Univerzita Pardubice

Fakulta ekonomicko-správní

Aplikace Obecného nařízení o ochraně osobních údajů v podnikové praxi

Bc. Michaela Pšeničková

Diplomová práce
2018

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2017/2018**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Michaela Pšeničková**
Osobní číslo:	**E16688**
Studijní program:	**N6209 Systémové inženýrství a informatika**
Studijní obor:	**Regionální a informační management**
Název tématu:	**Aplikace Obecného nařízení na ochranu osobních údajů v podnikové praxi**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce bude rozbor Obecného nařízení na ochranu osobních údajů a definovat dopady a nutná opatření na vybranou firmu.
Osnova:
- Právní úprava ochrany osobních údajů v ČR
- Obecné nařízení o ochraně osobních údajů
- Definovat dopady a nutná opatření pro splněné Obecného nařízení
- Aplikace Obecného nařízení na vybranou firmu

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 55 stran**

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

Seznam odborné literatury:

BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v aplikační praxi: vybrané otázky. 3. vyd. Praha: Linde Praha, 2013, 311 s. Praktická právnická příručka. ISBN 978-80-86131-96-2.
KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v otázkách a odpovědích. 1. vyd. Praha: BOVA POLYGON, 2010, 150 s. ISBN 978-80-7273-163-3.
MORÁVEK, Jakub. Ochrana osobních údajů v pracovněprávních vztazích. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2013. 435 s. ISBN 978-80-7478-139-1.
MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012, 206 s. Praktik (Leges). ISBN 978-80-87576-12-0.

Vedoucí diplomové práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2017**

Termín odevzdání diplomové práce: **30. dubna 2018**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

Ing. Pavel Petr
vedoucí ústavu

V Pardubicích dne 1. září 2017

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše. Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 4. 2018 Bc. Michaela Pšeničková

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala své vedoucí práce, Ing. Renátě Máchové, Ph.D., za její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování diplomové práce.

ANOTACE

Práce se zabývá Obecným nařízením o ochraně osobních údajů a definicí dopadů a nutných opatření ve vybrané firmě. Dále jsou v práci definovány vybrané pojmy týkající se zpracování osobních údajů a základní změny, které oproti stávající legislativě Obecné nařízení přinese.

KLÍČOVÁ SLOVA

Obecné nařízení o ochraně osobních údajů, GDPR, zákon o ochraně osobních údajů, osobní údaj, citlivý údaj, subjekt údajů, správce, zpracovatel.

TITLE

Application of the General Data Protection Regulation in the business practice

ANNOTATION

The thesis focuses on the General Data Protection Regulation and defines potential impacts and necessary measures to be taken by a selected company. Furthermore, the thesis defines fundamental concepts of personal data processing and core changes to legislation introduced by the General Data Protection Regulation.

KEYWORDS

General Data Protection Regulation, GDPR, personal data protection law, personal data, sensitive data, data entity, controller, processor.

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

BCR	Závazná podniková pravidla
ČR	Česká republika
DPIA	Posouzení vlivu zpracování na práva a svobody subjektů údajů
DPO	Pověřenec na ochranu osobních údajů
EHP	Evropský hospodářský prostor
EK	Evropská komise
EU	Evropská unie
GDPR	Nařízení o ochraně osobních údajů
LPS	Listina základních práv a svobod
ObčZ	Občanský zákon
Odst.	Odstavec
OchOsÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
Prohlášení	Prohlášení o ochraně osobních údajů
Protokol	Dodatkový protokol
RČ	Rodné číslo
Sb.	Sbírka zákonů
Sbor	Evropský sbor pro ochranu osobních údajů
SDEU	Soudní dvůr Evropské unie
Směrnice	Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů
Úmluva	Úmluva Rady Evropy č. 108/1981, o ochraně osob se zřetelem na automatizované zpracování osobních dat
ÚOOÚ	Úřad na ochranu osobních údajů
ÚS	Ústavní soud

USA	Spojené státy americké
VS OSSZ	Variabilní symbol okresní správy sociálního zabezpečení
WP29	Pracovní skupina zřízená dle čl. 29 Směrnice

ÚVOD

Ochranu osobních údajů v Evropské unii (EU), jakožto i v České republice, upravuje dodnes několik základních právních předpisů. Většina ale byla přijata v době, kdy se nedal předvídat tak velký rozvoj automatizace zpracování osobních údajů, a tak rychlý rozvoj technologií. To bylo motivem pro vytvoření nového regulačního předpisu, který by nahradil doposud platnou *Směrnici Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů*. Dalším motivem pro vytvoření nového regulačního předpisu bylo obchodování s daty ve velkém rozsahu, zejména telekomunikačními společnostmi.

V roce 2016 tedy EU přijala nové nařízení, *Obecné nařízení o ochraně osobních údajů*, které nabyde svoji platnost 25.5.2018. Od tohoto data Nařízení plně nahradí Směrnici. Nařízení, na rozdíl od Směrnice, nepotřebuje prováděcí zákon a je přímo vymahatelné ve členských zemích. Nařízení posiluje odpovědnost za zpracování osobních údajů, práva subjektů údajů a vymezuje nový, přísnější, rámec ochrany osobních údajů. Dalším velkým rozdílem nového Nařízení a stávající Směrnice je, že Nařízení za porušení vymezuje velké finanční pokuty.

Cílem práce bude rozbor Obecného nařízení o ochraně osobních údajů a definice dopadů a nutných opatření na vybranou firmu. V práci se budu postupně věnovat právní úpravě ochrany osobních údajů v ČR, Obecnému nařízení o ochraně osobních údajů, rozdílům Obecného nařízení od *zákona č. 101/2000 Sb., o ochraně osobních údajů*, definici dopadů a nutných opatření pro splnění Obecného nařízení, a nakonec aplikaci Obecného nařízení ve vybrané firmě.

1 PRÁVNÍ ÚPRAVA OCHRANY OSOBNÍCH ÚDAJŮ V ČR

Právní předpisy na ochranu osobních údajů ovlivňují společenský život již poměrně dlouhou dobu. Základ mají v mezinárodních smlouvách. K přijímání právních předpisů na ochranu osobních údajů na našem území docházelo od poloviny 70. let 20. století. Důvodem byl značný vývoj výpočetní techniky, který přinesl i jisté ohrožení v oblasti soukromí osob a potřeba centralizovaného zpracování velkého množství osobních údajů. Každé takové shromažďování bylo ale chápáno, jako značný zásah do soukromí občanů. Prvním takovým systematicky zpracovaným dokumentem byla *Úmluva Rady Evropy č. 108/1981, o ochraně osob se zřetelem na automatizované zpracování osobních dat* (dále jen Úmluva), která byla roku 2005 rozšířena o *Dodatkový protokol* (dále Protokol), definující orgány dozoru a toky dat přes hranice. Úmluva byla přijata 28. ledna 1981 ve Štrasburku. V platnost vstoupila v roce 1985. Českou republikou byla Úmluva přijata 8. září 2000 a v platnost vstoupila v listopadu roku 2001.[26][25]

Úmluva v §8 stanovuje, že *„každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence“*. Zároveň ale v §10 stanovuje svobodu projevu, která *„zahrnuje zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování státních orgánů a bez ohledu na hranice“*. K tomuto je tedy nutné podotknout, že Úmluva chápe výraz informace, jako pojem nadřazený pojmu osobní údaj.[25]

Z již zmíněné Úmluvy vychází další právní pramen, který vymezuje ochranu osobních údajů na území České republiky, *Listina základních práv a svobod* (dále Listina nebo LPS). LPS prohlašuje ochranu před shromažďováním a šířením informací, ale zároveň právo na jejich šíření a shromažďování. V §10 LPS prohlašuje, že *„každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života“* a dále, že *„každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“*. *V* §17 stejného zákona, ale odporuje prohlášením, že každý má právo na to, *„vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem“*, což zahrnuje i právo *„svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu“*. Z citovaného vyplývá, že ochrana soukromí je zaručena před neoprávněným zásahům, ale existují i zásahy oprávněné. Takové zásahy ovšem Listina nevymezuje.[25][5]

K ratifikaci Úmluvy Česká republika vydala *zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech*. Tento zákon měl značný nedostatek a to, že z důvodu rozpadajícího se státu (tehdejší Československé republiky) nedošlo ke zřízení nezávislého

orgánu, který by prováděl kontrolu nad zpracováním osobních údajů. Proto tento zákon nebyl dostatečně respektován.[25]

Nedostatky zmíněného zákona odstranil *zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů* (dále OchOsÚ). Teprve tímto zákonem došlo k souladu s Úmluvou. Zákon byl přijat v souvislosti se vstupem ČR do Evropské unie. V souvislosti se vstupem do Evropské unie bylo potřeba, aby se ČR vyrovnala také s podmínkami *Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů* (dále jen Směrnice) ze dne 24.10. 1995. Směrnice upřesňuje a dále rozvádí podmínky vytyčené Úmluvou. OchOsÚ byl několikrát novelizován, aby bylo dosaženo většího souladu se Směrnicí a dalšími právními předpisy.[25][15]

Zákon o ochraně osobních údajů v Hlavě i vymezuje působnost a základní pojmy týkající se ochrany osobních údajů, v Hlavě II práva a povinnosti při zpracování osobních údajů a v Hlavě III předání osobních údajů do jiných států. Hlavy IV, v a VI vymezují postavení a působnost, organizaci a činnost Úřadu na ochranu osobních údajů a Hlava VII je věnována správním deliktům.[6]

1.1 Základní zásady ochrany osobních údajů

Úmluva definuje základní zásady, které se využívají v oblasti ochrany osobních údajů. Tyto zásady se odrážejí v právních předpisech států, které tuto Úmluvu schválily, tedy i v právních předpisech České republiky. Jedná se o tyto zásady[26]:

1. Zásada legitimity
2. Zásada omezení účelem
3. Zásada časového omezení
4. Zásada potřebnosti a přiměřenosti dat
5. zásada průhlednosti
6. Zásada bezpečnosti
7. Zásada práva přístupu k datům
8. Zásada práva na opravu a výmaz
9. Zásada nezávislého dozoru

1.2 Úřad na ochranu osobních údajů

Úřad byl zřízen ke dni 21. června 2000 se sídlem v Praze a jeho působnost upravuje OchOsÚ zejména v hlavě IV, v a VI. Podle §28 OchOsÚ je Úřad nezávislý orgán, který se řídí pouze zákony a dalšími právními předpisy. Do jeho působnosti je možné zasahovat jen na základě zákona a jeho činnost je hrazena ze státního rozpočtu České republiky.[27][6]

Mezi hlavní činnosti Úřadu podle §29 OchOsÚ patří[6]:

a) provádět dozor nad dodržováním povinností stanovených zákonem při zpracování osobních údajů,

b) vést registr zpracování osobních údajů,

c) přijímat podněty a stížnosti na porušení povinností stanovených zákonem,

d) zpracovávat a zveřejňovat výroční zprávy o své činnosti,

e) vykonávat další působnosti stanovené zákonem,

f) projednávat přestupky a jiné správní delikty a udělovat pokuty podle tohoto zákona,

g) zajišťovat, plnění požadavků vyplívajících z mezinárodních smluv,

h) poskytovat konzultace v oblasti ochrany osobních údajů,

i) spolupracovat s odbornými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti osobních údajů.

Úřad je ústředním správním úřadem, v jehož čele stojí předseda. Ten je volen na 5 let prezidentem na návrh Senátu Parlamentu České republiky s možností jednoho opakovaného zvolení. Za kontrolu je zodpovědných 7 inspektorů a další pověření zaměstnanci Úřadu. Inspektoři jsou opět jmenováni prezidentem na návrh Senátu a jsou voleni na 10 let, mohou být zvoleni opakovaně. Nezávislost dohledového a kontrolního orgánu je zřízena zejména proto, že dohlíží a kontroluje jak soukromé subjekty, tak subjekty veřejného práva (ministerstva, korporace, aj.).[26][27][6]

1.3 Základní pojmy

Základní pojmy vycházejí ze Směrnice a jsou zakotveny v §4 zákoně o ochraně osobních údajů. Práva a povinnosti při zpracování údajů zpracovává Hlava II OchOsÚ a předání osobních údajů do jiných států zpracovává Hlava III stejného zákona.

1.3.1 Osobní údaj, citlivý údaj, anonymní údaj

Osobní údaj je *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*[6]

Osobní údaj se vždy musí vztahovat k fyzické osobě. K určení fyzické osoby je nutné, aby bylo možné ji dostatečně odlišit od ostatních až do té míry, kdy je vyhledatelná. Fyzickou osobu nemusíme identifikovat jen podle jména, příjmení a adresy (přímá identifikace), ale také pomocí jiných kombinací osobních údajů, na základě kterých, je možné od sebe jednotlivé fyzické osoby odlišit (nepřímá identifikace). Tato kombinace údajů by ale měla mít přiměřený rozsah, jinak se o osobní údaj nejedná.[2][27][25][23]

Základní identifikátory můžeme rozdělit[25]:

- identifikátory, které nám byly přiděleny pro obecnou identifikaci (jméno, příjmení),
- identifikátory, které nám byly vrozeny (otisk prstu, DNA, obličej),
- identifikátory, které nám byly přiděleny pro určitý účel (adresa bydliště, PIN, platební karta, karta pojištěnce).

Citlivý údaj je *„osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů. Citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.“*[6]

Citlivé údaje jsou tedy údaje, které mohou více vypovídat o soukromém životě subjektů údajů, a proto jsou pro manipulaci s nimi nastavena jiná pravidla. Nakládáním s těmito daty může dojít k vyšší újmě než při nakládání s osobními údaji. Ke zpracování citlivých údajů musí subjekt údajů podat výslovný souhlas.[2][27][25][23]

Anonymní údaj je údaj, který *„v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určitelnému subjektu údajů.“*[6]

Anonymním údajem je tedy takový údaj, který se týká fyzické osoby, na základě kterého, tato osoba nemůže být jednoznačně identifikována jakoukoliv jinou osobou pomocí prostředků, které lze volně k identifikaci využít. V souvislosti s anonymními údaji lze

hovořit o *anonymizovaných údajích*. To jsou osobní údaje, které dříve odkazovaly na určitelnou fyzickou osobu, ale nyní pomocí nich již tuto osobu určit nelze.[27][23]

1.3.2 Zpracování, shromažďování, uchovávání, blokování, likvidace osobních údajů

Zpracování je *„jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.“*[6]

Zpracováním osobních údajů tedy lze rozumět veškeré činnosti, při kterých dochází ke sběru nebo uspořádání osobních nebo citlivých údajů.[2][27][25]

Shromažďování osobních údajů je *„systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování.“*[6]

Shromažďováním osobních údajů lze nazvat jak činnost, která může předcházet zpracování osobních údajů (což znamená shromažďování, které není cílené), tak činnost, která je součástí procesu zpracování (cílené shromažďování osobních údajů).[27]

Uchováváním osobních údajů se rozumí *„udržování údajů v takové podobě, která je umožňuje dále zpracovávat.“*[6]

Uchováváním je možné rozumět například uložení údajů na nějaké paměťové médium. V dnešní době, v souvislosti se zpracováním dat, dochází spíše k uchovávání než k jejich shromažďování. Data tedy volně leží například na paměťových nosičích, aniž by jejich vlastník zamýšlel je dále zpracovávat. Taková data, i když původně nejsou osobními, mohou v budoucnu získat povahu osobních údajů.[27][25]

Blokování je *„operace nebo soustava operací, kterými se na stanovenou dobu omezí způsob nebo prostředky zpracování osobních údajů, s výjimkou nezbytných zásahů.“*[6]

Blokování je tedy činnost, která vede k zamezení zpracování chybných či nepřesných údajů nebo k nesprávnému zpracování těchto údajů.[27][25]

Likvidace osobních údajů je *„fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.“*[6]

K likvidaci a blokování osobních údajů v praxi dochází tehdy, pokud existuje oprávněné podezření na nezákonné zpracování osobních údajů, které může vést k újmě na subjektu údajů nebo pokud správce již ukončil zpracování. Správce si ale může některé osobní údaje ponechat, pro další zpracování těchto údajů (např. po skončení pracovního poměru, kvůli sociálnímu zabezpečení, daňové důvody, pro obranu při soudní při aj.).[27][25]

1.3.3 Správce, zpracovatel, subjekt údajů, příjemce údajů

Správcem se rozumí *„každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.“*[6]

Správcem osobních údajů může být jak fyzická, tak právnická osoba, ale v některých případech i stát, při vykonávání veřejné moci. Aby mohl být některý subjekt nazván správcem, nemusí však splňovat všechny prvky zmíněné definice. Mezi tyto prvky patří stanovení účelu zpracování, určení způsobu a prostředků zpracování, provádění zpracování a odpovědnost za zpracování osobních údajů. Za správce lze označit i osobu, která nestanovila účel, způsob ani prostředky zpracování, neprovádí zpracování, ale je zodpovědná za zpracování osobních údajů v legální rovině.[27][25]

Účelem zpracování osobních údajů se obecně rozumí cíl zpracování. J. Morávek v [27] vymezuje 3 skupiny účelů zpracování osobních údajů.

První takovou skupinou jsou účely, které jsou správci dané zákonem, tedy povinné (např. zpracování osobních údajů zaměstnavatelem pro daňové účely). Tyto účely jsou v praxi plněny bez problémů, jelikož zákon určuje jak účel zpracování osobních údajů, tak prostředky a rozsah, v němž mají být osobní údaje zpracovány. Problémy činí spíše překračování zákona v nastavených mezích např. doby uchovávání dat, které jsou v těchto případech jasně odlišitelné.[27]

Druhou skupinu tvoří účely, které správce určuje sám. Nejsou zakotveny v zákoně a závisí zcela na správci. Majoritně se jedná o ochranu majetku, zdraví či života správce nebo jiných osob. Tyto účely ale nejsou legálně zakotveny, proto se musí řídit určitými zákonnými mezemi, podmínkami, jak zpracování vypadat nesmí. Zde platí, že *„právo jednoho končí tam, kde začíná právo druhého“.* Jelikož účel, prostředky, způsob zpracování ani zabezpečení není určeno zákonem, je pouze na uvážení správce, jak s osobními údaji bude nakládat. Musí ale brát zřetel na meze určené OchOsÚ. Výjimku tvoří zákonné zpracování prováděné fyzickou osobou pro

vlastní potřebu, tohoto zpracování se působnost OchOsÚ netýká. V případě právnických osob tato výjimka ale není možná.[27][6]

Mezi třetí skupinu účelů lze zařadit případy, kdy správce může vybrat, zda chce nebo nechce zákonem nastavené zpracování osobních údajů provádět. Zpracování osobních údajů tedy není povinné, pokud se ale správce pro zpracování rozhodne, jsou pro toto zpracování daná pravidla.[27]

Stanovením způsobu a prostředků zpracování osobních údajů rozumíme cokoliv, čím správce může zpracovávat osobní údaje (např. kartotéka, počítačový program, formulář, v jistých případech i zpracovatel, aj.). Opět existují případy, kdy zákon správci ukládá povinnost využít určitý způsob či prostředek zpracování.[27]

Samotné zpracování ve vztahu ke správci pak znamená zpracování osobních údajů i prostřednictvím jeho zaměstnanců. Ti by však měli zpracovávat osobní údaje ve správcem stanovených mezích na základě smlouvy se správcem.[27]

Zpracovatelem je *„každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.“*[6]

Zpracovatelem opět může být fyzická osoba, právnická osoba i stát. Zpracovatelem ale není zaměstnanec správce údajů, který se podílí na zpracování osobních údajů. V dnešní době dochází k outsourcingu, kdy jsou zpracovatelům svěřovány rozsáhlé kompetence, co se týče způsobu a prostředků zpracování osobních údajů. Na základě množství zpracování, které zpracovatelé pro správce provádějí, dochází k tzv. řetězení zpracovatelů.[27][25]

Subjektem údajů je *„fyzická osoba, k níž se osobní údaje vztahují.“*[6]

Je možné říci, že se jedná o určenou nebo určitelnou fyzickou osobu. Podle §7 ObčZ všem fyzickým osobám okamžikem narození vznikají určitá práva a povinnosti a zanikají jejich smrtí. Na základě toho lze říci, že osobní údaje se tedy týkají žijící fyzické osoby. Pokud bychom ale k problému přistupovali takto, nemohli bychom za osobní údaj považovat údaje o zemřelé osobě. Osobní údaje by potom bylo možné rozlišovat na základě toho, zda údaje pocházejí z doby života fyzické osoby či po úmrtí dané osoby. Údaje z období života by bylo etické i dále chránit. Zákon o ochraně osobních údajů tuto povinnost ale neukládá. V případě úmrtí tedy každý údaj, který se váže se zemřelou fyzickou osobou, přestává být osobním údajem a zákon o ochraně osobních údajů by v tomto smyslu musel přijmout další ustanovení.[25][7]

Příjemcem je *„každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci nebo činností spojených se zpřístupňováním svazků bývalé Státní bezpečnosti.“*[6]

Z pojmu osobní údaj vyplývá, že se jedná o takovou informaci, na základě které, je její příjemce schopen určit, ke které fyzické osobě se vztahuje. Příjemce osobních údajů je proto ten, komu jsou osobní údaje přístupné. Příjemcem by tedy mohl být správce i zpracovatel. V § 4 OchOsÚ je ale uvedeno, že se za příjemce nepovažují ty subjekty, které osobní údaje zpracovávají, tedy ani správce ani zpracovatel.[27][6]

O pojmu příjemce se hovoří spíše ve smyslu rozsahu příjemců osobních údajů, kdy dochází k neoprávněnému zpracování. Jedná se o určení potenciálního počtu příjemců neoprávněně zpracovávajících osobní údaje k určení závažnosti správního přestupku.[27]

Souhlasem subjektu údajů se rozumí *„svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.“*[6]

Při udělení souhlasu musí být subjekt údajů informován o účelu zpracování jeho osobních údajů, ke zpracování, kterých osobních údajů dává souhlas, jakému správci a na jak dlouhý časový úsek. Při zpracování citlivých údajů musí být subjekt navíc informován o svých právech podle §12 a §21 OchOsÚ a při předávání osobních údajů do třetích zemí musí být informován o zabezpečení jeho osobních údajů podle §27 OchOsÚ.[27][6]

Subjekt údajů má právo na odvolání souhlasu se zpracováním osobních údajů. Souhlas se zpracováním dává subjekt údajů na omezenou dobu, i když tato doba může být omezena událostí nebo skutečností, o které není známo, kdy nastane. Nejdelší doba, po kterou subjekt údajů dává souhlas se zpracováním je do okamžiku jeho smrti.[27]

Existují i situace, kdy správce zpracovává osobní údaje bez souhlasu subjektů údajů. Příkladem může být záznam z kamerového systému v obchodě, kdy zákonné provozování je předpokladem souhlasu se zpracováním osobních údajů všech subjektů, kteří tvoří určitou skupinu.[27]

1.3.4 Zveřejněný údaj, evidence

Zveřejněným osobním údajem je *„osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.“*[6]

Údajem zpřístupněným hromadnými sdělovacími prostředky lze rozumět např. údaje v obchodním rejstříku, živnostenském rejstříku, aj. Co se týká citlivých údajů, tak je lze zpracovávat jen tehdy, pokud již byly zveřejněny subjektem údajů. Osobní údaje si obchodníci také mohou předávat jen v případě předešlého zveřejnění subjektem údajů.[27]

Evidencí nebo *datovým souborem osobních údajů* definujeme *„jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií.“*[6]

Tato definice má podle Směrnice spíše povahu dodatkovou.[27]

1.4 Práva a povinnosti při zpracování osobních údajů

Práva a povinnosti při zpracování osobních údajů zpracovává Hlava II OchOsÚ, konkrétně §5 až §26.[6]

Povinnosti správce jsou určeny zejména v §5 odst. 1. Jedná se o povinnost stanovit účel zpracování, definování prostředků a způsobů, kterými bude o účel zpracování usilováno, zpracování pouze přesných informací, shromažďování pouze osobních údajů, které odpovídají danému účelu, uchovávání osobních údajů pouze po dobu nezbytnou k účelu zpracování, zpracování osobních údajů pouze v souladu s účelem za kterým byly shromažďovány, shromažďování osobních údajů jen otevřeným způsobem a zákaz sdružování osobních údajů získaných pro odlišné účely.[6]

Jak již bylo řečeno, správce může zpracovávat osobní údaje jen se souhlasem subjektu údajů. Existují ale výjimky, které můžeme nalézt v §5 odst. 2. Těmito výjimkami jsou například zpracování pro nezbytné dodržení právní povinnosti, pokud je zpracování nezbytné pro plnění smlouvy, pokud se jedná o zpracování oprávněně zveřejněných údajů v souladu se zvláštním právním předpisem aj.[6]

Pokud subjekt údajů souhlasí se zpracováním osobních údajů, musí být srozumitelně a jasně předem informován o rozsahu zásahu do jeho soukromí. Zejména musí být informován o rozsahu zpracovávaných osobních údajů, o účelu zpracování, jakému správci osobní údaje předává, jakým způsobem budou osobní údaje zpracovány, komu mohou být údaje zpřístupněny a na jak dlouhé období. Správce má povinnost informovat subjekt údajů při zpracování osobních údajů, zda je poskytnutí těchto údajů povinné nebo dobrovolné. Správce dále musí být schopen po celou dobu zpracování prokázat souhlas subjektu údajů.[6]

Pokud správce nebo zpracovatel zpracovávají osobní údaje v souvislosti s nabízením obchodu či služeb, mohou z veřejného seznamu nebo v souvislosti se svou činností získat jméno, příjmení a adresu subjektu údajů. Pokud s tímto zpracováním subjekt údajů nesouhlasí,

nejsou správce ani zpracovatel oprávněni dále tyto informace zpracovávat. Subjekt údajů musí nesouhlas podat písemně.[6]

Podle §5 odst. 6 je správce oprávněn předat osobní údaje jinému správci jen pokud[6]:

a) byly osobní údaje získány v souvislosti s činností správce nebo jde o zveřejněné osobní údaje,

b) údaje budou využívány pouze pro účely nabízení obchodu a služeb,

c) subjekt údajů byl o tomto jednání předem informován a nevyslovil s ním nesouhlas.

