopie, s výjimkou situace, kdy právo Unie nebo členského státu požaduje uložení daných osobních údajů

- poskytne správci veškeré informace potřebné k doložení souladu a také umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil

Smlouva či jiný právní akt o zpracování osobních údajů musí být vyhotoveny písemně, s možností též elektronické formy [4].

I když smlouva o zpracování osobních údajů zní jako samostatné ujednání, není nutné, aby tomu tak bylo. Požadované náležitosti je možné zakomponovat i do jiné smlouvy či právního aktu, který správce se zpracovatelem uzavírá, např. v rámci obchodního vztahu. Samostatnost tedy není podmínkou. Využitím zpracovatele se správce v žádném případě nezbavuje odpovědnosti za zpracování osobních údajů [2].

Existovalo-li smluvní ujednání o zpracování osobních údajů ve formě smlouvy či jiného právního aktu ještě za účinnosti zákona o ochraně osobních údajů, musí být uvedeno do souladu do 2 let ode dne vstupu Obecného nařízení v platnost. Je tedy nutná přinejmenším revize, případně i nahrazení nevyhovující smlouvy [1].

Správce musí mít příležitost provést kontrolu u zpracovatele, a to na daném místě, kdykoliv, a i bez předchozího ohlášení. Pro takovou možnost musí zpracovatel správci zajistit dostatečná práva, která se jakkoliv týkají přístupu. Správce může ke kontrole využít externí zdroje. V situaci, kdy je zpracovatelská činnost prováděna formou práce z domova, musí pro možnost kontroly existovat smluvně dohodnuté právo na přístup do soukromého bytu [10].

4.4 ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Zásady zpracování osobních údajů tvoří samotný základ Obecného nařízení a ochrany osobních údajů jako takové. Nicméně nepředstavují nic nového, jelikož už dříve se jimi zabývala Směrnice 95/46/ES, resp. i zákon č. 101/2000 Sb., o ochraně osobních údajů. Obecné nařízení je však již přímo jmenuje jako zásady a současně stanovuje odpovědnost za jejich dodržení a povinnost tento soulad doložit, což již bylo zmíněno jako princip odpovědnosti správce [1].

4.4.1 ZÁSADA ZÁKONNOSTI

Správce musí zpracovávat osobní údaje legálně a aby tomu tak bylo, musí existovat právní důvody zpracování osobních údajů. Tyto právní důvody pak správce opravňují ke zpracování. Stejné údaje mohou být zpracovávány pro více různých účelů. Ve chvíli, kdy správce ztratí poslední právní důvod ke zpracování takových osobních údajů, musí dojít k jejich výmazu [5]. Může nastat situace, kdy se právní důvod uplatní pouze částečně, a ne na celý rozsah údajů. V takovém případě musí dojít k likvidaci těch údajů, jejichž zpracování není pokryto tímto právním důvodem [1].

Zásada zákonnosti může být velice dobře považována za nejdůležitější zásadu. Její dodržení je možné při splnění alespoň jedné z následujících podmínek a jsou-li osobní údaje zpracovávány pouze v odpovídajícím rozsahu:

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden nebo více konkrétních účelů
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt osobních údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu při výkonu veřejné moci, kterým je pověřen správce
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě [4]

Pakliže od počátku neexistoval řádný právní důvod ke zpracování osobních údajů, považuje se toto zpracování za nelegální a představuje zásadní nedostatek, který nelze vynahradit ani bezvadným plněním ostatních povinností vyplývajících z Obecného nařízení [1]. Je tedy klíčové, aby si každý, kdo se chystá ke zpracovávání osobních údajů, předem ověřil, zda existuje přítomnost právního důvodu, o který je možné se opřít. Zpracování bez validního právního základu je nepřípustné a téměř určitě povede k vysokým pokutám [10].

4.4.2 ZÁSADA KOREKTNOSTI

Zásada korektnosti představuje povinnost správce neutajovat před subjektem údajů účel, pro který jsou jeho osobní údaje zpracovávány, a informovat co možná nejlépe o tom, kdo, jakým způsobem a v jakém rozsahu osobní údaje zpracovává a komu jsou osobní údaje dále předávány [1].

4.4.3 ZÁSADA TRANSPARENTNOSTI

Je vyžadováno, aby veškeré informace a sdělení týkající se zpracování osobních údajů byly snadno přístupné a srozumitelné a poskytované za využití jasných a jednoduchých jazykových prostředků. Tato zásada je míněna zejména při informování subjektu údajů o totožnosti správce a účelech zpracování, případně o dalších záležitostech, které se týkají zajištění spravedlivého a transparentního zpracování.

Subjekty údajů by měly být informovány o rizicích, pravidlech a zárukách, které existují v souvislosti se zpracováním jejich osobních údajů, a také na jejich práva v souvislosti s tímto zpracováním a jak je uplatnit. Kritické je zejména to, aby konkrétní účely zpracování byly jednoznačné a legitimní a aby byly stanoveny už v okamžiku shromažďování osobních údajů [4].

Zásada transparentnosti se ale vyskytuje i v případě porušení zabezpečení ochrany osobních údajů. Pokud totiž tato situace představuje vysoké riziko pro práva a svobody subjektu, správci vzniká povinnost tento případ oznámit nejen dozorovému úřadu, ale právě i dotčenému subjektu údajů [1].

4.4.4. ZÁSADA OMEZENÍ ÚČELU

Osobní údaje smí být shromažďovány jen pro určité a legitimní účely, které jsou jasně a výslovně vyjádřené, a nesmí být zpracovány způsobem, který je s těmito účely neslučitelný [2].

Od účelu zpracování osobních údajů se odvíjí právní důvod zpracování osobních údajů a ve chvíli, kdy dojde ke splnění takového účelu zpracování, správce je povinen osobní údaje zlikvidovat, pakliže neexistuje jiný právní důvod, pro který by mohl tyto osobní údaje dále zpracovávat.

Obecné nařízení výslovně předepisuje, že další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu a pro statistické účely, které respektují zákonem stanovené podmínky, se nepovažuje za neslučitelné s původními účely. Pro tyto účely je tedy možné osobní údaje zpracovávat i nad rámec původního účelu [1].

4.4.5 ZÁSADA MINIMALIZACE ÚDAJŮ

Osobní údaje musí být přiměřené, relevantní a omezené na nezbytně nutný rozsah pro plnění účelu zpracování. Tato zásada zajišťuje to, že správce nemůže požadovat po subjektu údajů více údajů, než je nutné.

Zásadu minimalizace údajů lze považovat do jisté míry i za bezpečnostní prvek, protože v případě úniku osobních údajů je riziko pro subjekt údajů menší, právě kvůli zpracování pouze nezbytně nutných údajů [1].

4.4.6 ZÁSADA PŘESNOSTI

Aby mohlo být dosaženo účelu zpracování, je zapotřebí zpracovávat údaje v přesné a správné podobě. Tato zásada velice úzce souvisí se zásadou minimalizace účelů, protože zpracovávaný rozsah dat má být minimální. Zajištění přesnosti osobních údajů do jisté míry přispívá i ke splnění minimalizace.

Pro plnění této zásady by měl správce:

- realizovat přiměřené kroky k zajištění přesnosti všech osobních údajů, které získává a zpracovává
- zajistit jasnost a nezpochybnitelnost zdrojů osobních údajů
- vzít na vědomí veškeré možné problémy a nejasnosti ohledně přesností informací
- zvážit, zda je nutné informace aktualizovat, a pokud ano, jak často aktualizaci provádět

Ačkoliv Obecné nařízení přímo neuvádí či nedefinuje co je to přesnost osobních údajů, uvádí, kdy jsou údaje nepřesné. Je to ve chvíli, pokud jsou nesprávné či zavádějící ve vztahu k faktické skutečnosti [2].

Tato zásada přímo nevyžaduje, aby správce aktivně vyhledával nepřesnosti v osobních údajích nebo aby od subjektu údajů vyžadoval aktualizace jeho osobních údajů. Správce ale musí na žádost subjektu údajů, nebo pokud nalezne sám zjevně nepřesné údaje, rozhodnout s přihlédnutím k účelu zpracování, zda mají být nepřesné údaje opraveny nebo smazány. Taková akce pak bude provedena bezodkladně [1].

Zásada přesnosti je aplikována například při využití práva subjektu údajů na omezení zpracování dle čl. 18 odst. 1 písm. a) Obecného nařízení, podle kterého musí správce omezit zpracování osobních údajů v případě, kdy subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby mohl přesnost osobních údajů ověřit [4].
Na základě této zásady je možné, aby správce opravoval zjevné překlepy v křestním jméně nebo třeba doméně e-mailové adresy [1]. Nesmí však samovolně opravovat údaje, kde si není jistý, zda se jedná o překlep. Příkladem může být třeba záměna křestních jmen Michala a Michaela. U e-mailových adres se pak jedná především o tzv. místní část, jež se nachází před znakem @. Kreativitě se při vytváření této části téměř nekladou meze a jako omezení se tak často jeví jen již dříve zaregistrovaná adresa. Z tohoto důvodu nelze nikdy s jistotou říci, zda je takový osobní údaj přesný nebo ne.

4.4.7 ZÁSADA OMEZENÍ ULOŽENÍ

Tato zásada požaduje, aby byly osobní údaje uloženy ve formě umožňující identifikaci subjektu údajů po dobu ne delší, než je nezbytně nutné pro účely, pro které jsou zpracovávány. Existuje ale stejná výjimka jako pro zásadu omezení účelu, kdy pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, při dodržení zákonem stanovených podmínek, je možné osobní údaje uložit na dobu delší [4].
Zásada omezení uložení je jiným vyjádřením povinnosti likvidace osobních údajů, pomine-li účel jejich zpracování. Správce osobní údaje nepotřebuje ve chvíli, kdy byl splněn účel zpracování, a žádný další účel neexistuje. Zpracování takových osobních údajů by bylo nadále neúčelné a hlavně nežádoucí, proto musí dojít k jejich likvidaci.
Likvidace však nutně neznamená smazání dat. Někdy ani důsledkem různých technických či databázových vazeb není možné data nenávratně vymazat. Může dojít jen k odstavení informací mimo rámec zpracování, však za existence jistých záruk. Pokud informace stále existují v systému, ale jsou neaktivní, nesmí existovat úvaha o tom, že by správce údajů měl možnost tyto údaje znovu použít nebo k nim jakkoliv přistoupit.
„Lze předpokládat, že orgán dohledu bude spokojen s tím, že informace byly označeny příznakem „nezpracovávat“, pokud nelze z technických důvodů dosáhnout jejich skutečného vymazání.“ [2]

Anonymizace dat se za formu likvidace osobních údajů také považuje. Může-li mít správce přínos z vytěžování takových anonymních dat, toto představuje vhodnou formu likvidace osobních údajů [1]. Pseudonymizace není jako metoda likvidace dat přípustná, vzhledem k její samotné definici.

4.4.8 ZÁSADA INTEGRITY A DŮVĚRNOSTI

Jedná se o zajištění celistvosti systému, ve kterém jsou osobní údaje zpracovávány. To je dosaženo využitím vhodných technických a organizačních opatření, která chrání data před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, poškozením nebo zničením [1].

Důvěrností je míněno odepření neoprávněného přístupu a integrita znamená neporušenost informací [10]. V rámci této zásady se tedy jedná o ochranu osobních údajů jak z vnějšího, tak i vnitřního prostředí. Témata adekvátní pro plnění zásady integrity a důvěrnosti jsou fyzická a kybernetická bezpečnost.

Fyzická bezpečnost se zajišťuje technickými opatřeními spojenými nejen s hardwarovými prostředky, ale s celkovým fyzickým vybavením. Jedná se tedy například o zajištění přístupu do budovy bezpečnostními dveřmi na zámek, čip či kartu, o chránění prostorů kamerovým systémem a alarmem nejen proti krádeži, ale třeba i proti požáru, či o regulaci uložení a likvidace papírových dokumentů. Pokud nakonec zmíníme i počítačový hardware, pak to může být způsob nakládání s přenosnými paměťovými médii, uložení serverů apod.

Mluvíme-li o nefyzické bezpečnosti, jedná se o kybernetickou bezpečnost. Firemní systém se může stát cílem počítačové trestné činnosti a s takovou variantou je třeba počítat. Aktiva, která se útočník pokusí kompromitovat, mohou být právě osobní údaje, která jsou daným systémem zpracovávaná. Zajištění kybernetické bezpečnosti je komplexní a velice náročná činnost, obvykle je třeba mít k dispozici samostatné oddělení s experty v oboru nebo využít odborných konzultantů. Jako jedny ze základních řešení kybernetické bezpečnosti se mohou považovat aktualizace operačních systémů, využívání antivirových softwarů a firewallů, aktualizace ostatního softwaru, zálohování aj. Ruku v ruce se softwarovými opatřeními jde školení zaměstnanců a nastavení heslové politiky.

Dostání této zásadě, tedy splnění bezpečnostních opatření, je opět závislé na okolnostech doprovázejících danou organizaci.

4.5 SOUHLAS SUBJEKTU ÚDAJŮ

Souhlasem se rozumí jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým dá subjekt údajů prohlášení nebo jinak zjevné potvrzení svého svolení ke zpracování svých osobních údajů. Zmíněné vlastnosti musí platit najednou, jinak se nejedná o platný souhlas. Vyjádření souhlasu se dále řídí těmito podmínkami:

- pokud je zpracování vysloveně založeno na souhlasu, musí být správce schopen doložit, že takový souhlas byl subjektem údajů udělen
- je-li souhlas vyjádřen písemně a týká-li se toto vyjádření též dalších skutečností, musí být žádost o vyjádření souhlasu jasně odlišitelná, srozumitelná a snadno přístupná za použití jasných a jednoduchých jazykových prostředků
- subjekt údajů má právo svůj souhlas kdykoliv odvolat, tímto odvoláním není dotčena zákonnost zpracování vycházejícího ze souhlasu daného před odvoláním, odvolat souhlas musí být stejně snadné jako ho poskytnout
- pro posouzení, jestli je souhlas svobodný, se zohledňuje, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné [4]

4.5.1 ODLIŠITELNOST SOUHLASU

Obecné nařízení výslovně nepožaduje, aby byla žádost o souhlas se zpracováním osobních údajů předkládána samostatně. Není-li tak učiněno a žádost je zakomponována v rámci jiného smluvního ujednání, musí být rozumným způsobem odlišitelná od ostatního textu.

4.5.2 DOBROVOLNOST SOUHLASU

Svoboda při rozhodování se o udělení souhlasu je nejpodstatnějším atributem a nesmí být subjektu údajů upřena. Subjekt údajů není v žádném případě povinen souhlas udělit, nesmí být nucen a ani nijak trestán ze strany správce v případě jeho neudělení [1].

Zároveň nesmí být uzavření jakékoliv smlouvy podmíněno poskytnutím souhlasu se zpracováním osobních údajů. Samozřejmě existují situace, kdy správce musí zpracovávat osobní údaje subjektu pro plnění smlouvy či zákonem stanovených povinností. Tak se ale děje bez souhlasu [2]. Typicky je tomu tak například v pracovněprávních vztazích. Je-li subjektem zaměstnanec, je naprosto nelogické, aby dával souhlas se zpracováním osobních údajů, jelikož zaměstnavateli svědčí pro zpracování jiné právní důvody.

4.5.3 DOLOŽITELNOST SOUHLASU

Schopnost doložit souhlas je povinnost kladená na správce. Obsahově musí souhlas splňovat následující kritéria:

- totožnost správce, správců nebo společných správců
- účel zpracování osobních údajů
- rozsah zpracování osobních údajů, není-li jasný z kontextu
- informace o právu subjektu údajů souhlas odvolat

Souhlas je vždy udáván konkrétnímu správci, resp. správcům. Neexistuje možnost udělit neomezený souhlas. V praxi je, bohužel, taková snaha častým jevem, např. že souhlas je udělen všem subjektům holdingu. Takto koncipovaný souhlas je nekonkrétní, tudíž neplatný.

Souhlas je možné učinit v různých formách. Může být písemně, elektronicky, telefonicky atd. Na zvážení správce je jakou má možnost takový souhlas vždy doložit [1].

Udělení souhlasu musí být jednoznačným aktem subjektu údajů. Nelze, aby správce například ponechal ve formuláři již předem zaškrtnuté pole, tzv. opt-out.

Z důvodu nejen trvalého práva subjektu údajů na odvolání souhlasu či povinnosti existenci takového souhlasu doložit se správci často snaží opřít zpracování osobních údajů o jiný právní základ, než je souhlas subjektu údajů [10].

4.6 PRÁVA SUBJEKTU ÚDAJŮ

Obdobně jako zákon č. 101/2000 Sb., o ochraně osobních údajů, i Obecné nařízení přiznává subjektům údajů určitá práva. Ta tvoří pilíř ochrany osobních údajů a jejich účelem je vyrovnat vztah správce a subjektu údajů. Je nutné zmínit, že Obecné nařízení v porovnání s dřívějším zákonem o ochraně osobních údajů posiluje práva subjektu údajů, a to nejen aktualizací stávajících, ale také vytvořením nových [9].

