Ochrana osobních údajů v oblasti ochrany obyvatelstva

Tomáš Daníček

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Daníček**
Osobní číslo:	**L21567**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Ochrana osobních údajů v oblasti ochrany obyvatelstva**

Zásady pro vypracování

1. Popište základní problematiku ochrany osobních údajů.
2. Proveďte komplexní analýzu vybrané složky integrovaného záchranného systému s důrazem na ochranu osobních údajů.
3. Vyhodnoťte dosažené výsledky a zpracujte návrh na zlepšení.

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

Seznam doporučené literatury:

1. NAVRÁTIL, Jiří. *GDPR pro praxi. Pro praxi.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380--689-7.
2. VOIGT, Paul a Axel von dem BUSSCHE. T*he EU General Data Protection Regulation (GDPR)*: A *Practical Guide*. Cham: Springer, 2017. ISBN 978-3-319-57958-0.
3. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN 978-807-5541-529.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Lukáš Pavlík, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti, dne: 3. 5. 2024

Jméno a příjmení studenta: Tomáš Daníček

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se zaměřuje na problematiku ochrany osobních údajů v oblasti ochrany obyvatelstva. V teoretické části se práce věnuje historickému vývoji ochrany osobních údajů, odborné terminologii, Obecnému nařízení o ochraně osobních údajů a bezpečnosti osobních údajů. V praktické části je popsána a analyzována Zdravotnická záchranná služba Zlínského kraje s důrazem na ochranu osobních údajů. Jsou zde použity metody a analýzy, mezi něž patří expertní rozhovor a analýza SWOT a What-If. V poslední kapitole praktické části jsou uvedeny návrhy opatření ke zlepšení ochrany osobních údajů u Zdravotnické záchranné služby Zlínského kraje.

Klíčová slova: GDPR, ochrana, osobní údaje, SWOT, What-If

ABSTRACT

This bachelor thesis focuses on the issue of personal data protection in the field of population protection. The theoretical part of the thesis deals with the historical development of data protection, technical terminology, the General Data Protection Regulation and data security. The practical part describes and analyses the Medical Rescue Service of the Zlín Region with an emphasis on the protection of personal data. Methods and analyses are used, including expert interview and SWOT and What-If analysis. In the last chapter of the practical part, proposals for measures to improve the protection of personal data at the Medical Rescue Service of the Zlín Region are presented.

Keywords: GDPR, protection, personal data, SWOT, What-If

Tímto bych chtěl rád poděkovat panu Ing. Lukáši Pavlíkovi, Ph.D., za jeho ochotu, vstřícnost, cenné rady a odborné vedení mé bakalářské práce. Dále bych chtěl poděkovat mé rodině za podporu a trpělivost během celého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Ochrana osobních údajů již dnes bezpochyby patří mezi důležitá práva života každého člověka. Osobní údaje jsou nedílným prvkem identity nás všech, kteří se jakýmkoliv způsobem pohybují ve společnosti. Je proto žádoucí, aby každý člověk přistupoval ke svým osobním údajům zodpovědně, svědomitě a dbal na jejich ochranu. Historie totiž ukázala, že zneužití osobních údajů má i velmi smutné a tragické následky, ze kterých by se lidstvo mělo poučit. Vývoj ochrany osobních údajů je dynamický, mnohdy velice překotný vliv moderních prvků vstupuje do problematiky osobních údajů a přispívá k tomu, že se osobní údaje stávají čím dál víc cennou věcí, kterou je potřeba náležitě střežit.

V současné době plné moderních digitálních technologií, je důraz na ochranu soukromí jednotlivců kladen stále výše. Digitalizace napříč všemi obory přispívá k masivnímu získávání osobních údajů od všech obyvatel, kteří často, zcela dobrovolně, předávají své osobní údaje bez toho, aniž by věděli, komu je předávají nebo za jakých účelem. Z osobních údajů se tak stává nástroj pro možné zneužívání nebo vydírání. Pro tyto hrozby se ochrana osobních údajů začala řešit na úrovni Evropské unie, která v roce 2016 schválila Obecné nařízení o ochraně osobních údajů známější pod zkratkou GDPR. Toto nařízení stanovilo pravidla pro zacházení s osobnímu údaji při jejich zpracování a pro pohyb osobních údajů.

Ochrana osobních údajů také prostupuje do oblasti ochrany obyvatelstva. Konkrétně ve zdravotnictví, kde nabývá ochrana údajů velký význam, neboť zdravotní údaje pacientů patří mezi nejcitlivější osobní údaje vůbec. Není tak pochyb, že právě ochrana osobních údajů ve zdravotnictví by měla být priorita všech subjektů, které do zpracování osobních údajů vstupují, pracují s nimi nebo je odstraňují.