Správce, který obdrží tyto osobní údaje, je nesmí předávat jiné osobě. Nesouhlas se zpracováním musí subjekt údajů podat písemně a správce musí informovat každého dalšího správce, kterému jméno, příjmení a adresu předal o nesouhlasu subjektu údajů.[6]

Správce se zpracovatelem jsou povinni uzavřít smlouvu o zpracování osobních údajů, pokud toto zpracování nevychází z jiného právního předpisu. Smlouva musí být písemná a musí obsahovat rozsah zpracování, účel zpracování a období, na jaké je smlouva uzavřena. Musí v ní být také uvedeny záruky o zabezpečení zpracovávaných osobních údajů.[6]

Povinnosti vztahující se na správce platí také pro zpracovatele. Pokud zpracovatel zjistí, že ze strany správce dochází k porušování zákona, musí ho na tuto skutečnost upozornit a ihned ukončit zpracování osobních údajů. V opačném případě odpovídá správce i zpracovatel za škodu vzniklou subjektu údajů společně stejným dílem.[6]

Pokud dochází ke zpracování citlivých údajů, je potřebný výslovný souhlas subjektu údajů. Případy jejich zpracování jsou uvedeny v §9 OchOsÚ.[6]

Subjekt údajů má právo na přístup ke svým osobním údajům. Správce je povinen bezodkladně poskytnout požadované informace, pokud o ně subjekt údajů požádá. V §12 odst. 2 je uvedeno, že těmito informacemi mohou být[6]:

- účel zpracování,
- rozsah osobních údajů nebo kategorie osobních údajů, které jsou předmětem zpracování,
- způsob automatizovaného zpracování,
- další příjemci údajů.

Správce i zpracovatel při zpracování dbají na to, aby subjekt údajů neutrpěl újmu a na ochranu před zasahováním do soukromého a osobního života. Správce a zpracovatel musejí

přijmout ochranná opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k osobním údajům, ke změně, zničení nebo ztrátě těchto údajů nebo k jakémukoliv zneužití osobních údajů. Přijatá opatření musejí patřičně zpracovat a dokumentovat.[6]

Zaměstnanci správce a zpracovatele mohou zpracovávat osobní údaje jen v rozsahu vymezeném na základě smlouvy a stanoveném správcem či zpracovatelem. Zaměstnanci jsou povinni zachovat mlčenlivost o těchto údajích a o bezpečnostních prostředcích. Povinnost mlčenlivosti trvá i po ukončení pracovního poměru.[6]

Každý, kdo se chystá, jako správce, zpracovávat osobní údaje, je povinen to oznámit na ÚOOÚ ještě před zpracováním osobních údajů. Oznamovací povinnosti jsou uvedeny v §16 OchOsÚ. Toto oznámení musí obsahovat[6]:

- identifikační údaje správce,
- účel zpracování,
- kategorie subjektů údajů a osobních údajů,
- zdroje osobních údajů,
- popis způsobu zpracování osobních údajů,
- popis místa zpracování,
- příjemce nebo kategorie příjemců,
- předání do jiných států,
- popis opatření k zajištění ochrany.

Pokud oznámení obsahuje veškeré povinné údaje, je možné po uplynutí 30 dnů zahájit zpracování osobních údajů a ÚOOÚ zapíše uvedené informace do registru. V opačném případě ÚOOÚ v dané lhůtě zašle výzvu na doplnění chybějících náležitostí a určí lhůtu na doplnění. Pokud správce doplní požadované údaje, může po uplynutí 30 dnů zahájit zpracování. Pokud správce nedoplní požadované údaje v dané lhůtě, ÚOOÚ pohlíží na oznámení, jako by nebylo podáno. Na žádost správce může ÚOOÚ vydat osvědčení o registraci. Pokud vznikne oprávněná obava o porušení nebo přijde udání na porušení OchOsÚ, zahájí ÚOOÚ řízení. Na základě řízení ÚOOÚ rozhodne o dalším zpracovávání osobních údajů nebo o zrušení registrace. Výjimky v oznamovací povinnosti jsou uvedeny v §18 OchOsÚ.[6]

V momentu uplynutí účelu zpracování osobních údajů nebo na žádost subjektu údajů je správce a na základě jeho instrukcí i zpracovatel povinen provést likvidaci osobních údajů.

Existující výjimky se týkají uchovávání osobních údajů pro účely archivnictví, uplatňování práv v trestním řízení, soudním řízení a správním řízení.[6]

Pokud subjekt údajů zjistí, že správce zpracovává nebo se domnívá, že by mohl zpracovávat jeho osobní údaje v rozporu s OchOsÚ, může požádat o vysvětlení a o odstranění vzniklého stavu (blokování, oprava, doplnění, likvidace osobních údajů). Pokud se potvrdí zpracování v rozporu s OchOsÚ, je správce povinen vzniklý stav okamžitě odstranit a informovat další příjemce o žádosti subjektu údajů.[6]

1.5 Předání osobních údajů do jiných států

Předáním osobních údajů do jiných států se zabývá Hlava III OchOsÚ. Podle článku §27 odst. 1 OchOsÚ nemůže být omezován volný pohyb osobních údajů, pokud jsou předávány v rámci EU. Zákon umožňuje předání osobních údajů do třetích států, ale jen pouze pokud to vyplývá z mezinárodních smluv ratifikovaných Parlamentem České republiky, ze kterých pro ČR vyplývají určité povinnosti. O předání osobních údajů do třetích států může rozhodnout také EU, veškeré informace o takovýchto rozhodnutích jsou zapisovány a zveřejněny ve Věstníku ÚOOÚ.[6]

Členské státy EU splňují legislativní požadavky předání osobních údajů do zahraničí, jež jsou vymezeny ve Směrnici. Ta určuje požadavky na ochranu osobních údajů včetně povinnosti zřídit nezávislý kontrolní orgán a zavést potřebné mechanismy. Kromě členských států EU tyto požadavky splňují také státy zahrnuté do Evropského hospodářského prostoru (EHP), které se rovněž řídí Směrnicí. Tyto požadavky splňují také státy, jejichž úroveň ochrany osobních údajů byla prokázána jako vyhovující a schválena Evropskou komisí (EK). Mezi tyto státy patří například Kanada, Argentina, ostrovy Man a Guernsey aj.[25]

Dalším kritériem pro rozhodnutí o vyhovující míře právního zakotvení může být ratifikování Úmluvy. Ta ovšem nevytváří povinnost nezávislého prošetřování stížností. Aby stát měl odpovídající úroveň ochrany, musí kromě Úmluvy přijmout i jiné právní předpisy, které ho zavazují ke zřízení dozorového orgánu s pravomocemi stanovenými ve Směrnici a vymezují způsob předání osobních údajů do zahraničí. Pokud stát nepřijme takovéto právní předpisy, může přijmout Protokol, který udává povinnost zřídit nezávislý dozorový orgán a zavést požadovaná pravidla pro ochranu osobních údajů při jejich předání do zahraničí.[25]

Pokud není splněna ani jedna ze zmíněných podmínek, může podle §27 odst. 3 OchOsÚ dojít k předání, pouze pokud[6]:

- k předání osobních údajů dochází se souhlasem subjektu údajů nebo na základě jeho pokynu,
- je správce schopen dokázat, že třetí země, kam mají být údaje předány a kde mají být zpracovány, vytvoří dostatečná ochranná opatření (např. právní předpisy, smlouva mezi správcem a příjemcem, aj.),
- jedná se o osobní údaje, které jsou součástí veřejně přístupných datových souborů nebo o osobní údaje, které jsou přístupné tomu, kdo prokáže právní zájem (osobní údaje jsou potom zpřístupněné v rozsahu, který určí zvláštní zákon),
- k předání dochází na základě zvláštního zákona nebo mezinárodní smlouvy, kterou je ČR vázána a jedná se o předání nezbytné v rámci veřejného zájmu,
- je předání údajů nutné pro uzavření, změnu nebo uskutečnění smlouvy, jejíž smluvní stranou je subjekt údajů,
- je předání v zájmu subjektu údajů a je nutné k plnění smlouvy mezi správcem a příjemcem (třetí stranou),
- se jedná o ochranu práv a životně důležitých zájmů subjektu údajů.

Správce je povinen před každým předáním osobních údajů požádat ÚOOÚ o povolení k předání. ÚOOÚ přezkoumá veškeré okolnosti předání údajů, jako je zdroj, konečné určení, kategorie předávaných osobních údajů, účel zpracování, dobu zpracování, právní předpisy týkající se zpracování osobních údajů třetí země, zřízení nezávislého orgánu pro ochranu osobních údajů aj. Po přezkoumání vydá ÚOOÚ povolení k předání osobních údajů do třetí země, ve kterém určí dobu, po kterou může dojít k předání. Pokud se změní některé z okolností, za kterých bylo povolení vydáno, ÚOOÚ povolení stáhne nebo změní.[6]

Jestliže stát nevyhovuje některým pravidlům předání osobních údajů, například má nedostatečnou právní úpravu, může to být kompenzováno odvětvovými právními předpisy, jako byl tzv. Bezpečný přístav v USA. Za takovéto odvětvové opatření by se daly považovat také etické kodexy firem, pokud obsahují všechny požadavky Směrnice, OchOsÚ a jsou právně vymahatelné. Tam, kde není dostatečná právní úprava ani odvětvové právní normy, se mohou využít tzv. nástroje samoregulační povahy. Těmi jsou smluvní ujednání mezi tuzemským správce a zahraničním dovozcem osobních údajů a závazná podniková pravidla.[25][6][15]

Je možné vydat povolení k přenosu osobních údajů do zahraničí, kdy příjemcem bude výhradně podnik, který přísluší určitému sektoru státu, jehož principy ochrany osobních údajů jsou kontrolovatelné a vymahatelné nebo jsou zajištěny jinou, soukromoprávní cestou. Je možné, že zákony v některých zemích budou obdobou OchOsÚ a budou tedy ukládat veřejné správě stejné povinnosti, jako předpokládá OchOsÚ nebo zvláštní úprava bude použitelná např. pro internetové operátory nebo pro subjekty, které se nacházejí v určitém sektoru, jako jsou telekomunikace, pojišťovny, banky aj.[25][6]

2 NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Nařízení o ochraně osobních údajů neboli *2016/679/EC General Data Protection Regulation* (dále je GDPR nebo Nařízení) je nařízení EU, které přijde v platnost 25.května 2018. Jedná se o nejucelenější soubor upravující ochranu osobních údajů na světě dodnes. Nařízení v ČR nahradí do nynějška platnou ochranu osobních údajů, kterou reguluje OchOsÚ. Práva a povinnosti vycházející ze zákona na ochranu osobních údajů, který doteď určoval zacházení s osobními údaji, nahradí práva a povinnosti vyplývající z Nařízení. Neznamená to však, že by platností GDPR zanikal OchOsÚ. OchOsÚ bude dále upravovat působnost Úřadu a další důležité body, které jsou nezbytné pro ochranu osobních údajů a GDPR je neupravuje nebo jejich úpravu ponechává na vnitrostátní úrovni (např. právo na informace, právo na svobodu, vědecké bádání a uměleckou tvorbu). Nicméně platnost Směrnice účinkem Nařízení zaniká.[3][28][14]

GDPR se dotkne všech podnikatelů, podniků, institucí či online služeb, které zpracovávají data Evropanů (zaměstnanců, zákazníků, klientů či dodavatelů), ať už na území EU nebo mimo ni. Nařízení vyšlo v evropské působnosti, aby se zajistila jeho jednotná platnost na území celé EU a aby jednotlivé vlády nemohly jeho působnost jakýmkoliv způsobem přizpůsobovat místním zájmům. Týká se všech odvětví bez rozdílu a za jeho porušení jsou nastaveny vysoké sankce. Cílem GDPR je chránit také digitální práva Evropanů, pravidla proto zasáhnou i subjekty, které zpracovávají osobní údaje na internetu, analyzují chování uživatelů na webu, při využívání aplikací nebo jiných technologií.[3][28][22]

Dodnes byl hlavní autoritou, co se týče ochrany osobních údajů ÚOOÚ, kterému bude tato funkce ponechána. Přibydou mu ale pravomoci vyplývající z GDPR a bude nově podřízen Evropskému sboru pro ochranu osobních údajů (dále Sbor). Pokud tedy nastane jakákoliv nesrovnatelnost na straně českého regulátora, budou se moci subjekty odvolat ke Sboru.[3]

Změna oproti dosud platnému:

Rozdíl mezi směrnicí a nařízením, co se týká evropského práva, je v tom, že směrnice vydané EU jsou závazné pro členské státy, které na jejich základě musejí vydat nějaký legislativní dokument, kterým tuto směrnici zakotví do národního práva. Naopak nařízení je závazné pro všechny subjekty členských států a ty se jimi musejí řídit. EU zamýšlí novou regulací aktualizovat a sjednotit ochranu osobních údajů členských států, jelikož mnoho z nich vyšlo ještě před vznikem nových technologií a sociálních sítí a zajistit tak jednotnou vymahatelnost na celém jejím území.

2.1 Předmět a cíl

Nařízení v Kapitole I vymezuje předmět a cíl nařízení, věcnou a místní působnost a v neposlední řadě také definuje základní pojmy obdobné jako v OchOsÚ. Fyzické osoby jsou v Nařízení chráněny zejména tím, že jim jsou přiřazena určitá práva, pomocí kterých mohou kontrolovat zpracování svých osobních údajů a jsou určeny podmínky a povinnosti, za kterých dochází ke zpracování jejich osobních údajů. Cílem Nařízeni je chránit práva a svobody fyzických osob, zejména jejich osobních údajů. Nařízení stanovuje pravidla, která se týkají zpracování osobních údajů fyzických osob a jejich volného pohybu v rámci EU a zpracování osobních údajů mimo státy EU, pro které určuje rozdílné podmínky.[28][14]

Nařízení se podle čl. 2 odst. 1 použije, pokud se jedná o automatizované, částečně automatizované, nebo neautomatizované zpracování osobních údajů. O automatizované zpracování osobních údajů se jedná například při použití webového skriptu, který na základě nastavených parametrů vyhodnotí osobní údaje žadatele o úvěr. O částečně automatizované zpracování může jít v obdobném případě, ovšem s tím rozdílem, že rozhodnutí o tom, zda úvěr bude či nebude poskytnut, provede fyzická osoba. A o neautomatizované zpracování osobních údajů půjde tehdy, kdy se jedná o manuální zpracování, tedy pokud jsou osobní údaje obsaženy v určité evidenci a jsou systematicky uspořádány podle určitých kritérií.[28][14]

Podle čl. 2 se Nařízení nevztahuje na zpracování osobních údajů prováděné[28][14]:

a. při výkonu činností, které nespadají do oblasti působnosti práva Unie, např. zpracovávání při zajišťování bezpečnosti na národní úrovni,

b. členskými státy při výkonu činností, které spadají do oblasti působnosti Smlouvy o EU, jako je zpracování osobních údajů orgány Eurojust a Europol,

c. fyzickou osobou v průběhu osobních či domácích činností, které nemá profesní účel,

d. příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíháni trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

Pokud osobní údaje zpracovávají orgány, instituce a jiné subjekty EU, vztahuje se na ně nařízení Evropského parlamentu a Rady Evropy *č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů*.[14]

Místní působnost vymezuje čl. 3, podle kterého se Nařízení týká každého zpracování osobních údajů, které je prováděno správcem nebo zpracovatelem s provozovnou v EU, bez

ohledu na to, zda ke zpracování těchto údajů dochází v EU nebo mimo ni. Dále se jedná o zpracování osobních údajů subjektů údajů, které jsou evropskými občany, správci nebo zpracovateli, kteří se v EU nenacházejí a pokud zpracování souvisí[14]:

a. s nabídkou zboží nebo služeb subjektům údajů v EU,

b. s monitorováním jejich chování, pokud k němu dochází v rámci EU.

Nabízení zboží a služeb však musí být s úmyslem cílit svou nabídku na subjekty údajů v EU, to ovšem záleží na okolnostech případů. Jde například o nabídku s možností objednat si zboží a služby v jazyce členského státu, v měně členského státu, přehled uživatelů a zákazníků nacházejících se v EU aj. Naopak jen dostupnost webových stánek nebo kontaktních údajů správce v členském státě, používání jazyka třetí země, v níž je správce usazen, i když je současně jazykem členského státu neznamená úmyslnou a cílenou nabídku.[28]

Definici základních pojmů je věnován čl. 4 a je obdobná, jako v OchOsÚ. Nařízení definuje 26 základních pojmů, jejich případnou odlišnost zmíním v dalším textu.

Změna oproti OchOsÚ:

Nařízení má stejnou aplikovatelnost, jako OchOsÚ. Tedy použije se ve stejných případech. V tomto ohledu se pro správce a zpracovatele v ČR nic nemění. Místní působnost pro správce, kteří jsou usazeni mimo EU a provádí zpracování na území ČR, se také z tohoto hlediska působnosti nic nemění.

2.2 Zásady zpracování osobních údajů

Hlavními zásadami zpracování osobních údajů je podle Kapitoly II čl. 5 Nařízení zákonnost, korektnost a transparentnost. Shromažďovány musejí být osobní údaje pouze pro výslovné a zákonné účely a jejich zpracování musí být účelově omezené, tedy v souladu s těmito účely.[1] Nařízení dovoluje zpracovávat pouze přiměřený, relevantní a nezbytný rozsah osobních údajů, tak aby došlo k minimalizaci údajů v podniku. Nepřesné údaje musejí být aktualizovány, vymazány či opraveny. Doba uchovávání musí být omezena na dobu nezbytně nutnou pro jejich zpracování. Pokud správce již nepotřebuje data pro účel, pro který byly shromážděny, je povinen je vymazat nebo anonymizovat. Pokud na základě Nařízení lze uložit data po delší dobu (archivace ve veřejném zájmu, pro účely vědeckého výzkumu a statistické účely), musí správce zavést dostatečná

[1] Toto se nevztahuje na archivaci ve veřejném zájmu a pro vědecké či statistické účely.

technická a organizační opatření, aby nedošlo k ohrožení práv a svobod subjektu údajů. Při zpracovávání je správce povinen zajistit důvěrnost a integritu, tedy údaje vhodně zabezpečit pomocí potřebných technických či organizačních opatření, aby zamezil neoprávněnému nebo protiprávnímu zpracování. Data musí být chráněna také před ztrátou, zničením nebo poškozením. Vše zmíněné musí být správce schopen doložit.[28][29][50][14]

Účel zpracování musí být určitý, jasně vyjádřený a legitimní. Při určování účelu je nutné, abychom se vyhnuli obecným frázím, jako je například „marketingové zpracování“, ale nahradili ho jasnějším vyjádřením. Takovým by mohlo být například „zasílání nabídek produktů a služeb“. Jasným vyjádřením účelu znamená, že ho správce musí sdělit subjektu údajů. Účel zpracování ale také musí vycházet ze zákonného základu (určeného Nařízením či konkrétnějšími požadavky členského státu) a musí být nutný pro splnění úkolu, kterým je správce pověřen (ať už ve veřejném zájmu nebo při výkonu veřejné moci). Pokud je účel zpracování odlišný od účelu, pro který byla data shromážděna, je potřebný souhlas subjektu údajů. Jinak je správce povinen zvážit účel zpracování podle čl. 6 odst. 4.[28][29][50][40]

Co se týká přesnosti osobních údajů, je správce povinen bez dalšího odkladu nepřesné nebo chybné údaje vymazat, aktualizovat či opravit. Za nepřesné údaje lze považovat například neaktualizované údaje o dlužnících. Pokud by takový subjekt údajů už dlužníkem nebyl, mohlo by to pro něj znamenat například neposkytnutí úvěru či jiné další škody. Pokud však subjekt údajů správci poskytl nepřesné informace, potom správce nemá zodpovědnost za správnost takových údajů. Posouzení přesnosti také souvisí s účelem zpracování. Pokud pro účel zpracování bude postačovat přibližný údaj, nebude se považovat na nepřesný. Požadavek aktualizace osobních údajů se ovšem netýká zpracování za účelem archivace a historického či statistického zpracování, jelikož by došlo ke zmaření prvotního účelu.[28][29][50]

Jednou z možností, jak se vyhnout Nařízení je anonymizace osobních údajů. Jedná se však o velmi složitý proces, v některých případech skoro nemožný, a je nutné ho opakovat. Anonymizace je přípustným způsobem, jak zabezpečit osobní údaje, musí však být provedena v rámci možností „dokonale“ a subjekt údajů nesmí být možné zpětně identifikovat. Anonymizace totiž neznamená pouze odstranění jedinečného id, tímto způsobem by se došlo spíše k pseudonymizaci.[28]

Podle čl. 6 se jedná o zákonné zpracování pouze pokud je v plném rozsahu splněna alespoň jedna z podmínek[28][32][24][14]:

a. udělil-li subjekt údajů souhlas se zpracováním svých osobních údajů,
b. zpracování je nezbytné pro splnění smlouvy,
c. zpracování je nezbytné pro splnění právní povinnosti, která se vztahuje na správce,
d. zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
e. zpracování je nutné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
f. zpracování je nutné 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 subjekt údajů dítě.

Dále Nařízení ponechává na členských státech, zda zavedou konkrétnější požadavky na zpracování. Pokud správce nemá stanoven právní titul zpracování osobních údajů, jedná se vždy o nelegální zpracování údajů. Proto je definice právního titulu jedna z prvních věcí, kterou by měl společně s účelem zpracování určit.[28][32][24][14]

Podle Nařízení už souhlas subjektu údajů se zpracováním nepatří mezi hlavní právní titul a ostatní nejsou chápány, jako alternativy. Podmínky souhlasu subjektu údajů jsou poněkud zpřísněné, a proto by správce měl uvažovat nad použitím jiného právního titulu a souhlas získávat až v případě, že použití jiného právního titulu není možné.[28][49][24]

Za oprávněný zájem lze chápat, jakýkoliv zájem správce, který je oprávněný a pro splnění jeho účelu dochází ke zpracování osobních údajů. Osobní údaje ale nemůže zpracovávat v případě, kdy nad oprávněným zájmem převažují zájmy nebo základní práva a svobody subjektu údajů. Každý oprávněný zájem je proto nutné z tohoto hlediska posoudit.[28]

V této souvislosti musí brát správce v úvahu také právo subjektu údajů na omezení zpracování či právo na výmaz. Pokud správce zpracovává osobní údaje pod tímto titulem, musí zvážit, zda[28][24]:

- je stanovený zájem oprávněný a splňuje určité kvality,
- je zamýšlené zpracování osobních údajů nezbytné,
- nad tímto zájmem nepřevažují zájmy a základní práva a svobody subjektů údajů.

Poté, co dojde k posouzení, zda se jedná o oprávněný zájem a zda je zpracování osobních údajů nezbytné, je třeba provést tzv. Balanční test. Jedná se o posouzení následujících faktorů[28][24]:

a. posouzení váhy oprávněného zájmu,
b. posouzení důsledků zpracování osobních údajů pro subjekty údajů,
c. vyvážení oprávněného zájmu s důsledky, které zpracování může mít pro subjekty údajů,
d. přijetí záruk pro ochranu práv a svobod subjektů údajů.