4.6.1 VÝKON PRÁV SUBJEKTU ÚDAJŮ

Zajištění řádného výkonu práv subjektu údajů představuje nezbytnou podmínku pro soulad zpracování osobních údajů jako celku s Obecným nařízením. Byl-li jmenován pověřenec pro ochranu osobních údajů, představuje významnou součást při zajišťování souladu zpracování, tím pádem také výkonu práv subjektu údajů. Pokud jmenován nebyl, vždy lze doporučit pověření určité osoby, která se bude věnovat ochraně osobních údajů, a to včetně reagování na požadavek výkonu práv ze strany subjektu údajů [1].

Dle Obecného nařízení, správce musí provádět výkon práv subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků. Informace poskytne písemně nebo i za použití jiných prostředků, mezi které se ve vhodných případech řadí i elektronická forma. Vyžádá-li si to subjekt údajů, lze informace poskytnout i ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

Povinností správce je také poskytnutí subjektu údajů na jeho žádost informace o přijatých opatřeních, a to bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu je možné prodloužit až o další dva měsíce, je-li to s ohledem na složitost a počet žádostí nutné. Správce informuje subjekt údajů o jakémkoliv takovém prodloužení lhůty do jednoho měsíce od obdržení žádosti včetně důvodů pro tento odklad.

Pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje jej bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti subjektu údajů o důvodech nepřijetí opatření a také o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.

Informace dle článků 13 a 14 a veškerá sdělení a úkony podle článků 15 až 22 a 34 se poskytují a činí bezplatně. Nastane-li případ, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, smí správce:

- uložit přiměřený poplatek, který zohledňuje administrativní náklady
- odmítnout žádosti vyhovět

V takovém případě zjevnou nedůvodnost nebo nepřiměřenost musí doložit správce.

Pokud má správce důvodnou pochybnost o totožnosti fyzické osoby, která podává žádost, smí požádat o poskytnutí dodatečných informací, které nezbytně povedou k potvrzení totožnosti subjektu údajů [4].

Protože výkon jednoho práva subjektem údajů nevylučuje výkon dalšího práva, lze říci, že výkon jednotlivých práv smí být prováděn souběžně. Takový souběžný výkon práv subjektem údajů ale nezakládá nedůvodnost ani nepřiměřenost [1].

4.6.2 PRÁVO NA INFORMACE

Naprosto základní právo představuje právo na informace. To jde ruku v ruce se zásadou transparentnosti, kterou naplňuje. Smyslem tohoto práva je zaručit subjektu údajů úplnou informovanost o zpracování jeho osobních údajů.

Pro subjekt údajů se jedná o pasivní právo, nicméně pro správce toto představuje aktivní povinnost, kterou musí plnit automaticky bez požádání subjektem údajů [1].

Obecné nařízení rozlišuje dva případy získání osobních údajů, a to buď přímo od subjektu údajů, nebo z jiného zdroje. Na základě způsobu získání osobních údajů se pak rozlišuje, jaké informace musí správce poskytnout v rámci tohoto práva. Správce takové informace poskytuje v okamžiku získání osobních údajů.

Informace elementárně poskytované v případě, kdy jsou osobní údaje získány od subjektu údajů:

- totožnost a kontaktní údaje správce a jeho případného zástupce
- kontaktní údaje případného pověřence pro ochranu osobních údajů
- účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování
- oprávněné zájmy správce či třetí strany v případě, že je zpracování založeno na nezbytnosti plnění těchto oprávněných zájmů
- příjemce nebo kategorie příjemců osobních údajů
- případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci, a to včetně právních podkladů využitých pro toto předání

Je-li to nezbytné pro zajištění spravedlivého a transparentního zpracování, poskytují se mimo základních informací též tyto:

- doba, po kterou budou osobní údaje uloženy, nelze-li určit konkrétně, pak kritéria použitá pro její stanovení
- existence práva požadovat od správce přístup k osobním údajům týkajících se subjektu údajů, jejich opravu nebo výmaz, omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů
- existence práva kdykoliv odvolat souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním
- existence práva podat stížnost u dozorového úřadu

- skutečnost, jestli je poskytování osobních údajů zákonným či smluvním požadavkem, zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů
- skutečnost, jestli dochází k automatizovanému rozhodování, včetně profilování a smysluplné informace týkající se použitého postupu

V případě, že osobní údaje nebyly získány přímo od subjektu údajů, je povinností správce sdělit subjektu údajů výše jmenované elementární informace a k nim navíc:

- kategorie dotčených údajů

Pro nezbytné zajištění spravedlivého a transparentního zpracování jsou to opět výše uvedené informace plus:

- zdroj, ze kterého osobní údaje pocházejí, případně informace o tom, zda se jedná o veřejný zdroj

V případě zpracování osobních údajů, jež nebyly získány od subjektu údajů, vzniká správci povinnost poskytnout výše vyjmenované informace:

- v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce
- nejpozději v okamžiku, kdy dojde poprvé ke komunikaci se subjektem údajů, pokud mají být osobní údaje použity pro účely této komunikace
- nejpozději při prvním zpřístupnění osobních údajů, má-li je v úmyslu zpřístupnit jinému příjemci [4]

Jestliže nebyly osobní údaje získány přímo od subjektu údajů, není nutné zmíněné informace poskytovat v případech, kdy subjekt údajů již dané informace má, nebo když je patrné, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí. Informace není nutné poskytovat také v situaci, kdy je zpracování osobních údajů výslovně stanoveno právem Evropské unie či členského státu, jež se vztahuje na správce, nebo pokud se na správce vztahuje povinnost zachování mlčenlivosti [1].

4.6.3 PRÁVO NA PŘÍSTUP K OSOBNÍM ÚDAJŮM

Toto právo může být interpretováno téměř totožně jako právo na informace, podstatný rozdíl je ale v čase a v tom, že právo na přístup k osobním údajům je aktivním právem subjektu údajů. To znamená, že subjekt údajů musí podat žádost o přístup k osobním údajům a správci vzniká povinnost právě až tehdy, kdy toto nastane. Právo na přístup k osobním údajům, podobně jako právo na informace, souvisí s plněním zásady transparentnosti.

Předmětem tohoto práva je právo subjektu údajů získat od správce potvrzení, jestli dochází ke zpracování jeho osobních údajů, a v případě, že ano, má dále právo přístupu k těmto osobním údajům a k následujícím informacím:

- účely zpracování
- kategorie dotčených osobních údajů
- příjemce nebo kategorie příjemců osobních údajů, jimž byly či budou osobní údaje zpřístupněny
- doba, po kterou budou osobní údaje uloženy, nelze-li určit konkrétně, pak kritéria použitá pro její stanovení
- existence práva požadovat od správce přístup k osobním údajům týkajících se subjektu údajů, jejich opravu nebo výmaz, omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů
- existence práva podat stížnost u dozorového úřadu
- zdroj, ze kterého osobní údaje pocházejí, pokud nebyly získány od subjektu údajů
- skutečnost, jestli dochází k automatizovanému rozhodování, včetně profilování a smysluplné informace týkající se použitého postupu

Využití tohoto práva slouží primárně pro získání potvrzení, zda jsou osobní údaje fyzické osoby zpracovávány. Jestliže ano, správce umožní subjektu údajů přístup k nim a sdělí mu výše zmíněné informace [1]. Pakliže správce o dané fyzické osobě žádné údaje nezpracovává, musí poskytnout informaci, že osobní údaje subjektu údajů nejsou předmětem zpracování na straně správce [2].

Účelem tohoto práva rozhodně není získání přístupu k samotným médiím, která se využívají jako nosiče pro data, nýbrž ke kopii zpracovávaných osobních údajů. Nejedná se ani o kopii celého nosiče, ale doopravdy jen daných osobních údajů. Má-li subjekt údajů potřebu domoci se kopií celých nosičů, Obecné nařízení neposkytuje takové právo a je tak třeba využít jiných práv, vyplývajících z jiných právních předpisů [9]. Naopak, Obecné nařízení výslovně stanovuje, aby při využití práva na přístup k osobním údajům nebyla nepříznivě dotčena práva a svobody jiných subjektů [4].

4.6.4 PRÁVO NA OPRAVU

Právo na opravu prakticky plní zásadu přesnosti. Subjekt údajů má právo na to, aby správce opravil nepřesné údaje, které se ho týkají, a to bez zbytečného odkladu. S přihlédnutím k účelům zpracování má subjekt údajů též právo na doplnění neúplných údajů a poskytnutí dodatečného prohlášení [4].

Toto právo nikterak nepředstavuje povinnost správce aktivně vyhledávat nepřesnosti či požadovat pravidelné aktualizace údajů od subjektu údajů. Má-li subjekt údajů podezření, že správce zpracovává jeho nepřesné osobní údaje, může uplatnit toto právo a upozornit ho. Správci tímto oznámením vzniká povinnost zabývat se žádostí o opravu údajů [2].

Pro některé správce může být vhodné, v závislosti na kontextu, při kontaktu se subjektem údajů požádat o kontrolu aktuálnosti, a to především identifikačních a kontaktních osobních údajů [1]. Správce by se měl snažit o zajištění možnosti podání žádosti o opravu on-line, a to hlavně v případech, kdy ke zpracování osobních údajů dochází elektronickou formou [6].

4.6.5 PRÁVO NA VÝMAZ

Často je možné setkat se i s názvem „právo být zapomenut“. Dle Obecného nařízení má subjekt údajů právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají. Správci vzniká povinnost bezodkladného výmazu osobních údajů, je-li mu dán alespoň jeden z následujících důvodů:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány
- subjekt údajů odvolá souhlas, dle něhož byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování
- subjekt údajů vznese námitky vůči zpracování a neexistují žádné převažující oprávněné důvody pro zpracování
- osobní údaje byly zpracovány protiprávně
- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti přímo dítěti [4]

Je nutné si uvědomit, že právo na výmaz není absolutním právem subjektu údajů na výmaz údajů za jakékoliv situace. K povinnosti správce údaje vymazat vedou jedině výše uvedené důvody [1].

Existují ale výjimečné případy, kdy se tyto důvody neuplatní, a to když je zpracování daných osobních údajů nezbytné:

- pro výkon práva na svobodu projevu a informace
- pro splnění povinnosti, jež je vyžadována dle práva Unie či členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen
- z důvodu veřejného zájmu v oblasti veřejného zdraví
- pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu či pro statistické účely
- pro určení, výkon nebo obhajobu právních nároků [4]

Povinnost správce k vymazání osobních údajů vede k jejich likvidaci. Likvidace samotná nicméně představuje také proces zpracování osobních údajů, za kterou je správce odpovědný. Jinak řečeno, odpovědnost správce za zpracování pomine až úspěšnou likvidací.

Způsob provedení likvidace je zde klíčový. V praxi jsou viditelné jasné chyby, kdy se například papírové dokumenty s osobními údaji prostě vyhodí do kontejneru. Takový přístup je naprosto nepřípustný. Správné provedení likvidace musí vycházet z vědomí důležitosti této operace a hlavně z druhu a rozsahu zpracování. Požadavky na likvidaci budou rozdílné u různých forem, jako například listinné dokumenty, digitální databáze apod. Pokud se správce rozhodne využít k likvidaci externí společnosti, staví se taková společnost do pozice zpracovatele osobních údajů. Je doporučováno, aby ale i v takovém případě na likvidaci dohlížela správcem pověřená osoba [1].

Velký problém může představovat likvidace osobních údajů, které jsou správcem zveřejňovány. Tuto situaci Obecné nařízení přímo upravuje způsobem, že správce přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace [4].

4.6.6 PRÁVO NA OMEZENÍ ZPRACOVÁNÍ

Obecné nařízení stanovuje případy, kdy má subjekt údajů právo na to, aby správce omezil zpracování. To nastává ve chvíli, když:

- subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a místo toho požaduje omezení jejich použití
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků
- subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů

Omezením zpracování je dle definice myšleno označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu [4]. Omezení zpracování se od likvidace osobních údajů liší svou dočasností.

Pokud se na některé osobní údaje vztahuje omezení zpracování, znamená to, že s výjimkou uložení je lze zpracovávat jedině se souhlasem subjektu nebo pro určení, výkon nebo obhajobu právních nároků a z důvodu ochrany práv jiné fyzické či právnické osoby. Ve chvíli, kdy má být omezení zpracování zrušeno, musí správce předem upozornit subjekt údajů o této skutečnosti [1].

„Způsoby, jak omezit zpracování osobních údajů, by mohly mimo jiné zahrnovat dočasný přesun vybraných údajů do jiného systému zpracování, znepřístupnění vybraných osobních údajů uživatelům nebo dočasné odstranění zveřejněných údajů z internetových stránek. V systémech automatizovaného zpracování by omezení zpracování mělo být v zásadě zajištěno technickými prostředky tak, aby se na osobní údaje již nevztahovaly žádné další operace zpracování a aby nemohly být změněny. Skutečnost, že zpracování osobních údajů je omezeno, by měla být v systému jasně vyznačena.“ [4]

4.6.7 OZNAMOVACÍ POVINNOST SPRÁVCE O OPRAVĚ NEBO VÝMAZU OSOBNÍCH ÚDAJŮ ČI OMEZENÍ ZPRACOVÁNÍ

Dle čl. 19 Obecného nařízení je správce povinen oznámit jednotlivým příjemcům, kterým byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování. Výjimku představují případy, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce také informuje subjekt údajů o těchto příjemcích, pokud je to požadavek subjektu údajů [4].

4.6.8 PRÁVO NA PŘENOSITELNOST

Právo na přenositelnost údajů je novým právem subjektu údajů, které Obecné nařízení stanovuje. V podstatě působí jako rozšíření práva na přístup. Aby mohl subjekt údajů využít tohoto práva, musí být splněny tyto podmínky, a to současně:

- zpracování je založeno na souhlasu či smlouvě
- zpracování se provádí automatizovaně [4]

První podmínka tedy znamená, že se musí jednat o zpracování osobních údajů na základě souhlasu dle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) nebo na smlouvě dle čl. 6 odst. 1 písm. b). Především touto podmínkou se podstatně zužuje možný okruh aplikací tohoto práva. Na jiné právní důvody zpracování osobních údajů se právo na přenositelnost nevztahuje.

Druhá podmínka stanovuje, že se musí zároveň jednat o automatizované zpracování. Je-li zpracování prováděno manuálně, opět není možné uplatnit toto právo [1].

Podstatou tohoto práva je, že subjekt údajů má právo získat osobní údaje, které se ho týkají a jež poskytl správci, a právo předat tyto údaje dále jinému správci, a to i prostřednictvím původního správce, je-li to technicky možné, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Tyto údaje získá subjekt údajů ve formátu, který je:

- strukturovaný
- běžně používaný
- strojově čitelný [4]

Záměrem práva na přenositelnost je usnadnit uživatelům přechod mezi jednotlivými poskytovateli služeb, posílit sdílení osobních údajů mezi různými správci a poskytovat tak lepší služby [6].

Právo lze uplatnit pouze na osobní údaje týkající se přímo subjektu údajů. Tím pádem, jakákoliv jiná data či data anonymizovaná nejsou brána v úvahu. Nicméně, v mnoha případech není možné zcela se vyhnout údajům třetích osob. Příkladem může být služba poskytující hovory on-line, kdy budou detaily vztahující se na třetí osoby vždy přítomné třeba v seznamu příchozích a odchozích hovorů. Při předávání takových dat ale musí být vždy dodržena práva a svobody daných třetích osob.

Subjekt údajů může aplikovat toto právo na osobní údaje, které správci sám poskytl aktivním a vědomým chováním, např. prostřednictvím on-line formuláře. Ačkoliv jako takové chování se bere i využívání různých služeb, které mohou být monitorovány a zaznamenávány, čímž vznikají také osobní údaje. Jako příklad lze jmenovat GPS zařízení, jež generuje data o lokalitě subjektu. Na údaje, které správce vyvodí na základě jiných údajů, které poskytl subjekt údajů, se ale již právo na přenositelnost nevztahuje [11].

Právo na přenositelnost je poněkud unikátní, jelikož předpokládá součinnost dvou správců. Reálně lze spatřit využití v sektorových odvětvích, jako například bankovnictví, telekomunikace aj. Toto právo je možné chápat nejen jako právní normu, ale i jako ideu, jakým směrem by se mohl vývoj v digitálních technologiích ubírat v budoucnu [1].

4.6.9 PRÁVO VZNÉST NÁMITKU

Z důvodů týkajících se konkrétní situace má subjektu údajů právo kdykoliv vznést námitku vůči zpracování osobních údajů, které se ho týkají, na základě nezbytného zpracování pro splnění úkolu prováděného ve veřejném zájmu nebo nezbytného zpracování pro účely oprávněných zájmů správce či třetí strany, a to včetně profilování založeného na těchto ustanoveních.

Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

Pakliže se osobní údaje zpracovávají pro účely přímého marketingu, má subjekt právo vznést kdykoliv námitku proti takovému zpracování, což zahrnuje i profilování, týká-li se tohoto přímého marketingu. V případě, že subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou jeho osobní údaje dále zpracovávány.

Subjekt musí být na toto právo výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoliv jiných informací, a to nejpozději v okamžiku první komunikace s ním. Subjekt smí uplatnit toto právo prostřednictvím automatizovaných prostředků [4].

4.6.10 PRÁVO NEBÝT PŘEDMĚTEM AUTOMATIZOVANÉHO INDIVIDUÁLNÍHO ROZHODOVÁNÍ

Ačkoliv se toto právo může zdát jako nové, není tomu tak, protože bylo součástí již Směrnice 95/46/ES, stejně jako zákona o ochraně osobních údajů [1].

Subjekt údajů má právo nebýt předmětem žádného rozhodnutí, které by bylo založeno výhradně na automatizovaném zpracování, a to včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně týká. Toto právo není možné uplatnit v případech, když je rozhodnutí:

- nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem
- povoleno právem Unie nebo členského státu, které se vztahuje na správce
- založeno na výslovném souhlasu subjektu údajů

V těchto situacích však musí správce dohlédnout na to, aby byla dodržena práva a svobody a oprávněné zájmy subjektu údajů.

Zvláštní kategorie osobních údajů, resp. citlivé údaje, mohou být použity pro výhradně automatizované rozhodování jen v případě, kdy subjekt údajů dal výslovný souhlas, nebo pro nezbytné zpracování z důvodu veřejného zájmu na základě práva Unie či členského státu, opět při zaručení zajištění práv a svobod a oprávněných zájmů subjektu údajů [4].

Definice automatizovaného individuálního rozhodování není zakotvena v Obecném nařízení, nicméně se dá najít ve starší Úmluvě 108 Rady Evropy. Dle ní automatizované rozhodování zahrnuje operace uskutečňované zčásti či zcela pomocí automatizovaných postupů. Ty zahrnují ukládání dat na nosiče, provádění logických a aritmetických operací s těmito daty, jejich změnu, výmaz, vyhledávání nebo rozšiřování [9]. Z této definice je možné chápat, že součástí automatizovaného zpracování může být lidský faktor.

4.7 POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

GDPR svou podstatou stanovuje novou pracovní pozici. Nazývá se Data Protection Officer, zkráceně DPO, česky pověřenec pro ochranu osobních údajů. Náplní práce DPO je hlavně sledování souladu zpracování osobních údajů s povinnostmi, které vycházejí z Obecného nařízení. Dále je to provádění interních auditů, školení pracovníků a celkové řízení agendy týkající se interní ochrany dat [6].

Povinnost pro správce a zpracovatele jmenovat pověřence pro ochranu osobních údajů vzniká v každém případě, kdy:

- zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů, které jednají v rámci svých soudních pravomocí
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli povaze, rozsahu nebo účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektu údajů
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů

Pověřenec může být správcem či zpracovatelem jmenován i dobrovolně. Jako pověřenec se označují pouze takové osoby, které byly jmenovány dle výše uvedených povinností či právě dobrovolně, a které se řídí pravidly pro pověřence dle článků 37, 38 a 39 Obecného nařízení. Za pověřence rozhodně není možné považovat osobu, jež byla jen pověřena dozorováním nad zpracováním osobních údajů u správce či zpracovatele, na které se povinnost jmenovat pověřence nevztahuje, aniž by správce nebo zpracovatel vůči této osobě dodržoval pravidla stanovená v článcích 37, 38 a 39 Obecném nařízení.

Roli pověřence může vykonávat jak fyzická osoba, která je zaměstnancem dané organizace, tak i osoba, která je externí a činnost vykonává na základě smlouvy o poskytování služeb. Není přímo vyloučena možnost, aby byla jako pověřenec jmenována právnická osoba. Pokud ale taková situace nastane, vždy musí být jmenována fyzická osoba, která funkci skutečně vykonává [1].

Skupina podniků smí jmenovat jediného pověřence pro ochranu osobních údajů, je-li snadno dosažitelný z každého podniku. Obdobně je tomu u orgánů veřejné moci a veřejných subjektů, s přihlédnutím k jejich organizační struktuře a velikosti.

Pověřenec musí být jmenován na základě svých profesních kvalit, a to zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany osobních údajů [4]. Nicméně, Obecné nařízení se přímo nezaobírá vzděláním pověřence ve smyslu například dosažených akademických titulů. Každý správce či zpracovatel se tak musí rozhodnout dle svého uvážení, jaké vzdělání pověřence akceptuje. Též nestanovuje žádnou povinnou certifikaci a jako pověřenec tak může být jmenována i osoba necertifikovaná [2].

4.7.1 ÚKOLY POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

Pověřenec plní úkoly, jimiž pomáhá správci či zpracovateli dosáhnout a udržet soulad zpracování s Obecným nařízením. Mezi tyto úkoly se řadí minimálně:

- poskytování informací o povinnostech dle Obecného nařízení a dalších předpisů Evropské unie nebo členských států v oblasti ochrany osobních údajů
- monitorování souladu s Obecným nařízením a dalšími předpisy, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů
- poskytování poradenství na požádání, jedná-li se o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování dle článku 35
- spolupráce s dozorovým úřadem
- fungování coby kontaktní místo pro dozorový úřad v záležitostech, které se týkají zpracování, včetně předchozí konzultace dle článku 36, a případně vedení konzultací v jakékoliv jiné věci [4]

Povinnosti pověřence směřují k zajištění souladu zpracování s GDPR nejen interně u správce či zpracovatele, nýbrž i navenek. Pověřenec musí fungovat jako kontaktní místo nejen pro dozorový úřad, ale též pro subjekty údajů, které musí informovat, věnovat se výkonu jejich práv apod. Jeho úkolem je i vyřizování stížností, jež jsou obdrženy od subjektů údajů. Samozřejmě, pověřenec může plnit jakékoliv další úkoly, jimiž je nápomocný v oblasti ochrany osobních údajů. Typicky to může být podpora při vypracování a vedení záznamů o činnostech zpracování nebo vypracování vnitřních politik, které se týkají zpracování osobních údajů a bezpečnosti při něm. Není vyloučeno, aby pověřenec vykonával i jiné činnosti, které nijak nesouvisí s ochranou osobních údajů, ale jen v případě, že se nejedná o střet zájmů. Ten by vzniknul, kdyby pověřenec byl zároveň osoba rozhodující o účelech a prostředcích zpracování, a tím by došlo k narušení informační a poradní funkce pověřence [1].

4.7.2 POSTAVENÍ POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

Pro žádoucí výkon úkolů spojených s rolí pověřence je zapotřebí, aby tomu odpovídalo postavení pověřence uvnitř organizace. Je naprosto nezbytné, aby byl pověřenec včas a náležitě zapojen do veškerých aktivit, jež souvisejí s ochranou osobních údajů [4]. To představuje mimo jiné i seznámení s vnitřním prostředím firmy. Běžné by pak mělo být informování o všech podstatných okolnostech, které mají vliv na výkon jeho činnosti. Pověřenec by měl být také pravidelně zván na schůze vysokého a středního managementu, je-li předmětem jednání téma ochrany osobních údajů [1].

Pro řádné plnění úkolů musí být správce nebo zpracovatel pověřenci nápomocný poskytnutím nezbytných zdrojů, přístupem k osobním údajům a operacím zpracování a podporou vzdělání pro udržení odborných znalostí.

Je nutné, aby byla zajištěna nezávislost pověřence, tedy aby nedostával žádné pokyny, které by se týkaly výkonu jeho úkolů. Také nesmí být v rámci plnění svých úkolů nijak sankcionován či propuštěn. Pověřenec je dle Obecného nařízení přímo podřízen vrcholovému managementu správce či zpracovatele. Tím je ale míněno, aby měl potřebný přístup k vrcholovým řídícím pracovníkům, především ke komunikaci s nimi, nikoliv, že by byl jejich podřízeným pracovníkem [4].

Obecné nařízení nikterak nevylučuje jmenování pověřence na zkoušku. Eventuálně to může být například fyzická osoba v zaměstnaneckém poměru s klasickou zkušební dobou. Podobně není vyloučeno ani sjednání pověřence na dobu určitou. Nicméně, z kontextu Obecného nařízení lze vyvodit, že funkce pověřence předpokládá do určité míry stálost. Tím pádem, časté střídání osob ve funkci pověřence by nebylo vhodné.

Pověřenec je vzhledem k výkonu svých úkolů vázán tajemstvím a důvěrností, a to v souladu s právem Unie nebo členského státu. Ačkoliv není v Obecném nařízení povinnost mlčenlivosti pověřence více rozpracována, lze předpokládat, že v případě závažných porušení mlčenlivosti může dojít k jeho trestní odpovědnosti [1].

4.8 DOKLÁDÁNÍ SOULADU ZPRACOVÁNÍ

Správce má povinnost nejen dosáhnout souladu s Obecným nařízením, ale také tento soulad doložit. Je důležité pochopit, že soulad nemá být jednorázový stav, nýbrž stav trvalý. Tomuto faktu pak musí odpovídat činnosti, které zajišťují a zároveň i dokazují tento stav souladu. Prokazování souladu se dá shrnout jako komplex činností, které jsou vykonávány neustále [1].

GDPR v tomto smyslu nabízí správcům nástroje, pomocí kterých je prokázání souladu výrazně jednodušší.

4.8.1 ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

Obecné nařízení zrušilo oznamovací povinnost, ale záznamy o činnostech zpracování v podstatě představují její náhradu. Správce a zpracovatel, pakliže se na ně nevztahuje výjimka z povinnosti vést záznamy o činnostech zpracování, jsou povinni vést tyto záznamy [2].

Všechny povinné informace, jež musí správce obsáhnout ve svých záznamech o činnostech zpracování, jsou:

- jméno a kontaktní údaje správce, jeho případného zástupce a pověřence pro ochranu osobních údajů
- účely zpracování
- popis kategorií subjektů údajů a kategorií osobních údajů
- kategorie všech příjemců osobních údajů, včetně příjemců ve třetích zemích nebo mezinárodních organizacích
- informace o případném předání do třetí země nebo mezinárodní organizace, a to včetně identifikace a doložení vhodných záruk
- plánované lhůty pro výmaz jednotlivých kategorií údajů, je-li to možné
- obecný popis technických a organizačních bezpečnostních opatření, je-li to možné

Zpracovatel potom vede záznamy, které musí obsahovat:

- jméno a kontaktní údaje zpracovatele, každého správce, pro kterého jedná, případného zástupce zpracovatele nebo správce a pověřence pro ochranu osobních údajů
- kategorie zpracování prováděného pro každého ze správců
- informace o případném předání do třetí země nebo mezinárodní organizace, a to včetně identifikace a doložení vhodných záruk
- obecný popis technických a organizačních bezpečnostních opatření, je-li to možné [4]

Záznamy se vyhotovují písemně s možností i elektronické formy. Obecné nařízení stanovuje pouze minimum informací, které musí být zaznamenány. Je samozřejmé, že s ohledem na různorodost zpracování budou mít záznamy o činnostech zpracování různé podoby u různých správců či zpracovatelů, a to včetně dodatečných informací, které se rozhodnou také zahrnout [1].

Zaměstnává-li podnik nebo organizace méně než 250 osob, vztahuje se na ně výjimka z povinnosti vést záznamy o činnostech zpracování. Výjimka však neplatí v případě, že zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů [4].

4.8.2 KODEXY CHOVÁNÍ

Kodex chování představuje samoregulační nástroj, který má pomoci se zohledňováním specifik, která se vyskytují v rámci různých odvětví. Jeho cílem je řešení těchto specifik a jimi zapříčiněných nejasností v daném odvětví (např. pojišťovnictví, zdravotnictví, školství apod.). Měly by upřesňovat především povinnosti vyplývající z rizik, které pravděpodobně nastanou při zpracování osobních údajů.

Kodex chování se řadí mezi nepovinné nástroje pro vyhodnocení a prokázání souladu operací zpracování s Obecným nařízením. V podstatě je to textový dokument opatřený závazkem správce nebo zpracovatele k dodržování popsaných postupů. Návrh kodexu se předkládá dozorovému úřadu, který ho schvaluje. Pakliže je kodex v souladu s Obecným nařízením, je schválen a zaregistrován [9].

4.8.3 OSVĚDČENÍ

Pro správce představuje osvědčení zajímavou konkurenční výhodu, jelikož je to způsob, jak dát subjektům údajů najevo, že řádně zpracovává osobní údaje. Osvědčení lze získat na dobu nejvýše 3 let, ale je možné ho znovu obnovit. Také existuje možnost odejmutí osvědčení, a to v případě, že již přestaly být plněny požadavky pro toto osvědčení.
Vydávat osvědčení mohou pouze akreditované subjekty. Ty jsou určeny dle volby každého členského státu buď vlastním dozorovým úřadem, nebo vnitrostátním akreditačním orgánem [1].

4.9 POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

Posouzení vlivu na ochranu osobních údajů je úplná novinka přicházející s Obecným nařízením. Předchozí zákon č. 101/2000 Sb., o ochraně osobních údajů, resp. Směrnice 95/46/ES nic podobného neupravovaly. Často je možné setkat se i s originálním anglickým názvem Data Protection Impact Assessment či se zkratkou DPIA.
Je-li pravděpodobné, že jistý druh zpracování, především při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, je správce povinen provést před samotným zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Byl-li ustanoven pověřenec pro ochranu osobních údajů, správce si v rámci tohoto posouzení vyžádá jeho posudek.
Posouzení vlivu na ochranu osobních údajů je dle Obecného nařízení nutné především v těchto případech:

- systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která ve vztahu k fyzickým osobám vyvolávají právní účinky nebo mají podobně závažný dopad
- rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů
- rozsáhlé systematické monitorování veřejně přístupných prostorů [4]

Účelem posouzení vlivu na ochranu osobních údajů je především identifikace a minimalizace či eliminace rizik, které mohou nastat při vysoce rizikovém zpracování pro práva a svobody subjektu údajů. Posouzení vlivu na ochranu osobních údajů a předchozí konzultace s dozorovým úřadem z něj vycházející slouží správci také i jako nástroj plnění a prokazování souladu, jelikož správce si je tímto vědom vysokého rizika, které jeho zpracování představuje pro subjekty údajů [1].

4.9.1 PROCES PROVÁDĚNÍ POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

Na tento proces je třeba nahlížet jako na kontinuální, nikoliv jednorázový. Správce by měl provést přezkum a posouzení vždy, když dojde ke změně rizika, které představují operace zpracování osobních údajů.

Pokud byl jmenován pověřenec pro ochranu osobních údajů, správce od něj získá posudek. Pokud však nebyl, může za správce posouzení vlivu vypracovat osoba, která byla pověřena k zajištění souladu zpracování u správce, ale i jiná osoba. Ta osoba má pak na starosti i případné aktualizace [1].

Posouzení vlivu musí obsahovat minimálně:

- systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů
- posouzení rizik pro práva a svobody subjektů údajů
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s Obecným nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob

Při posouzení vlivu na ochranu osobních údajů se řádně zohlední též kodex chování, pokud je správce zavázán jeho dodržováním. Ve vhodných případech správce získá k zamýšlenému zpracování stanovisko subjektů údajů nebo jejich zástupců.

4.9.2 PŘEDCHOZÍ KONZULTACE

Ke konzultaci správce s dozorovým úřadem musí dojít ještě před samotným zpracováním osobních údajů, a to ve chvíli, kdy z posouzení vlivu na ochranu osobních údajů vyplyne, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal potřebná opatření ke zmírnění tohoto rizika. Účelem této předchozí konzultace je zvládnout hrozbu vysokého rizika [4].

„Povinnost absolvovat předchozí konzultaci vzniká tehdy, pokud identifikovaná vysoká rizika v rámci posouzení vlivu nemohou být dostatečně eliminována správcem, tj. i po přijetí adekvátních opatření ze strany správce by zamýšlené zpracování představovalo vysoké riziko pro práva a svobody fyzických osob (přítomno je tedy zbytkové vysoké riziko).“ [1]

Správce musí při předchozí konzultaci poskytnout dozorovému úřadu tyto informace:

- ve vhodných případech rozdělení odpovědnosti správce, společných správců a zpracovatelů zapojených do zpracování, zejména v případě zpracování v rámci skupiny podniků
- účely a způsoby zamýšleného zpracování
- opatření a záruky poskytnuté za účelem ochrany práv a svobod subjektů údajů
- kontaktní údaje případného pověřence pro ochranu osobních údajů
- vyhotovené posouzení vlivu na ochranu osobních údajů
- jakékoliv další informace, o které dozorový úřad požádá [4]

4.10 DOZOROVÝ ÚŘAD

Každý členský stát stanovuje jeden nebo více nezávislých orgánů veřejné moci jakožto dozorový úřad. Jejich primární účel je monitorovat uplatňování Obecného nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů. V případě, že se členský stát rozhodne zřídit více než jeden dozorový úřad, musí také určit jeden, který bude tyto úřady zastupovat ve sboru a který zajistí, že budou ostatní dozorové úřady dodržovat pravidla jednotnosti [4].