Hlavním cílem práce je na základě provedené analýzy vybrané složky integrovaného záchranného systému, a to Zdravotnické záchranné služby Zlínského kraje, s důrazem na ochranu osobních údajů vyhodnotit dosažené výsledky a zpracovat návrhy na zlepšení. Ke splnění hlavního cíle práce byly stanoveny následující dílčí cíle práce, a to popsat základní problematiku ochrany osobních údajů a provést komplexní analýzu ochrany osobních údajů u vybrané složky integrovaného záchranného systému.

I. TEORETICKÁ ČÁST

1 HISTORICKÝ VÝVOJ OCHRANY OSOBNÍCH ÚDAJŮ

V současném světě může ochrana osobních údajů připadat téměř všem občanům jako samozřejmost, jistota a součást jejich základních práv a svobod, ovšem historický vývoj v této oblasti naznačuje, že důraz na ochranu údajů sice lidstvo provází již od nepaměti, ale formální řešení této problematiky se začalo prosazovat relativně v nedávné minulosti. Níže je popsán vývoj v oblasti ochrany osobních údajů jak na světové a evropské úrovni, tak na území České republiky (dále jen „ČR“).

1.1 Vývoj v Evropě a ve světě

Historie ochrany soukromí spadá do období náboženských válek, kdy byly pronásledovány osoby s jiným náboženským přesvědčením. S tímto přicházel také strach o vlastní život a zdraví, proto se stalo soukromí velmi důležitým aspektem života lidí. Dalším významným okamžikem v problematice soukromí se stalo období Velké francouzské revoluce, ve kterém docházelo k vraždění a stíhání obyvatelstva kvůli rozlišným názorům. Doba nacismu naplno ukázala světu potřebu ochrany nejen soukromí, ale i osobních údajů. Masivní zneužití osobních údajů z pohledu státní moci vážně zasáhlo životy nespočet jedinců a jejich rodin. S rozvojem elektronické komunikace, sociálních sítí a digitalizací všech možných informací se začíná shromažďovat a sbírat obrovské množství osobních údajů. Z tohoto jevu také vzniká prostředí pro možné zneužívání a obchodování s osobními údaji (Navrátil, 2018).

Především po skončení druhé světové války vzešla nutnost začlenit ochranu údajů do ústavní ochrany. Rozšiřování výpočetní techniky v 50. letech 20. století kladlo stále větší význam na ukotvení pravidel pro zacházení s osobními údaji. Nové technologie také zvyšovaly význam při zpracování osobních údajů ve veřejné, ale i soukromé sféře (Melotíková, 2020).

Všeobecná deklarace lidských práv, přijatá Valným shromážděním Organizace spojených národů v roce 1948, byla prvním důležitým nadnárodním dokumentem, který se zabýval otázkou ochrany soukromí. Čl. 12 této deklarace zakazoval jakýkoliv zásah do osobního života jednotlivců. Podobně i Evropská úmluva o ochraně lidských práv a základních svobod, uzavřená v roce 1950, v čl. 8 zaručovala ochranu soukromí a rodinného života. Oba tyto dokumenty byly významnými kroky k ochraně soukromí, avšak neposkytovali podrobné směrnice pro zpracování osobních údajů, které tvořilo podstatnou část práva na soukromí. (Žůrek, 2018).

V dalším období, kdy se společnost komplexně rozvíjela a tento vývoj doprovázel nástup nových systémů a technologií, které vstupovaly do problematiky ochrany osobních údajů stále výrazněji, povstala touha, která by přišla s výraznějším řešením ochrany osobních údajů při jejich zpracovávání. V důsledku toho byly v 70. a 80. letech 20. století přijaty v západních zemích jako Rakousko, Dánsko, Francie nebo Norsko první normy upravující otázku ochrany osobních údajů fyzických osob a náležitostí při jejich zpracovávání (Žůrek, 2018).

Především se jedná o Úmluvu o ochraně osob se zřetelem na automatizované zpracování údajů, známější pod označením Úmluva č. 8 z roku 1981 a její dodatkový protokol z roku 2001. Na rozdíl od Evropské úmluvy o ochraně lidských práv a základních svobod z roku 1950 obsahuje definice týkající se zásad ochrany osobních údajů, které byly doposud jen tolerovány z nepsaných zvyklostí (Navrátil, 2018).

Žůrek považuje 28. leden 1981, tedy den přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování údajů jako okamžik, kdy se právo na ochranu osobních údajů při jejich zpracování, stalo samostatným aspektem ochrany soukromí. Samotné přijetí Úmluvy č. 8 se tedy stává historickým okamžikem ve vývoji ochrany osobních údajů a 28. leden se proto stal mezinárodním dnem ochrany osobních údajů (Žůrek, 2018).