Podrobněji je možné se o tomto testu dočíst v [28], autor M. Nulíček.

Podle Nařízení by měl být souhlas využíván pouze doplňkově. Správce bude muset prokázat, že rozhodnutí subjektu údajů je jednoznačný projev jeho vůle ke zpracování jeho osobních údajů. Mění se i způsob získávání souhlasu. Pokud je získáván písemně, musí být oddělen od ostatních skutečností, musí být jasný a přesný. Nařízení dále řeší svobodu, kterou by měl správce subjektu údajů udělit při poskytování souhlasu. Za nesvobodné udělení souhlasu Nařízení chápe situaci, kdy podmínkou poskytnutí služby, je udělení souhlasu se zpracováním pro účely, které nejsou nezbytné pro plnění smlouvy, souhlas udělený zaměstnancem zaměstnavateli, fyzickou osobou orgánu veřejné moci aj. Obecně tedy platí, že pokud subjektu údajů hrozí při neposkytnutí souhlasu nějaký trest/ újma, nejedná se o svobodný projev vůle. Souhlas se zpracováním může navíc subjekt údajů kdykoliv odvolat.[28][17][49][47]

Zpracování osobních údajů nezbytné pro ochranu životně důležitých zájmů lze použít, pokud nelze využít jiný právní titul, např. pokud se jedná o zpracování osobních údajů obětí autonehody, které nejsou schopné poskytnou souhlas, pro humanitní účely, při monitorování epidemií, naléhavých humanitních situacích aj. Navíc oproti současné úpravě není nutné žádat o dodatečný souhlas se zpracováním osobních údajů.[28]

Co se týká zpracování ve veřejném zájmu nebo při výkonu veřejné moci, tak veřejné orgány mohou tento titul využívat pouze tehdy, pokud je zpracování osobních údajů nezbytné k výkonu daného účelu, který orgán veřejné moci provádí.[28]

Existují případy, kdy je možné zpracovávat osobní údaje i pro jiný účel, než pro který byly shromážděny, to je však možné pouze pokud[28][24][14]:

a. dalšímu zpracování dal souhlas subjekt údajů,
b. jedná se o účely archivace ve veřejném zájmu, účely historického výzkumu či statistické účely,
c. je povoleno právem EU nebo členského státu,
d. nový účel je slučitelný s předchozím účelem zpracování a slučitelnost byla zajištěna podle posouzení slučitelnosti, více v [28].

Správce musí být podle čl. 7 schopen doložit souhlas subjektu údajů například písemným prohlášením. Souhlasu dítěte se dopodrobna věnuje čl. 8. Žádost o vyjádření souhlasu musí být srozumitelná a subjekt údajů má právo tento souhlas kdykoliv odvolat. Odvolání souhlasu by podle Nařízení mělo být stejně jednoduché, jako jeho odsouhlasení. Byl-li souhlas udělen přes webový formulář, měl by existovat také formulář na jeho odvolání, byl-li udělen telefonicky, měl by také jít stejně dobře odvolat (tady je ale související problém identifikace subjektu údajů) apod.[28][29][14]

Jak již bylo řečeno, podmínky udělení souhlasu jsou Nařízením zpřísněny. Souhlas musí být svobodný, konkrétní, informovaný a jednoznačný projev vůle subjektu údajů, který tak dává potvrzení se pracováním svých osobních údajů. Svobodný je souhlas jen tehdy, pokud má subjekt údajů možnost volby a není riziko nátlaku, zastrašování nebo jiných negativních důsledků, pokud souhlas neudělí. Konkrétním souhlasem se rozumí souhlas s konkrétním účelem zpracování. O informovaný souhlas se jedná pouze, pokud byl subjekt údajů informován o skutečnostech zpracování způsobem, který je dále popsán v čl. 12 a jednoznačný souhlas jde, pokud nejsou pochybnosti, zda subjekt údajů opravdu směřuje k udělení svolení se zpracováním.[28][17][49][47][14]

Ze záznamu prohlášení o souhlasu musí být jasné, kdo souhlas udělil, kdy jej udělil, o čem byl subjekt údajů před udělením souhlasu informován, jak byl souhlas udělen a případně údaj o tom, zda byl souhlas odvolán, případně kdy.[28][49][47]

V čl. 9 odst. 1 se uvádí, že se „zakazuje zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či

filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo o sexuální orientaci fyzické osoby.“ Vymezení citlivých údajů Nařízení přejímá ze Směrnice a byly určeny na základě předcházení diskriminaci. Údaje o odsouzení za trestný čin jsou nově zařazeny do vlastní kategorie a jsou pro ně určeny zpřísněné podmínky zacházení definované ve čl. 10.[28][14]

Výjimky ze zpracování zvláštních kategorií osobních údajů, tedy citlivých údajů, jsou uvedeny ve stejném článku odst. 2. Mezi ně patří například, pokud subjekt údajů udělil výslovný souhlas, zpracování je nutné pro ochranu životně důležitých zájmů nebo se zpracování týká osobních údajů zveřejněných subjektem údajů. Obecně rozsáhlé zpracování zvláštních kategorií osobních údajů znamená pro správce povinnost jmenovat pověřence pro ochranu osobních údajů.[28][14]

Zpracování citlivých údajů na rozdíl od osobních údajů vyžaduje výslovný souhlas s jejich zpracováním. Takový souhlas je například potvrzen zaškrtnutím pole pro souhlas se zpracováním aj.[28][17][20][24]

Nařízení podle čl. 10 oproti OchOsÚ rozšiřuje kategorii údajů na veškeré údaje o odsouzení z trestných činů. Mezi tyto údaje oproti české legislativě řadí také informace o podmíněném zastavení trestného stíhání, informace o narovnání aj. Nově se tedy jedná o jakékoliv informace, které hovoří o rozsudcích v trestních věcech, trestných činech nebo souvisí s bezpečnostním opatřením (dále jen údaje o trestných činech). Zpracování údajů o trestných činech musí být prováděno pouze pod dozorem orgánu veřejné moci nebo musí být oprávněné podle práva EU (popř. členského státu), kdy správce musí poskytnout dostatečné záruky, co se týká ochrany základní práv a svobod subjektu údajů.[28][14]

Změna oproti OchOsÚ:

Oproti doposud platné legislativě rozšiřuje Nařízení zásady zpracování osobních údajů. Těmito stávajícími zásadami jsou zákonnost, korektnost, účelové omezení, minimalizace údajů, přesnost, omezení uložení a nově jsou přidány transparentnost, integrita, důvěrnost a odpovědnost.

Pro zákonné zpracovávání osobních údajů je nutné určit právní základ, ještě před samotným započetím zpracování osobních údajů. GDPR určuje 6 právních základů. Ve zkratce se jedná o souhlas se zpracováním, plnění smlouvy, plnění právní povinnosti, ochrana životně důležitých zájmů, veřejný zájem nebo výkon veřejné moci, oprávněný zájem.

Všechny tyto zákonné základy zpracování mají stejnou váhu, jen souhlas by měl být, podle výkladů WP29, využíván spíše doplňkově. To proto, že GDPR přikládá subjektům údajů nová práva, díky kterým mohou tento souhlas kdykoliv odvolat nebo požádat o vymazání aj. Pokud ale správce nebo zpracovatel zpracovává citlivé údaje, tomuto zákonnému základu se nelze vyhnout.

Určení právního titulu zpracování není nové, nyní ale instituce tento titul musejí zdokumentovat, aby prokázaly soulad s GDPR a tento právní titul sdělit subjektům údajů, tím dochází k transparentnosti zpracování osobních údajů.

Právní základ může ovlivnit některá práva subjektů údajů, např. právo na výmaz se nevztahuje na zpracování na základě právní povinnosti nebo veřejného zájmu, právo na přenositelnost se vztahuje pouze na zpracování na základě souhlasu nebo smlouvy a právo vznést námitku proti zpracování se vztahuje pouze na zpracování na základě veřejných zájmů nebo oprávněných zájmů.

Při určování právního základu by organizace měly zvážit více právních základů pro jednotlivá zpracování a každý z nich patřičně zdokumentovat. Při určování by mohlo pomoci zodpovězení některých z těchto otázek[22]:

- jaký je váš cíl zpracování, čeho se zpracováním snažíte dosáhnout?
- můžete cíle zpracování rozumně dosáhnout jiným způsobem?
- máte na výběr, zda chcete data zpracovat nebo ne?
- jste veřejná moc?

Odpovědnosti a integrity organizace mohou dojít pomocí záměrné a standardní ochrany osobních údajů. Těmto aspektům se věnuji dále v kapitole Správce, zpracovatel a pověřenec osobních údajů.

Odpovědnost je v Nařízení zakotvena zejména v ohlašovací povinnosti, kdy správce musí hlásit ÚOOÚ, popřípadě i subjektům údajů, každé porušení ochrany osobních údajů, které přináší vyšší rizika pro práva a svobody subjektů údajů. Správce je povinen zaevidovat každé porušení ochrany osobních údajů, i když nepřináší vysoká rizika pro práva a svobody subjektů.

2.3 Práva subjektu údajů

Práva subjektu údajů Nařízení uvádí v Kapitole III. Nařízení zde řeší zejména komunikaci se subjekty údajů, otevřenost, co se týče zpracování, a jednání se subjekty údajů, rozšiřuje množství informací, které je nutné subjektu údajů sdělit a v neposlední řadě také klade velký

důraz na to, aby veškeré sdělené informace byly jasné, srozumitelné a celkově přizpůsobené adresátovi. V Nařízení jsou také určeny lhůty, ve kterých je správce povinen tyto informace poskytnout.[28]

Správci dále musejí napomáhat uplatňování práv subjektů údajů, ověřovat totožnost subjektu údajů, na žádost subjektu údajů jsou povinni až na výjimky reagovat do jednoho měsíce a veškeré tyto služby vykonávat bezplatně.[28]

Změna oproti OchOsÚ:

Další novinky, které GDPR přináší je posílení práv subjektů údajů. Těmito právy jsou právo na informace, právo na přístup, právo na opravu, právo na výmaz, právo být zapomenut, právo na omezení zpracování, právo na přenositelnost údajů a právo vznést námitku proti zpracování. OchOsÚ vymezoval pouze právo získat informace, právo na přístup k údajům, právo vznést námitku proti zpracování údajů. Konkrétněji se těmto právům budu věnovat v následujících kapitolách.

2.3.1 Právo na informace

Nařízení v čl. 12 hovoří o tom, že správce musí být schopen poskytnout informace subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jednoduchých jazykových prostředků. Informace budou tedy správci poskytovat nejčastěji písemně nebo elektronicky, zveřejňováním na webových stránkách nebo pomocí elektronické pošty. Jednoduchosti a srozumitelnosti může správce docílit například pomocí vizualizací, různým členěním textu, vyhnutím se právnickým či technickým termínům nebo vhodnými hypertextovými odkazy, pomocí kterých bude uživatel moci mezi jednotlivými sděleními pohybovat a v neposlední řadě správci mohou využít tzv. vrstvené podmínky ochrany osobních údajů[2]. Ideálním případem je zavést tzv. privacy dashboard[3] (v ČR se využívá prohlášení o ochraně osobních údajů), která bude umístěná na webových stránkách správce. Informace, které jsou správci a zpracovatelé povinni sdělovat subjektům údajů, ukazuje Tabulka 1.[28][49][40][14]

[2] Podmínky ochrany osobních údajů jsou obvykle nějaký dokument, který je zveřejněný na webových stránkách správce, kde jsou přehledně vyspány informace, které je správce povinen sdělovat. Známé jsou zejména pod anglickým názvem „privacy policy“.[28]

[3] Samostatná část webových stránek, kde si subjekty údajů budou moci přečíst všechny potřebné informace o zpracování osobních údajů, upravit nastavení soukromí, budou zde umístěny potřebné formuláře aj.[28]

Tabulka 1 Informační povinnost

Jaké informace mají být poskytnuty?	**Data získána přímo od subjektu údajů**	**Data nezískána přímo od subjektu údajů**
Identita a kontaktní údaje správce a jeho zástupce	X	X
Identita a kontaktní údaje pověřence na ochranu osobních údajů	X	X
Účel zpracování a právní titul zpracování osobních údajů	X	X
Kategorie osobních údajů		X
Příjemce nebo kategorie příjemců	X	X
Podrobnosti o přesunu dat do třetích zemí a mezinárodních organizací	X	X
Doba, po kterou budou osobní údaje uloženy	X	X
Existující práva subjektů údajů (právo na přístup, opravu, výmaz, omezení zpracování, vznést námitku prosti zpracování)	X	X
Právo odvolat souhlas se zpracováním, pokud je to relevantní	X	X
Právo podat stížnost u ÚOOÚ	X	X
Zdroj, ze kterého pocházejí osobní údaje, zda pocházejí z veřejně přístupných zdrojů		X
Zda je subjekt údajů povinen podat osobní údaje či nikoliv (zda se jedná o zákonný nebo smluvní požadavek) a následky neposkytnutí osobních údajů	X	
Zda dochází k automatizovanému zpracování osobních údajů	X	X
Kdy mají být informace poskytnuty?	V okamžik, kdy jsou data získána	Do měsíce, po získání dat. Pokud jsou data získána za účelem komunikace se subjekty údajů, nejpozději v okamžiku první komunikace.

Zdroj: zpracováno podle [28][49][40][14]

Aby nedošlo k nějaké újmě, musí správce ověřit totožnost subjektu údajů, pokud se domáhá svých práv. Identifikace subjektu údajů může být různá a doporučuje se identifikace založená na možném riziku, které by vzniklo, kdyby se práv domáhala jiná osoba. Pokud osoba bude vyžadovat jen potvrzení, že jsou osobní údaje zpracovávány, je riziko újmy menší a není potřeba tak důkladná identifikace, jako kdyby osoba vyžadovala kopii všech zpracovávaných osobních údajů. Vhodné je určit už při shromažďování osobních údajů identifikátory nutné pro výkon práv. Takovými identifikátory mohou být emailová adresa, různé způsoby autentizace, doklad totožnosti, elektronický podpis aj.[28]

Pokud správce obdrží žádost, je podle čl. 12 povinen do jednoho měsíce učinit alespoň jednu z těchto tří věcí[28][14]:

a. žádosti vyhovět, provést potřebná opatření a informovat subjekt údajů,
b. žádost zamítnout, informovat subjekt údajů o důvodech odmítnutí a informovat ho o dalším postupu,
c. lhůtu o dva měsíce prodloužit, informovat o důvodech prodloužení subjekt údajů s tím, že prodlouženou žádost již nelze zamítnout.

Lhůtu může správce prodloužit jen z důvodu složitosti nebo počtu žádostí. Ovšem počet žádostí se může vztahovat jen k jednomu žadateli, nikoliv argumentovat tím, že je správce přehlcen žádostmi více žadatelů.[28][14]

Aby nedošlo k zneužívání práv subjektů údajů, má správce právo odmítnout nebo zpoplatnit ty žádosti, které vyhodnotí, jako nedůvodné nebo nepřiměřené. Poplatek by měl být ve výši administrativních nákladů, které plynou z vyřízení žádosti. V tomto případě by správce měl o výši poplatku žadatele informovat a požádat o souhlas, že mu bude vyměřen.[28]

Informační povinnost by měl správce splnit buďto písemně nebo jinými, například elektronickými, prostředky. Ústně se nedoporučuje tyto informace poskytovat, jelikož se pak bude jen těžko dokazovat splnění informační povinnosti. Poskytnuté informace musí být srozumitelné, stručné, snadno přístupné za využití jasných a jednoduchých jazykových prostředků.[28][49][14]

Pokud se správce dostane do situace, kdy účel plně nepokrývá jeho zpracování, musí o tom informovat subjekt údajů, a to ještě před začátkem takového zpracovávání.[28][14]

Správce tyto informace nemusí poskytnout, pokud subjekt údajů již tyto informace má nebo by informování vyžadovalo nepřiměřené úsilí[4]. Takovým případem může být například, pokud již byly tyto informace správcem nebo zpracovatelem poskytnuty, nebo pokud subjekt údajů podepisuje dodatek ke smlouvě, kterým se nemění účel ani rozsah zpracování. Dále informace neposkytuje, pokud je získání nebo zpřístupnění dáno zákonem Unie, případně členského státu anebo se jedná o povinnost zachovat služební tajemství či jinou zákonnou povinnost mlčenlivosti.[28][14]

Kromě informací, které je správce subjektu údajů povinen poskytnout, má subjekt údajů podle čl. 15 také právo na jednu bezplatnou kopii zpracovávaných údajů, pokud nejsou dotčena

[4] To platí pro zpracování za účelem archivace, vědeckého zájmu či historického výzkumu.[28]

práva jiných osob, další kopie již správce poskytne za určitou úhradu. Ta by však neměla přesahovat náklady, které jsou potřebné k získání této kopie. Bezplatné by ale mělo být poskytování těchto informací i po uplynutí nějaké delší doby od poslední žádosti o přístup k informacím.[28][39][14]

Podle odůvodnění Nařízení je doporučeno, aby správce umožnil přímý vzdálený přístup ke zpracovávaným údajům v rámci zabezpečeného systému. Zabezpečeným systémem se rozumí takový systém, kdy k údajům subjektu údajů nebude mít přístup nikdo jiný. Dále by mělo být možné, aby subjekt údajů v rámci tohoto systému své údaje upravoval. Jedná se však pouze o doporučení, které není závazné.[28][14]

Pokud dochází k předání osobních údajů jiným příjemcům, má subjekt údajů, dle čl. 15 na požádání právo i na informace, kterým příjemcům byla data poskytnuta a se kterými osobními údaji jednotliví příjemci zacházejí. Pokud nedochází k předání osobních údajů, bude stačit pouze informace o kategorii možných příjemců. Správce je podle tohoto článku dále povinen informovat subjekt údajů o všech jeho právech vztahujících se ke zpracování osobních údajů[5].[28][39][14]

Pokud správce předává osobní údaje do třetí země nebo mezinárodních organizací, tak se musí jednat o bezpečné předání, tzn., musí existovat vhodné záruky, o kterých by měl být subjekt údajů informován.[28][14]

Změna oproti OchOsÚ:

Správce i zpracovatel bude oproti OchOsÚ povinen subjektům údajů poskytnout více informací. Těmito informacemi jsou kontaktní údaje pověřence na ochranu osobních údajů, existující práva subjektů údajů, právo odvolat souhlas se zpracováním, právo podat stížnost u ÚOOÚ a zdroj, ze kterého osobní údaje pocházejí (pokud nepocházejí přímo od subjektu údajů). Nařízení navíc zdůrazňuje, že veškeré informace musejí být poskytnuty prostřednictvím jednoduchých jazykových prostředků, srozumitelným a snadno přístupným způsobem.

2.3.2 Právo na opravu, výmaz a omezení zpracování

Podle čl. 5 je jednou z hlavních zásad přesnost osobních údajů. Proto má subjekt údajů, podle čl. 16, právo na opravu nepřesných osobních údajů. Pokud subjekt údajů požádá o opravu nepřesných informací, je správce povinen přezkoumat, zda jsou údaje, ke kterým se žádost

[5] Těmito právy jsou právo na opravu (čl. 16), právo na výmaz (čl. 17), právo na omezení zpracování (čl.18), právo vznést námitku proti zpracování (čl. 21), právo podat stížnost u dozorového orgánu (čl. 77).[28]

vztahuje, nepřesné. Po dobu, kdy dochází k ověření, je přerušeno zpracování těchto osobních údajů. Po ověření správce informuje subjekt údajů a zpracování opět pokračuje. Správce informuje subjekt údajů o přijatých opatřeních písemnou, elektronickou či jinou formou.[28][34][44][14]

Podle stejného článku, má subjekt údajů právo také na doplnění neúplných osobních údajů. Při uplatňování tohoto práva by měl správce přihlížet na účel zpracování, zda jsou dodatečně poskytované osobní údaje skutečně potřebné k plnění účelu zpracování. V praxi dochází k uplatňování pomocí elektronického formuláře nebo pomocí jakéhokoliv prohlášení adresovaného správci.[28][34][44][14]

Dalším právem subjektu údajů je právo na výmaz neboli právo být zapomenut, které zakotvuje čl. 17 Nařízení. To může subjekt údajů uplatnit jen, pokud vznese žádost a pokud bude splněna alespoň jedna z následujících podmínek[28][37][42][14]:

a) správce nepotřebuje osobní údaje pro účel, pro který byly shromážděny anebo je zpracovává jiným způsobem (v takovém případě byl měl správce osobní údaje vymazat sám, žádost subjektu údajů to ale nevylučuje),

b) správce zpracovává osobní údaje nebo citlivé údaje na základě souhlasu, který subjekt údajů odvolá (to by měl správce opět vykonat automaticky, jelikož po odvolání souhlasu již nemá právní titul pro zpracovávání těchto osobních údajů),

c) subjekt údajů vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, a po prozkoumání dle tohoto článku vyjde najevo, že v situaci převažuje zájem subjektu údajů nad zájmem,

d) osobní údaje byly zpracovány protiprávně,

e) na správce se vztahuje právní povinnost vyplývající z práva EU nebo z práva členského státu, která mu ukládá povinnost osobní údaje vymazat,

f) jedná se o osobní údaje dětí shromážděné správcem.

Právo na výmaz má i některé výjimky, těmi jsou například právo svobody projevu a právo na informace, tedy v žurnalistice, kde jsou vydané články projevem svobody projevu nebo dále nelze vymazat záznamy z veřejných rejstříků, kde se zase jedná o právo na informace. Další výjimkou může být, pokud právo EU nebo právo členského státu správci udává povinnost osobní údaje uschovávat. Takovým příkladem u nás může být povinnost úschovy účetních záznamů dle § 31 zák. č. 563/1991 Sb., o účetnictví. Dalším důvodem pro odmítnutí žádosti výmazu osobních údajů může být zpracování nezbytné z důvodu veřejného zájmu v oblasti

veřejného zdraví anebo je zpracování nezbytné pro výkon nebo obhajobu právních nároků. Výjimky se mohou uplatnit pouze v tom případě, že cíle není možné dosáhnout jiným způsobem než zpracováním daných osobních údajů.[28][42][14][8]

Pokud je splněna alespoň jedna podmínka pro výmaz, musí správce žádosti vyhovět a zpracovávané osobní údaje vymazat a také musí v přiměřené míře, co se týče technologie a nákladů, informovat ostatní správce, že subjekt údajů požádal o výmaz zpracovávaných osobních údajů, včetně odkazů na ně a jejich kopií.[28][42][14]

Subjekt údajů má dále podle čl. 18 odst. 1 právo na omezení zpracování osobních údajů v jednom z těchto případů[45][14]:

a) subjekt údajů uplatní právo na opravu osobních údajů a může požádat správce, aby po dobu, po kterou bude ověřovat přesnost osobních údajů, omezil jejich zpracování,

b) správce zpracovával osobní údaje protiprávní formou, ale subjekt údajů nepožaduje výmaz osobních údajů, pouze omezení jejich zpracování,

c) správce již nepotřebuje zpracovávat osobní údaje pro splnění účelu zpracování, ale subjekt údajů je potřebuje pro určení, výkon nebo obhajobu právních nároků (správce tedy nebude moci osobní údaje vymazat, jelikož vymazání se považuje za zpracovávání),

d) subjekt údajů vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, na dobu, po kterou bude správce posuzovat, zda zájmy a práva subjektu údajů převažují nad zájmy a oprávněnými důvody správce při zpracování.