K plnění úkolů má každý dozorový úřad pravomoci, které se dají generálně rozdělit do tří skupin: vyšetřovací, nápravná a povolovací a poradní. Tyto pravomoci dozorový úřad vhodně využívá, a to i kombinovaně [1]. Úplný výčet jednotlivých pravomocí je dostupný v článku 58 Obecného nařízení.

Dozorovou činnost v České republice zajišťuje Úřad pro ochranu osobních údajů.

4.11 PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

V Obecném nařízení je porušení zabezpečení osobních údajů definováno jako porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovaných osobních údajů [4].

Případy porušení zabezpečení mohou být rozličné, obecně je lze dělit na:

- porušení důvěrnosti – neautorizované či náhodné prozrazení
- porušení dostupnosti – neautorizovaná či náhodná ztráta nebo zničení
- porušení integrity – neautorizovaná či nežádoucí změna

Samozřejmě se může jednat i o kombinaci některých nebo všech případů současně.

Nastane-li případ porušení zabezpečení osobních údajů, správce musí posoudit riziko a přijmout potřebná opatření. Závažnost rizika se bude vždy řídit především kategorií dotčených osobních údajů a formou incidentu. Vždy se musí porovnávat, jaký dopad může mít porušení zabezpečení na subjekty údajů, a to především v situaci, kdy by došlo ke ztrátě kontroly nad jejich údaji, škodě na reputaci, možnosti omezení jejich práv atd.

Co se týče porušení dostupnosti jako takové, ne vždy se jedná o porušení zabezpečení osobních údajů. Roli zde totiž hraje doba. Dojde-li k dočasnému porušení dostupnosti, například výpadkem elektrické energie, nejedná se o porušení zabezpečení. Ztratí-li se ale přístup trvale, například ztrátou šifrovacího klíče, již se jedná o porušení zabezpečení, resp. porušení dostupnosti. To může nastat i u náhodného zničení dat, ale opět zde figurují další skutečnosti. Pokud lze smazaná data například obnovit ze zálohy, incident sice nastal, ale nijak neznamenal riziko pro práva a svobody subjektů údajů. Až teprve ve chvíli, kdy by ztráta byla nenávratná, se jedná o porušení zabezpečení [1].

Riziko porušení zabezpečení dále vychází z okolnosti, zda došlo k úmyslnému či nedbalostnímu porušení zabezpečení. Úmyslné jednání samozřejmě výrazně zvyšuje riziko takového případu. Obvykle se totiž v takové situaci jedná o komplexní porušení zabezpečení s jasným cílem útoku na osobní údaje [9].

4.11.1 OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ DOZOROVÉMU ÚŘADU

V případě jakéhokoliv porušení zabezpečení osobních údajů, při kterém vznikne riziko pro práva a svobody fyzických osob, je správce povinen bez zbytečného odkladu, pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit tento případ dozorovému úřadu. Neprovede-li správce ohlášení do 72 hodin, musí být současně s ohlášením uvedeny též důvody tohoto zpoždění.

Pokud k porušení zabezpečení osobních údajů dojde u zpracovatele, neprodleně jej oznámí správci, resp. dotčeným správcům.

Ohlášení musí v každém případě obsahovat následující informace:

- popis povahy daného případu porušení zabezpečení osobních údajů, a to včetně kategorií a přibližného počtu dotčených subjektů údajů, je-li to možné určit, a přibližného množství dotčených záznamů osobních údajů
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které poskytne bližší informace
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů

Může nastat situace, že správce nebude moci poskytnout veškeré informace současně. Tehdy je smí poskytovat postupně bez dalšího zbytečného odkladu [4].

4.11.2 OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ SUBJEKTU ÚDAJŮ

Jestliže je pravděpodobné, že daný případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, správce musí oznámit toto porušení subjektu údajů, a to bez zbytečného odkladu.

Na rozdíl od ohlašování těchto případů dozorovému úřadu, kde postačí přítomnost jakéhokoliv rizika, pro oznámení případů porušení zabezpečení subjektu údajů musí být splněna podmínka vysokého rizika.

Toto oznámení musí být sepsáno za použití jasných a jednoduchých jazykových prostředků. Obsah oznámení je téměř totožný s obsahem ohlášení pro dozorový úřad, ale s jediným rozdílem, a to takovým, že se týká pouze osobních údajů daného subjektu údajů. Oznámení subjektu údajů se nevyžaduje, nastane-li alespoň jedna z těchto podmínek:

- správce zavedl náležitá technická a organizační ochranná opatření a ta byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, a to především taková, která činí tyto údaje nesrozumitelnými pro kohokoliv, kdo není oprávněn k nim mít přístup (např. šifrování)
- správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektu údajů se pravděpodobně neprojeví
- vyžadovalo by to nepřiměřené úsilí, v takovém případě však musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření [4]

4.12 SANKCE

Tak jako každá právní norma, i Obecné nařízené má vlastní sankční část. Její hlavní rolí je donutit adresáty dodržovat stanovená pravidla.

Ukládání správních pokut má být účinné, přiměřené, ale také odrazující. Nikoliv likvidační. Správní pokuty se udělují dle okolností a rozhodně není pravda, že každé porušení Obecného nařízení se trestá uložením pokuty. Pokud zpracování, které správce provádí, nějakým způsobem porušuje Obecné nařízení, může mu být uděleno napomenutí nebo mu být nařízeno vyhovět žádosti subjektu údajů. Též mu může být nařízeno uvést zpracování do souladu apod. [9]

Při rozhodování o uložení správní pokuty, resp. její výši, dozorový úřad zohledňuje:

- povahu, závažnost a délku trvání porušení s přihlédnutím k povaze, rozsahu a účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, která jim byla způsobena
- zda k porušení došlo úmyslně či nedbalostí
- kroky podniknuté správcem nebo zpracovatelem ke zmírnění škod způsobených subjektům údajů
- míru odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedených
- veškerá relevantní předchozí porušení správcem nebo zpracovatelem
- míru spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků
- kategorie dotčených osobních údajů
- způsob, jakým se dozorový úřad dozvěděl o porušení, především zda správce nebo zpracovatel porušení oznámil a v jaké míře
- jestli v minulosti existoval případ, kdy vůči správci či zpracovateli byla nařízena některá nápravná opatření, a pokud ano, zdali došlo k jejich splnění
- dodržování schválených kodexů chování nebo schváleného mechanismu pro vydávání osvědčení
- jakoukoliv jinou polehčující nebo přitěžující okolnost vztahující se na daný případ, jako například získaný finanční prospěch či zamezení ztrátám, přímo nebo nepřímo vycházející z porušení

Stane-li se, že správce nebo zpracovatel, ať úmyslně nebo z nedbalosti, poruší více ustanovení Obecného nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení [4].

Je patrné, že dozorový úřad má při ukládání pokuty rozličné možnosti, včetně jejího neuložení nebo uložení některého z nápravných opatření uvedených v čl. 58 odst. 2 písm. a) až h) a j) Obecného nařízení, buď místo pokuty, nebo současně s ní [1].

„Z udílení správních pokut jsou vyloučeny orgány veřejné moci a veřejné subjekty. V případě, že s takovým subjektem povede Úřad řízení o přestupku pro porušení povinností stanovených Obecným nařízením, je povinen od uložení správní pokuty upustit. Vůči těmto správcům a zpracovatelům uplatňuje Úřad jiné druhy správních trestů, resp. nápravných pravomocí dle čl. 58 odst. 2 Obecného nařízení.“ [9]

4.12.1 VÝŠE POKUT

Obecné nařízení dělí porušení na dva druhy, které mají rozdílné maximální výše pokut. Pokuta až do výše 10 000 000 EUR, resp. 2 % celkového ročního obratu celosvětově za předchozí finanční rok, jedná-li se o podnik, může být uložena za porušení:

- povinnosti správce a zpracovatele podle článků 8, 11, 25 až 39, 42 a 43
- povinnosti subjektu pro vydávání osvědčení podle článků 42 a 43
- povinnosti subjektu pro vydávání osvědčení podle čl. 41 odst. 4

Pokuta až do výše 20 000 000 EUR, resp. 4 % celkového ročního obratu celosvětově za předchozí finanční rok, jedná-li se o podnik, může být uložena za porušení:

- základní zásady pro zpracování, včetně podmínek týkajících se souhlasu podle článků 5, 6, 7 a 9
- práva subjektů údajů podle článků 12 až 22
- předání osobních údajů příjemci ve třetí zemi nebo mezinárodní organizaci podle článků 44 až 49
- jakékoliv povinnosti vyplývající z právních předpisů členského státu, jež se týká zvláštních situací, při nichž dochází ke zpracování
- nesplnění příkazu nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem podle čl. 58 odst. 2 nebo neposkytnutí přístupu v rozporu s čl. 58 odst. 1 [4]

5 PRAKTICKÁ ČÁST

ERP systém představuje hlavní součást informačního systému podniku. Díky svým vlastnostem výrazně usnadňuje řízení většiny či všech oblastí činnosti podniku. ERP pracuje s velkým objemem dat, ať jsou strukturovaná či nikoliv. Nezpracovává je jen v rámci vlastní funkcionality, ale data získává a předává i prostřednictvím dalších aplikací nejen uvnitř, ale také vně podniku. Je téměř nemyslitelné, že by ERP systém nezpracovával osobní údaje. Z tohoto faktu pramení povinnost ERP plnit Obecné nařízení.

Pro velké firmy, které jsou většinou reprezentovány nadnárodními korporacemi, jakož i pro drobné firmy, které mají méně než 10 zaměstnanců, není otázka, zda ERP plní Obecné nařízení, příliš relevantní. Velké firmy si mohou dovolit kvalitní poskytovatele ERP systémů, kteří sami zajišťují soulad systému s Obecným nařízením. Drobné firmy naopak zpravidla ERP systémy nepoužívají.

Malé a střední podniky nicméně ERP systémy ve většině případů implementují, však nemusí se nutně jednat o hotové řešení od některého z poskytovatelů, případně se nemusí jednat o celé řešení, ale jen o jeho část. Mohou nastat různé okolnosti, které ovlivní rozhodnutí podniku v otázkách implementace ERP.

Tato část práce si klade za cíl obeznámení s ERP systémy a způsoby, jakými zpracovávají data, resp. osobní údaje. Dále je to definování kroků, které by malé a střední podniky měly podniknout pro zjištění, jestli ERP systém plní Obecné nařízení. V případě zjištění nesouladu pak určení obecných postupů a doporučení, pomocí kterých bude souladu dosaženo.

5.1 DEFINICE ERP SYSTÉMU

Pro uvědomění si, co je to ERP systém, jak a co tento systém zpracovává, především mluvíme-li o osobních údajích, a jakým způsobem je zapotřebí ho customizovat, aby podnik dosáhl souladu zpracování s podmínkami Obecného nařízení, je třeba vrátit se k samotným definicím.

ERP představuje zkratku názvu Enterprise Resource Planning (česky Plánování podnikových zdrojů). ERP software pokrývá značnou část podnikového řízení, a to především na taktické a operativní úrovni řízení. Dle své pozice v informačním systému podniku představuje ERP zdroj dat pro ostatní aplikace [12].

„ERP má oproti neintegrovaným systémům dvě hlavní přednosti: sjednocený celopodnikový pohled na vše, co se v různých divizích odehrává, a společnou podnikovou databázi, sdružující a uchovávající veškerá podniková data. S určitou mírou zjednodušení můžeme říci, že ERP systém je informační systém pokrývající svými funkcemi veškeré agendy. S tím dodatkem, že řadu funkcí nabízí ve svém základu s širokou možností jejich parametrizace a současně poskytuje prostor pro vývoj a integraci specifických požadavků společnosti.“ [13]

5.1.1 VLASTNOSTI ERP SYSTÉMU

Charakteristické pro ERP systém, jakožto aplikační software, je schopnost automatizovat a integrovat podnikové procesy, funkce a data [12]. A právě tyto dvě vlastnosti jsou klíčové i z pohledu plnění požadavků nařízení GDPR.

Cílem automatizace je jednak úspora nákladů a jednak také zvýšení produktivity práce a snížení chybovosti. Umožní také vyřazení činností jako například kontrola a korekce dat, které jsou jinak nutně vázané k lidské práci. Činnosti nebo procesy vhodné k automatizaci jsou ty, které se dějí opakovaně a mají jasně definovaný obsah a výstup [14].

Mezi takové činnosti se řadí i operace zpracování osobních údajů. Pamatovat na tuto skutečnost je klíčové, neboť Obecné nařízení rozlišuje různé případy a povinnosti z nich vycházející při využívání automatizovaných procesů. Kupříkladu při úplné automatizaci nějakého procesu, jež se použije pro zpracování osobních údajů, se může jednat o automatizované individuální rozhodování a podnik by musel být připraven například plnit právo subjektů údajů nebýt předmětem automatizovaného individuálního rozhodování nebo plnit zpřísněné povinnosti, jako třeba v rámci informační povinnosti poskytovat podrobné informace týkající se použitého automatizovaného postupu a jeho důsledků pro práva a svobody fyzických osob. V případě částečné automatizace, kdy v procesu stále někde dochází k lidskému zásahu, se může jednat spíše o profilování, které má Obecným nařízením také definovaná pravidla.

Pojmem integrace je míněna skutečnost, že ERP sjednocuje události, které se dějí v různých útvarech uvnitř podniku. Typicky se jedná o tyto čtyři hlavní okruhy:

- finance
- personalistika
- výroba (a logistika)
- marketing a prodej

Díky ERP jsou tyto okruhy propojeny neboli integrovány [15]. Na základě tohoto faktu je poté zcela jasné, že ERP systém získává data z jiných aplikací, ale také že pro ně může představovat zdroj. Tok dat je tedy z pohledu ERP oboustranný [12].
Ve smyslu této definice a návaznosti na Obecné nařízení je důležité si uvědomit, že ERP centralizovaně operuje s velkým množstvím dat, a tedy i osobních údajů.

5.1.2 MODULY

Softwarová architektura ERP systému je tvořena tzv. moduly. Ty se dají považovat za základní stavební kameny, jelikož s jejich pomocí je zajištěna funkcionalita v jednotlivých hlavních okruzích. Správná struktura modulů je velmi důležitá, protože je třeba dosáhnout správného poměru mezi integritou a nezávislostí jednotlivých modulů. Jinak řečeno, je požadováno, aby moduly spolupracovaly mezi sebou, ale zároveň nebyly vzájemně závislé, resp. aby mohly být implementovány individuálně.
Moduly si podnik volí především ve fázi návrhu ERP systému, ačkoliv jejich povaha dovoluje dodatečnou implementaci. Volba se řídí dle potřeb daného podniku, resp. jeho existujících či plánovaných podnikových procesů, které se definují provedením analýzy ideálně ve fázích návrhu a výběru ERP. Podnik se na základě této analýzy může rozhodnout implementovat kompletní konkrétní funkcionalitu, kterou vybraný dodavatel nabízí, nebo jen částečnou selekcí určitých modulů. Může nastat i situace, kdy podnik bude potřebovat specifický modul, který svou funkcionalitou podpoří činnost určitého oddělení či dokonce jen určité pracovní pozice [16].
Lze rozlišit několik druhů modulů:

- aplikační – zajišťují činnosti v hlavních okruzích
- dokumentační – obsahují on-line uživatelskou dokumentaci
- implementační – jsou využívané k přípravě a nasazení do podniku
- technologické a správní – používané k nastavení uživatelských oprávnění
- nástroje pro customizaci – upravují software pro dosažení kýžené funkcionality
- vývojové prostředí – pro tvorbu např. vlastního programovacího jazyka
- rozhraní pro přístup do systému [17]

Různé podniky mají rozdílné priority a požadavky a na jejich základě se moduly volí a nasazují. Kupříkladu podnik, který nic nevyrábí, nebude potřebovat funkcionalitu týkající se plánování výroby, ale naopak může uplatnit funkcionalitu pro řízení a plánování prodeje, kterou výrobní podniky potřebovat nemusí.

Rozhodně není podmínkou, že každý ERP systém obsahuje výše uvedené moduly, ačkoliv se dá předpokládat jistá podobnost, právě na základě priorit jednotlivých podniků. Kvůli rostoucím nárokům na kompatibilitu s nejnovějšími digitálními trendy (např. propojení ERP a IoT) se už moduly neomezují, ale vzniká řada dalších užitečných nástrojů [12].