Evropská unie (dále jen „EU“) přijala v roce 1995 směrnici Evropského parlamentu a Rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Cílem této směrnice bylo na území EU implementovat jednotnou právní úpravu ochrany osobních údajů, což mělo také souvislost s volným pohybem osob v Schengenském prostoru (Navrátil, 2018).

Směrnice č. 95/46/ES také výrazně přispěla k sounáležitosti jednotlivých právních předpisů členských státu EU, protože se jevila jako dostatečně kvalitní základ pro ochranu osobních údajů (Melotíková, 2020).

Podle Žůrka je nezpochybnitelné, že směrnice č. 95/46/ES úspěšně sjednotila základní rámec ochrany osobních údajů v Evropě. Nicméně jednotlivé členské státy EU velice často interpretovaly provedení této směrnice individuálně, což způsobilo rozdílný přístup interpretace v některých důležitých aspektech této směrnice, a to mělo za následek, že se samotné provedení v jednotlivých státech od sebe nemálo odlišovalo. (Žůrek, 2018).

V následujícím období, za přijetí dalších novelizací zákonů, se stav právních norem přijatých v jednotlivých zemích EU stále drastičtěji odlišoval od původní Směrnice 95/46/ES. K tomuto odlišování výrazně přispěl i obrovský rozmach výpočetních technologií a rozvoj internetu. Postupem času se i samotná Směrnice 95/46/ES stala čím dál zastaralejší a neaktuální. V důsledku zkušeností a neakceptovatelné Směrnice 95/46/ES a rozmachu technologií přistoupila EU k vytvoření nařízení, které by již upravovalo povinnosti a práva přímo jeho adresátům. Toto nařízení nese název Nařízení Evropského parlamentu a Rady č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů (dále jen „GDPR“) (Žůrek, 2018).

GDPR vstoupilo v účinnost 24. května 2018 a zrušilo platnost již nedostačující Směrnice 96/46/ES. GDPR bylo přijato za primárním účelem dosažení jednoty v oblasti ochrany osobních údajů a jejího vymáhání ve všech členských státech EU (Melotíková, 2020).

1.2 Vývoj na území České republiky

Na území ČR byla problematika ochrany osobních údajů řešena ústavním zákonem č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního, který patřil mezi první normu, přijatou na našem území od vzniku Československa (Navrátil, 2018).

Jistou zmínku o ochraně osobních údajů lze najít v tehdejší československé ústavě, zákona č. 121/1920 Sb., který v §112 upravoval domovní svobodu a v §116 tajemství listovní. Tento zákon ale v podrobnostech odkazoval na již zmíněný ústavní zákon č. 293/1920 Sb., o ochraně svobody, domovní a tajemství listovního (Melotíková, 2020).

V následujících letech se žádné další normy týkající se osobních údajů v našem právní řádu neobjevují. Výjimky tvoří prakticky jen úprava pravidel pro vydávání dokladů z důvodu cestování nebo vydávání dokladů, ve kterých se osobní údaje vyskytují. Přelomem se staly 90. léta 20. století, kdy dochází k postupnému přijetí právních norem, které se ochranou osobních údajů zabývají. Zpočátku to byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech (Navrátil, 2018).

Nedostatkem tohoto zákona bylo, jak již z názvu patrné, že upravoval zpracování osobních údajů v informačních systémech, ovšem drtivá většina osobních údajů byla v té době zpracována v tištěných evidencích (Žůrek,2018).

Následovalo přijetí Listiny základních práv a svobod (dále jen „LZPS“) Usnesením předsednictva České národní rady č. 2/1993. Sb., která byla vyhlášena až několik měsíců po vydání již zmíněného zákona 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Klíčovými články LZPS pro problematiku ochrany osobních údajů se staly čl. 7 odst.1, který deklaruje nedotknutelnost soukromí osoby a čl. 10 odst. 3, který každému deklaruje právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o jeho osobě (Žůrek, 2018).

Až do roku 2000 neexistoval na území ČR celkově kompletní právní předpis, který by prováděl na zákonné úrovni čl. 10 odst. 3 LZPS. O komplexním zákonu o ochraně osobních údajů při jejich zpracování lze pojednávat až od 1. června 2000. V tento den nabyl právní účinnost zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Tento zákon dal také za vznik Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“), který podrobněji popisuje třetí kapitola této práce. V návaznosti vstupu ČR do EU, byl zákon č. 101/2000 Sb., o ochraně osobních údajů v roce 2004 podstatně novelizován v souvislosti aplikace Směrnice 95/46/ES (Žůrek, 2018).