Správce opět musí na žádost reagovat bez zbytečného odkladu a žádosti do jednoho měsíce buď vyhovět, nebo ji zamítnout. Pokud je výklad práva složitý, lze lhůtu prodloužit o 2 měsíce. Skutečnost, že se na dané osobní údaje vztahuje omezení by měla být v systému dostatečně vyznačena, aby všichni, kdo k nim mají přístup, věděli, že je jejich zpracování omezeno. Výjimky omezení zpracování vyjmenovává čl. 18 odst. 2.[28][33][45][14]

Pokud důvody, které vedly k omezení zpracování osobních údajů, pominou, správce omezení zruší a předem o tom informuje subjekt údajů.[28][45][14]

Správce má dále podle čl. 19 oznamovací povinnosti co se týče opravy nebo výmazu osobních údajů nebo omezení zpracování. V OchOsÚ je tato povinnost zachycena v §12 odst. 5. Nařízení k této povinnosti přidává také povinnost informovat subjekt údajů o všech příjemcích, pokud o to subjekt údajů požádá. Pokud dojde k oznámení opravy, potom je příjemce povinen daný osobní údaj automaticky opravit. Původní správce již za tuto opravu

dále neodpovídá. Při oznámení o výmazu nebo omezení zpracování musejí zpracovatelé osobní údaje vymazat nebo omezit jejich zpracování v rozsahu součinnosti dle čl. 28 Nařízení. Pokud oznámení obdrží správce, bude s těmito informacemi zacházet, jako by šlo o žádost o výmaz nebo o omezení zpracování podle čl. 17 a čl. 18 Nařízení. Musí tedy posoudit podmínky výmazu nebo omezení zpracování a potom této žádost vyhovět nebo ji zamítnout.[28][14]

Povinnost oznamovat opravy správcům odpadá například v případě, že osobní údaje zveřejnili, tedy zpřístupnili neomezenému množství subjektů. Potom by bylo oznámení nemožné a vyžadovalo nepřiměřené úsilí.[28][14]

Úplně novým právem subjektu údajů je právo na přenositelnost údajů, tedy právo na portabilitu. Jeho cílem je umožnění převodu osobních údajů mezi správci tak, aby došlo k usnadnění přesouvání, kopírování a předávání osobních údajů z jednoho IT systému do druhého.[6] Právo na portabilitu pro subjekt údajů znamená možnost stáhnout si od správce své osobní údaje ve strukturovaném, běžně používaném, strojově čitelném formátu[7] a právo poskytnutí osobních údajů prvním správcem správci druhému. Rozsah osobních údajů, které lze poskytnout na základě práva na přenositelnost je zúžen jen na ty, které subjekt údajů aktivně sdělil správci (např. pomocí formuláře) nebo jsou generována na základě aktivity subjektu údajů (lokalizační údaje, srdeční tep zaznamenávaný pomocí náramku, data přihlášení do aplikace aj.).[28][41][14]

Právo na portabilitu má ale své podmínky. Podle čl. 20 odst. 1 se musí jednat o[28][35][41][14]:

- zpracování prováděné automatizovaně,
- zpracování založené na souhlasu subjektu údajů,
- zpracování založené na plnění smlouvy.

Pokud subjekt údajů uplatní právo na portabilitu, neznamená to pro správce, že musí dané osobní údaje vymazat nebo přenést smluvní náležitosti k novému správci. Pokud si subjekt údajů přeje služeb správce dále nevyužívat, musí své právo na výmaz uplatnit zvlášť.[28][35][14]

Pokud nastane situace, kdy subjekt údajů nemá možnost ovlivnit, že jeho osobní údaje budou zpracovány a nejedná se o plnění právní povinnosti nebo životně důležitý zájem, Nařízení mu

[6] Od zavedení tohoto práva si EU slibuje zvýšení soupeření zejména mezi poskytovateli internetových služeb a e-commerce, které by mělo zvýšit kvalitu jimi poskytovaných služeb.[28]
[7] Strojově čitelný formát je takový, který softwarové aplikace jednoduše naleznou, rozpoznají a jsou schopné získat z něj potřebné údaje.[28]

udává podle čl. 21 právo na to, vznést námitku proti zpracování. Správce je povinen subjekt údajů na toto právo upozornit, a to nejpozději v okamžiku první komunikace s ním. Podle Nařízení má subjekt údajů právo vznést celkem tři druhy námitek[28][38][43][14]:

- proti zpracování na základě právního titulu oprávněného zájmu,
- proti zpracování pro výkony přímého marketingu,
- proti zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely.

Dalším právem subjektu údajů je podle čl. 22 právo nebýt předmětem automatizovaného individuálního rozhodování[8] včetně profilování[9]. Nařízení se vztahuje pouze na výhradně automatizované zpracování osobních údajů. Nevztahuje se tedy na zpracování, do kterého v některém mezikroku zasahuje člověk (např. pokud rozhodnutí ověřuje). Automatizované individuální rozhodování je podle čl. 21 zakázáno. Povoleno je podle čl. 22 odst. 2 pouze v případech, kdy správce splní jednu z následujících podmínek[28][46][14]:

a) rozhodnutí je nezbytné k uzavření nebo plnění smlouvy,
b) je toto zpracování povoleno právem EU nebo členského státu,
c) subjekt údajů udělil výslovný souhlas.

Pokud správce provádí individuální automatizované zpracování podle předchozích případů, musí zavést vhodná ochranná opatření. Tato opatření musí obsahovat minimálně[28][46][14]:

- právo obdržet lidský zásah ze strany správce,
- právo vyjádřit svůj názor ohledně automatizovaného rozhodnutí,
- právo napadnout takové rozhodnutí.

Pro zajištění transparentnosti a spravedlivého zpracování by měl správce také[28]:

- používat vhodné matematické nebo statistické postupy profilování,
- zavést technická a organizační opatření vedoucí k opravě nepřesností osobních údajů a minimalizaci rizika chyb.

[8] Takové rozhodování, kdy o právech a povinnostech subjektů údajů rozhoduje jen algoritmus, tedy předem stanovený postup, který je prováděn automatizovaně.[28]
[9] Forma automatizovaného zpracování osobních údajů, při kterém dochází k hodnocení osobních aspektů FO za účelem analýzy nebo předvídání různých aspektů týkajících se subjektu údajů (ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování aj.)[28]

Pro automatizované individuální rozhodování na základě citlivých údajů jsou stanoveny přísnější podmínky. Takové zpracování je možné jen v případě, že správce zavede předešlá opatření, a navíc obstará výslovný souhlas subjektu údajů a zpracování je nezbytné z důvodu veřejného zájmu na základě práva EU nebo členského státu.[28][46][14]

Nařízení dále v čl. 23 umožňuje EU a členským státům přijmou dodatečná legislativní opatření například na základě odlišných politicko-ekonomických poměrů v členských státech aj. V odst.1 Nařízení vymezuje 10 cílů na základě kterých je možné omezit práva a povinnosti, které plynou z Nařízení. Pokud přijaté legislativní opatření není v souladu s čl. 23 odst. 2, potom dochází k rozporu vnitrostátního opatření s Nařízením a v takovém případě má přednost Nařízení.[28][36][14]

Změna oproti OchOsÚ:

Z těchto práv je naprosto novým právem právo na výmaz a jeho rozšířená forma, právo být zapomenut, tedy aby byly vymazány i veškeré odkazy na osobní údaje subjektu údajů. GDPR ale definuje některé výjimky, ve kterých bude velmi složité, tato práva uplatňovat. Těmi jsou například zpracování z důvodu veřejného zájmu, v oblasti veřejného zdraví aj. Veškeré podrobnosti pro výmaz a právo být zapomenut zmiňuji v předchozí kapitole.

Dalším naprosto novým právem je právo na přenositelnost údajů. Toto právo je možné využít pouze, pokud instituce zpracovává osobní údaje automatizovaně, na základě souhlasu subjektu údajů anebo na základě smlouvy. Jedná se o možnost přenesení zpracovávaných údajů mezi správci z jednoho IT systému do druhého.

2.4 Správce, zpracovatel a pověřenec pro ochranu dat

Články 24-27 Nařízení se věnují povinnostem správce. Těmi jsou podle zejména záměrná a standardní ochrana osobních údajů. Záměrná ochrana osobních údajů se obecně chápe, jako přijímání technických a organizačních opatření před a při zpracování osobních údajů, a to zejména na základě posouzení rizik práv a svobod subjektů údajů. Standardní ochranu lze chápat, jako povinnost správce přijmout organizační a bezpečností opatření k zajištění zpracování pouze těch osobních údajů, které jsou nutné pro splnění daného účelu zpracování.[28][21][1]

Jednou z hlavních povinností, které Nařízení správci ukládá je možnost prokázání souladu zpracování s Nařízením. Jako nejvhodnější formu dokazování uvádí dokumentaci vedenou správcem, která by prokazovala soulad zpracování osobních údajů s povinnostmi, které ukládá

Nařízení. Další povinnosti správce, zejména ty, které se týkají zapojení zpracovatele, upravují články Nařízení 28-30.[28][21][1][14]

Mezi základní povinnosti zpracovatele se řadí zejména dodržování pokynů správce, provádění zabezpečení zpracování, ohlašování porušení zabezpečení správci nebo pověřenci aj. Správce i zpracovatel jsou potom povinni pořizovat záznamy o zpracování osobních údajů, které musejí být schopni na vyžádání předložit ÚOOÚ. Zpracovatel může do zpracování zapojit i další zpracovatele, ale pouze za předpokladu, že má písemné svolení správce. Takto může docházet k tzv. řetězení zpracovatelů.[28][21][4][14]

Správce i zpracovatel jsou podle čl. 30 povinni vést záznamy o zpracování osobních údajů. Tyto záznamy musí být v písemné podobě, přičemž za písemnou podobu Nařízení považuje také formu elektronickou. Tyto záznamy si může dozorový orgán kdykoliv vyžádat. Obsah záznamů o zpracování osobních údajů ukazuje Tabulka 2.[28][11][14]

Tabulka 2 Obsah záznamů o zpracování osobních údajů

Záznam	Správce	Zpracovatel
Kontaktní údaje (jméno a příjmení)	X	X
Účel zpracování Kategorie subjektů údajů (zaměstnanci, zákazníci, uchazeči o zaměstnání), kategorie osobních údajů (osobní údaje, citlivé údaje, údaje týkající se rozsudků trestů)	X	X
Kategorie příjemců	X	
Předání do zahraničí	X	X
Lhůta pro výmaz	X	
Technická a organizační opatření	X	X

Zdroj: zpracováno podle[28][21][11][14]

Výjimku vést záznamy o zpracování tvoří správci a zpracovatelé s méně než 250 zaměstnanci, pokud jimi prováděné zpracování[28][21][11][14]:

a) nepředstavuje riziko pro práva a svobody subjektů údajů,

b) je příležitostné,

c) nezahrnuje

   1. citlivé údaje,

   2. osobní údaje, které se vztahují k rozsudkům v trestních věcech a k trestným činům.

Další povinností správce či zpracovatele, dle čl. 31 Nařízení, je povinnost spolupracovat s dozorovým úřadem tam, kde dozorový úřad jedná v konkrétní věci.[28][21][14]

Mezi další povinnosti správce a zpracovatele patří zabezpečení zpracování osobních údajů. To vymezuje Nařízení v čl. 32. Podstatou zabezpečení osobních údajů stále zůstává posouzení rizika, které by mohlo při zpracování hrozit. Co se týče posuzování rizika z hlediska čl. 32, jde zejména o porušení důvěrnosti a integrity zpracování. Je proto nutné zohlednit následující nežádoucí vlivy, jako je náhodné nebo protiprávní zničení osobních údajů, ztráta osobních údajů, pozměnění osobních údajů, neoprávněné zpřístupnění osobních údajů třetím osobám nebo neoprávněný přístup k osobním údajům při zpracování.[28][14]

Nejedná se o zabezpečení pouze IT systémů, ale v úvahu by se měl vzít také lidský faktor, fyzické prostředí (kde jsou umístěny systémy), subdodavatelé nebo obchodní partneři správce či zpracovatele.[28]

Po posouzení rizika by správce či zpracovatel měl přijmout vhodná technická a organizační opatření pro zmírnění rizik. Některé z nich navrhuje Nařízení, ale existují i jiná bezpečnostní opatření. Těmi mohou být obecně uznávané normy, jako ISO 27001, ISO 27002, ISO 2701810 aj.[28][18][21]

Nařízení v čl. 32 navrhuje některá bezpečnostní opatření, která ale nejsou povinná a v některých případech mohou být značně nedostačující. Mezi tyto opatření patří[28][14]:

a) pseudonymizaci a šifrování osobních údajů,

b) schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování

   - pro zajištění důvěrnosti slouží i pseudonymizace a šifrování, využít lze ale také různé úrovně autentizace a autorizace,

   - pro zajištění integrity je třeba chránit osobní údaje před zničením, ztrátou nebo pozměněním, toho můžeme dosáhnout pomocí monitorování přístupu osob k osobním údajům, monitorováním změn, které tyto osoby v osobních údajích provedly, minimalizací přístupu, vytváření a ukládání hashů souborů, vytváření kopií souborů při jejich změně a následná kontrola aj.,

[10] ISO 7001, 7002- normy pro specifikaci systému pro řízení bezpečnosti informací (ISMS)[18]
ISO 27018- soubor postupů pro ochranu osobně identifikovatelných informací[9]

- dostupnosti lze dosáhnout pomocí záložních zdrojů, které jsou k dispozici v případě jakéhokoliv výpadku,
- zajištění odolnosti souvisí s dostupností, jedná se o schopnost systému, resp. jeho prvků odolávat selháním a zachovávat funkci a bezpečnost, pokud dojde k selhání,

c) schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických problémů (např. tvorba záloh),

d) proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření k zajištění bezpečnosti zpracování.

Podobně jako v čl. 24 Nařízení je správce i zpracovatel povinen prokázat zavedení dostatečných bezpečnostních opatření. K tomu obdobně může využít kodexů chování nebo osvědčení o ochraně osobních údajů, viz dále.[28][14]

Změna oproti OchOsÚ:

Nařízení nově správcům udává povinnost záměrné a standardní ochrany. Za záměrnou ochranu Nařízení považuje přijetí technických a organizačních opatření na ochranu osobních údajů před a při zpracování. Standardní ochranou je potom přijetí takových opatření, aby docházelo ke zpracování pouze těch osobních údajů, které jsou nutné pro dosažení cíle zpracování.

Další novinkou legislativy je povinnost organizací prokázat, že jejich zpracování je v souladu s Nařízením.

Pokud správci nebo zpracovatelé mají více než 250 zaměstnanců, jejich zpracování představuje riziko pro práva a svobody subjektů údajů, zpracovávají citlivé údaje nebo údaje o rozsudcích v trestních věcech nebo trestných činech a nejedná se o příležitostné zpracování, jsou nově povinni vést záznamy o zpracování osobních údajů. Tyto záznamy ukazuje Tabulka 2.

2.4.1 Odpovědnost správce

Novou povinností správce je podle čl. 33 odst.1 Nařízení je povinnost ohlásit porušení zabezpečení osobních údajů dozorovému orgánu. Jakmile se správce o porušení zabezpečení dozví, běží 72hodinová lhůta na ohlášení porušení. Obsah ohlášení je vymezen v témže článku odst. 3. To, že se správce o porušení nedozví, ho ale nezbavuje odpovědnosti, jelikož je pravidelně povinen testovat a posuzovat opatření k zajištění bezpečnosti osobních údajů.

Správce nemusí oznamovat porušení zabezpečení, pokud by nepředstavovalo riziko pro práva a svobody fyzických osob. Proto správce při detekci nějaké skutečnosti, která by mohla představovat porušení zabezpečení, provede prvotní posouzení[28][14]:

1) vyhodnotí, zda se skutečně jedná o porušení zabezpečení,
2) provede posouzení rizika a jeho vyhodnocení, zda není riziko tak nízké, že nevznikne povinnost porušení zabezpečení oznamovat, nebo naopak tak vysoké, že by bylo nutné porušení zabezpečení oznamovat i subjektům údajů,

Správce musí vytvářet a spravovat dokumentaci všech porušení zabezpečení, i těch s vyhodnocením nízké pravděpodobnosti rizika pro práva a svobody fyzických osob. Spolu s dokumentací porušení zabezpečení by měla být uchovávána i přijatá opatření.[28][14]

Ze stejného článku Nařízení plyne, že zpracovatel nemá povinnost oznamovat porušení zabezpečení dozorovému orgánu. Bude ale povinen zjištění takovéto skutečnosti posoudit a vyhodnotit, zda tato skutečnost představuje riziko pro práva a svobody fyzických osob. Pokud vyhodnotí, že skutečnost představuje porušení zabezpečení, ihned to oznámí správci.[28][14]

Pokud na základě čl. 34 Nařízení správce vyhodnotí, že skutečnost může mít za následek vysoké riziko pro práva a svobody fyzických osob, je povinen oznámit porušení zabezpečení, kromě ÚOOÚ, také dotčeným subjektům údajů. Toto může správci nařídit i dozorový úřad. Oznámit porušení není nutné, pokud již správce zavedl potřebná opatření, která jsou použita u zasažených osobních údajů (tím může být například, že osobní údaje jsou v nečitelné formě pro kohokoliv, kdo k nim nemá oprávněný přístup) nebo příjme dodatečná opatření, která vyloučí vysoké riziko pro práva a svobody fyzických osob. Poslední možností, kdy správce porušení nemusí oznamovat je situace, kdy by pro něj oznámení subjekt údajů znamenalo nepřiměřené úsilí. V takové případě ale musí informovat subjekty jiným způsobem (veřejným prohlášením, oznámením na úvodní stránce při přihlášení do systému aj.[28][14]

Pokud správce vyhodnotí, že skutečnost může mít vzhledem k využitým technologiím, povaze, rozsahu a kontextu za následek vysoké riziko pro práva a svobody fyzických osob, má povinnost provést posouzení vlivu zpracování na ochranu osobních údajů (DPIA) podle čl. 35.[28][10][14]

Při DPIA si správce vyžádá posudek pověřence pro ochranu osobních údajů, pokud ho ovšem jmenoval. DPIA se podle čl. 35 odst. 3 provádí povinně v případech[28][10][14]:

a) systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají závažný dopad na fyzické osoby,

b) rozsáhlého zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10,

c) rozsáhlého systematického monitorování veřejně přístupných prostorů.

Pokud dané zpracování představuje velké riziko pro práva a svobody subjektů údajů a správce nepřijme opatření ke zmírnění tohoto rizika, je povinen konzultovat před zpracování s dozorovým úřadem. Celý tento postup povinnosti předchozí konzultace, žádosti o konzultace, postupu dozorového orgánu při předchozí konzultaci, předchozích povolení a návrhů legislativních opatření popisují čl. 36 a čl. 58 Nařízení.[28][10][14]

Jak jsem již zmínila, klíčovou složkou povinnosti správce je přijetí odpovídajících technických a organizačních opatření pro zajištění souladu s Nařízením a dále schopnost tuto skutečnost dokázat. Správce by v souvislosti s těmito povinnostmi měl posoudit rizika pro práva a svobody subjektů údajů, které jsou součástí zpracovávání. Způsob zajišťování souladu s Nařízením by měl potom vycházet z úrovně rizika, které dané zpracování představuje. Činnosti, při kterých je vhodné provést posouzení rizik, si lze přečíst v Příloze A.[28][14]

Vedle zajišťování souladu s Nařízením je správce také povinen tento soulad prokázat. Jak již bylo uvedeno, nejlépe lze soulad prokázat určitou a srozumitelnou dokumentací o plnění jednotlivých povinností. Určitou, protože by se měla věnovat pouze informacím, které se týkají zpracování. Neměla by se tedy skládat z nepotřebné dokumentace nebo obsahovat příliš obecné informace. A srozumitelnou, protože by měla být srozumitelná pro člověka, který nepochází z dané organizace a nezná veškeré firemní procesy. Komplexnost této dokumentace se odvíjí od okolností jednotlivých zpracování, tedy jeho rizikovosti. Při vedení dokumentace by se správce měl zaměřit zejména na klíčové povinnosti, jako je posuzování rizik pro práva a svobody subjektů údajů, plnění zásad Nařízení, jmenování právního základu zpracování, řešení žádostí k uplatnění práv subjektů údajů, technická a organizační opatření pro zabezpečení souladu s Nařízením aj.[28][14]

Dokumentace může být v listinné formě nebo lépe v elektronické, kde je možné, aby se na její tvorbě podílelo více lidí a byla pravidelně aktualizována.[28]

V souladu s Nařízením by měl správce zavést tzv. interní koncepce (nebo také anglicky data protection policies). Pod těmi si lze představit nějaký interní předpis nebo soustavu předpisů, kterými se budou při zpracování osobních údajů zaměstnanci řídit. Tyto interní politiky by měly splňovat následující kritéria[28]:

a) měly by být podrobné a srozumitelné (obsahovat povinnosti a postupy zaměstnanců při zpracování osobních údajů tak, aby jim každý zaměstnanec rozuměl a nemohlo dojít ke dvojímu výkladu dané skutečnosti),

b) koncepce musí umožňovat ověření jejího plnění (možnost určit soulad či nesoulad s danou koncepcí),

c) koncepce by měla být proveditelná (povinnosti by měly být formulovány tak, aby bylo možné zajistit jejich dodržení),

d) koncepce musí být aktuální (koncepce musí odrážet technologie a zpracování, které se v současnosti v organizaci používá).

V rámci organizace se tyto koncepce budou lišit. Jiné koncepce bude mít IT oddělení, marketingové oddělení nebo třeba oddělení lidských zdrojů.[28]

Zajištění souladu s Nařízením by také mělo obsahovat úvodní školení členů organizace a následné průběžné proškolování ohledně individuálních povinností. Tato školení je také nutné dokumentovat.[28][14]

Doložit soulad s Nařízením lze pomocí kodexů chování nebo pomocí schválených mechanismů pro vydávání osvědčení. Kodexům chování, osvědčením a akreditovaným subjektům, které je mohou udělovat, se Nařízení věnuje v čl. 40-43. Kodexy chování jsou dokumenty, které zpracují různá sdružení a schvaluje je dozorový orgán, v ČR se jedná o ÚOOÚ. Tím, že správce příjme kodexy chování, dovoluje, aby u něj mohl autorizovaný subjekt provádět monitoring dodržování těchto dokumentů.[28][14]

Pokud si správce zvolí doložit soulad pomocí osvědčení o ochraně osobních údajů, nastaví si vlastní mechanismy a potom požádá akreditovaný subjekt o udělení osvědčení. Akreditovaný subjekt u správce provede audit a posoudí soulad. Pokud uzná, že správce zpracovává osobní údaje v souladu s Nařízením, udělí subjektu osvědčení s platností maximálně na 3 roky.[28]

Kromě doložení souladu musí správce také zajistit záměrnou a standardní ochranu. Pro efektivní zajištění záměrné ochrany se lze inspirovat osmi strategiemi vydanými Evropskou agenturou pro síťovou a informační bezpečnost.[28]

Standardní ochrana osobních údajů spočívá ve vhodném organizačním a bezpečnostním opatření tak, aby byly zpracovány pouze ty osobní údaje, které jsou nezbytně nutné. Vyplývá z povinnosti správce minimalizace údajů a jedná se o zajištění[28]:

- zpracování nezbytně nutného množství osobních údajů,
- v nezbytném rozsahu,
- uchování po nezbytně nutnou dobu,
- dostupnost co nejmenšímu okruhu osob.

Pokud nastane situace, kdy se na zpracování podílí více správců, potom podle čl. 26 Nařízení musejí uzavřít smlouvu, ve které upraví vzájemný vztah takovým způsobem, aby byla zajištěna ochrana práv a svobod subjektů údajů.[28][14]

Nařízení dále v čl. 27 vymezuje způsoby a pravidla pro určení zástupců správců nebo zpracovatelů, kteří nejsou usazeni v EU a také vymezuje i výjimky z této povinnosti. Zástupce správce či zpracovatele je usazen v jednom ze členských států EU, ve kterém se vyskytují subjekty údajů, jejichž osobní údaje jsou zpracovávány. Na tyto zástupce se potom mohou obracet dozorové orgány či subjekty údajů s otázkami, které se týkají zpracování osobních údajů.[28][14]

Změna oproti OchOsÚ:

GDPR posiluje odpovědnost správců za zpracování osobních údajů a každý správce musí prokázat, že zavedl příslušná technická a organizační opatření na ochranu osobních údajů a doložit soulad s Nařízením. Technická a organizační opatření mohou obsahovat různá interní opatření, školení zaměstnanců, audity zpracovatelských činností, jmenování pověřence na ochranu osobních údajů, dodržování kodexů chování nebo různé certifikace a jejich rozsah záleží zejména na riziku, které zpracování přináší. Vše by měl správce opět patřičně dokumentovat.

Jak jsem již zmínila, úplně novou povinností správce, je hlásit porušení zabezpečení osobních údajů ÚOOÚ a to do 72 hodin od zjištění incidentu. GDPR vymezuje také obsah takového ohlášení. Při zjištění správce, že porušení zabezpečení přináší vysoké riziko pro práva a svobody subjektů údajů, je povinen toto porušení ohlásit také dotčeným subjektům.

Pokud ale správce vyhodnotí, že porušení zabezpečení přináší nízké riziko pro práva a svobody subjektů údajů, není povinen porušení hlásit, je ale povinen ho zdokumentovat.

Pokud existuje pravděpodobnost, že zpracování bude představovat vysoké riziko pro práva a svobody subjektů údajů, je správce povinen provést posouzení vlivu na ochranu osobních údajů (DPIA) a v případě, že toho vysoké riziko nelze odstranit či zmírnit, konzultovat zpracování s ÚOOÚ. GDPR také definuje podmínky, za kterých je vypracování DPIA povinné.