5.1.3 PROVOZNÍ PRINCIPY

Moduly ERP systému pracují s daty zpravidla dvěma způsoby. Buď je přístup k datům zajištěn sdílenou databází, nebo se data předávají mezi aplikacemi navzájem formou datových výstupů a vstupů. V případě tohoto přístupu pak platí, že:

- transakce v jednom modulu může automaticky generovat akci v jiném modulu (prodej zboží se projeví v cash flow)
- transakce jsou navzájem konzistentní (kontrola přijaté faktury oproti skladové kartě)
- je možné verifikovat průběh funkcí jednotlivých modulů a dohledat důsledky a příčiny jednotlivých transakcí (kontrola určitého stavu účtu dle záznamů v účetní knize)

Z výše zmíněných skutečností lze vyvodit účinnost ERP, jež je zajištěna jeho integrací. Vložení dat stačí provést jednou, protože vazby se projevují i v souvisejících modulech, a každý uživatel má přístup jen k relevantním datům.

Jakožto základ informačního systému podniku musí být ERP schopný mimo vlastních modulů integrovat i mnoho dalších aplikací a technologií a předávat si s nimi data. Obvyklé jsou vazby například na:

- CAD software
- geografické systémy GIS
- aplikace a technologie pro řízení skladů
- aplikace pro řízení výrobních linek
- systémy sběru dat [12]

5.1.4 ŘÍZENÍ PŘÍSTUPŮ

Pro ERP systém je příznačný jeho multiuživatelský charakter. Více uživatelů potřebuje mít přístup současně. ERP musí těmto uživatelům zajistit bezpečný a efektivní přístup k informacím a funkcionalitě, a to na základě jejich oprávnění [12].

Určení oprávnění, popř. přístupových práv a uživatelských rolí je zde klíčové. Role a oprávnění s ní související by měly korespondovat s úlohami uživatele. Kupříkladu některý uživatel data do systému vkládá, jiný tato data vizualizuje a další zase nesmí daná data ani číst [18].

Řízení přístupů představuje jedno z hlavních interních bezpečnostních rizik. Pokud není dobře nastavené, hrozí přinejmenším neoprávněný přístup. Naopak je-li dobře definované a spravované, představuje základ kvalitní koncepce zabezpečení [10].

Právě oblast řízení přístupů bude jednou z hlavních, co se týče splnění souladu zpracování s požadavky Obecného nařízení, protože s jejím použitím lze dosáhnout splnění hned několika zásad zpracování. Téma řízení přístupů bude podrobněji rozebráno v samostatné kapitole 5.4.4.

5.2 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V RÁMCI FUNKCIONALITY ERP SYSTÉMU

Jak již bylo řečeno, ERP systémy pokrývají svou funkcionalitou různé okruhy. Ve většině okruhů dochází k formě zpracování osobních údajů. Je důležité identifikovat jaké údaje jsou zpracovávány a jak.

Také je důležité uvědomit si fakt, že podnik využívající ERP systém jakožto prostředek pro zpracování osobních údajů se staví do pozice správce osobních údajů. A je to správce, kdo musí uvést své zpracování do souladu s Obecným nařízením. Nařízení vlastně žádným způsobem nestanovuje povinnost dodavatelům systémů, aby jejich systémy plnily požadavky. Záleží tedy především na správci, jaký ERP zvolí (v případě, že si ho nechá dodat) a zdali je tento systém připravený plnit Obecné nařízení, nebo jestli vyvine vlastní systém, kde si bude jistý, že souladu s nařízením dosáhne.

5.2.1 OSOBNÍ ÚDAJE V JEDNOTLIVÝCH OBLASTECH

Dle aktivity podniku a celkové architektury ERP systému, který podnik využívá, bude docházet ke zpracování různých osobních údajů různých subjektů k různým účelům a na základě různých právních důvodů.

Je patrné, že v některých okruzích bude podle dostupných modulů docházet ke zpracování osobních údajů, zatímco v jiných nikoliv. Například v modulech zařizujících řízení financí se budou určitě vyskytovat osobní údaje fyzických osob vůči kterým má podnik závazek či pohledávku. V modulech pro řízení lidských zdrojů to budou zase osobní údaje o zaměstnancích. A naopak, v modulech podporujících výrobu se nemusí vyskytovat vůbec žádné osobní údaje.

5.3 GDPR Z POHLEDU DODAVATELE ERP SYSTÉMU

Dodavatel ERP systému se dle Obecného nařízení neřadí do role správce či zpracovatele, tím pádem pro něj nejsou povinnosti vycházející z Obecného nařízení příliš relevantní. Rozhodne-li se neprovádět úpravy či opatření pro dosažení souladu s GDPR, neexistuje žádná výslovná povinnost, která by ho k tomu donutila. Ačkoliv se dá předpokládat, že takové chování by bylo nelogické, jelikož připravenost dodávaného systému plnit Obecné nařízení představuje výhodu v konkurenčním boji, není vyloučeno, že se někteří dodavatelé rozhodnou nevěnovat mu žádnou pozornost.

Je to tedy záležitost především podniků v roli správců, aby vhodnými argumenty přesvědčili a v podstatě donutili dodavatele, aby jim dodávali ERP systémy a další služby s nimi spojené způsobem, jaký jim pomůže dosáhnout souladu s Obecným nařízením.

I v případě, že má podnik dobře sjednanou smlouvu s dodavatelem, jejíž součástí je tzv. legislativní update, tedy aktualizace v případě změn právních předpisů, nepředstavuje to pro dodavatele ERP systému povinnost k úpravám. Příčinou je fakt, že Obecné nařízení se nevztahuje na operace systému, nýbrž na zpracování správcem, resp. podnikem, který operace systému k němu využívá.

Přestože nejsou nároky správců na dodavatele nijak zakotveny v legislativě, neznamená to, že by se dodavatelé ERP systémů neměly plněním GDPR zabývat. Naopak, spíše se dá očekávat, že z vlastní iniciativy provedou technická opatření pro vyhovění požadavkům Obecného nařízení. Vyhnout se tak tlaku ze strany správců, kteří představují odběratele, a spíše posílí svou pozici v konkurenčním boji právě díky připravenosti plnit povinnosti stanovené Obecným nařízením.

S ohledem na čas se dá i říci, že dodavatelé, kteří nebudou schopni dodat „GDPR ready“ systém, nebudou vůbec konkurenceschopní. Z dlouhodobého hlediska je nepředstavitelná situace, kdy podnik v roli správce či zpracovatele využívá funkcí

systému, který mu nijak neusnadní plnění povinností dle Obecného nařízení, obzvlášť, když je jejich neplnění sankcionováno [19].

5.3.1 PRIVACY BY DESIGN

Přestože není zásada Privacy by Design v Obecném nařízení nijak definována či vůbec zmíněna, vychází z něj jakoby mimochodem [19]. Dle bodu 78 preambule Obecného nařízení je mimo jiné zmíněno, že:

„Pokud jde o vývoj, koncepci, výběr a používání aplikací, služeb a produktů, které jsou založeny na zpracování osobních údajů nebo osobní údaje za účelem plnění svých funkcí zpracovávají, je třeba zhotovitele těchto produktů, služeb a aplikací vybízet k tomu, aby při vývoji a koncipování těchto produktů, služeb a aplikací zohledňovali právo na ochranu údajů a brali náležitý ohled na stav techniky s cílem zajistit, aby správci a zpracovatelé mohli plnit své povinnosti v oblasti ochrany údajů.“ [4]

Privacy by Design tedy představuje přístup, dle kterého by měla být ochrana soukromí a osobních údajů brána v úvahu již při návrhu a tvorbě systémů. Celý princip stojí na sedmi základních pilířích:

- Proaktivní ne reaktivní (Proactive not Reactive) – je třeba předvídat rizika dopředu a zabránit invazivním událostem ještě před jejich děním
- Ochrana soukromí jako výchozí nastavení (Privacy as the Default Settings) – osobní údaje jsou automaticky chráněny
- Ochrana osobních údajů je součástí návrhu (Privacy Embedded into Design) – ochrana není brána jako doplněk, nýbrž je základním prvkem
- Plná funkčnost – pozitivní součet, nikoliv nula (Full Functionality – Positive-Sum not Zero-Sum) – ochrana soukromí v systému nenarušuje další funkce, řešení představuje „win-win“ situaci, tedy že ochrana je ku prospěchu celého systému, ne na jeho úkor
- Plná ochrana v celém životním cyklu (Full Lifecycle Protection) – ochrana je nepřetržitá po dobu celého životního cyklu systému
- Viditelnost a transparentnost (Visibility and Transparency) – prvky pro nastolení odpovědnosti a důvěry
- Respektování soukromí uživatelů (Respect for User Privacy) – systém by měl být navržen tak, aby umožnil uživatelům řídit jejich vlastní data [20]

Společně s pravidlem Privacy by Design se často pojí pravidlo Privacy by Default. Je důležité si uvědomit, že ačkoliv se zdá, že se jedná o dva rozdílné přístupy, Privacy by Default je vlastně, i dle výše zmíněných pilířů, imanentní vůči pravidlu Privacy by Design. Přístup Privacy by Default rozšiřuje druhý pilíř přístupu Privacy by Design, a to tak, že osobní údaje jsou nejen chráněny automaticky od počátku, ale jsou chráněny nejvyšší možnou mírou, kterou systém dovoluje. Uživatel se samozřejmě může rozhodnout pro snížení ochrany soukromí, ale tato situace typicky nastává až v pozdějších fázích životního cyklu systému [1].

5.4 OBECNÝ NÁVRH FUNKCIONALITY PRO IMPLEMENTACI POŽADAVKŮ GDPR DO ERP SYSTÉMŮ

Jak již bylo zmíněno, právně není dodavatel systémů nijak nucen provést úpravy systému pro plnění Obecného nařízení. Má-li však motivaci k tomu potřebná opatření a úpravy provést, bude potřeba identifikovat nedostatky funkcionality systému. Ty budou tvořeny především rozdíly a novinkami oproti předchozí právní úpravě, zákonu č. 101/2000 Sb., o ochraně osobních údajů, ačkoliv není řečeno, že povinnosti vycházející z této předchozí právní úpravy byly ve funkcionalitě již zahrnuty.

Následující návrh rozšíření funkcionality vychází z povinností a požadavků Obecného nařízení, které jsou detailně popsány v teoretické části práce, a to především v kapitolách 4.4, 4.5, 4.6 a 4.8. Návrh pro úspěšnou implementaci požadavků Obecného nařízení je obecný, to znamená, že pojednává o tom, čeho dosáhnout, nikoliv však už jakým způsobem. Dodavatelé systémů, pokud se pro implementaci rozhodnou, budou řešit způsob dosažení kýžené funkcionality vlastním způsobem především na úrovni zdrojového kódu.

Zatímco některé povinnosti nelze plnit funkcionalitou ERP systému, např. zásada minimalizace musí být plněna nastavením samotných operací zpracování a nikoliv nastavením systému, jiné mohou být plněny, jako třeba zásada zákonnosti. Návrh funkcionality vychází právě z těchto povinností a požadavků, které mohou být splněny funkcionalitou ERP systému. Následující kapitoly byly vytvořeny systematicky dle zmíněných odpovídajících kapitol z teoretické části práce a rámcově popisují, jaké povinnosti vycházející z Obecného nařízení mohou být danými funkcemi plněny.

5.4.1 SPRÁVA SOUHLASŮ PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Při plnění zásady zákonnosti může být jedním z právních důvodů zpracování osobních údajů i souhlas subjektu údajů.

ERP systém může správci v tomto smyslu velice usnadnit veškerou správu souhlasů pro zpracování osobních údajů. Mezi funkcionalitu by se mohlo řadit:

- integrace do webového rozhraní
- automatizované zpracování souhlasů z e-mailových zpráv
- ukládání souhlasů do databáze
- třídění souhlasů dle kategorie údajů, účelu zpracování apod.
- automatické hlídání doby platnosti souhlasů
- rozesílání e-mailů pro obnovení platnosti souhlasů

Výše zmíněné funkce představují jen návrhy funkcionality pro správu souhlasů. Není možné konkrétně určit co a jak implementovat, jednak proto, že Obecné nařízení je obecné a každý podnik tak plní odlišné podmínky, a jednak protože i architektura ERP systémů je ve vysoké míře customizovatelná.

Pro dodržení povinnosti usnadnit odvolání souhlasu do té míry, jako je snadné ho poskytnout, bylo by vhodné analogicky rozšířit funkcionalitu správy souhlasů i na odvolání souhlasů.

5.4.2 EVIDENCE ÚČELŮ ZPRACOVÁNÍ

Pro efektivní spravování osobních údajů a jejich zpracování bude vhodné, aby systém povolil speciálně evidovat a spravovat účely zpracování. Ke každému účelů se vztahuje jiný právní důvod pro zpracování. Bude-li zpracování probíhat na základě souhlasu, pak bude účel propojen s příslušnými souhlasy. Pro jiný účel bude zase možné zpracovávat osobní údaje na základě plnění smlouvy, a funkcionalita ERP by mohla dovolit propojit evidované smlouvy právě s tímto daným účelem.

Hlavním smyslem evidence účelů zpracování je prokazatelné plnění zásady zákonnosti Obecného nařízení a zároveň také částečně zásady omezení účelu. Zde je však nutné zmínit, že plnění zásady omezení účelu bude závislé především na nastavení na straně podniku, jakož i plnění zásady minimalizace údajů, které s ním úzce souvisí.

5.4.3 ULOŽENÍ OSOBNÍCH ÚDAJŮ

Správně strukturovaná data uložená v databázi mohou v mnoha ohledech výrazně zlepšit plnění souladu s GDPR. Na takto uložené osobní údaje poté může navazovat nespočet dalších operací.

Umožní-li ERP ukládat do databáze osobní údaje a provázat je s databází souhlasů, bude například možné hlídat zákonnost zpracování na základě platnosti souhlasu. Zpracování na základě jiných právních důvodů, představované například plněním pracovní smlouvy, by poté mohlo být představované adekvátním propojením mezi databází s osobními údaji a pracovními smlouvami. Zmíněná provázanost mezi různými daty pak výrazně usnadní plnění a jeho dokazování týkající se například zásad zákonnosti, omezení účelu, omezení uložení apod.

Centralizované uložení dat prostřednictvím ERP s dobře zvolenou strukturou uložených osobních údajů představuje potenciální výhodu pro plnění zásad dle Obecného nařízení. Například dodržení zásady přesnosti, kdy má správce za povinnost zpracovávat údaje v přesné a správné podobě, bude jednodušší, protože může být snazší odhalit nepřesnosti.

Práva subjektů na opravu, omezení zpracování či přístup k osobním údajům může být správným uložením dat opět velmi usnadněno. Oprava představuje obdobný postup jako plnění zásady přesnosti, kdy je činnost podstatně ulehčena správnou strukturalizací. Omezení zpracování může být při správném nastavení otázka několika málo operací stejně jako výkon práva subjektu údajů na přístup k osobním údajům.

Důležité bude, aby funkcionalita ERP systému umožňovala plnit i právo na přenositelnost údajů, které je upravováno Obecným nařízením nově v porovnání s předchozím zákonem o ochraně osobních údajů, a může být, vzhledem k automatizované povaze systému, v tomto případě uplatnitelné, pokud se údaje zpracovávají na základě souhlasu či smlouvy. Jedná se o získání výpisu všech zpracovávaných osobních údajů daného subjektu, který je ve strukturovaném, běžně používaném a strojově čitelném formátu. Správce, v této chvíli tedy podnik využívající ERP systém, musí být v některých případech též schopný dané osobní údaje ve zmíněném tvaru předat jinému správci. V rámci tohoto práva se však poskytují jen údaje, které byly vědomě poskytnuty subjektem, a nikoliv údaje z nich odvozené nebo vypočítané.

V rámci uplatňování tohoto práva jsou zde kladeny vysoké nároky na funkcionalitu, které by měl podporovat hlídání podmínek pro výkon (nejen) tohoto práva, provázanost s databází požadovaných údajů a označení údajů, které se naopak výkonu práva netýkají (jimiž mohou být například zmíněné odvozené údaje).

Právo, které je svým způsobem velmi záludné, je právo na výmaz. Praxe doposud neukázala, jak dalece toto právo sahá. Dle Obecného nařízení jde o vymazání veškerých osobních údajů, které správce o subjektu údajů zpracovává. Pokud zpracování údajů pozbude svůj účel jeho naplněním, výmaz je předpokládaný a naprosto samozřejmý. Problém nastává ve chvíli, kdy by došlo např. k odvolání souhlasu se zpracováním, a údaje daného subjektu údajů jsou zpracovávány například v rámci algoritmu velice komplexního obchodního rozhodování či jsou obsaženy v zálohách systémů. Zálohy systémů obsahují osobní údaje, ale technicky není možné se zálohami manipulovat takovým způsobem, aby došlo k jejich vymazání. Pokud by došlo k takovému pokusu, zálohy by se mohly poškodit a v jistých případech by to mohlo znamenat ohrožení chodu podniku [21]. Z jiného úhlu pohledu by se však dalo říci, že osobní údaje obsažené v zálohách systému nejsou zpracovávány až do chvíle, kdy by došlo k faktickému obnovení. Pak by se podnik, jakožto správce osobních údajů, musel postarat o dodatečný výmaz daných osobních údajů v rámci plnění práva na výmaz.