Navíc vstup platnosti Lisabonské smlouvy v roce 2009, která novelizovala Smlouvu o Evropské unii začala jednoznačně upravovat v čl. 8 v Listině základních práv a svobod Evropské unie právo na ochranu osobních údajů (Navrátil, 2018).

Ke dni nabytí právní účinnosti GDPR na území ČR měl být zákon o ochraně osobních údajů zrušen a nahrazen, pro veřejnost známějším adaptačním zákonem, jehož úkolem bylo připravit ČR na celkové nasazení GDPR do českého právního řádu. Dne 24. dubna 2019 nabyl právní účinnost zákon č. 110/ 2019 Sb., o zpracování osobních údajů a tímto krokem byl definitivně zrušen zákon č. 101/ 2000 Sb., o ochraně osobních údajů (Žůrek, 2018).

Podle Melotíkové: „*můžeme tedy z širšího pohledu shrnout, že právní úprava na poli ochrany osobních údajů prochází postupným nikoli překotným vývojem“*. Je zapotřebí také pochválit samotnou EU, především vliv Rady Evropy, jejíž vliv se výrazně podepsal v zachycení trendů v této oblasti ale i v komplexním přístupu k ochraně osobních údajů v působnosti práva a soukromí, kdy se do GDPR promítly aktuální potřeby v problematice ochrany osobních údajů. EU lze ocenit za přístup GDPR ke státům, kde nebyla zajištěna stejná ochran práv, včetně stanovení působnosti pověřence pro ochranu osobních údajů, který se jeví jako klíčový pro vysokou míru ochrany práv subjektů údajů (Melotíková, 2020).

2 CHARAKTERISTIKA ODBORNÉ TERMINOLOGIE V OBLASTI OCHRANY OSOBNÍCH ÚDAJŮ

Pro pochopení problematiky ochrany osobních údajů je nutné znát klíčové pojmy a definice, které jsou uvedeny v Obecném nařízení o ochraně osobních údajů neboli GDPR, plným názvem nařízení Evropského parlamentu a Rady EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

2.1 Odborná terminologie

Pro účely nařízení GDPR se tedy v čl. 4 rozumí následující pojmy, ze kterých vychází veškerá práva a povinnosti, která z GDPR plynou:

Biometrické údaje - *„biometrickými údaji jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Genetické údaje - „*genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

- **Osobní údaj** – osobní údaj se tedy může charakterizovat jako jakýkoliv údaj, který se vztahuje k fyzické osobě, ovšem pod podmínkou, že osoba bude pod těmito údaji identifikovatelná. Osobní údaj patří mezi základní a nejdůležitější pojmy celé problematiky ochrany osobních údajů (Janečková, 2020).

V čl.4 GDPR je uvedeno*: „**osobními údaji** jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě neboli subjektu údajů; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Porušení zabezpečení osobních údajů - *„porušením zabezpečení osobních údajů je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Profilování - „*profilováním je jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Příjemce - *„příjemcem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

- **Pseudonymizace** – pseudonymizace znamená možnost nepracovat s klasickými identifikátory, ale volbu správce zvolit jiné identifikátory. Za běžný příklad využití pseudonymizace údajů je možné považovat přiřazení identifikačního čísla zaměstnancům místo jejich jména a příjmení (Žůrek, 2022).

Čl. 4 upravuje: *„**pseudonymizaci** jako zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

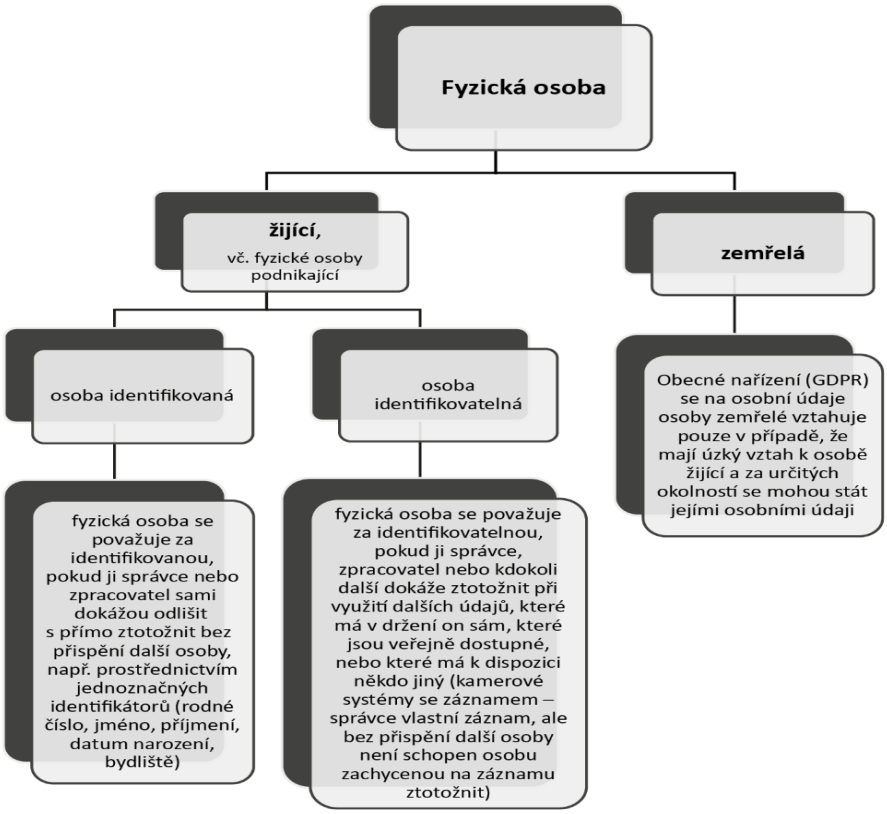
- **Souhlas** – souhlas znamená v kontextu GDPR projev vůle. Tímto krokem předá subjekt své svolení ke zpracování osobních údajů. Souhlas nemusí mít formu písemnosti, musí být ale především zcela bez pochybností jasně zřetelné, že se jedná o svobodný, jednoznačný a konkrétní projev vůle (Janečková, 2020).