2.4.2 Odpovědnost zpracovatele

Správce může pověřit zpracováním osobních údajů pouze ty zpracovatele, kteří poskytují dostatečné záruky, co se týče technických a organizačních opatření plynoucích z Nařízení. Správce může pověřit jednoho nebo více zpracovatelů, kdy rozsah zpracování osobních údajů je plně na rozhodnutí správce.[28][14]

Za vhodná technická a organizační opatření lze podle pracovní skupiny WP29 a jejího stanoviska[11] v oblasti cloud computingu považovat integritu, důvěrnost, transparentnost, izolovanost, součinnost, odpovědnost.[28]

Požadavek integrity stanoví, že během zpracování nebude docházet jakémukoliv pozměnění osobních údajů. Důvěrnost se týká zejména toho, že zaměstnancům budou přístupné pouze ty údaje, které jsou nezbytně nutné k vykonávání jejich činnosti, povinnosti mlčenlivosti a dále důvěrnosti ve smyslu šifrování nebo pseudonymizaci, které mohou přispět k zabezpečení osobních údajů. Transparentnost technických a organizačních opatření se požaduje zejména proto, aby byl správce schopen posoudit tato opatření a jmenovat pouze ty zpracovatele s dostatečnými opatřeními. Pokud zpracovatel zpracovává osobní údaje od více správců, musí zajistit jejich izolovanost, tedy zajistit, aby nedošlo ke sloučení těchto osobních údajů. Součinnost znamená umožnění řádného výkonu práv subjektů údajů, ale také spolupráci se správcem. A odpovědnost směřuje na sankce a postihy vůči zaměstnancům nebo jiným pracovníkům, kteří poruší dané povinnosti.[28]

Zpracovatel je v pozici podřízené správci z hlediska zpracování osobních údajů. Osobní údaje může zpracovávat jen k tomu účelu, ke kterému mu byly svěřeny a podle pokynů správce. Pokud tyto pokyny poruší, dostává se do pozice správce a bere veškerou odpovědnost za související povinnosti.[28][14]

[11] Stanovisko WP29 č. 5/2012 ze dne 1.července 2012 ke *cloud computingu*, WP 196, s. 14.

Mezi povinnosti zpracovatele patří[28][14]:

- vést záznamy o zpracování,
- spolupracovat s dozorovým úřadem,
- zavést vhodná technická a organizační opatření,
- hlásit porušení zabezpečení osobních údajů správci,
- jmenovat pověřence pro ochranu osobních údajů.

Zpracovatel může zpracovávat osobní údaje pouze na základě smlouvy se správcem (tato smlouva se také nazývá zpracovatelská smlouva nebo data processing agreement). Další možností zpracování osobních údajů je na základě jiného právního titulu, kterým se zpracovatel zavazuje vůči správci a který je v souladu s právem EU nebo členského státu. Náležitosti zpracovatelské smlouvy jsou zahrnuty v Příloze B.[28][4][14]

Změna oproti OchOsÚ:

Pokud správce využívá zpracovatele, je nutné, aby tento vztah byl ošetřen zpracovatelskou smlouvou. Smlouva by měla sloužit hlavně k tomu, aby obě strany pochopily své povinnosti a odpovědnosti. GDPR nově oproti OchOsÚ definuje konkrétní položky, které by tato smlouva měla splňovat (náležitosti smlouvy si zle přečíst v Příloze B). Správce je povinen pověřit zpracováním pouze ty zpracovatele, kteří poskytují dostatečné záruky pro zpracování osobních údajů. Zpracovatel je povinen se řídit pokyny správce definovanými v smlouvě. Další konkrétnější kontrolní listy, které se týkají smluvního vztahu mezi správci a zpracovateli si lze přečíst na stránkách ICO v [4].

2.4.3 Pověřenec pro ochranu osobních údajů

Jmenování, postavení a úkoly pověřence pro ochranu osobních údajů (DPO) vymezují čl. 37, čl. 38 a čl. 39. Pověřenec pro ochranu osobních údajů by měl dohlížet na soulad zpracování osobních údajů s Nařízením a radit správci nebo zpracovateli, kdy postupuje v rozporu s tímto Nařízením. Pověřenec by měl dále sloužit jako kontaktní osoba pro subjekty údajů a dozorový úřad v otázkách, které se týkají zpracování osobních údajů.[28][14]

Pověřence je dle Nařízení čl. 37 odst. 1 nutné jmenovat, když[28][30][12][14]:

- zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých pravomocí,

- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, rozsahu nebo svým účelům vyžadují rozsáhlé, pravidelné a systematické monitorování subjektů údajů,
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v čl. 9 Nařízení a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10 Nařízení.

Pověřence může jmenovat i správce nebo zpracovatel, kterému to Nařízení přímo neukládá, jako povinnost a nemusí být nutně nový pracovník, může být zvolen z řad pracovníků, kteří se již v organizaci o ochranu osobních údajů starají. Je ale třeba, aby takovýto zaměstnanec měl potřebnou kvalifikaci, absenci střetů zájmů a přístup k nejvyššímu vedení.[28][30]

Kvalifikace pověřence by měla odpovídat úrovni ochrany osobních údajů při zpracování. Je tedy na správci nebo zpracovateli, aby určil kritéria pro pověřence v dané organizaci, která se budou organizace od organizace lišit. Mezi základní požadavky by měla patřit znalost národních a evropských předpisů, které se týkají ochrany osobních údajů a předpisů, které s ochranou osobních údajů souvisí. Dále by pověřenec měl znát zpracování, které správce, resp. zpracovatel provádí a veškerá bezpečnostní opatření, která přijal.[28][30][12]

Nařízení v čl. 39 vymezuje minimum úkolů, které musí pověřenec vykonávat. Správce nebo zpracovatel mu však mohou přidělit i další úkoly, které souvisí s ochranou osobních údajů. Podle Nařízení musí pověřenec vykonávat minimálně tyto úkoly[28][30][14]:

- poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování o jejich povinnostech podle tohoto Nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany osobních údajů,
- pověřenec musí nejen znát předpisy, které se týkají ochrany osobních údajů, ale také je musí umět vysvětlit a aplikovat v praxi,
- pověřenec by měl zavést takové komunikační prostředí, aby se na něj zaměstnanci mohli obracet,
- pověřenec by měl správce, resp. zpracovatele informovat o povinnostech, které vycházejí ze stávajících předpisů a zajišťovat např. školení, informační brožury aj.,
- monitorování souladu s Nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti

ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů,

- pověřenec by měl neustále prověřovat procesy zpracování osobních údajů,
- poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle čl. 35,
- správce má podle čl. 35 povinnost si od pověřence, pokud je jmenován, vyžádat posouzení vlivu na ochranu osobních údajů,
- správce by si měl vyžádat stanovisko (zda provádět posouzení, zda provádět interní nebo externí posouzení jakou metodiku pro posouzení zvolit, jaká opatření přijmout ke zmírnění rizik pro práva a svobody fyzických osob),
- spolupráce s dozorovým úřadem,
- působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle čl. 36, a v případě vedení konzultací v jakékoliv jiné věci.

Podle stejného článku, odst. 2, by se měl pověřenec při vykonávání své práce zaměřit zejména na ta zpracování, která představují největší riziko pro práva a svobody subjektů údajů. Měl by si vytvořit seznam priorit, na základě kterých, bude plnit své úkoly. Na ty nejrizikovější oblasti by měl také zaměřit své aktivity týkající se školení, monitorování, poradenství aj.[28][30][12][14]

Změna oproti OchOsÚ:

Nařízení stanovuje, že někteří správci, resp. zpracovatelé jsou povinni jmenovat DPO. Mezi ty se řadí:

- veřejné orgány,
- správci/ zpracovatelé provádějící rozsáhlé monitorování,
- správci/ zpracovatelé provádějící rozsáhlé zpracování citlivých údajů nebo údajů týkajících se rozsudků v trestních věcech a trestných činů.

Jmenovat lze jednoho DPO, nebo celou skupinu, ve které je ale nutné určit jednoho pracovníka, na kterého se subjekty údajů a ÚOOÚ mohou obracet. Jmenovat DPO mohou i organizace, kterým tak GDPR přímo neukládá. Úkolem DPO je informovat a radit

organizaci a jejím pracovníkům o jejich povinnostech, které vyplývají z GDPR a dalších zákonů souvisejících s ochranou soukromých údajů, monitorovat dodržování GDPR a souvisejících zákonů, provádět školení zaměstnanců, interní audity a v neposlední řadě být kontaktním místem pro ÚOOÚ a subjekty údajů, jejich osobní údaje organizace zpracovává.

2.5 Předání osobních údajů do třetích zemí

Předpoklady předání osobních údajů do třetích zemí nebo mezinárodním organizacím mimo EU se zabývají čl. 44-50 Nařízení. Za třetí zemi se považuje jakákoliv země, která leží mimo EU. Předání osobních údajů do zahraničí je jakékoliv poskytnutí osobních údajů správci, resp. zpracovateli mimo EU. Pokud jsou však osobní údaje zveřejněny na internetu, kde k nim má přístup kdokoliv z kterékoliv země, o předání osobních údajů do zahraničí se nejedná.[28][14]

Pro předání osobních údajů do zemí mimo EU stanovilo Nařízení dodatečná pravidla, která musí být splněna pro legální předání. To zejména proto, že v dalších zemích může platit odlišná právní úprava, která nutně nemusí zajišťovat dostačující úroveň ochrany osobních údajů.[28]

V rámci EU je možné předávat osobní údaje bez omezení, ale pokud mají být údaje předány do zemí mimo EU, musí toto předání splňovat určité podmínky[28][14]:

1) předání do zemí, s nimiž má ČR uzavřenou mezinárodní smlouvu, která zakazuje omezování pohybu osobních údajů (státy jejichž předpisy zaručují odpovídající úroveň ochrany osobních údajů),
2) předání do zemí, které jsou podle Evropské komise (EK) stanoveny, jako země s adekvátní úrovní ochrany osobních údajů,
3) správce nebo zpracovatel má stanovený právní důvod pro předání,
4) předání je povoleno ÚOOÚ.

Dle současného OchOsÚ lze volně předávat osobní údaje v rámci států EU a ostatních států Evropského hospodářského prostoru[12] (EHP), to ale dle Nařízení dále nebude možné. Aby mohlo dojít k volnému předávání, bude muset být Nařízení zařazeno do Dohody o EHP.[28]

[12] Mezi tyto země navíc krom zemí EU patří také Norsko, Island a Lichtenštejnsko.

Mezi právní důvody předání osobních údajů pro správce nebo zpracovatele patří[28][14]:

a) rozhodnutí EK o odpovídající ochraně,

b) vhodné záruky dle čl. 46 odst. 2 a 3,

c) výjimky pro specifické situace dle čl. 49 Nařízení.

Podle čl. 45 lze volně předávat osobní údaje do zemí a mezinárodních organizací mimo EU, o kterých EK vydá rozhodnutí, že je zde odpovídající úroveň ochrany osobních údajů. Toto rozhodnutí může EK vydat také pouze na určité území nebo pro dané odvětví. Odpovídající úroveň ochrany osobních údajů, je podle Soudního dvoru Evropské unie taková úroveň ochrany osobních údajů, která je rovnocenná s ochranou v EU. Tato právní úprava ale nemusí být identická, stačí, když zajišťuje ochranu základních práv a svobod, která je rovnocenná s ochranou poskytovanou Nařízením.[28][14]

EK vydá seznam třetích zemí a mezinárodních organizací, o kterých rozhodla, že vyhovují odpovídající ochraně osobních údajů v Úředním věstníku EU nebo na svých internetových stránkách. Tento seznam bude neustále aktualizován. Specifika rozhodování EK o odpovídající ochraně jsou shrnuta v Příloze C.[28][14]

Pokud neexistuje rozhodnutí EK o odpovídající úrovni ochrany, může správce, resp. zpracovatel předat osobní údaje, pokud poskytl vhodné záruky a zároveň jsou ve třetí zemi nebo mezinárodní organizaci k dispozici vymahatelná práva subjektů údajů a je zajištěna jejich právní ochrana.[28][14]

Nařízení dělí vhodné záruky na dvě skupiny[28]:

1 záruky, jejichž splněním správce, resp. zpracovatel může předávat osobní údaje bez dalšího dodatečného povolení dozorového úřadu,

2 záruky, které nejprve musí schválit dozorový úřad a teprve potom je možné zahájit předání osobních údajů.

Do první zmíněné skupiny se podle čl. 46 odst. 2 řadí[28][14]:

a) právně závazné a vymahatelné nástroje mezi orgány veřejné moci nebo veřejnými subjekty,

   – mezi takové nástroje patří např. bilaterální dohody mezi EU a třetími zeměmi pro předání jmenné evidence cestujících (evidence předávají letecké společnosti, aby předešli teroristickým činům),

- bilaterální dohoda mezi EU a USA pro sledování finančních transakcí a předcházení tak financování terorismu (TFTP),

b) závazná podniková pravidla,

- schvaluje místní dozorový úřad hlavní pobočky podniků, potom lze volně předávat osobní údaje,
- užíváno u nadnárodních podniků, kde si dceřiné, případně sesterské společnosti, předávají osobní údaje z různých států,
- na jejich základě lze předávat osobní údaje pouze v rámci určité skupiny organizací,

c) standardní smluvní doložky,

- text smlouvy, kterou správce, resp. zpracovatel z EU uzavře se správcem nebo zpracovatelem ve třetí zemi,
- pokud dojde ke změně standardních smluvních doložek, vyžadují předchozí schválení dozorového úřadu,
- mohou být součástí zpracovatelské nebo jiné smlouvy,
- do budoucna se zvažuje vytvoření odvětvových standardních doložek, které by zohledňovaly např. zpracování citlivých údajů ve zdravotnictví aj.,
- podle přijetí EK existují dvě sady standardních doložek, mezi správcem a správcem a mezi správcem a zpracovatelem,

d) schválený kodex chování nebo schválený mechanismus pro vydávání osvědčení (podle čl. 40-43 Nařízení).

Do druhé skupiny lze dle čl. 46 odst. 3 zařadit[28][14]:

a) smluvní doložky uzavřené mezi správcem nebo zpracovatelem v EU a příjemcem ve třetí zemi, resp. V mezinárodní organizaci,

b) ustanovení vložená do správních ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektů údajů.

Pokud předání nesplňuje podmínky rozhodnutí EK o odpovídající úrovni ochrany nebo vhodné záruky, je možné předat osobní údaje, pokud je splněna alespoň jedna podmínka čl. 49 Nařízení, který vymezuje výjimky předání pro specifické situace. Jedná se o situace, kdy je

riziko pro práva a svobody subjektů údajů poměrně malé nebo nad právy subjektů údajů převáží jiné zájmy.[28][14]

2.6 Dozorové orgány

Vymezení činnosti, pravomocí a povinností dozorových orgánů věnují Kapitoly VI a VII, tedy čl. 51–76. Nařízení stanovuje každému členskému států EU zřídit alespoň jeden nezávislý dozorový úřad, který by dohlížel nad dodržováním Nařízení v odpovídajícím členském státu. V ČR je tímto úřadem, jak již bylo zmíněno, ÚOOÚ. Pro kompetence a povinnosti ÚOOÚ se podle Nařízení nic zásadního nezmění. Dozorové úřady členských států budou dále povinné dodržovat mechanismy spolupráce a jednotnosti (tzn., že se budou muset účastnit mezinárodní spolupráce, která vyplývá ze stále častějšího přeshraničního zpracování osobních údajů).[28][14]

2.6.1 Úřad na ochranu osobních údajů

Podle Nařízení by měl být ÚOOÚ nezávislým úřadem. To se týká funkční, finanční i personální činnosti. Funkční nezávislost se týká, jak samotného úřadu, tak jeho předsedy a inspektorů. Co se týká finanční nezávislosti, tak pokud dozorový úřad nebude schopen vykonávat své úkoly, budou členské státy povinny s potřebnou kapacitou pomoci, jak už s finanční, tak například s personální nebo odbornou. ÚOOÚ je již finančně nezávislý, jelikož, jak již bylo řečeno výše, hospodaří na základě vlastního rozpočtu. Personální nezávislost ÚOOÚ podle [28] nesplňuje, jelikož většina pracovníků je podřízena Ministerstvu vnitra nebo Vládě České republiky. Nad těmito subjekty by ale ÚOOÚ měl vykonávat kontrolu.[28][14]

Členové dozorových úřadů by měly být jmenováni transparentním způsobem. Jmenováni musí být Parlamentem, Vládou, hlavou státu nebo jiným nezávislým subjektem. Člen by měl mít odpovídající kvalifikaci, dovednosti, zkušenosti z oblasti ochrany osobních údajů a k plnění svých úkolů. Jeho povinnosti končí uplynutím jeho funkčního období a odvolán může být pouze, pokud již nesplňuje podmínky pro plnění daných povinností nebo pokud se dopustil závažné chyby. Členy ÚOOÚ jsou předseda a inspektoři. Jak již bylo řečeno, v ČR jsou členové voleni Senátem a jmenováni prezidentem ČR. Nařízení je ale přísnější, co se týká kompetencí členů dozorových úřadů. Kompetence, znalosti a dovednosti z oblasti ochrany osobních údajů nebyly podle OchOsÚ nutností pro členy ÚOOÚ.[28][14]

Úkoly dozorových úřadů vymezuje čl. 57 Nařízení. ÚOOÚ má oproti stávající právní úpravě nové postupy, které mu Nařízení ukládá (např. posouzení vlivu na ochranu osobních údajů, vydávání osvědčení, aj.). Mezi tyto úkoly se podle jmenovaného článku řadí[28][14]:

a) povinnost sledovat uplatňování Nařízení, tedy sledování dopadu Nařízení do praxe a jeho následné vymáhání,

b) vzdělávání a poradenská činnost pro veřejnost (odbornou i laickou), pro zvyšování obecného povědomí o právech, povinnostech a pravidlech spojených se zpracováním osobních údajů,

c) individuální správní dozor, kontrola, ukládání nápravných a sankčních opatření a vedení jejich spisové služby,

d) mezinárodní spolupráce s dozorovými úřady členských států, spolupráce se Sborem,

e) úkoly, které se týkají konkrétních institutů nebo procesů, jako je přijímání standardních smluvních doložek, vytvoření seznamu činností, které podléhají posouzení vlivu na ochranu osobních údajů, poskytování předběžné konzultace, úkoly spojené s kodexy chování, udělování osvědčení o ochraně osobních údajů a úkoly týkající se předávání osobních údajů do třetích zemí,

f) ostatní úkoly, které spadají do ochrany osobních údajů podle jiných právních předpisů, sledování rozsáhlých IS (např. Schengenský IS),

g) usnadňování podávání stížností, např. vytvořením elektronických formulářů,

h) poskytování bezplatných úkolů, jako jsou konzultace pro správce, zpracovatele a pověřence, informování o právech subjektu údajů, vyřizování stížností aj.

Pokud se však bude jednat o nepřiměřený úkol (stížnost, dotaz, žádost), může dozorový úřad tento úkol zpoplatnit nebo dokonce zamítnout. Tímto chce Nařízení předejít zneužívání některých práv.[28][14]

Co se týká pravomocí ÚOOÚ, tak podle čl. 58 nedojde od stávající úpravy podle OchOsÚ, správního řádu a kontrolního řádu k významné změně. Nově jsou upraveny pouze kompetence, jako je ohlašování porušení zabezpečení, přezkum osvědčení aj. Novinkou Nařízení je audit, který bude představovat zjišťování skutečného stavu při zpracování osobních údajů, tedy pouze běžnou kontrolu. Další novou kompetencí je ohlašování správci nebo zpracovateli možné

porušení Nařízení (například na základě nějaké stížnosti nebo upozornění od dotčené osoby).[28]

Jednotlivé dozorové úřady členských států by mezi sebou měly spolupracovat, tyto principy spolupráce a jednotnosti jsou popsány v čl. 60–63. Principy spolupráce tvoří vzájemná pomoc a společné postupy. Vzájemná pomoc je chápána, jako poskytování potřebných informací a provedení některých úkonů na žádost jiného dozorového úřadu. Společné postupy jsou například společné vyšetřování a slouží k usnadnění úředních postupů.[28][14]

Mechanismus jednotnosti tkví v jednotném prosazování Nařízení na území členských států EU a je prosazována zejména pravomocemi Sboru a EK. Jednotnost je zajišťována zejména vydáváním stanovisek, řešením sporů, vydáváním postupů pro naléhavé případy a výměnou informací. Všechny tyto činnosti, včetně závaznosti rozhodnutí a časových lhůt pro rozhodnutí jsou upraveny v čl. 64–67 Nařízení.[28][14]

Změna oproti OchOsÚ:

Organizacím na základě Nařízení odpadá povinnost hlásit, resp. registrovat zpracování osobních údajů ÚOOÚ. Tato povinnost je nahrazena funkčností výše zmíněných povinností, jako je povinnost vedení záznamů o zpracování, posouzení vlivu zpracování (DPIA), případná konzultace s ÚOOÚ a celkově zvýšenou odpovědností správce a zpracovatele a jejich povinností dokládat soulad s Nařízením.

Nařízení zakotvuje nezávislost, jednotné postupy, vzájemnou spolupráci a vyšetřovací pravomoci dozorových úřadů.

2.6.2 Evropský sbor pro ochranu osobních údajů

Evropský sbor pro ochranu osobních údajů (Sbor), je zcela novým úřadem, který vznikl z WP29. Ta byla jedním z nejdůležitějších poradních orgánů pro ochranu osobních údajů v EU. WP29 byla původně založena na základě Směrnice a její činnost spočívala ve vydávání stanovisek a doporučení. Zřízení, povinnosti a pravomoci jsou vymezeny v čl. 68–76 Nařízení.[28][31][14]

Sbor, který nahradí WP29, má rozšířené pravomoci, například může rozhodovat spory mezi dozorovými úřady, rozhodovat o postupech v naléhavých případech aj. Jeho hlavní činností je zajišťovat jednotnost uplatňování Nařízení, podpora jeho uplatňování a za tímto účelem i jeho monitorování, vydávání výkladů, pokynů, doporučení v oblasti ochrany osobních údajů. Rozhodnutí Sbor přijímá prostou většinou.[28][31][14]

Sbor je složen z vedoucích pracovníků dozorových úřadů členských států a evropského inspektora pro ochranu osobních údajů. V čele Sboru stojí předseda a dva místopředsedové, kteří jsou voleni ze stávajících členů na pět let. Pokud má členský stát více dozorových úřadů, jako například Německo, zvolí si jednoho společného zástupce. Účastnit se zasedání Sboru má právo také zástupce EK, který ale nemá hlasovací právo. Jedná se pouze o informační povinnost, kterou má Sbor vůči EK.[28][16]

Tak, jako jednotlivé dozorové úřady členských států, musí být dle Nařízení i Sbor nezávislým orgánem, což v praxi znamená, že nemůže přijímat pokyny od orgánů EU.[28]

Úkoly Sboru jsou vymezeny v čl. 70. Tyto úkoly Sbor vykonává samostatně nebo na žádost EK. Jak již bylo řečeno, hlavním úkolem Sboru je zajistit jednotnost uplatňování Nařízení v členských státech EU, a to zejména tím, že monitoruje a zajišťuje jeho uplatňování, prošetřuje některé otázky Nařízení, vydává pokyny, doporučení a osvědčené postupy, vydává pokyny pro dozorové orgány a přezkoumává jejich uplatňování, podporuje vydávání kodexů chování, zavádění mechanismů pro vydávání osvědčení, vydávání známek a pečetí dokládající ochranu osobních údajů a vydává k nim stanoviska, provádí akreditaci subjektů pro vydávání osvědčení a provozuje elektronický registr rozhodnutí přijatých dozorovými úřady a soudy.[28]

Sbor je podobně, jako dozorové úřady, povinen vydávat výroční zprávy o ochraně osobních údajů, které předá Evropskému parlamentu, Radě a EK. Ty budou sloužit zejména pro transparentnost činnosti Sboru, jako podklad pro úpravu legislativy a pro přehled ochrany osobních údajů fyzických osob v EU, třetích zemích a mezinárodních organizacích.[28]

Jako podpůrný orgán Sboru bude sloužit Sekretariát evropského inspektora pro ochranu osobních údajů. Bude zajišťovat zejména analytickou, administrativní a logistickou činnost.[28]

3 DOPADY A NUTNÁ OPATŘENÍ PRO SPLNĚNÍ OBECNÉHO NAŘÍZENÍ

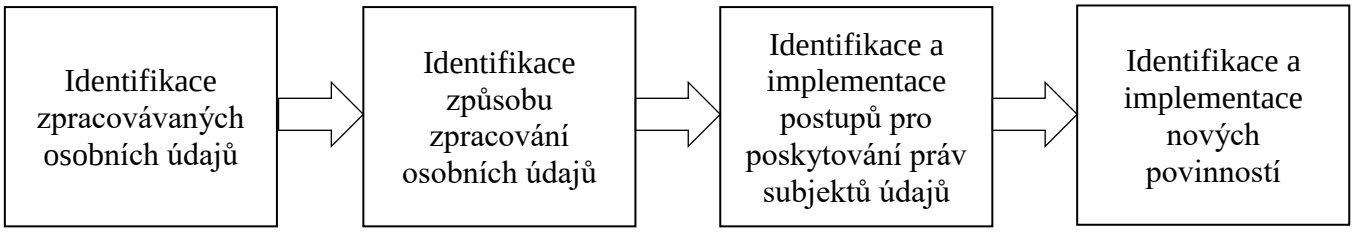
Jak již bylo řečeno, Nařízení se týká všech organizací, které zpracovávají osobní údaje občanů EU, ať už se jedná o živnostníky, e-shop, který zaměstnává dva zaměstnance nebo velkou mezinárodní organizaci. Avšak na každou z těchto institucí bude GDPR dopadat jinou vahou a budou se na ni vztahovat jiná opatření. Proto by organizace měly provést analýzu stávajícího stavu, zjistit soulad nebo nedostatky s Nařízením a následně zavést změny, které zjištěné nedostatky odstraní.