5.4.4 PŘÍSTUPOVÁ PRÁVA K OSOBNÍM ÚDAJŮM

Přístupová práva by se zpravidla měla definovat pro co nejkonkrétnější části systému. Je nepřípustné, aby byla práva nastavena obecně v rámci celého systému, protože pak by ve své podstatě popírala svůj účel – řízení přístupů. Pro ERP systém by bylo ideální definovat přístupová práva na úrovni jednotlivých funkcí modulů. Tento přístup může být sice náročný jak časově, tak technicky, ale kvalitní zajištění přístupových práv napomůže minimalizovat případy neautorizovaného přístupu a v rámci požadavků Obecného nařízení tím dokáže plnit hned několik zásad.

Nelze dosáhnout plného potenciálu řízení přístupů pomocí přístupových práv, pokud by nedocházelo k pravidelné revizi. Nutné je revidovat nejen aktivní účty, ale i ty neaktivní či neplatné. Kdyby se například do systému po několika měsících přihlásil bývalý zaměstnanec, mohlo by to představovat závažný bezpečnostní incident, kterému jednoduše zabrání právě pravidelná a důkladná revize přístupových práv.

Přístupová práva k osobním údajům se budou nastavovat především dle účelu a právního důvodu zpracování. Je potřeba, aby byl přístup k různým osobním údajům povolen jen vybranému okruhu uživatelů. Typicky se může jednat o zpracování osobních údajů zaměstnanců pro potřebu oddělení HR. Správně nastavené řízení přístupů chrání nejen proti neoprávněnému přístupu, ale například i proti neodbornému nakládání s daty či proti náhodné změně nebo ztrátě. Přístupová práva pomáhají řešit otázku bezpečnosti osobních údajů z interního prostředí podniku.

Ačkoliv se dá předpokládat, že řízení přístupových práv je standartně dostupné v běžných modulech ERP systémů, zde je důležitá návaznost právě například na evidenci účelů zpracování. Nejedná se tedy explicitně o novou funkcionalitu, nýbrž spíše o rozšíření té stávající.

Klíčové je pamatovat také na skutečnost, že řízení přístupů musí fungovat i v rámci fyzických přístupů. Je zcela zbytečné zabývat se komplexním rozdělením přístupových práv mezi uživatele systému, když například běžně dochází ke sdílení osobních počítačů mezi zaměstnanci, zaměstnanci si nezamykají počítače při odchodu na přestávku či když jsou kanceláře přístupné někomu, kdo do takových prostor nemá mít oprávnění ke vstupu.

5.4.5 ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Nespornou výhodou ERP systémů je centralizace uložení dat. Některé formy uložení dat, jako například dokumenty v textovém formátu, mají nízký standard ochrany. Uložení v prostředí ERP systému však výrazně pomůže se zabezpečením, ať je forma dat téměř jakákoliv.

Obecné nařízení stanovuje, že správce je povinen podniknout veškerá vhodná technická a organizační opatření pro zabezpečení osobních údajů. Dá se tedy předpokládat, že podnik zůstane dle zásady Privacy by Default u bezpečnostního nastavení, se kterým dodavatel systém dodává, jelikož se automaticky jedná o nejvyšší možné zabezpečení systému. Výjimky se ale mohou vyskytnout v případě, kdy má podnik sám o sobě schopnost zařídit ještě vyšší úroveň zabezpečení, a je kvůli tomu třeba snížit úroveň zabezpečení ERP systému.

Dle Obecného nařízení se v rámci zabezpečení osobních údajů doporučuje využít pseudonymizace či šifrování. ERP by tedy měl disponovat i náležitými funkcemi, které toto usnadní.

Do schopnosti zabezpečit osobní údaje se řadí také způsobilost obnovit dostupnost osobních údajů v případě fyzických či technických incidentů. Zálohování nejen dat, ale i systému se jeví jako vhodná volba. Situace, kdy by k zálohování mělo docházet, jsou zpravidla dvě – pravidelné zálohy závislé na čase a zálohy před podstatnými změnami, např. instalace nového softwaru, update systému nebo restrukturalizace dat v databázi.

5.4.6 HLÁŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Zabezpečení není nepřekonatelné, ať je sebelepší. Dojde-li k prolomení zabezpečení, může vzniknout riziko pro práva a svobody fyzických osob. Únik dat je dle Obecného nařízení nutné v různých situacích dle vzniklého rizika ohlašovat dozorovému úřadu nebo i dotčenému subjektu údajů.

Funkcionalita ERP může v tomto směru pomoci se zjištěním incidentu a rizika, které vzniklo v jeho důsledku. Systém může automaticky vytvořit report, který bude obsahovat informace o tom jaká data v jaké části systému jsou zasažena tímto incidentem, jak jsou daná data chráněna (např. šifrování) a jaký je charakter incidentu (např. náhodné smazání chybou disku, neautorizovaný přístup chybou politiky přístupů, škodlivý kód z vnějšího prostředí podniku aj.), a odeslat ho pověřené osobě například formou e-mailu nebo SMS zprávy. Takový report pak může být i součástí ohlášení porušení zabezpečení osobních údajů dozorovému úřadu, kdy je nutné posílat i popis povahy incidentu, jehož součástí jsou kategorie dotčených údajů, počet dotčených subjektů údajů a záznamů osobních údajů.

Je velmi nepravděpodobné, však nevyloučitelné, že by systém nabídl funkce pro automatické oznamování incidentů subjektům údajů. Podmínkou je totiž přítomnost vysokého rizika a povinnost oznámení není nutné splnit v případě, že správce přijme opatření, díky kterým se vysoké riziko pravděpodobně neprojeví. Toto jsou okolnosti, které by měly být zváženy za přítomnosti lidského faktoru, protože nejsou natolik předvídatelné, aby se tato činnost dala automatizovat.

5.4.7 LIKVIDACE OSOBNÍCH ÚDAJŮ

Pozbude-li správce poslední právní důvod pro zpracování osobních údajů, je povinen je zlikvidovat. Ačkoliv se nejčastěji jedná o výmaz, likvidace může být provedena i jinými způsoby.

Nejčastější formou likvidace mimo vymazání je anonymizace údajů. Převedení do anonymní podoby odstraní veškeré vazby vedoucí k identifikaci fyzické osoby a tím splní podmínku pro likvidaci takových osobních údajů. Převod do anonymní formy může být díky automatizaci jednoduchý i v případě velkého objemu dat.

5.4.8 DOKUMENTACE PRO SOUČINNOST S DOZOROVÝM ÚŘADEM

Ačkoliv malé a střední podniky zpravidla nejsou povinny vést záznamy o činnosti zpracování, v případě, kdy by se na ně vztahovala výjimka, může ERP systém pomoci s exportem důležitých informací pro zpracování v záznamu o činnosti. Jedná se především o účely zpracování, popisy kategorií subjektů údajů a popisy kategorií osobních údajů.
Pokud podnik nemá povinnost vést záznam o činnosti zpracování, existují jiné důvody pro komunikaci s dozorovým úřadem. Ať se jedná o již zmíněné ohlašování porušení zabezpečení osobních údajů, které má správce povinnost ukládat, či různé dokumenty pro kooperaci při šetření dozorovým úřadem.

5.5 IMPLEMENTACE FUNKCIONALITY DO ERP SYSTÉMU

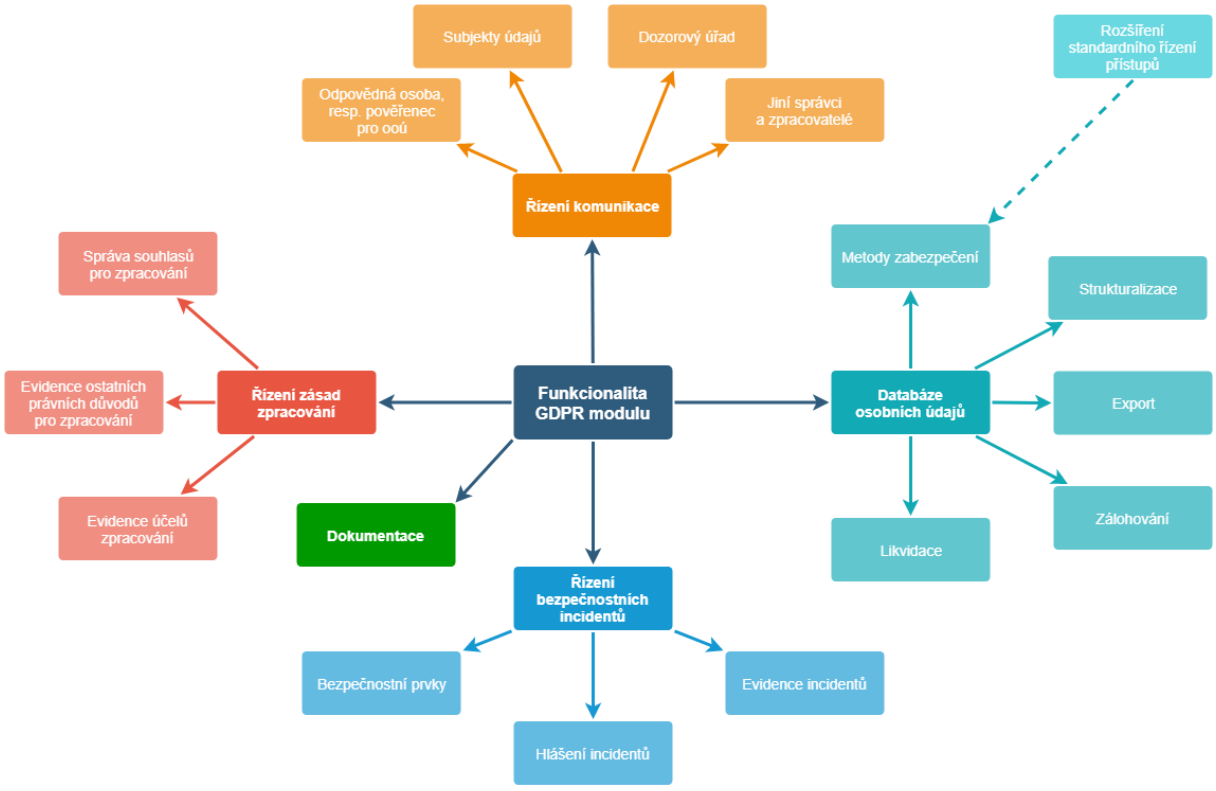
Dá se předpokládat, že pro implementaci funkcionality pro plnění požadavků Obecného nařízení se dá v rámci architektury ERP systému využít samostatného modulu. Takový modul by nabízel nové funkcionality pro pohodlné plnění nových požadavků a provázal by dle potřeby funkce se stávajícími moduly.
Možná funkcionalita „GDPR“ modulu je graficky znázorněna schématem na obrázku 2, kde jsou zahrnuty nejen důležité funkce, které byly zmíněny výše, ale i další podpůrné funkce týkající se operací zpracování osobních údajů. Barevně jsou odlišeny jednotlivé tematické bloky, pro lepší orientaci. Schéma je orientováno směrem ze středu ke krajům
K jeho vzniku došlo systematickým zpracováním výstupů analýzy přehledové studie, jež vycházely především z teoretické části práce a jejích kapitol 4.4, 4.5, 4.6 a 4.8. Jednotlivé funkce jsou analogické k povinnostem a požadavkům, které jsou zmíněny v rámci těchto kapitol.
Funkční blok Databáze osobních údajů vychází především z plnění zásad zpracování a povinnosti plnit práva subjektu údajů. Toto usnadňují funkce Strukturalizace, Export, Zálohování a Likvidace. Funkce Metody zabezpečení obsahují především technická opatření pro dostatečné zabezpečení dat zvenčí, ale existuje zde i návaznost na již fungující řízení přístupů, aby byla zajištěna i dostatečná ochrana z vnitřního prostředí.

Blok pro Řízení bezpečnostních incidentů obsahuje jednak Bezpečnostní prvky, které jsou technickými prostředky pro zajištění ochrany dat, a jednak také funkci pro Hlášení incidentů, díky které se odpovědná osoba ihned dozví o nastalém incidentu. Tato funkce může plnit ohlašovací povinnost dozorovému úřadu a umí připravit podklady pro případné plnění oznamovací povinnosti subjektům údajů. V neposlední řadě Evidence incidentů dovoluje ukládat záznamy o incidentech a například i dle určených kritérií incidenty porovnávat a hodnotit.

Dokumentace je multifunkční blok, může obsahovat mnoho druhů dokumentace, kterou podnik vyhodnotí jako relevantní k tématu GDPR. Potenciálně to je dokumentace k vnitropodnikovým politikám, kodexům, operacím zpracování či samostatnému nastavení ERP systému a jednotlivých modulů.

Řízení zásad zpracování se týká specificky správy veškerých právních důvodů zpracování, a to jak jejich druhů, tak i konkrétních podob, jako například souhlas se zpracováním, smlouva apod.

Blok nazvaný Řízení komunikace zajišťuje nejen komunikaci jako takovou, ale hlavně plnění práv a povinností vůči ostatním subjektům, jako jsou subjekty údajů, dozorový úřad či zpracovatelé, jiní správci aj. Též zahrnuje odpovědnou osobu, resp. pověřence pro ochranu osobních údajů.



Obrázek 2: Schéma funkcionality modulu „GDPR“ pro ERP systém, vlastní zpracování autora

Rozhodně se nejedná o jedinou možnost implementace, vlastně bude záležet především na rozhodnutí dodavatele systému. Samostatný modul však nabízí několik nesporných výhod. Tak, jako je jednoduché modul přidat, je opět jednoduché ho odebrat. V každém případě, kdyby se podnik rozhodl řešit soulad s Obecným nařízením jinak než využitím funckionality ERP systému, nebude toto činit problém. Další výhodou je, že soustřeďování funkcí do jednoho modulu usnadní jejich úpravy do budoucna.

Očekává se, že jednotlivé funkční okruhy modulu jsou provázané a vychází jeden ze druhého, jak bylo popsáno v předchozí kapitole. V případě potřeby dojde ke spojení i s funkcemi z jiného modulu, např. se správním modulem v případě řízení přístupů.

S dodáním modulu by podniku měla být k dispozici též dokumentace, obsahující detailnější popisy jednotlivých částí. Též by bylo vhodné zahrnout připomenutí, že aplikací tohoto modulu nedojde automaticky ke splnění požadavků kladených Obecným nařízením. Dosažení souladu je povinnost podniku jakožto správce a ERP systém osazený tímto modulem není samospásný.

To se týká i jednotlivých funkcionalit. Systém nabízí možnosti, kterými docílit souladu, ale podnik, resp. nějaký odpovědný pracovník je musí nejdříve správně nastavit. Se správným nastavením lze poté předpokládat dostatečnou úroveň automatizace.

Nyní následuje rekapitulace povinností a požadavků, které jednotlivé tematické bloky „GDPR“ modulu dokážou plnit:

- Databáze osobních údajů – zásada přesnosti, zásada omezení uložení, zásada integrity a důvěrnosti, právo na přístup k osobním údajům, právo na opravu, právo na výmaz, právo na omezení zpracování, právo na přenositelnost
- Řízení bezpečnostních incidentů – zásada integrity a důvěrnosti, ohlašovací povinnost při porušení zabezpečení
- Dokumentace – veškeré zásady, dokládání souladu zpracování
- Řízení zásad zpracování – veškeré zásady, doložitelnost souhlasu se zpracováním, právo na informace
- Řízení komunikace – zásada korektnosti, zásada transparentnosti, veškerá práva, předchozí konzultace s dozorovým úřadem, ohlašovací povinnost při porušení zabezpečení, oznamovací povinnost při porušení zabezpečení

Z výčtu je patrné, že „GDPR“ modul může být schopný zajistit téměř veškeré povinnosti a požadavky vycházející z Obecného nařízení. Výjimku tvoří blok Dokumentace, protože ve chvíli, kdy správce vloží špatné dokumenty, ze kterých vychází nastavení modulu,

nemusí dojít ke správnému plnění všech zásad. Kupříkladu zásada minimalizace je výslovně založena na správném nastavení od správce, resp. odpovědné osoby, jelikož funkcionalita systému sama o sobě nedokáže vyhodnotit plnění této zásady.
Funkce zajišťující plnění ostatních zásad, práv a povinností mohou být v podstatě tohoto výkonu schopny již s nastavením od dodavatele, tedy například zásada omezení uložení bude plněna díky propojení Databáze osobních údajů a konkrétních údajů se Správou souhlasů pro zpracování, resp. Evidencí ostatních právních důvodů pro zpracování.

5.6 GDPR Z POHLEDU SPRÁVCE OSOBNÍCH ÚDAJŮ JAKOŽTO UŽIVATELE ERP SYSTÉMU

Podnik se jako správce osobních údajů staví do pozice, kdy může být sankcionován za nesplnění podmínek stanovených Obecným nařízením. Rozhodne-li se podnik využívat ERP systému pro zpracování osobních údajů, je především jeho povinností zajistit, že je takový systém kompatibilní s nařízením. Ačkoliv může dodavatel tvrdit, že systém požadavky plní, je téměř nemožné přenést na něj odpovědnost v opačném případě, pakliže neexistuje například smlouva, kde je tento bod explicitně vyjádřen. Ani tehdy však nemůže dojít k úplnému přenesení odpovědnosti.