Čl. 4 GDPR uvádí: *„souhlasem subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

- **Správce** – tento termín sděluje, že správcem se stává kdokoliv, kdo zpracovává osobní údaje nebo ten, kdo k tomu má ze zákona povinnost a zároveň rozhoduje o účelu a metodách zpracování osobních údajů (Janečková, 2020).

Dle čl. 4 GDPR: „*správcem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

- **Subjekt údajů** – samotné GDPR neobsahuje tuto definice, je proto součástí pojmu osobního údaje. Je důležité poznamenat, že subjektem údajů je pouze žijící osoba, protože se samotné GDPR nevztahuje na již zemřelé osoby (Úvod do problematiky GDPR, GDPR pro e-shopy, 2018).



Obrázek 1 – Grafické znázornění subjektu údajů (Janečková, 2020).

Třetí strana *„třetí stranou je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jenž je oprávněna ke zpracování osobních údajů“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

- **Zpracovatel** – pod pojem zpracovatele spadá jakýkoliv subjekt, který byl najat správcem, aby pro něj uskutečňoval zpracovatelské operace s osobními údaji. Primární rozdíl mezi správcem a zpracovatelem je ten, že zpracovatel provádí výhradně jenom takové operace, ke kterým byl správcem určen (Janečková, 2020).

Čl. 4 GDPR: *„zpracovatelem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

- **Zpracování –** pod pojem zpracování spadá jakékoliv nakládání nebo operace s osobními údaji. Důležité je poznamenat, že pojem zpracování neznamená ucelený soubor procesů, ale může se jednat pouze o použití jedné činnosti. Cílem zpracování je proces, při kterém je využito osobních údajů k dosažení záměrů jejich správcem (Janečková, 2020).

Čl. 4 GDPR uvádí: *„zpracováním je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Další odborná terminologie, ačkoliv není uvedená v čl. 4 GDPR jako předchozí, je důležitá pro doplnění kontextu základní problematiky terminologie GDPR a patří sem definice jako:

- **Anonymní údaje** – hlavní rozdíl mezi osobními údaji a anonymními údaji je ten, že anonymní údaji nelze vztáhnout k identifikované nebo identifikovatelné osobě. Za anonymní údaje se tedy považují takové údaje, které netvoří vztah mezi subjektem údajů a tento vztah nemůže být ani správcem údajů obnoven (Žůrek, 2018).
- **Zvláštní kategorie osobních údajů –** za zvláštní kategorii osobních údajů se považují osobní údaje, jejichž charakter by mohl způsobit újmu jejímu subjektu ve společnosti, školním zařízení, zaměstnání nebo podněcovat k diskriminačnímu

jednání. Za tyto údaje se dá považovat například národnostní či etnický původ, politické preference, náboženská příslušnost, zdravotní stav nebo sexuální orientace. Zvláštní kategorii osobních údajů doprovází vyšší míra ochrany než u osobních údajů, která se promítá především do průběhu jejich zpracování (Ochrana osobních údajů dle GDPR, 2021).

Podle GDPR je tedy nepřípustné zpracovávat tyto údaje, pokud další právní předpis nestanoví odlišný pohled. Většinou se tak jedná v případě, je-li to ve veřejném zájmu, zejména v oblastech jako jsou pracovní právo a sociální ochrana člověka. GDPR také umožňuje archivaci zvláštní kategorie údajů osob ve veřejném zájmu, pro statistické účely nebo soudní řízení (Navrátil, 2018).