Vůbec prvním krokem organizace by mělo být uvědomění vedoucích pracovníků, že přichází změna v legislativě, uvědomění, jaké změny přináší oproti OchOsÚ a určení oblastí jejího podnikání, kterých by se tyto změny mohly dotknout. V rámci tohoto by si měli uvědomit, kterou roli ve zpracování organizace zaujímá, zda správce či zpracovatele. GDPR na ně klade podobně, jako OchOsÚ, rozdílné požadavky, ale o něco větší zodpovědnost. Obecně platí, že veškerou zodpovědnost za zpracování osobních údajů má správce.

Pokud správce přenechá zpracování na zpracovateli, nezbavuje ho to jeho odpovědnosti a veškeré náležitosti musí být ošetřeny smluvně, podle GDPR. Správce může pověřit zpracováním pouze ty zpracovatele, o kterých usoudí, že disponují dostatečnými technickými a organizačními opatřeními pro ochranu osobních údajů. Zpracovatel potom může osobní údaje zpracovávat pouze v tom rozsahu a k tomu účelu, ke kterému mu je správce předal. Musí zajistit, aby nedošlo ke sloučení osobních údajů více správců a musí upozornit správce, pokud dojde k úniku dat.

Pokud organizace zpracovává osobní údaje ve více než jednom členském státě EU, potom by měla zjistit, která z provozoven v jednotlivých státech je její hlavní a na základě toho zjistí, který bude její vedoucí dozorový orgán. Hlavní provozovna může být tam, kde se nachází hlavní správa či jiné vedoucí složky organizace, které určují účel zpracování. WP29 vytvořila pokyny pro určení řídícího dozorového orgánu.

Postup uvedení organizace do souladu s GDPR by se mohl shrnout do několika základních kroků. Tyto kroky ukazuje Obrázek 1. Jedná se o identifikaci osobních údajů, které organizace zpracovává, identifikace způsobu zpracování, identifikaci a implementaci postupů pro poskytování práv subjektů údajů a identifikaci a implementaci nových povinností, které organizacím GDPR ukládá.



Obrázek 1 Postup uvedení organizace do souladu s Nařízením

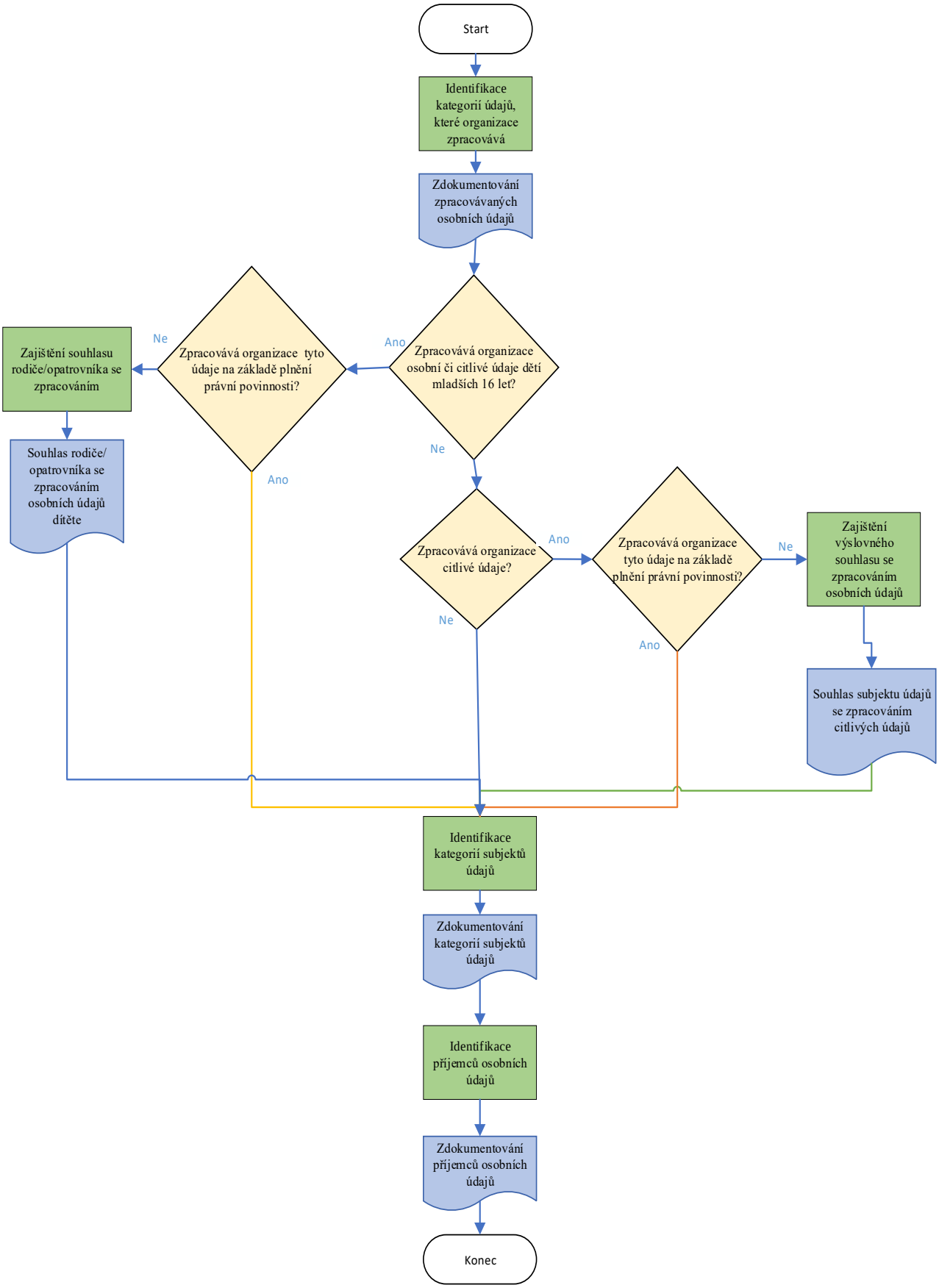
Zdroj: vlastní zpracování

3.1 Identifikace zpracovávaných osobních údajů

Prvním krokem organizace by mělo být zjištění, jaké osobní údaje vůbec zpracovává. Postup identifikace zpracovávaných osobních údajů ukazuje Obrázek 2. Nejprve organizace musí identifikovat veškeré osobní údaje, které zpracovává (jméno, příjmení, RČ, pohlaví, aj.) a určit o jaké kategorie osobních údajů se jedná (osobní údaje, citlivé údaje, údaje dětí). Pokud organizace zpracovává osobní údaje dětí, měla by myslet na ověření jejich věku a případně na získání souhlasu jejich rodiče nebo opatrovníka se zpracováním osobních údajů (pokud Nařízení neurčí jinak). Nařízení se nově více zaměřilo na ochranu osobních údajů dětí, zejména kvůli rozšiřujícím se internetovým službám, jako jsou sociální sítě. Pokud dítě nedovršilo 16 let, musí organizace získat souhlas rodiče nebo opatrovníka se zpracováním jeho osobních údajů. Při zpracovávání citlivých údajů musí organizace také zajistit souhlas subjektu údajů se zpracováním (pokud Nařízení neurčí jinak).

Je dobré také identifikovat kategorie subjektů údajů, kterých se tyto osobní údaje týkají (zaměstnanci, zákazníci, dodavatelé, odběratelé, aj.). Nakonec by organizace měla zdokumentovat příjemce, kterým osobní údaje předává. Tím si organizace usnadní další postupy, které se týkají např. opravy osobních údajů nebo konkrétních práv subjektů údajů. Vhodné je všechny tyto informace zdokumentovat pro usnadnění dalších postupů.

Výsledkem této fáze by mělo být zdokumentování kategorií osobních údajů, které organizace zpracovává (pro lepší přehlednost zdokumentování kategorií osobních údajů, které zpracovávají jednotlivá oddělení organizace) a v případě zpracovávání citlivých údajů či údajů dětí, obstarání souhlasu se zpracováním těchto údajů, pokud Nařízení neurčí jinak. Dále zdokumentování kategorií subjektů údajů, pokud se jedná o větší firmu, která nezpracovává osobní údaje pouze svých zaměstnanců nebo pouze klientů. A nakonec zdokumentování, zda tyto osobní údaje organizace předává třetím osobám, případně kterým.



Obrázek 2 Identifikace zpracovávaných osobních údajů

Zdroj: vlastní zpracování

3.2 Identifikace způsobu zpracování osobních údajů

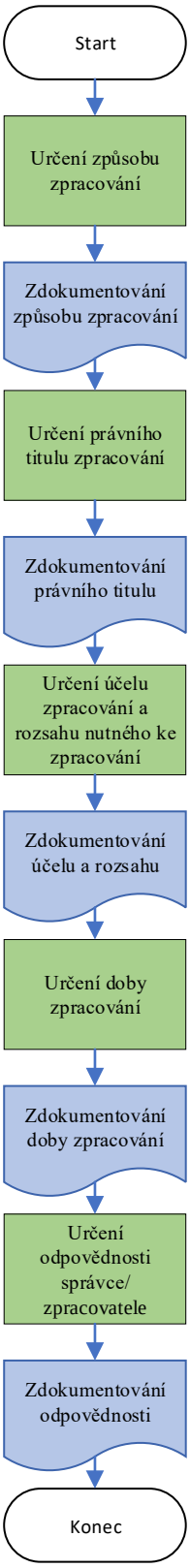
V okamžiku, kdy organizace zdokumentovala zpracovávané osobní údaje, musí určit účel a právní titul zpracování těchto údajů, definovat změny, které Nařízení konkrétně pro jejich zpracování stanoví a případně vytvořit plán implementace těchto změn. Identifikaci způsobu zpracování osobních údajů uvádí Obrázek 3. Hlavními principy zpracování dle Nařízení jsou mimo jiné zákonnost, transparentnost a odpovědnost. Při zpracovávání osobních údajů mají organizace povinnost informovat subjekty údajů o způsobu zpracování, jejich právním titulu pro zpracování, účelu zpracování a rozsahu osobních údajů nutných pro toto zpracování, o době, po kterou budou jejich údaje ukládány, že se subjekty mohou obracet na ÚOOÚ aj. To se v praxi provádí prostřednictvím prohlášení o ochraně osobních údajů. Tyto informace by měly být pro subjekty údajů jasné a srozumitelné.

Nejprve si organizace musí určit způsob zpracování, tedy které osobní údaje zpracovává automatizovaně, automatizovaně se zásahem člověka anebo manuálně. Plně automatizovaně totiž organizace mohou zpracovávat osobní údaje pouze pro účely vymezené Nařízením a pro veškerá automatizovaná zpracování musí organizace vytvářet v další části DPIA.

Dále si organizace musí určit právní titul zpracování (Nařízení určuje 6 možných právních titulů, jako je souhlas, plnění smlouvy, právní základ, veřejný zájem aj.). Když organizace zná svůj právní titul zpracování, musí určit účel zpracování a rozsah osobních údajů potřebný ke splnění tohoto účelu. Osobní údaje, které organizace nepotřebuje ke splnění účelu zpracování, by měla ihned vymazat a přestat zpracovávat. V neposlední řadě by organizace měla určit dobu, po kterou osobní údaje zpracovává.

Nakonec by si organizace měla určit jakou odpovědnost ve zpracování má, tedy zda zpracovává osobní údaje v roli správce nebo zpracovatele.

Výsledkem této fáze by měl být dokument, ve kterém bude k osobním údajům určen právní titul zpracování, účel zpracování, rozsah osobních údajů, který je ke zpracování třeba, doba zpracování těchto údajů a odpovědnost, kterou ve zpracování organizace zastává.



Obrázek 3 Identifikace způsobu zpracování osobních údajů

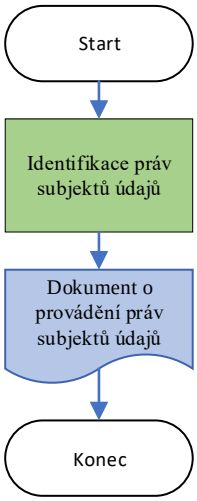
Zdroj: vlastní zpracování

3.3 Identifikace a implementace postupů pro poskytování práv subjektů údajů

Pokud organizace uvede do souladu s Nařízením zpracování osobních údajů, měla by také identifikovat postupy, kterými zajišťuje práva subjektů údajů, viz. Obrázek 4. Těmito právy jsou právo na informace, právo na přístup, právo na opravu, právo na výmaz, právo na omezení zpracování, právo na přenositelnost údajů a právo vznést námitku proti zpracování.

Organizace by si měla určit postupy, jak provádět požadavky na uplatňování těchto práv, určit kdo o provedení rozhodne, uvést do souladu s Nařízením časové lhůty pro poskytování těchto práv apod. Jak již bylo zmíněno, úplně novým právem je právo na přenositelnost osobních údajů, to je ale možné uplatnit pouze, pokud organizace získala osobní údaje přímo od subjektu údajů, pokud je zpracování založeno na souhlasu subjektu údajů nebo smlouvě anebo se jedná o automatizované zpracování osobních údajů. Co se týká práva na výmaz, si organizace může zjistit, zda jim jejich systémy umožňují vyhledat osobní údaje daného subjektu údajů a následně tyto údaje vymazat. Pokud organizace zpracovává velké množství žádostí o přístup, bylo by vhodné zvážit zapojení nějakého systému pro online přístup subjektů údajů k jejich údajům. Ve většině případů nebude možné tyto požadavky zpoplatnit. Požadavkům je nutné vyhovět do jednoho měsíce. Žádost lze zamítnout nebo zpoplatnit, pokud je neopodstatněná nebo představuje nadměrné úsilí. Pokud dojde k zamítnutí žádosti, je nutné individuálně upozornit subjekty údajů na právo podat stížnost u ÚOOÚ.

Výsledkem této fáze by měl být opět dokument, ve kterém by měly být uvedeny postupy provádění práv subjektů údajů, lhůty, ve kterých je třeba tato práva poskytovat a popřípadě kdo je za tuto činnost v organizaci odpovědný.



Obrázek 4 Identifikace a implementace práv subjektů údajů

Zdroj: vlastní zpracování

3.4 Identifikace a implementace nových povinností

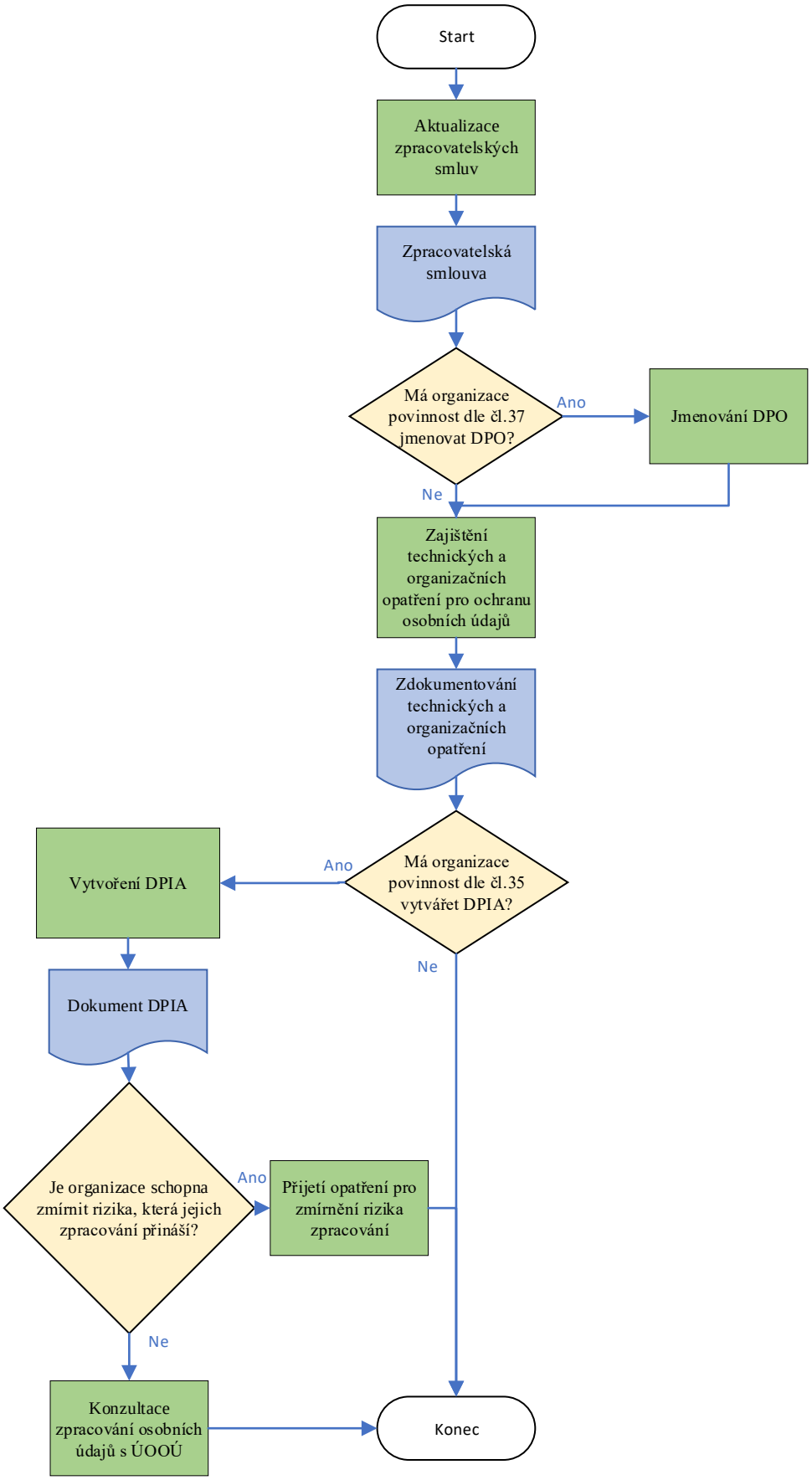
Organizace na základě nových povinností, které jim Nařízení ukládá, musí určit, které z těchto povinností se týká konkrétně jí, viz. Obrázek 5.

Nejprve by si organizace měly aktualizovat své zpracovatelské smlouvy dle toho, jak definuje Nařízení. Dalším krokem je rozhodnutí, zda je podle Nařízení nutné, aby organizace jmenovala DPO, tedy pověřence pro ochranu osobních údajů. Mezi organizace, které musejí jmenovat DPO se řadí veřejné orgány, organizace provádějící rozsáhlé monitorování, organizace provádějící rozsáhlé zpracování citlivých údajů nebo údajů týkajících se rozsudků v trestních věcech a trestných činů. Pověřence mohou jmenovat i organizace, kterým tak Nařízení nenařizuje a může organizaci pomoci s dalšími kroky.

Dalším krokem organizace musejí být bezpečnostní opatření. Organizace musí přijmout opatření na ochranu osobních údajů a případně si ujasnit, jaké postupy využívají k detekování, vyšetřování a k zaznamenávání úniků dat. Některé úniky dat budou totiž organizace nově povinny hlásit ÚOOÚ a subjektům údajů. ÚOOÚ musí organizace informovat, pokud dojde k ohrožení práv a svobod subjektů údajů (kvůli úniku by mohlo dojít k jejich diskriminaci, finanční ztrátě, sociálnímu znevýhodnění aj.). Pokud únik dat bude mít za následek velké riziko pro práva a svobody subjektů údajů, budou organizace povinny ohrožení hlásit i subjektům údajů, kterých se únik dat týká. Z předchozího zmapování kategorií osobních údajů by již organizace měla vědět, jaké osobní údaje zpracovává a na základě těchto informací si může vypracovat vodítka, podle kterých by věděla, kdy informovat ÚOOÚ nebo přímo subjekty údajů.

S bezpečností osobních údajů souvisí také posouzení vlivu zpracování (DPIA). Pro organizace, jejichž zpracování přináší velké riziko pro práva a svobody subjektů údajů, je vypracování DPIA povinné. Pokud organizace může dané riziko, které přináší její zpracování zmírnit, příjme opatření pro zmírnění tohoto rizika. Pokud organizace dojde k závěru, že zpracování osobních údajů přináší velká rizika, která organizace nemůže zmírnit, bude muset své zpracování konzultovat s ÚOOÚ.

Výsledek této fáze se bude lišit organizace od organizace. V každém případě by to mělo být přijetí dostatečných bezpečnostních opatření, která se odvíjejí od citlivosti a způsobu zpracování osobních údajů a aktualizace zpracovatelských smluv. Případně by to mělo být přijetí DPO, sepsání DPIA a podle toho, zda lze snížit rizika, která mají vliv na zpracování osobních údajů nebo ne, přijetí opatření pro snížení rizika nebo konzultace s ÚOOÚ.



Obrázek 5 Identifikace a implementace nových povinností

Zdroj: vlastní zpracování

Shrnutí kapitoly

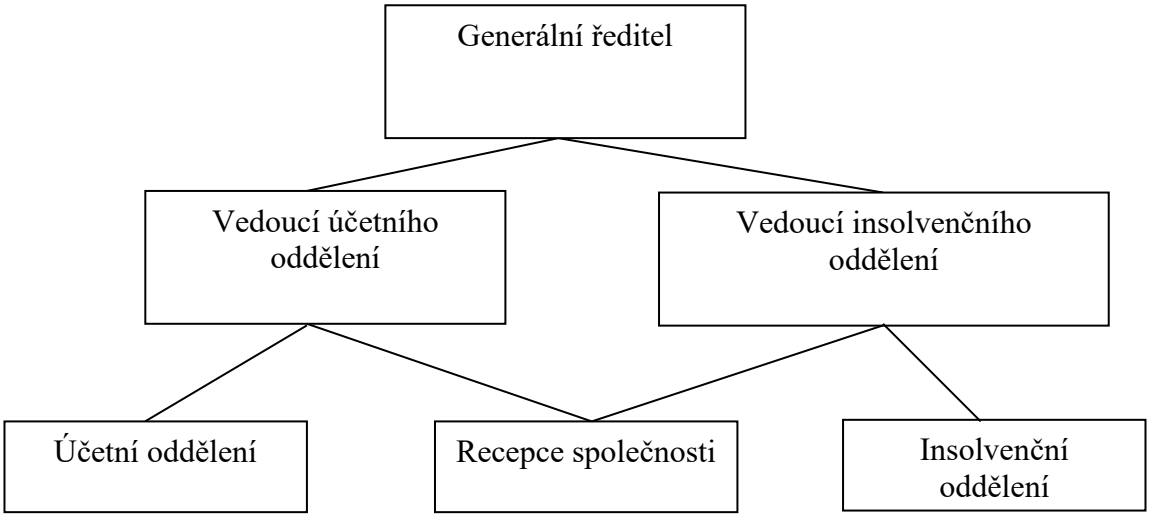
Výsledkem uvedení organizace do souladu s Nařízením by mělo být několik dokumentů. V těch by mělo být zaznamenáno, jaké osobní údaje organizace zpracovává, zda tyto osobní údaje získává přímo od subjektů údajů či nikoliv, o údaje kterých subjektů údajů se jedná a jakým třetím osobám tyto osobní údaje předává. Dále dokument s informacemi, jakou roli v tomto zpracování organizace zastává, jaký je právní titul a účel tohoto zpracování, rozsah potřebný ke splnění účelu zpracování a po jakou dobu dochází ke zpracování. Další dokument by měl obsahovat informace o tom, jak a jaká práva subjektů údajů organizace poskytuje. V neposlední řadě by měl být vytvořen dokument, ve kterém budou zaznamenány technická a organizační opatření pro ochranu těchto údajů.