5.7 OBECNÉ KROKY ANALÝZY SOULADU FUNKCIONALITY ERP SYSTÉMU S GDPR

V situaci, kdy správce potřebuje analyzovat zpracování osobních údajů v prostředí ERP systému a zjistit, zda je možné ho považovat za vyhovující, je nutné provést analýzu i ve srovnání vůči podnikovým procesům mimo ERP systém. Úspěšné provedení analýzy souladu ERP systému s požadavky Obecného nařízení provází několik kroků, které budou dále popsány. Opět se jedná o obecné kroky, protože každý podnik má specifické prostředí a plní různé povinnosti pro dosažení souladu s GDPR.
Také je třeba zmínit, že podnik se může rozhodnout zjistit soulad ERP systému s Obecným nařízením jinak, například v rámci celopodnikové analýzy souladu zpracování osobních údajů. Zde zmíněné kroky budou vhodné například v situacích, kdy podnik provází změny v systému a dá se předpokládat, že mimo ERP tímto nedošlo k nesouladu s podmínkami Obecného nařízení.

5.7.1 AUDIT OSOBNÍCH ÚDAJŮ

Nejprve je potřeba určit veškeré osobní údaje, které správce, tedy podnik, zpracovává. Ačkoliv toto ještě přímo nesouvisí se samotným ERP systémem, zjištění poslouží jako podklad k následujícím krokům. Především půjde o posouzení, ve kterých oblastech ke zpracování osobních údajů dochází, jaké osobní údaje se zpracovávají, za jakým účelem a na základě jakého právního důvodu.

Výstupem auditu je katalog osobních údajů. Jedná se o seznam veškerých osobních údajů, včetně jejich kategorizace, které podnik zpracovává. Též by měl obsahovat účel zpracování a právní důvody k němu. Zde by také už mělo dojít k označení těch osobních údajů, jež jsou zpracovávány v prostředí ERP systému [22].

5.7.2 KATALOG OPERACÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

V závislosti na vazbě k jednotlivým kategoriím osobních údajů je nutné též určit operace, které se v rámci funkcionality ERP systému s danými osobními údaji dějí. Zmíněný katalog bude obsahovat především:

- příjemce
- typy zpracování
- osoby oprávněné k přístupu
- dobu uchování
- způsob likvidace

Ideální je popsat i celý standartní životní cyklus zpracování osobních údajů:

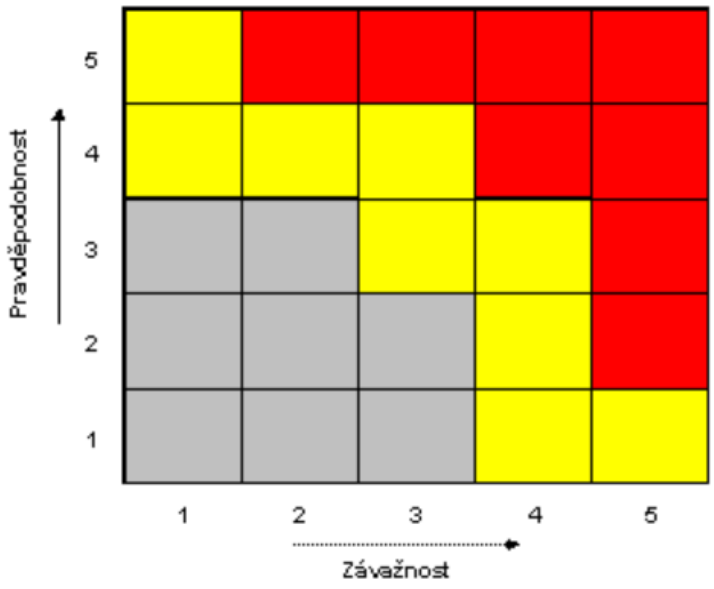
- sběr
- uchování
- využití
- předávání
- likvidace [22]

Ve výjimečných situacích se může stát, že operace zpracování osobních údajů v systému ERP mohou pozměnit účel. Nemusí to nutně znamenat, že přibyly nové operace, které se s osobními údajů provádí, ale správce si například nemusel být do této doby jistý plnou funkcionalitou systému. V takové situaci je zapotřebí, aby si správce uvědomil, zda je vhodné tyto operace zahrnout a účel zpracování přeformulovat či jestli musí dojít k omezení využití těchto operací pro zpracovávání údajů pro současně definovaný účel.

5.7.3 ANALÝZA RIZIK

Obecné nařízení mimo jiné podporuje tzv. přístup založený na riziku. Ten obecně znamená, že správce je povinen s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování a možným rizikům přijmout adekvátní technická a organizačná opatření, aby došlo k zajištění zabezpečení osobních údajů, které je odpovídající riziku, jež dané zpracování pro subjekty údajů představuje [1]. Analýza by měla prvně stanovit, v jakých případech představuje zpracování riziko nebo vysoké riziko. Pro vyhodnocení se dá použít například klasická matice pro vyhodnocení rizik, která může být v potřebných případech náležitě upravena, kdy šedá pole nepředstavují riziko, žlutá pole představují riziko a červená pole představují vysoké riziko. Míra rizika se určí na základě kombinace pravděpodobnosti (frekvence výskytu) a závažnosti. Tato míra rizika poté ukládá, mimo nutných technických a organizačních opatření, také povinnosti ohlašování a oznamování případů porušení zabezpečení osobních údajů. Samozřejmě je možné, aby podnik vyhodnotil rizika i pomocí jiných metod, které využívá například v rámci vlastního managementu rizik.

Dalším krokem, který následuje po vyhodnocení situací, je posouzení následků a přijetí potřebných opatření pro minimalizaci či eliminaci těchto rizik, případně přijetí rizik [22]. Na základě analýzy a posouzení následků je nutné navrhnout již konkrétní opatření, která podnik buď samovolně nebo za pomoci dodavatele systému aplikuje.



Obrázek 3: Matice rizik [23]

5.7.4 VOLBA TECHNICKÝCH OPATŘENÍ

Na základě předchozích kroků by již měl mít podnik stanoveno, jaká opatření je třeba podniknout pro splnění souladu zpracování osobních údajů prostřednictvím ERP systému s Obecným nařízením. Nyní je nutné rozhodnout, zda je podnik schopný a je kompetentní provést opatření vlastními prostředky (např. nastavení funkcí v ERP systému) či bude nezbytná asistence dodavatele systému (úprava softwarové části systému).

Co se týče opatření, která může provést podnik samotný, je důležité uvědomit si, které zásady a povinnosti vycházející z Obecného nařízení není možné plnit samotnou funkcionalitou systému. Typicky se bude jednat například o dosažení zásady minimalizace. Ač může být ERP systém sebevíce připraven plnit nařízení, sám o sobě neumí rozpoznat správné plnění této zásady. Nastavení potřených funkcí a operací je v kompetenci samotného podniku, který se musí postarat o sběr pouze těch údajů, které jsou přiměřené, relevantní a omezené na nezbytně nutný rozsah pro plnění účelu zpracování. Teprve po správné definici těchto údajů je možné od systému očekávat asistenci v tomto smyslu.

5.7.5 VYHODNOCENÍ ANALÝZY

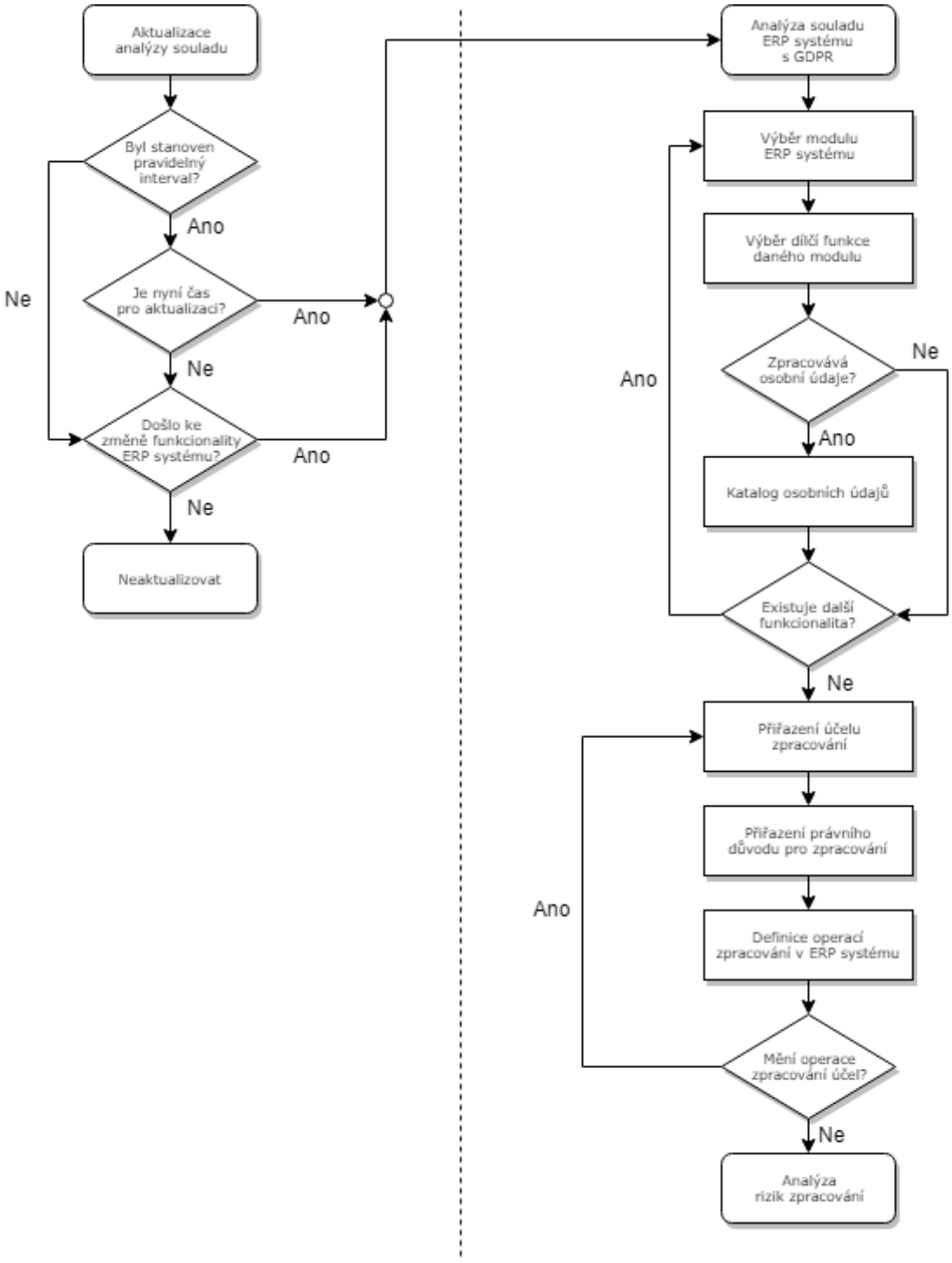
Obrázek 4 znázorňuje pomocí procesního diagramu možný postup výše zmíněné analýzy souladu funckionality ERP systému s Obecným nařízením. Ačkoliv se předpokládá, že tímto postupem bude souladu nakonec dosaženo, bude-li dodavatel systému nepřístupný co se týče nutných změn pro dosažení dostatečných technických opatření, může nastat situace, že podnik bude disponovat systémem, který není připravený plnit nařízení.

V takovém případě se nabízí několik možností, které podnik může volit. Buď, je-li to možné, změnit operace zpracování mimo systém (aby došlo k minimalizaci rizika takovým způsobem, že zpracování v systému nepředstavuje nezvladatelné riziko), nebo se pokusit o spolupráci s jiným dodavatelem.

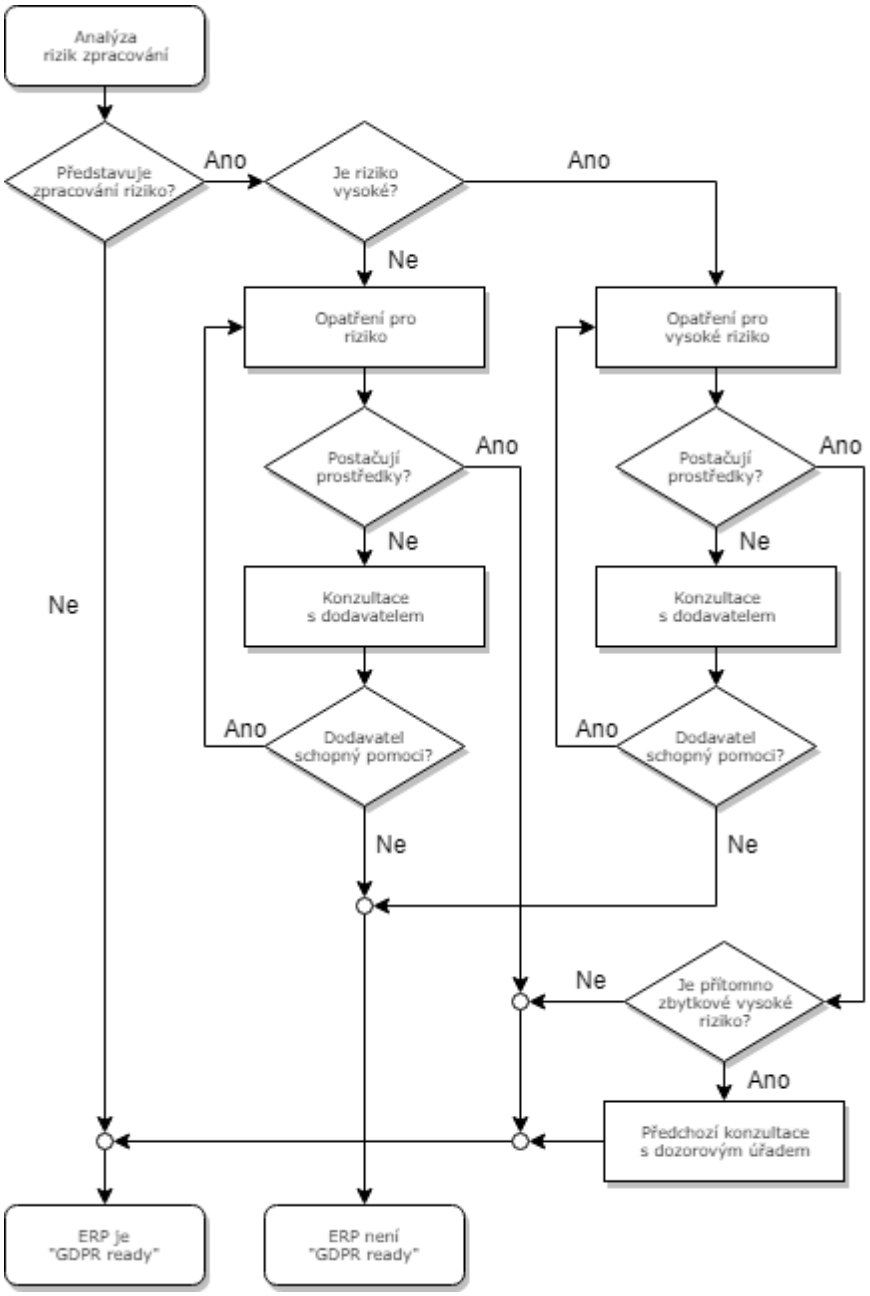
5.7.6 AKTUALIZACE ANALÝZY

Samozřejmě bude nutné znovu kontrolovat soulad funkcionality ERP systému na základě různých okolností. Ačkoliv není úplně nezbytné provádět aktualizace analýzy pravidelně, rozhodne-li se podnik stanovit pravidelné intervaly kontroly souladu, bude to jen k dobru. V každém případě, kdykoliv dojde ke změně funkcionality systému či rozšíření operací zpracování prováděných prostřednictvím systému, mělo by dojít k aktualizaci.

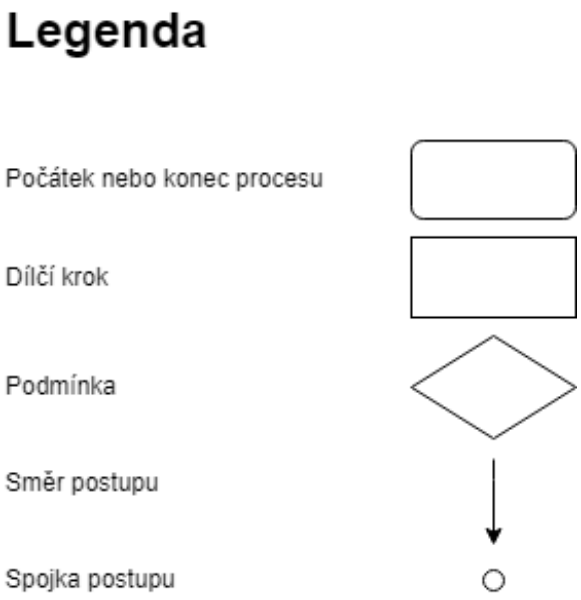
Analýza by měla být provedena znovu i v případech porušení zabezpečení osobních údajů, aby byl opět kriticky zhodnocen stav systému. Při porušení ochrany se dá téměř jistě očekávat, že byla špatně provedena analýza rizik nebo byla přijata špatná či nedostačující opatření, případně nastala nepředvídatelná situace, která s sebou přinesla nová rizika, která je aktuálně nutné zvážit.