Zde je podle Nezmara uvedeno několik důvodů, kdy lze zvláštní kategorii osobních údajů zpracovávat:

- subjektem údajů byl udělen výslovný souhlas,
- zpracování údajů je nezbytné pro plnění povinností v oblastech pracovního práva nebo sociální péče,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektů údajů,
- zpracování je nezbytné z důvodu všeobecného zájmu v oblasti veřejného zdraví (Nezmar, 2017).

2.2 Právní základ v oblasti ochrany osobních údajů

V této části jsou představeny právní předpisy obsažené v právním řádu ČR, které upravují problematiku ochrany osobních údajů. Nejprve je uveden ústavní základ ochrany osobních údajů, následuje výčet právních předpisů a procesních předpisů, které vstupují do úpravy ochrany osobních údajů.

Ústavní základ ochrany osobních údajů:

- Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod

Článek 7

(1) *„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem“* (ČESKO, 1993).

Článek 10

(1) *„Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.*

(2) *Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.*

(3) *Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“* (ČESKO, 1993).

Článek 13

„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením“ (ČESKO, 1993).

- Listina základních práv Evropské unie

Článek 8

(1) *„Každý má právo na ochranu osobních údajů, které se ho týkají.*

(2) *Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.*

(3) *Na dodržování těchto pravidel dohlíží nezávislý orgán“* **(**Listina základních práv Evropské unie, 2016).

- Smlouva o fungování Evropské unie

Článek 16

(1) *„Každý má právo na ochranu osobních údajů, které se jej týkají.*

(2) *Evropský parlament a Rada přijmou řádným legislativním postupem pravidla o ochraně fyzických osob při zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a pravidla o volném pohybu těchto údajů. Dodržování těchto pravidel podléhá kontrole nezávislými orgány.*

Pravidly přijatými na základě tohoto článku nejsou dotčena zvláštní pravidla uvedená v článku 39 Smlouvy o Evropské unii“ (Konsolidované znění Smlouvy o fungování Evropské unie, 2016).

- Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních údajů

Ochranu osobních údajů upravuje celá řada právních předpisů. Zde je přehled vybraných právních předpisů.

Obecné právní předpisy ochrany osobních údajů:

- Zákon č. 89/2012 Sb., občanský zákoník,
- Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR),
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti,
- Zákon č. 262/2006 Sb., zákoník práce,
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě,
- Zákon č. 239/2000 Sb., o integrovaném záchranném systému,
- Zákon č. 258/2000 Sb., o ochraně veřejného zdraví,
- Zákon č. 389/2013 Sb., o elektronických dokladech,
- Zákon č. 374/2011 Sb., o zdravotnické záchranné službě,
- Zákon č. 372/2011 Sb., o zdravotních službách,
- Zákon č. 110/2019 Sb., o zpracování osobních údajů (Právní předpisy, c2013).

Procesní právní předpisy:

- Zákon č. 500/2004 Sb., správní řád,
- Zákon č. 150/2002 Sb., soudní řád správní,
- Zákon č. 255/2012 Sb., kontrolní řád,
- Zákon č. 99/1963 Sb., občanský soudní řád (Právní předpisy, c2013).

3 OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

GDPR je výsledek dlouhého a náročného vyjednávání, které obsahovalo velké množství změn v legislativě. Právě nejednotnost právních norem v oblasti ochrany osobních údajů jednotlivých členských států EU, vedoucích k právním nejistotám, byla považována za primární překážku především ve výkonu hospodářských činností na úrovni EU. GDPR disponuje, na rozdíl od předchozí platné Směrnice 95/46/ES, tou výhodou, že se vztahuje přímo na jeho adresáty. Tímto tedy již není důvod k dalším prováděcím předpisům právě ze strany států EU. To byl také důvod k přijetí komplexní legislativy, neboť GDPR vede k větší právní jistotě v problematice ochrany osobních údajů a odstranění možných překážek pro zacházení s osobními údaji (Voigt, Bussche, 2017).

Význam GDPR není možné přeceňovat. Jeho úkolem je chránit spotřebitele a uživatele před vážnými újmami, které by mohli vyplynout ze zneužití jejich osobních údajů a tím se vyhnout poškození lidské důstojnosti (Gal, Aviv, 2020).

To mělo dočinění především s nástupem nových digitálních technologií. Internetové bankovnictví, služby, sociální sítě, všechno mělo za následek sbírání a zpracováni ohromného množství osobních údajů. V souvislosti s tím bylo potřeba zavést nová organizační a technická opatření, aby se zajistilo kvalitní fungování ochrany osobních údajů. Zapotřebí bylo, ale také dosáhnout personálního obsazení pozic, které měly za úkol dodržovat ochranu osobních údajů. GDPR tuto povinnost vyřešila stanovením jmenováním pověřence pro ochranu osobních údajů (Navrátil 2018).