Na základě těchto informací potom organizace dokáže rozhodnout, zda se na ni vztahují další povinnosti plynoucí z Nařízení, jako je povinnost jmenování DPO, dokumentace DPIA, konzultace s ÚOOÚ anebo na základě těchto informací může vytvořit záznamy o zpracování.

V neposlední řadě je třeba aktualizovat nebo doplnit zpracovatelské smlouvy, jejichž obsah Nařízení nově vymezuje.

4 APLIKACE OBECNÉHO NAŘÍZENÍ VE VYBRANÉ SPOLEČNOSTI

Společnost ESOF s.r.o. poskytuje především služby, které souvisí se zpracováním účetní agendy a daňovým poradenstvím. Vedlejším cílem společnosti je vytvořit full servis odběratelům (např. služby v oblasti korporátního práva – přeměny společností, úpravy notářských zápisů apod.). Společnost byla založena 22. prosince 1992 Ing. Vítězslavem Javůrkem seniorem a v současné době je součástí teamu Mgr. Vítězslav Javůrek mladší. Statutárním úřadem společnosti je Mgr. Vítězslav Javůrek, který společnost také zastupuje navenek a je jejím jediným společníkem. Služby společnosti nelze jednoznačně identifikovat, jelikož se liší podle požadavků a potřeb jednotlivých klientů. Team společnosti tvoří 22 zaměstnanců, kteří podle aktuálních potřeb klientů spolupracují s odborníky. Organizační strukturu společnosti ukazuje Obrázek 6.[13]



Obrázek 6 Organizační struktura společnosti ESOF s.r.o.

Zdroj: zpracováno dle[13]

Každé oddělení má svého vedoucího pracovníka, který odpovídá nejvyššímu vedení společnosti. Mezi řídící management společnosti patří generální ředitel společnosti, následně pak vedoucí účetního oddělení a vedoucí insolvenčního oddělení.[13]

Organizace v rámci poskytování služeb účetnictví vystupuje v roli zpracovatele, a co se týká personálních věcí, stojí v roli správce.

4.1 Identifikace zpracovávaných osobních údajů

V rámci této části bylo zjištěno, **jaké osobní údaje** jsou zpracovávány jednotlivými odděleními, jakých **kategorií subjektů údajů** se týkají a kterým **příjemcům** se osobní údaje předávají. Jak již bylo řečeno, obecně by se společnost dala rozdělit na účetní oddělení, insolvenční oddělení a administrativu (recepci). **Každé** toto **oddělení** využívá ke své činnosti **jiné osobní údaje**.

Účetní oddělení zpracovává pouze osobní údaje, které mu poskytuje klient a které jsou povoleny zpracovávat na základě *zákona č. 563/1991 Sb., o účetnictví* (dále jen zákon o účetnictví). Ve zpracovatelské smlouvě se společnost zavazuje, že osobní údaje nebude poskytovat třetím stranám. Jedná se o následující osobní údaje:

- jméno, příjmení, adresa, RČ (DIČ), tel. číslo, e-mailová adresa, č. bankovního účtu, zdravotní stav, jméno dítěte, příjmení dítěte, RČ dítěte

Do účetního oddělení by se také dalo zahrnout oddělení mzdového účetnictví. To zpracovává stejné osobní údaje na základě stejného zákona o účetnictví. Toto oddělení, krom již zmíněných osobních údajů, zpracovává navíc také VS OSSZ (Variabilní symbol Okresní správy sociálního zabezpečení).

I když společnost zpracovává osobní údaje dětí a citlivé údaje, nemusí vyžadovat souhlas (jak rodiče/opatrovníka nebo samotného subjektu údajů) se zpracováním osobních údajů, za případné získání souhlasu se zpracováním by byl zodpovědný správce. Souhlas ale není třeba, jelikož údaje společnost zpracovává na základě zákona ČR.

Administrativa zpracovává kontaktní údaje klientů a údaje pro spisovou evidenci, která je opět vyžadována zákonem o účetnictví, *zákonem č. 280/2009 Sb., daňovým řádem* (daňový řád), zákonem o příslušné dani, popř. na základě *zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení* (insolvenční zákon). Tyto osobní údaje také neposkytuje třetím stranám:

- jméno, příjmení, č. bankovního účtu, RČ (DIČ), adresa, tel. číslo, e-mail, VS OSSZ, jméno dítěte/dětí, příjmení dítěte/dětí, RČ dítěte/dětí.

Insolvenční oddělení zpracovává osobní údaje subjektů údajů, jimž byl přidělen pracovník tohoto oddělení, jako insolvenční správce. Osobní údaje získává z veřejného Insolvenčního rejstříku, kam osobní údaje doplní sám subjekt údajů a věřitelé. Rozsah informací, které z něj

získá, vychází ze *zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení* (insolvenční zákon). Mezi tyto osobní údaje patří:

- jméno, příjmení, adresa, č. bankovního účtu, RČ (DIČ), jméno dítěte/dětí, příjmení dítěte/dětí, RČ dítěte/dětí.

Insolvenční oddělení zpracované osobní údaje **předává každé 3 měsíce** ve formátu PDF příslušnému **krajskému soudu** prostřednictvím datové schránky.

Kategorií subjektů údajů společnost spravuje pět. **Klienti (K), vlastní zaměstnanci (Z), dodavatelé služby (D), uchazeči o zaměstnání (U) a jiná osoba** ve smluvním vztahu ke správci **(J)**. Potřebné informace o osobních údajích byly doplněny do přehledných tabulek, viz. Tabulka 3 a Tabulka 4, podle toho, zda v nich společnost vystupuje jako správce nebo zpracovatel. Do těchto tabulek budou v dalších fázích doplněny potřebné informace.

Tabulka 3 Osobní údaje, které organizace zpracovává v roli správce

Oddělení	Osobní údaje	Kategorie subjektů údajů	Oddělení	Osobní údaje	Kategorie subjektů údajů
Administrativa (recepce)	– jméno – příjmení – č. bankovního účtu – RČ – tel. číslo – email – adresa	Z, D, U, J	Mzdové účetní (ESOF)	– jméno – příjmení – č. bankovního účtu – RČ – tel. číslo – email – VS OSSZ – zdravotní stav – jméno dítěte – příjmení dítěte – RČ dítěte	Z
Účetní (ESOF)	– jméno – příjmení – RČ – č. bankovního účtu – RČ – tel. číslo – email – adresa – zdravotní stav – jméno dítěte – příjmení dítěte – RČ dítěte	Z			

Zdroj: vlastní zpracování

Tabulka 4 Osobní údaje, které organizace zpracovává v roli zpracovatele

Oddělení	Osobní údaje	Kategorie subjektů údajů	Oddělení	Osobní údaje	Kategorie subjektů údajů
Administrativa (recepce)	– jméno – příjmení – č. bankovního účtu – RČ – tel. číslo – email – adresa – VS OSSZ – jméno dítěte – příjmení dítěte – RČ dítěte	K	Mzdová účtárna	– jméno – příjmení – č. bankovního účtu – RČ – tel. číslo – email – VS OSSZ – zdravotní stav – jméno dítěte – příjmení dítěte – RČ dítěte	K
Účetní oddělení	– jméno – příjmení – adresa – RČ – č. bankovního účtu – email – tel. číslo – zdravotní stav – jméno dítěte – příjmení dítěte – RČ dítěte	K	Insolvence	– jméno – příjmení – č. bankovního účtu – adresa – RČ – jméno dítěte – příjmení dítěte – RČ dítěte	K

Zdroj: vlastní zpracování

4.2 Identifikace způsobu zpracování osobních údajů

V této části si společnost určila **způsob zpracování** osobních údajů, **právní titul** pro zpracování, **účel zpracování**, nutný **rozsah** osobních údajů, které zpracovává, **dobu**, po kterou jsou osobní údaje zpracovávány a **roli**, kterou společnost ve zpracování zastává.

Společnost zpracovává osobní údaje **manuálně**, případně pomocí **výpočetní techniky** v několika softwarech (SW). Těmito SW jsou **POHODA, PAMICA, TaxEdit a MARKTIME**. POHODA slouží pro účetnictví a sestavení faktur, PAMICU společnost využívá pro personalistiku a mzdy, TaxEdit slouží pro zpracování daňových přiznání a MARKTIME slouží jako cloudové uložiště.

V těchto výše zmíněných činnostech, krom personální agendy, vystupuje společnost v roli zpracovatele a osobní údaje zpracovává v rozsahu, v jakém určuje zákon. Osobní údaje jsou s výjimkou insolvenční činnosti získávány přímo od subjektů údajů. Ve zpracovatelských činnostech, kde společnost vystupuje v roli zpracovatele, má získávání osobních údajů na starosti správce.

Každé oddělení zpracovává osobní údaje na základě jiného právního titulu, za rozdílným účelem a zpracovává je rozdílně dlouhou dobu (tedy i ukládá, jelikož i samotné uložení se pokládá za zpracování).

Zpracovatelské činnosti, ve kterých **vystupuje organizace jako správce**, ukazuje **Tabulka 5**, ve které jsou uvedeny všechny následující informace. Jedná se o oddělení administrativy, účetnictví a mzdového účetnictví. Všechna tato oddělení zpracovávají osobní údaje za účelem podnikatelské činnosti, která v souvislosti s činností společnosti znamená jednání o smluvním vztahu, plnění smlouvy, ochrana práv správce, příjemce nebo jiných dotčených osob (např. vymáhání pohledávek správce), archivnictví vedené na základě zákona, výběrová řízení na volná pracovní místa, plnění zákonných povinností ze strany správce a ochrana životně důležitých zájmů subjektu údajů.

Oddělení administrativy zpracovává osobní údaje pro podnikatelské účely, tomu odpovídá také rozsah osobních údajů, které oddělení zpracovává. Osobní údaje jsou uloženy v uzamykatelných skříních a na interním serveru, kde k nim mají přístup pouze pracovníci administrativního oddělení a vedení. Osobní údaje společnost dále nepředává a archivuje je 10 let ve fyzické i elektronické podobě. Po uplynutí této doby dokumenty ve fyzické podobě skartuje a dokumenty v elektronické podobě smaže z interního serveru.

Účetní oddělení zpracovává osobní údaje pro podnikatelské účely (vedení vlastního účetnictví) v rozsahu, kterém určuje zákon o účetnictví. Dokumenty jsou uloženy v uzamykatelných kancelářích a na interním serveru firmy. Osobní údaje společnost obdobně dále nepředává a archivace probíhá dle zákonných požadavků, 10 let. Po uplynutí této lhůty společnost dokumenty skartuje a jejich elektronickou podobu smaže ze svých uložišť.

Oddělení mzdového účetnictví zpracovává osobní údaje pro podnikatelské účely (účel vypracování mzdového účetnictví vlastních zaměstnanců) v rozsahu, který určuje zákon o účetnictví. Dokumenty jsou uloženy v uzamykatelných kancelářích, na interním serveru. Archivace dokumentů je opět určena zákonnou lhůtou, tentokrát 25 let. Po uplynutí této lhůty společnost dokumenty skartuje a jejich elektronickou podobu smaže ze svých uložišť.

Na základě této fáze bylo zjištěno, že společnost v roli správce zpracovává osobní údaje v rozsahu, který potřebuje pro splnění účelu zpracování, proto není třeba mazat žádné osobní údaje.

Tabulka 5 Identifikace způsobu zpracování osobních údajů-správce

Oddělení	Osobní údaje		Právní titul	Účel zpracování	Uložení	Přístup	Příjemci osobních údajů	Doba zpracování
Administrativa (recepce)	jméno	RČ	oprávněný zájem, souhlas subjektu údajů[13]	podnikatelská činnost	administrativní oddělení – uzamykatelné skříně, server firmy	administrativa, vedení	ne	10 let
	příjmení	tel. číslo						
	č. bankovního účtu	email						
		adresa						
Účetní oddělení (ESOF)	jméno	adresa	právní základ – zákon o účetnictví	podnikatelská činnost	uzamykatelné kanceláře, server firmy	účetní, vedení	ne	10 let
	příjmení	zdravotní stav						
	č. bankovního účtu	jméno dítěte						
	RČ	příjmení dítěte						
	tel. číslo	RČ dítěte						
	email							
Mzdová účtárna (ESOF)	jméno	VS OSSZ	právní základ – zákon o účetnictví	podnikatelská činnost	uzamykatelné kanceláře, server firmy	mzdový účetní, vedení	ne	25 let
	příjmení	zdravotní stav						
	č. bankovního účtu	jméno dítěte						
	RČ	příjmení dítěte						
	tel. číslo	RČ dítěte						
	email							

Zdroj: vlastní zpracování

[13] použití osobních údajů za účelem personálních řízení

Zpracovatelské činnosti, ve kterých **vystupuje organizace jako zpracovatel**, ukazuje **Tabulka 6**, ve které jsou doplněny veškeré následující informace. Jedná se o oddělení insolvence, administrativy, účetnictví a mzdového účetnictví.

Oddělení insolvence zpracovává osobní údaje za účelem insolvenčního řízení. Osobní údaje získává z veřejného Insolvenčního rejstříku a zpracovává je v rozsahu stanoveném insolvenčním zákonem a zpracovatelskou smlouvou. K dokumentům má přístup příslušný insolvenční správce a fyzicky jsou uloženy v insolvenčním oddělení, elektronicky na cloudu. Elektronicky podepsané dokumenty insolvenční správce posílá každé 3 měsíce ve formátu PDF, pomocí datové schránky, příslušnému krajskému soudu. Dokumenty jsou archivovány v rámci zákonem určených lhůt 10 let.

Oddělení administrativy zpracovává osobní údaje za účelem daňového poradenství. Osobní údaje zpracovává v rozsahu stanoveném zákonem o účetnictví, daňovým řádem, zákonem o příslušné dani a zpracovatelskou smlouvou. Dokumenty jsou uloženy v uzamykatelných skříních a v archivu společnosti. Přístup k nim mají administrativní pracovníci a vedení. Dokumenty se archivují ze zákona 5 let.

Účetní oddělení zpracovává osobní údaje za účelem vedení účetnictví, jakožto službu objednanou zákazníkem. Osobní údaje zpracovává v rozsahu, ve kterém určuje zákon o účetnictví a ve kterém jsou mu předány příslušným správcem na základě zpracovatelské smlouvy. Dokumenty jsou uloženy v uzamykatelných kancelářích 1 rok, poté jsou předány příslušnému správci a o další archivaci se stará sám. Přístup k dokumentům má odpovídající účetní a vedení.

Oddělení mzdového účetnictví zpracovává osobní údaje za účelem vedení mzdového účetnictví, jakožto službu objednanou zákazníkem. Osobní údaje zpracovává v rozsahu, ve kterém určuje zákon o účetnictví a ve kterém jsou mu předány příslušným správcem na základě zpracovatelské smlouvy. Dokumenty jsou uloženy v uzamykatelných kancelářích a na serveru firmy. Dokumenty společnost archivuje 1 rok, poté jsou předány příslušnému správci, který se o archivaci ve lhůtě stanované zákonem stará sám. Přístup k dokumentům má příslušný mzdový účetní pracovník.

Na základě této fáze bylo zjištěno, že společnost v roli zpracovatele zpracovává osobní údaje v rozsahu, který potřebuje pro splnění účelu zpracování, proto není třeba mazat žádné osobní údaje.

Tabulka 6 Identifikace způsobu zpracování osobních údajů-zpracovatel

Oddělení	Osobní údaje		Právní titul	Účel zpracování	Uložení	Přístup	Příjemci osobních údajů	Doba zpracování
Insolvence	jméno	jméno dítěte	právní základ – insolvenční zákon, smlouva	insolvenční řízení	uzamykatelné kanceláře, cloud	insolvenční správce, vedení	ano	10 let
	příjmení	příjmení dítěte						
	č. bankovního účtu	RČ dítěte						
	RČ							
	adresa							
Administrativa (recepce)	jméno	adresa	právní základ – zákon o účetnictví, daňový řád + zákon o příslušné dani[14], smlouva	daňové poradenství – služba objednaná zákazníkem	administrativní oddělení – uzamykatelné skříně, samostatný archiv, server firmy	administrativa, vedení	ne	5 let
	příjmení	VS OSSZ						
	č. bankovního účtu	jméno dítěte						
	RČ	příjmení dítěte						
	tel. číslo	RČ dítěte						
	email							
Účetní	jméno	adresa	právní základ – zákon o účetnictví, smlouva	vedení účetnictví – služba objednaná zákazníkem	uzamykatelné kanceláře, server firmy	účetní, vedení	ne	1 rok
	příjmení	zdravotní stav						
	č. bankovního účtu	jméno dítěte						
	RČ	příjmení dítěte						
	tel. číslo	RČ dítěte						
	email							
Mzdová účtárna	jméno	VS OSSZ	právní základ – zákon o účetnictví, smlouva	vedení mzdového účetnictví – služba objednaná zákazníkem	uzamykatelné kanceláře, server firmy	mzdový účetní, vedení	ne	1 rok
	příjmení	zdravotní stav						
	č. bankovního účtu	jméno dítěte						
	RČ	příjmení dítěte						
	tel. číslo	RČ dítěte						
	email							

Zdroj: vlastní zpracování

[14] Zákon o daních z příjmu, zákon o rezervách pro zjištění základu daně z příjmu, zákon o dani z nemovitých věcí, zákonné opatření Senátu o dani z nabytí nemovitých věcí, zákon o dani silniční, zákon o DPH, zákon o spotřebních daních a energetické daně, zákon o dani z hazardních her

4.3 Identifikace a implementace postupů pro poskytování práv subjektů údajů

V rámci této fáze bylo určeno, **která práva subjektů údajů** je povinna společnost poskytovat, **jak bude tato práva poskytovat** a také **odpovědnou osobu za komunikaci** se subjekty údajů.

Správce, zprostředkovaně i zpracovatel, je povinen poskytovat práva subjektům údajů. Subjekty údajů mají tato práva:

- právo na informace, právo na přístup, právo na opravu, právo na výmaz, právo na omezení zpracování, právo na přenositelnost údajů, právo vznést námitku proti zpracování a právo nebýt předmětem automatizovaného zpracování osobních údajů, případně profilování.

Pro **provádění práva na informace** bylo vytvořeno **Prohlášení o ochraně osobních údajů** (dále jen Prohlášení), které se nachází v Příloze D. To obsahuje veškeré informace, viz. **Tabulka 1**. Tento dokument bude umístěn do složky, ve které se nacházejí veškeré firemní směrnice a zaměstnanci jsou povinni si tyto dokumenty přečíst. Dále bude předložen každému klientovi v průběhu jednání před samotným poskytnutím osobních údajů a bude také zveřejněn na webových stránkách společnosti. Ostatní práva subjektů údajů jsou založena na jejich aktivitě, tedy musejí o ně podat žádost.

Součástí práva na informace je také právo subjektů údajů požádat o veškeré osobní údaje, které o něm správce zpracovává, tedy **právo na přístup**. Tyto údaje by měly být poskytnuty v písemné formě nebo dostupnými elektronickými prostředky. Společnost pracuje se SW, které tuto skutečnost umožňují.

Jak jsem již zmínila, SW se kterými společnost pracuje jsou POHODA, PAMICA, TaxEdit a MARKTIME. Všechny tyto SW umožňují rychle reagovat na požadavky subjektů údajů. Dokáží jednoduše vyhledat, opravit, vymazat nebo vyexportovat osobní údaje o daném subjektu údajů ve strukturované, strojově čitelné formě. Společnost tak může za běžného chodu reagovat na požadavky subjektů údajů na poskytnutí osobních dat, které o daném subjektu společnost zpracovává, na žádost o poskytnutí rozsahu osobních údajů, které o daném subjektu společnost zpracovává, požadavky na opravu osobních údajů apod.

Pomocí těchto SW může společnost **provádět práva na přístup, na opravu, omezení zpracování, výmaz** nebo **přenositelnost osobních údajů**.

Co se týká vymazání osobních údajů o daném subjektu, je společnost ve většině svých zpracovatelských činností vázána archivační lhůtou danou zákonem ČR a vymazání před uplynutím této časové lhůty proto není možné.

Vznést námitku proti zpracování může subjekt údajů, pokud nemá možnost ovlivnit, že jeho osobní údaje budou zpracovány a nejedná se o plnění právní povinnosti nebo životně důležitý zájem. Může vznést přesně tři druhy námitek, a to námitku proti zpracování na základě oprávněného zájmu, námitku proti zpracování pro účely přímého marketingu a námitku proti zpracování pro účely vědeckého zájmu, historického výzkumu nebo pro statistické účely.

Automatizované zpracování ani profilování společnost neprovádí, toto právo subjektů údajů se jí proto netýká.

Pro veškeré tyto požadavky byla ve společnosti **určena zodpovědná osoba**, jejíž kontaktní údaje jsou uvedeny na Prohlášení a kterou mohou subjekty údajů kontaktovat v případě požadavků a otázek o zpracování jejich osobních údajů. Tato osoba bude vykonávat veškeré činnosti týkající se poskytování práv subjektů údajů.

4.4 Identifikace a implementace nových povinností

Prvním krokem této fáze bylo přezkoumání zpracovatelských smluv a **aktualizace stávajících zpracovatelských smluv**. Nejprve byly určeny závazky zpracovatele, které Nařízení pro zpracovatelskou smlouvu definuje a následně vyhledány nedostatky v existujících smlouvách.

Stávající smlouvy zpracovatele (ESOF), jakožto i jeho pracovníky zavazovaly ke:

- zpracování pouze pro výslovný účel,
- zpracování osobních údajů definovaným způsobem,
- zpracování osobních údajů po přesně určenou dobu,
- zajištění součinnosti (s tím souvisí i vykonávání práv subjektů údajů, jako je oprava, výmaz, přenositelnost aj.),
- mlčenlivosti.

Stávající smlouvy neobsahovaly některé prvky, které Nařízení výslovně definuje. Ve stávajících smlouvách bylo **nutné doplnit**:

- jaké osobní údaje jsou zpracovávány a kterých kategorií subjektů údajů se týkají,
- zavázání zpracovatele, že příjme veškerá technická a organizační opatření na ochranu osobních údajů,
- podmínky pro řetězení zpracovatelů (zpracovatel může předat osobní údaje dalšímu zpracovateli jen s povolením správce),
- podmínky po ukončení spolupráce (kdy na základě pokynů správce, nejen předá, ale také vymaže veškeré údaje a existující kopie),
- spolupráci při vykonávání bezpečnostních auditů, popř. inspekcí,
- zpracovatel by měl být nápomocen při ohlašování porušení zabezpečení, konzultacích s ÚOOÚ.

Dalším krokem společnosti bylo **určení, zda musí dle Nařízení jmenovat DPO**. DPO musí jmenovat úřad nebo veřejný subjekt, společnost, jejíž zpracování vyžaduje rozsáhlé pravidelné systematické monitorování subjektů údajů anebo společnost, jejíž hlavní činností je rozsáhlé zpracování citlivých údajů nebo údajů týkajících se rozsudků v trestních věcech a trestných činů. Ani jednu z těchto nutných podmínek společnost ESOF nesplňuje, tudíž se na ni tato povinnost nevztahuje. Místo DPO ale musí určit osobu, která bude zodpovědná za komunikaci se subjekty údajů a komunikaci s ÚOOÚ.

Nařízení dále požaduje dostatečná organizační a technická opatření pro ochranu osobních údajů. Pro tento účel si společnost vytvořila dokument, ve kterém jsou **zdokumentována organizační a technická opatření**.

Mezi **organizační opatření** společnosti patří interní **směrnice firmy**, které jsou uloženy na jejím serveru, jsou přístupné všem pracovníkům, pravidelně se aktualizují a pracovníci jsou povinni se jimi řídit. Dalším organizačním opatřením je **školení o GDPR** a ochraně osobních údajů, které pracovníci absolvovali. V rámci této fáze byly **sepsány odpovědnosti** jednotlivých pracovníků podle oddělení, ve kterém pracují.

V oddělení administrativy (recepce) jsou za činnosti zodpovědní odpovídající administrativní pracovníci. Ti jsou zodpovědní za získání potřebných informací (zahrnujících osobní údaje), které zpracují dle interních směrnic. Dále odpovídají za uložení do

uzamykatelných skříní v místě provozovny a na interní server. Dokumenty dále archivují do cloudového řešení MARKTIME.

V insolvenčním oddělení za svou činnost odpovídá příslušný insolvenční pracovník. Pracovník sám získá informace z veřejného Insolvenčního rejstříku a ty zpracuje dle interních směrnic. Dokumenty uloží na určené místo a do externí archivační služby MSBusiness, kterou společnost využívá a se kterou má uzavřenou zpracovatelskou smlouvu.