Obrázek 4: Procesní diagram analýzy souladu ERP systému s GDPR, 1. část, vlastní zpracování autora



Obrázek 5: Procesní diagram analýzy souladu ERP systému s GDPR, 2. část, vlastní zpracování autora



Obrázek 6: Legenda významu prvků procesního diagramu, vlastní zpracování autora

5.7.7 POPIS PROCESNÍHO DIAGRAMU ANALÝZY SOULADU

Procesní diagram představuje grafické znázornění posloupnosti aplikace výše zmíněných kroků. Opět se jedná o obecný návrh, nejsou tedy vyloučeny změny zapříčiněné individuálními potřebami podniku, jako již bylo zmíněno dříve.

Proces Analýza souladu ERP systému s GDPR začíná obrázkem 4 a pokračuje od kroku Analýza rizik zpracování, který je na obrázku 5. Legenda s významem prvků, které jsou použity v procesním diagramu, je vysvětlena v obrázku 6.

Při procesu Analýzy souladu je nutné postupovat systematicky, vybrat modul a dále jeho jednotlivé funkce. Pokud taková funkce zpracovává osobní údaje, zapíše se formou záznamu do katalogu osobních údajů, pokud ne, nezapisuje se. Po dokončení analýzy veškerých modulů a jejich funkcí následuje zpracování záznamů v katalogu osobních údajů, kdy se k nim přiřazují účely zpracování, právní důvody pro zpracování a hlavně samotné operace zpracování. V některých případech se může stát, že přiřazené operace změní účel zpracování a je potřeba se vrátit ke kroku přiřazování účelu a přehodnotit ho ve vztahu k určenému záznamu. Ačkoliv tato situace nastane zřídka.

Nyní, když je k dispozici v podstatě kompletní záznam osobních údajů a operací zpracování, které se s nimi provádí, je možné provést analýzu rizik tohoto zpracování. Je odpovědností každého podniku nastavit si správně kritéria pro provedení této analýzy.

Nelze je ale nijak konkrétně doporučit, a to především proto, že Obecné nařízení samo nekonkretizuje, jak hodnotit míru rizika, pouze, že musí být posouzena dle povahy, rozsahu, kontextu a účelu zpracování. Pro podnik tak může být identifikace hranice mezi rizikem a vysokým rizikem poměrně choulostivou záležitostí. Obecné nařízení ale podává alespoň nápovědu ve smyslu příkladů možných vysokých rizik při zpracování. Mohou jimi být například využití nových technologií pro zpracování či zpracování citlivých údajů.

Části se zavedením opatření pro riziko a pro vysoké riziko jsou velmi podobné. Je to především kvůli již zmíněné neurčitosti hranice mezi rizikem a vysokým rizikem. Podstatný rozdíl je zde v tom, že opatření při normální míře rizika mohou zajistit přijetí rizika, ale při vysokém riziku je nutné, aby opatření minimalizovala míru tohoto rizika. Není-li podnik schopný toho dosáhnout svými prostředky, resp. prostředky dodavatele, vyvstane pro něj povinnost předchozí konzultace s dozorovým úřadem.

I když se očekává, že výsledkem této analýzy bude připravenost systému, protože donutí podnik přijmout potřebná opatření, může nastat situace, kdy podnik nebude disponovat prostředky pro dosáhnutí souladu, a to ani za pomoci dodavatele. Tehdy bude závěrem analýzy nepřipravenost ERP systému a podnik bude zřejmě nucen provést radikální změny, aby tohoto souladu dosáhl.

Obrázek 4 obsahuje nejen první část procesu Analýzy souladu, ale obsahuje také druhý, spřízněný proces, jímž je Aktualizace analýzy souladu. Kdykoliv jsou totiž naplněny podmínky pro provedení aktualizace analýzy, provádí se všechny kroky procesu Analýzy souladu znovu. Podmínku představuje buď plnění pravidelného intervalu aktualizace, nebo změna funkcionality systému, která může mít vliv na zpracování osobních údajů. Za změnu funkcionality se může považovat jak rozšíření té dosavadní, tak i důležité úpravy, které se provádí po předchozím negativním výsledku analýzy souladu

6 SHRNUTÍ VÝSLEDKŮ

Obecné nařízení GDPR nemá přímý legislativní dopad na ERP systémy ani na jejich budoucí vývoj. Jsou-li však brány v potaz dopady, které nejsou legislativního charakteru, těch je několik, přičemž práce zmiňuje ty hlavní.

První dopad se projeví u dodavatelů ERP systémů. Ačkoliv nemají zákonnou povinnost implementovat řešení požadavků Obecného nařízení do nabízených systémů, v průběhu času nebudou mít jinou možnost, jelikož ERP systém, který nebude schopný integrovat procesy týkající se Obecného nařízení, resp. ochrany osobních údajů všeobecně, nebude konkurenceschopný. Jako řešení tohoto dopadu je v práci navržena obecná funkcionalita ERP systému, která je schopná pomoci s plněním požadavků Obecného nařízení. Taková funkcionalita představuje rozšíření té stávající například prostřednictvím soustředění do „GDPR“ modulu. Kromě vyjádření slovním popisem je tento návrh funkcionality také vyjádřen graficky schématem.

Klíčové u této funkcionality je vzájemná provázanost jednotlivých funkčních bloků, kdy jejich součinností dojde ke splnění téměř všech zásad zpracování a dalších povinností a požadavků kladených Obecným nařízením. Za zmínku stojí blok Dokumentace, protože neplní jen pasivní funkci úložiště dokumentů, ale z dokumentů aktivně vychází a upravuje nastavení všech ostatních bloků. Přistupuje-li podnik zodpovědně k vedení těchto dokumentů, funkcionalita bloku Dokumenty významně pomůže například s jinak náročným splněním zásady minimalizace údajů. Toto je hlavní důvod, proč vůbec došlo k vytvoření bloku Dokumenty. Funkcionalita „GDPR“ modulu by jinak nedokázala automatizovaně plnit některé zásady, u kterých je nutný lidský úsudek (zmíněná zásada minimalizace). Tímto je zajištěna alespoň částečná automatizace tím, že lidé vytvoří dokumenty, dle kterých se další bloky automaticky nastaví.

Další dopad úzce souvisí s prvním zmíněným a bude znatelný u podniků, které ERP systémy využívají. Tyto podniky se staví do role správce, resp. zpracovatele osobních údajů a za neplnění povinností vyplývajících z Obecného nařízení mohou být sankcionovány. Budou proto tlačit na dodavatele ERP systémů, aby poskytovali „GDPR ready“ systémy. Je však jejich vlastní povinností zajistit soulad s nařízením, a tak musí v rámci tohoto zajištění sami analyzovat připravenost používaného ERP systému. Pro tento účel byly v práci zmíněny obecné kroky, které se může podnik rozhodnout aplikovat zcela či částečně, aby zjistil, jestli s využitím daného ERP systému bude plnit požadavky Obecného nařízení.

Posledním, neméně důležitým dopadem, je v rámci přístupu založeném na riziku vytvoření technických opatření, na kterých budou muset podniky spolupracovat s dodavateli. Tato opatření však již musí být konkrétní a aplikovatelná v praxi, tudíž jsou v práci zmíněny jen krátce a obecně. Avšak z tohoto lze usoudit, že customizace ERP systémů bude muset být pro tento záměr prováděna nikoliv na úrovni modulů, ale mnohem detailněji.

7 ZÁVĚR

Prvním cílem práce bylo seznámit s nařízením GDPR a povinnostmi, které z něj vycházejí, tak, aby byl výklad relevantní pro aplikaci v praktické části práce, resp. pro oblast ERP systémů. Tento cíl byl naplněn, a to včetně porovnání změn oproti předchozí právní úpravě, kterou v České republice tvořil především zákon č. 101/2000 Sb., o ochraně osobních údajů.

Druhý a hlavní cíl představovala aplikace poznatků z teoretické části pro ERP systémy. Cíl byl plněn prostřednictvím praktické části práce, kdy nejdříve byly představeny ERP systémy všeobecně, jejich architektura a základní principy. Poté následoval popis obecných kroků a doporučení pro implementaci požadavků Obecného nařízení, které zmiňovala teoretická část práce, do ERP systémů a jejich funkcionality. Byl vytvořen obecný návod pro implementaci jak ze strany dodavatele ERP systému, tak ze strany uživatele, tedy podniku. Oba přístupy implementace byly převedeny i do grafické podoby ve formě diagramů.

Během aplikace teoretických poznatků došlo k zásadnímu poznání, a to, že dodavatel ERP systému není vůbec žádným legislativním způsobem nucen požadavky Obecného nařízení plnit, a to dokonce ani v případě, kdy se prostřednictvím systému zpracovávají osobní údaje. Dodavatel ERP systémů se totiž neřadí do žádné role, kterou definuje Obecné nařízení. Rozhodne-li se dodavatel implementovat požadavky kladené nařízením GDPR, bude to buď z důvodu dobrého vztahu s odběratelem, nebo z důvodu zvýšení konkurenceschopnosti v nabídce ERP systémů. Dá se totiž předpokládat, že podniky budou upřednostňovat systémy s náležitou funkcionalitou, která usnadní plnění požadavků Obecného nařízení, a systémy, které ji obsahovat nebudou, se postupem času stanou neschopné jim konkurovat. Dodání „GDPR ready“ systému nyní představuje příležitost, avšak v budoucnosti to bude spíše nutnost.

Pokud se dodavatel rozhodne pro uzpůsobení svých systémů požadavky Obecného nařízení plnit, bude muset patřičně rozšířit funkcionalitu. V práci bylo takové rozšíření obecně navrženo, tedy bylo řešeno co implementovat, ale ne jak. Konečné řešení bude totiž vždy konkretizováno jednak vývojovými metodami dodavatele, jednak individuálními potřebami daného podniku, který bude systém využívat.

Naopak podnik, který se coby uživatel daného ERP systému řadí dle Obecného nařízení do role správce osobních údajů, musí požadavky plnit. V případě jejich neplnění může být i sankcionován. Pro dosažení souladu zpracování s požadavky je nutné mít náležitě připravený i ERP systém, který integruje firemní procesy, a tedy i ty zahrnuté do zpracování osobních údajů. V práci byl navržen obecný postup pro podnik, jak zjistit připravenost systému. Kroky se vztahují právě na analýzu funkcionality ERP systému. Opět se nemůže jednat o konkrétní postup, protože potřeby různých podniků se liší a nemůže se vyloučit například možnost, že podnik analyzuje ERP systém v rámci celopodnikové implementace požadavků GDPR.

Je důležité pamatovat na skutečnost, že využití softwaru nebo jeho části samo o sobě nesplní požadavky kladené Obecným nařízením. Je povinností správce, aby podnik plnil nařízení jako celek. V tomto smyslu musí být připraven celý informační systém podniku, jehož součástí není pouze ERP systém, ale i zaměstnanci nebo listinné dokumenty, jejichž obsah mohou tvoři právě osobní údaje.

Pokud se jedná o ERP systém, ve výsledku je důležitá součinnost podniku a jeho dodavatele. Podnik je jakožto odběratel ten, kdo požaduje určitou funkcionalitu a musí tlačit na dodavatele. Integrace většiny či všech firemních procesů je nesporná výhoda, kterou ERP systém podniku poskytuje. Nedává tedy příliš smysl, aby podnik řešil požadavky na ochranu osobních údajů mimo systém, když se ho také týká.

8 SEZNAM POUŽITÉ LITERATURY

[11] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on the right to "data portability".* Brusel : ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017.

[13] Co je ERP? - Enterprise Resource Planning. *Blue Dynamic.* [Online] Blue Dynamic, 20. listopad 2018. https://bluedynamic.cz/blog/co-je-erp-enterprise-resource-planning/.

[12] Gála, Libor, Pour, Jan a Šedivá, Zuzana. *Podniková informatika.* Praha : GRADA, 2009. ISBN 978-80-247-2615-1.

[7] Gemalto World leader in Digital Security. *Biometrics: authentication and identification (2019 review).* [Online] Gemalto, 2019. https://www.gemalto.com.

[5] Goddard, Michelle. The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research.* November, 2017, Sv. 59, 6.

[23] Horehleďová, Šárka. *Proces komplexního posouzení rizik v kontextu integrace systémů managamentu.* Praha : Výzkumný ústav bezpečnosti práce, 2009.

[3] Mates, Pavel a Neuwirt, Karel. *Právní úprava ochrany osobních údajů v ČR.* Praha : IFEC, 2000. ISBN 80-86412-02-4.

[4] 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). *EUR-Lex Access to European Union law.* [Online] 2019. https://eur-lex.europa.eu.

[2] Nezmar, Luděk. *GDPR Praktický průvodce implementací.* Praha : GRADA, 2017. ISBN 978-80-271-0668-4.

[8] Nulíček, Michal, a další. *GDPR - obecné nařízení o ochraně osobních údajů.* Praha : Wolters Kluwer, 2017. ISBN 978-80-7552-765-3.

[19] Otevřel, Petr. Je váš informační systém „GDPR Ready“? *IT Systems.* IT právo, 2018, 1-2.

[16] Parr, A. N. a Shanks, G. A Taxonomy of ERP Implementation Approaches. *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences.* 2000, Sv. 10, 1.

[14] Poláková, Irena. Automatizace procesů v ERP systému. *SystemOnLine.* [Online] 16. duben 2019. https://m.systemonline.cz/erp/automatizace-procesu-v-erp-systemu.htm.

[21] Politou, Eugenia, a další. Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Elsevier B.V.* Computer Law & Security Review, 2018, Sv. 34, 6.

[20] Privacy by Design. *Sociální síť pro business - ManagementMania.com.* [Online] ManagementMania.com, 10. listopad 2018. https://managementmania.com/cs/privacy-by-design.

[6] Škorničková, Eva. GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů – prakticky.* [Online] 2018. https://www.gdpr.cz.

[22] Těšitelová, Vladimíra, a další. *JAK IMPLEMENTOVAT NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY 2016/679.* Praha : autor neznámý, 2016.

[17] Tvrdíková, Milena. *Aplikace moderních informačních technologií v řízení firmy: Nástroje ke zvyšování kvality informačních systémů.* Praha : GRADA, 2008. ISBN 978-80-247-2728-8.

[10] Uřičař, Miroslav. *GDPR v kostce.* Praha : C. H. Beck, 2018. ISBN 978-80-7400-704-0.

[9] Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů.* [Online] Úřad pro ochranu osobních údajů, 2019. https://www.uoou.cz.

[15] Vollmann, Thomas E., a další. *Manufacturing Planning and Control Systems for Supply Chain Management.* New York : McGraw-Hill, 2005. ISBN 007144033X.

[18] Worley, J. Hermosillo, a další. Implementation and optimisation of ERP systems: A better integration of processes, roles, knowledge and user competencies. *Elsevier B. V.* Computers in Industry, 2005, Sv. 56, 6.

[1] Žůrek, Jiří. *Praktický průvodce GDPR.* Ostrava : ANAG, 2018. ISBN 978-80-7554-152-9.

9 SEZNAM OBRÁZKŮ

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2019/2020

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. Škop Ladislav	Petříkovice 34, Chvaleč - Petříkovice	I1600317

TÉMA ČESKY:

Dopad GDPR na ERP systémy

TÉMA ANGLICKY:

Impact of GDPR on ERP systems

VEDOUCÍ PRÁCE:

Ing. Pavel Čech, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je seznámení s nařízením GDPR, jeho návazností na český zákon č. 101/2000 Sb. a vytvoření souboru obecných postupů a doporučení pro implementaci požadavků do systémů ERP.

Osnova:
1 Úvod
2 Cíl práce
3 Metodika zpracování
4 Teoretická část
5 Praktická část
6 Shrnutí výsledků
7 Závěr
8 Seznam použité literatury

SEZNAM DOPORUČENÉ LITERATURY:

Úřad pro ochranu osobních údajů (dostupné na: https://www.uoou.cz/)
Žůrek, Jiří: Praktický průvodce GDPR 2018
Nezmar, Luděk: GDPR: Praktický průvodce implementací
Nulíček, Michal: GDPR - obecné nařízení o ochraně osobních údajů
kolektiv autorů: GDPR v kostce : praktický průvodce povinnostmi pro podniky a spolky
Gára, Pour, Šedivá: Podniková informatika

Podpis studenta: ..... **Datum:** 21.6.2019

Podpis vedoucího práce: ..... **Datum:** 21.6.2019