Jedním z hlavních cílů GPDR bylo přesvědčit občany k větší odpovědnosti se zacházením s vlastními osobními údaji. To samozřejmě mělo souvislost především s digitalizací, při které se objem zpracovaných osobních údajů zvětšil. GDPR zaujímá široké pole působnosti, ve kterém se museli přizpůsobit všechny subjekty, kterých se GDPR dotýká, aby byly jejich postupy v oblasti ochrany osobních údajů v souladu s GDPR (Voigt, Bussche, 2017).

V GDPR jsou zahrnuty dva klíčové body ochrany osobních údajů, a to právo na soukromí a právo na ochranu osobních údajů. Ne nadarmo je tedy GDPR všeobecně považováno za zlatý standard předpisů týkající se ochrany osobních údajů (Ke, Sudhir, 2023).

3.1 Pověřenec pro ochranu osobních údajů

Pozice pověřence pro ochranu osobních údajů přišla s GDPR, protože v zákoně o ochraně osobních údajů tento pojem zmíněn nebyl. Naopak mnohé evropské země i sousední státy

ČR jako Německo nebo Slovensko již jistou formu pověřence pro ochranu osobních údajů znaly. Pověřenec pro ochranu osobních údajů našel uplatnění také v orgánech EU, proto byla následně tato pozice implementována do GDPR (Žůrek, 2018).

Ministerstvo vnitra ČR také publikovalo vzorový obsah pracovní činnosti pověřence pro ochranu osobních údajů ve služebních úřadech, a to v Metodickém doporučení k problematice pověřenců pro ochranu osobních údajů (Pověřenec pro ochranu osobních údajů, c2023).

Povinné jmenování pověřence pro ochranu osobních údajů je dle čl. 37 GDPR pro:

- veškeré veřejné organizace státní moci (bez ohledu na povahu shromažďovaných a zpracovávaných údajů),
- subjekt údajů, jehož hlavní činnosti vyžadují rozsáhlé monitorování a prováděcí operace zpracování,
- hlavní činností správce nebo zpracovatele je obsáhlé zpracování zvláštních kategoriích údajů uvedených v čl. 9 a osobních údajů, které se týkají rozsudků v trestních věcech a trestných činu uvedených v čl. 10 (Žůrek, 2018).

Hlavní činnosti pověřence pro ochranu osobních údajů souvisí s jeho postavením, pro které byl organizací přijat. Do úkolů pověřence patří především dohled na zpracovaní osobních údajů dle GDPR a dalšími právními normami, edukace ostatních zaměstnanců zapojených do oblasti osobních údajů nebo pořádání odborných školení v rámci kybernetické bezpečnosti. Pověřenec se také zabývá posuzováním a prošetřováním stížností, které daný správce obdržel od subjektů údajů a z toho vyplývající nutnost spolupráce s dozorovým úřadem, kdy pověřenec zároveň existuje jako komunikační střed mezi dozorovým úřadem a subjektem údajů. Pověřenec má též možnost řídit ostatní činnosti přímo nesouvisející s ochranou osobních údajů. Zde je ale podmínka, že se pověřenec nesmí dostat do střetu zájmu s činností pověřence. Z tohoto hlediska by proto měla být dodržena poradní a informační funkce pověřence (Žůrek, 2018).

K funkci pověřence uvnitř organizace by mělo odpovídat komplexní zapojení do celé řady chodů a postupů, protože je to předpoklad k zdárnému plnění úkolů pověřence. Pověřenec by se měl účastnit jednání středního a vyššího managementu organizace a rovněž být seznámen se všemi podstatnými souvislostmi s ochranou osobních údajů. Pověřenec musí vystupovat nezávisle, jelikož podle GDPR správce a zpracovatel stanoví, že pověřenec neobdrží žádné nařízení výkonu jeho činnosti. Během výkonu své funkce se pověřenec setkává s celou

řadou důvěrných informací nebo tajemstvím organizací, musí proto v souvislosti s jeho výkonem dodržovat mlčenlivost o zjištěných informacích (Žůrek, 2018).

Jak již vyplývá z předchozího textu, požadavek na výkon funkce pověřence musí být především odbornost. Je sice pravdou, že GDPR nestanovuje konkrétní požadavky na výkon pověřence, nicméně je zde předpoklad minimálně profesních či odborných kvalit. Přispívá k tomu i skutečnost, že každému správci a zpracovateli vyhovuje jiné zaměření a odbornost pověřence pro ochranu osobních údajů (Žůrek, 2018).