V účetním oddělení a oddělení mzdové účtárny za zpracování zodpovídá odpovídající účetní či mzdový účetní. Jednotliví pracovníci získávají potřebné informace, ty zpracovávají dle interních směrnic. Dokumenty potom ukládají do místa jejich určení, tedy do uzamykatelných skříní a na interní server firmy. Pracovníci mají přístup jen k informacím (osobním údajům) jejichž zpracování jim přísluší.

Mezi **technická opatření** společnosti patří **přístupová práva**, **SW**, které společnost využívá při svých činnostech, **archivační systémy**, způsob elektronického **předávání osobních údajů** a **fyzické zabezpečení** provozovny.

Každý pracovník se při příchodu na své pracoviště musí přihlásit na server společnosti pomocí přihlašovacího jména a hesla. Přihlašovací údaje jsou přiřazeny každému pracovníkovi individuálně a v tištěné formě jsou uloženy v trezoru, do kterého mají přístup pouze 2 pracovníci z vedení firmy a správce serveru.

Ve společnosti funguje minimalizace přístupových práv, tedy každý pracovník má přístup pouze k těm informacím, které potřebuje ke své práci. Nejnižší přístupová práva má pracovník mzdové účtárny a administrativy. Pracovník mzdové účtárny má přístup pouze k dokumentům klientů, kteří mu jsou přiděleni. Pracovník oddělení účetnictví může nahlížet také do dokumentů mzdové účtárny, ale pouze těch klientů, kteří mu jsou přiřazeni. Nejvyšší přístupová práva má vedení společnosti. Každé oddělení má vedoucího pracovníka, který díky této hierarchii práv může kontrolovat práci svých podřízených pracovníků a dokumenty dále využívat.

Společnost pro svou činnost využívá několik SW. Těmi jsou POHODA, PAMICA, MARKTIME a TaxEdit. SW POHODA je program určený pro zpracování účetnictví. SW PAMICA slouží pro personalistiku a zpracování mezd. SW MARKTIME slouží jako informační systém společnosti pro evidenci zakázek a jsou v něm uchovávány veškeré potřebné informace k fakturaci. Také je určen pro sdílení úkolů a podkladů řešení mezi pracovníky, úkolování a plánování. Posledním SW, který společnost využívá je TaxEdit. TaxEdit slouží pro zpracování všech druhů daňových přiznání.

Společnost ESOF má v místě provozovny vlastní archivační prostory, kam ukládá většinou zpracovávaných dokumentů. Elektronicky jsou dokumenty ukládány na interní servery. Společnost disponuje 3 interními servery, 2 hlavními a 1 záložním. Záložní server funguje jako rezervní uložiště dat, kdy je při výpadku hlavního serveru schopen během několika minut tento server zcela zastoupit. Pokud dojde k výpadku hlavního serveru a společnost bude fungovat na záložním serveru, nelze se do systému společnosti připojit přes vzdálenou plochu. Jeden ze serverů slouží, jako „domácí“ uložiště a je v síti neviditelný a nezjistitelný. Každou noc se připojí na hlavní server a vykoná rozdílovou kopii dat.

Samotná budova je zabezpečena pomocí kódu, který musejí pracovníci při příchodu zadat. Každý pracovník disponuje svými klíči od budovy. Společnost nechala vyhotovit 4 druhy klíčů, podle přístupu pracovníků do prostor budovy.

Pokud společnost předává dokumenty okresnímu soudu, předává je pomocí datové schránky a zabezpečí pomocí elektronického podpisu. Svým klientům společnost dokumenty předává šifrované ve formátu PDF a odesílá je na odpovídající e-mailovou adresu. Dokumenty ve fyzické formě si klient vyzvedává osobně v místě provozovny.

Další novou povinností je **vypracování DPIA**, tedy posouzení vlivu zpracování. Společnost nezpracovává osobní údaje pomocí nových technologií, neprovádí systematické rozsáhlé vyhodnocování, rozsáhlé zpracování citlivých údajů nebo osobních údajů tykajících se rozsudků v trestních věcech a trestných činů ani monitorování veřejně přístupných prostor, proto není třeba tento dokument vypracovávat.

Shrnutí kapitoly

Výsledkem uvedení společnosti do souladu s Nařízením je řada dokumentů.

Prvním takovým dokumentem je dokument, ve kterém jsou vyznačeny osobní údaje, které společnost zpracovává, kategorie subjektů údajů, případně příjemci osobních údajů. Takový dokument může mít podobu, viz. Tabulka 3 a Tabulka 4, ke kterému může být přiložený jiný dokument s detailnějšími informacemi např. o příjemcích osobních údajů aj.

Druhým dokumentem by měl být dokument týkající se způsobu zpracování osobních údajů, který uvádí Tabulka 5 a Tabulka 6. Ten musí obsahovat právní titul zpracování, účel zpracování, rozsah osobních údajů nutný ke splnění účelu zpracování, dobu, po kterou dochází ke zpracování a roli, kterou ve zpracování společnost zastává. V tomto dokumentu by společnost měla také definovat způsob zpracování osobních údajů.

Dalším dokumentem by mělo být Prohlášení o ochraně osobních údajů (Příloha D), ve kterém subjekty údajů společnost mimo jiné informuje i o jejich zbylých právech a o osobě, na kterou se mohou obrátit v souvislosti s otázkami ochrany osobních údajů dané společnosti.

Dalším typem dokumentů musí být aktualizované zpracovatelské smlouvy, které mají mít aspekty uvedené v Příloze B. Společnost také musí sepsat organizační a technická opatření, která přijala na ochranu osobních údajů a v případě, že zpracovatelské činnosti společnosti přinášejí vysoká rizika pro práva a svobody subjektů údajů, musí sepsat DPIA.

Na základě těchto dokumentů potom společnost může dokázat soulad s Nařízením při případně kontrole ÚOOÚ.

ZÁVĚR

Nařízení v některých částech ponechává prostor pro legislativu členských států, aby uvedly konkrétnější požadavky pro zpracování. Nový zákon o ochraně osobních údajů pravděpodobně nevyjde v platnost stejně, jako Nařízení (25.5.2018), jelikož návrh zákona byl předložen Sněmovně teprve 28.3.2018. Daná skutečnost ale příliš nevadí, jelikož Nařízení ke své vymahatelnosti nepotřebuje prováděcí zákon.

Práce je rozdělena do 4 částí. V první části práce jsem se věnovala stávající legislativě na území České republiky, tedy zákonu č. 101/2000 Sb., o ochraně osobních údajů. Vymezila jsem základní zásady ochrany osobních údajů, pravomoci ÚOOÚ, základní pojmy, práva a povinnosti při zpracování osobních údajů a předání osobních údajů do třetích zemí.

Druhá část práce byla věnována nové legislativě přijaté EU, tedy Obecnému nařízení o ochraně osobních údajů a na konci každé kapitoly jsem shrnula změny, které oproti OchOsÚ nastanou. Základním změnou oproti stávající legislativě je rozdíl v právní vymahatelností směrnice a nařízení, kdy nařízení nepotřebuje prováděcí zákon. Dalším rozdílem jsou nové zásady zpracování rozšířené o transparentnost a odpovědnost za zpracování. Dále posílení práv subjektů údajů, zejména nové právo na přenositelnost a právo na výmaz, záměrná a standardní ochrana osobních údajů, prokázání souladu zpracování s Nařízením, hlášení porušení ochrany osobních údajů, posouzení vlivu zpracování, jmenování DPO a předání osobních údajů do třetích zemí. Nařízení dále vymezuje a rozšiřuje pravomoci ÚOOÚ a nově zřizuje Evropský sbor pro ochranu osobních údajů, jakožto centrální dozorový orgán, který vznikne z poradní skupiny WP29.

V třetí části jsem definovala dopady a nutná opatření pro splnění Obecného nařízení. Nebrala jsem v úvahu variantu, že organizace předává osobní údaje do třetích zemí, pouze na území našeho státu. Definovala jsem postup organizace, kterým by se mohla řídit, aby dospěla k souladu s Nařízením.

Prvním krokem organizace je identifikace osobních údajů, které zpracovává, určení kategorií osobních údajů a v případě citlivých údajů nebo údajů dětí získání souhlasu s jejich zpracováním, pokud Nařízení neurčí jinak. Dále identifikace kategorií subjektů údajů a příjemců osobních údajů. Druhým krokem je identifikace a přiřazení právních titulů, účelů zpracování, rozsahu osobních údajů, doby zpracování a odpovědnosti k zpracovávaným osobním údajům. Třetím krokem je identifikace a implementace práv subjektů údajů a posledním, čtvrtým krokem, potom

identifikace a implementace nových povinností. Těmito povinnostmi jsou aktualizace zpracovatelských smluv, standardní a záměrná ochrana, jmenování DPO a vypracování DPIA.

V poslední, páté části práce, jsem se věnovala aplikaci Obecného nařízení ve vybrané společnosti, kdy jsem na základě výše definovaných kroků postupovala s pomocí vedení a definovala situaci ve společnosti ESOF.

Cílem práce byl rozbor Obecného nařízení o ochraně osobních údajů a definice dopadů a nutných opatření na vybranou firmu. Po popsání Obecného nařízení a definici změn, které oproti dosavadní legislativě přinese byly sestaveny dopady Obecného nařízení pro podnikovou praxi, jakožto posloupnost čtyř základních kroků. Na základě těchto kroků byly určeny dopady a opatření pro dosažení souladu společnosti ESOF s Obecným nařízením.

POUŽITÁ LITERATURA

[1] Accountability and governance. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

[2] BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v aplikační praxi: vybrané otázky. 3. vyd. Praha: Linde Praha, 2013, 311 s. Praktická právnická příručka. ISBN 978-80-86131-96-2.

[3] Co je to GDPR a jak bude aplikováno v Česku: Nařízení o ochraně osobních údajů prakticky. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2017-10-28]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

[4] Contracts. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

[5] Česko. Usnesení předsednictva České národní rady č.2/1993 Sb., o vyhlášení Listiny základních práv a svobod. In: *Sbírka zákonů České republiky*. 1993, ročník 1993, částka 1, s. 15-22. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5989

[6] Česko. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In *Sbírka zákonů České republiky*. 2000, Ročník 2000, Částka 32, s. 17-28. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3420

[7] Česko. Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů České republiky*. 2012, ročník 2012, částka 586, s. 1-344. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6144

[8] Česko. Zákon č.563/1991 Sb., o účetnictví. In: *Sbírka zákonů České republiky*. 1991, ročník 1991, částka 107, s. 2-9. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=2519

[9] ČSN ISO/IEC 27018 (369709). Normy.biz [online]. 2017 [cit. 2018-02-19]. Dostupné z: https://shop.normy.biz/detail/501548

[10] Data protection impact assessments. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-

the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[11] Documentation. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

[12] DPO ochrání firmu a její klienty. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-19]. Dostupné z: https://www.gdpr.cz/blog/dpo-ochrani-firmu/

[13] ESOF. Hradec Králové, Čechova 1100. Směrnice o organizačním řádu. 2017 [cit. 2018-03-12]

[14] Evropská unie. Nařízení Evropského parlamentu a Rady: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník Evropské unie*. Brusel, 2016, Ročník 2016, číslo 679. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679

[15] Evropská unie. Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *Úřední věstník Evropské unie*. Brusel, 1995, Ročník 1995, číslo 46. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:31995L0046

[16] Evropský sbor pro ochranu osobních údajů. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-01-29]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/evropsky-sbor-pro-ochranu-osobnich-udaju/

[17] GDPR v otázkách a odpovědích. *Bulletin-advokacie.cz* [online]. 2017 [cit. 2017-11-15]. Dostupné z: http://www.bulletin-advokacie.cz/gdpr-v-otazkach-a-odpovedich

[18] ISMS: normy ISO 27001 a ISO 27002. Risk Analysis Consultants [online]. 2013 [cit. 2018-02-19]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/BS7799

[19] Jak se připravit na GDPR? *Portál.POHODA.cz* [online]. 2018 [cit. 2018-02-24]. Dostupné z: https://portal.pohoda.cz/zakon-a-pravo/gdpr/jak-se-pripravit-na-gdpr/

[20] Jak získat výslovný souhlas se zpracováním osobních údajů v rámci přímého marketingu? *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit.

2017-11-15]. Dostupné z: https://www.gdpr.cz/blog/jak-ziskat-vyslovny-souhlas-se-zpracovanim-osobnich-udaju-v-ramci-primeho-marketingu/

[21] Jaké povinnosti ukládá GDPR institucím a firmám. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-19]. Dostupné z: https://www.gdpr.cz/gdpr/povinnosti/

[22] Key definitions. *ICO: Information Commisioner´s Office* [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

[23] KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v otázkách a odpovědích. 1. vyd. Praha: BOVA POLYGON, 2010, 150 s. ISBN 978-80-7273-163-3.

[24] Lawful basis for processing. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[25] MAŠTALKA, J. Osobní údaje, právo a my. 1. vyd. Praha: C. H. Beck, 2008. ISBN 987-80-7400-033-1.

[26] MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012, 206 s. Praktik (Leges). ISBN 978-80-87576-12-0.

[27] MORÁVEK, J. Ochrana osobních údajů v pracovněprávních vztazích. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2013. 435 s. ISBN 978-80-7478-139-1.

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

[29] Osobní údaje. *Europa.eu* [online]. 2017 [cit. 2017-11-15]. Dostupné z: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_cs.htm

[30] Pokyny týkající se pověřenců pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů.* [online]. 2017 [cit. 2018-02-19] Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29166

[31] Pracovní skupina 29. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-01-29]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pracovni-skupina-29/

[32] Právní důvody zpracování. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravni-duvody-zpracovani-ou/

[33] Právo na omezení zpracování. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravo-na-omezeni-zpracovani/

[34] Právo na opravu. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravo-na-opravu/

[35] Právo na přenositelnost. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravo-na-prenositelnost/

[36] Právo na přístup. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-16]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravo-na-pristup/

[37] Právo na výmaz. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravo-na-vymaz/

[38] Právo vznést námitku proti zpracování. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravo-vznest-namitku-proti-zpracovani/

[39] Right of access. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

[40] Right to be informed. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

[41] Right to data portability. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

[42] Right to erasure. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

[43] Right to object. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

[44] Right to rectification. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

[45] Right to restrict processing. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

[46] Rights related to automated decision making including profiling. ICO: Information Commisioner´s Office [online]. UK, 2017 [cit. 2018-03-06]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

[47] Souhlas se zpracováním osobních údajů. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/souhlas-se-zpracovanim-osobnich-udaju/

[48] Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti. *Úřad pro ochranu osobních údajů.* [online]. 2017 [cit. 2018-02-14] Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28920

[49] Vodítka k souhlasu podle Nařízení 2016/679. *Úřad pro ochranu osobních údajů.* [online]. 2017 [cit. 2018-02-14] Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29162

[50] Zásady Obecného nařízení. *GDPR: Nařízení o ochraně osobních údajů prakticky* [online]. 2017 [cit. 2018-02-12]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/zasady-obecneho-narizeni/

SEZNAM PŘÍLOH

Příloha A	Zpracování DPIA
Příloha B	Zpracovatelská smlouva
Příloha C	Rozhodnutí EK o úrovni ochrany osobních údajů
Příloha D	Prohlášení o ochraně osobních údajů

Příloha A

Posouzení rizik je vhodné provádět zejména při[28]:

a) zavádění opatření pro schopnost doložit soulad s Nařízením,

b) zpracování na základě oprávněného zájmu,

c) posouzení slučitelnosti údajů,

d) zavádění ochranných opatření v souvislosti s automatizovaných zpracování osobních údajů,

e) provádění záměrné ochrany osobních údajů,

f) posuzování výjimky ze zpracování,

g) přijímání technických a organizačních opatření k zajištění ochrany osobních údajů,

h) posuzování nutnosti ohlásit porušení zabezpečení osobních údajů,

i) posuzování vlivu na ochranu osobních údajů,

j) posuzování nutnosti předchozí konzultace,

k) posuzování nutné kvalifikace pověřence na ochranu osobních údajů,

l) určování priorit práce pověřence.

Postup, resp. obsah posouzení vlivu zpracování osobních údajů vymezuje čl. 35 v odst. 7 a obsahuje minimálně[28][14]:

1) popis operací zpracování, účel zpracování, včetně oprávněných zájmů správce,

2) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,

3) posouzení rizik pro práva a svobody subjektů údajů,

4) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Příloha B

Zpracovatelská smlouva by měla mít následující náležitosti[28][14]:

- předmět a dobu trvání zpracování,
- povahu a účel zpracování,
- typ osobních údajů a kategorie subjektů údajů,
- doložené pokyny správce.

Zpracovatelská smlouva nebo jiný právní akt zavazují zpracovatele k[28]:

1) mlčenlivosti
    - zpracovatel má povinnosti zajistit, aby byl okruh osob, které zpracovávají osobní údaje, vázán mlčenlivostí,
2) zabezpečení
    - zajištění technických a organizačních opatření,
3) řetězení zpracovatelů
    - zapojovat další zpracovatele pouze na základě povolení správce,
4) součinnosti
    - zpracovatel musí v nejvyšší možné míře pomocí vhodných technických a organizačních opatření poskytnout součinnost správci (zejména při žádosti o výkon práv subjektu údajů),
5) být nápomocen
    - při zavádění opatření na ochranu osobních údajů,
    - ohlašování porušení zabezpečení,
    - posuzování vlivu zpracování na ochranu osobních údajů,
    - konzultacích s dozorových úřadem,
6) poskytovat informace
    - k doložení toho, že zpracovatelem prováděné zpracování je v souladu se zpracovatelskou smlouvou,

7) provádět inspekce a audity

   - umožnění provádění auditů a inspekcí ze strany správce,

8) ukončit zpracování

   - pokud dojde k ukončení poskytování služeb zpracování, je zpracovatel povinen všechny osobní údaje vymazat nebo předat správci a vymazat existující kopie.

Příloha C

Pokud EK rozhoduje o odpovídající úrovni ochrany, posuzuje podle čl. 45 odst. 2[28][14]:

a) zda je třetí země právním státem, který chrání lidská práva a základní svobody a dodržuje právní předpisy, včetně pravidel pro další předání osobních údajů mezinárodním organizacím nebo jiným zemím a pravidel pro přístup orgánů veřejné moci k osobním údajům,

b) jestli tato země zajišťuje existenci účinných a vymahatelných práv subjektu údajů a prostředků účinné soudní a správní ochrany subjektu údajů, jehož práva jsou předávána,

c) jestli v této zemi existuje dozorový úřad nebo jeho působnosti podléhá daná mezinárodní organizace, zda je nezávislý a funguje účinně, zajišťuje a vymáhá soulad s pravidly pro ochranu osobních údajů a za tímto účelem má dané pravomoci, poskytuje poradenství subjektům údajů při výkonu jejich práv a základních svobod a spolupracuje s dozorovými úřady členských států,

d) jaké mezinárodní závazky, závazné úmluvy a nástroje třetí země, resp. mezinárodní organizace přijala.

EK ve svém rozhodnutí také určí mechanismus pro pravidelný přezkum odpovídající úrovně ochrany, který provede minimálně každé 4 roky, kvůli zohlednění vývoje třetí země nebo mezinárodní organizace. EK bude tento vývoj neustále sledovat. Pokud třetí země, resp. mezinárodní organizace dále odpovídající úroveň ochrany nebude zajišťovat, zruší nebo změní EK rozhodnutí o odpovídající úrovni. Rozhodnutí o změně EK přijímá přezkumným postupem podle pravidel Nařízení definovaných v čl. 93 odst.2.[28][14]

Příloha D

Prohlášení o zpracování osobních údajů dle nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a poučení subjektů údajů (dále jen „GDPR“)[19]

1. Správce osobních údajů

Společnost ESOF s.r.o. se sídlem Čechova 1100/20, 500 02 Hradec Králové, zapsaná v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, spisová značka C 3608, (dále jen „správce“) Vás tímto v souladu s čl. 12 GDPR informuje o zpracování Vašich osobních údajů a o Vašich právech.[19]

2. Rozsah zpracování osobních údajů

Společnost zpracovává osobní údaje v rozsahu, v jakém je správci poskytl daný subjekt údajů v souvislosti s uzavřením smluvního vztahu, právního vztahu nebo které správce shromáždil jinak a zpracovává je v souladu s platnými právními předpisy.[19]

3. Zdroje osobních údajů

- přímo od subjektů údajů,
- veřejně přístupné rejstříky, seznamy a evidence (např. obchodní rejstřík, živnostenský rejstřík, katastr nemovitostí, veřejný telefonní seznam apod.).

4. Kategorie osobních údajů, které jsou předmětem zpracování

- identifikační údaje (např. jméno, příjmení, titul, RČ, datum narození, adresa, DIČ) a údaje umožňující kontakt se subjektem údajů (kontaktní údaje – např. kontaktní adresa, tel. číslo, e-mailová adresa),
- popisné údaje (např. č. bankovního účtu),
- údaje nezbytné pro plnění smlouvy (např. jméno, příjmení, RČ manžela/manželky subjektu a dětí subjektu),
- údaje zpracovávané v rámci uděleného souhlasu subjektu údajů (použití osobních údajů za účelem personálních řízení aj.)

5. Kategorie subjektů údajů

- zákazník správce,
- zaměstnanec správce,

- dodavatel služby,
- jiná osoba, která je ve smluvním vztahu ke správci,
- uchazeč o zaměstnání.

6. Kategorie příjemců osobních údajů

- veřejné úřady,
- zpracovatel,
- státní orgány v rámci plnění zákonných povinností určených právními předpisy.

7. Účel zpracování osobních údajů

- jednání o smluvním vztahu,
- plnění smlouvy,
- ochrana práv správce, příjemce nebo jiných dotčených osob (např. vymáhání pohledávek správce),
- archivnictví vedení na základě zákona,
- výběrová řízení na volná pracovní místa,
- plnění zákonných povinností ze strany správce,
- ochrana životně důležitých zájmů subjektu údajů.

8. Způsob zpracování a ochrany osobních údajů

Zpracování je prováděno v provozovně a sídle správce pověřenými zaměstnanci správce, příp. zpracovatelem. Ke zpracování dochází prostřednictvím výpočetní techniky nebo manuálním způsobem u osobních údajů v listinné. Za účelem dodržení bezpečnostních zásad zpracování osobních údajů přijal správce technicko–organizační opatření k zajištění ochrany osobních údajů. Zejména opatření, proti neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení, ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování nebo k jinému zneužití osobních údajů. Veškeré subjekty, kterým mohou být osobní údaje zpřístupněny, respektují právo subjektů údajů na ochranu soukromí a jsou povinny postupovat dle platných právních předpisů týkajících se ochrany osobních údajů.[19]

9. Doba zpracování osobních údajů

Zpracování probíhá po dobu nezbytně nutnou k zajištění práv a povinností plynoucích jak ze smluvního vztahu a z příslušných právních předpisů. Veškeré lhůty jsou v souladu s příslušnými smlouvami, spisovým a skartačním řádem správce a v příslušnými právními předpisy.[19]

10. Poučení

Správce zpracovává údaje se souhlasem subjektu údajů s výjimkou zákonem stanovených případů, kdy zpracování osobních údajů nevyžaduje souhlas subjektu údajů.[19]

V souladu se čl. 6 odst. 1 GDPR může správce bez souhlasu subjektu údajů zpracovávat tyto údaje[14]:

- subjekt údajů udělil souhlas,
- zpracování je nezbytné pro splnění smlouvy,
- zpracování je nezbytné pro splnění právní povinnosti,
- zpracování je nezbytné pro ochranu životné důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci,
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany.

11. Práva subjektů údajů

1) v souladu se čl. 12 GDPR informuje správce na žádost subjektu údajů subjekt údajů o právu na přístup k osobním údajům a k následujícím informacím[14]:

- účelu zpracování,
- kategorii dotčených osobních údajů,
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- plánované době, po kterou budou osobní údaje uloženy,
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,

- skutečnosti, zda dochází k automatizovanému rozhodování, včetně profilování.

2) Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může[14]:

- požádat správce o vysvětlení,
- požadovat, aby správce odstranil takto vzniklý stav,
- je-li žádost subjektu údajů podle odst. 1 shledána oprávněnou, správce odstraní neprodleně závadný stav,
- nevyhoví-li správce žádosti subjektu údajů podle odst. 1, má subjekt údajů právo obrátit se přímo na dozorový úřad, tedy ÚOOÚ,
- postup podle odst. 1 nevylučuje, aby se subjekt údajů obrátil se svým podnětem na dozorový úřad přímo,
- správce má právo za poskytnutí informace požadovat přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace,

Toto prohlášení je veřejně přístupné na internetových stránkách správce.