V obecné rovině se ale dají předpokládat odborné znalosti z oblastí práva, a to jak národního práva, tak práva evropského, především na výbornou znalost GDPR, s přihlédnutím na možné rozdíly mezi zařazením GDPR do jednotlivých právních řádů jiných států. Znalost práva patří mezi základní pilíře předpokladů pro výkon funkce pověřence, dále se může jednat o konkrétní právní odvětví, ve kterém správce nebo zpracovatel figurují. Vše se odvíjí od komplexnosti a rozsahu zpracovávaných údajů. Například pokud bude správce či zpracovatel spolupracovat se zahraničními dozorovými orgány EU, budou k požadavkům na pověřencem patřit nejenom odborné znalosti z oblasti práva ale i nutnost znalosti minimálně jednoho úředního jazyku EU na dostatečné úrovni, aby mohl řešit agendu s těmito orgány (Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?, 2018).

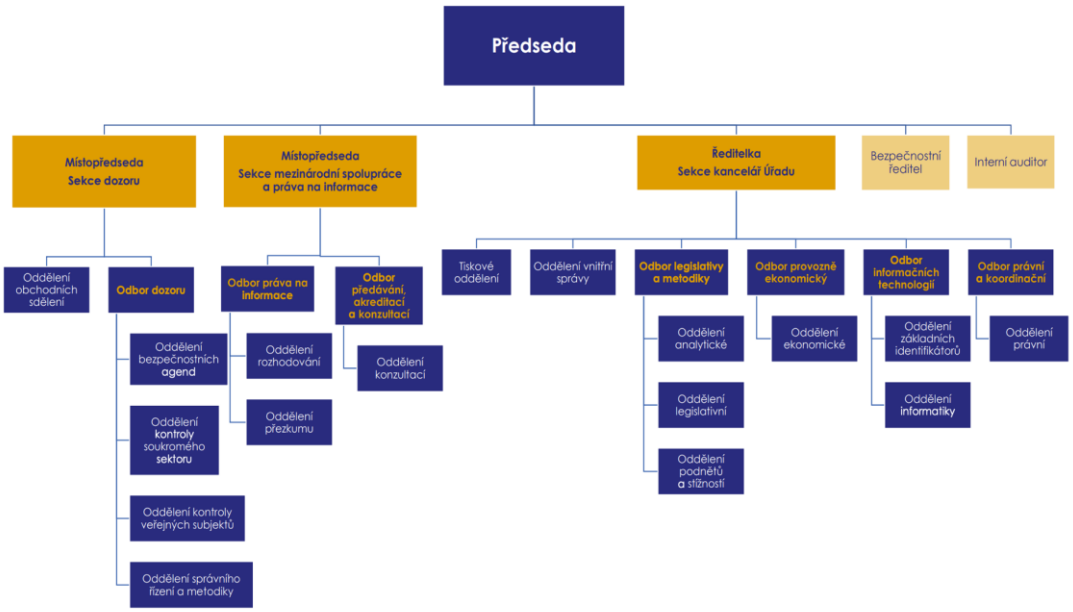
Podle GDPR je možné, aby funkci pověřence vykonával zaměstnanec správce či zpracovatele nebo externí subjekt. Existuje tedy možnost, že pověřenec nemusí být fyzická osoba, ale právnická osoba, která funguje na základě smlouvy o poskytování služeb. Správce či zpracovatel by tedy měl dbát zvýšené pozornosti při výběru osoby na pozici pověřence, ať už z důvodu vysoké náročnosti a složitosti operací spojených se zpracováním osobních údajů, tak v souladu s právními předpisy, neboť špatné rozhodování při řešení problémů ze strany pověřence může vést k finančním sankcím nebo reputačním újmám (Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?, 2018).

3.2 Úřad pro ochranu osobních údajů

Historie ÚOOÚ se začala psát dne 1. června 2000, kdy vznikl jako samostatný správní úřad, který se specializuje se na ochranu osobních údajů v ČR. Úřad jednal v působnosti zákona č. 101/2000Sb., o ochraně osobních údajů a zahrnoval činnosti spočívají ve vedení registru

dovolujících zpracování osobních údajů, přijímání podnětů k porušení zákona, edukace v ochraně osobních údajů a legislativní aktivity (Historie úřadu, c2024).

V roce 2003 začal být ÚOOÚ uznávanou autoritou v oblasti ochrany osobních údajů napříč mnoha evropskými státy. Byl zapojen do Rady Evropy, s níž spolupracoval na celé řadě aktivit se zkušenostmi a znalostmi v oblasti ochrany údajů. Podstatné zlepšení ochrany osobních údajů přišlo v roce 2018 s přijetím GDPR. ÚOOÚ vystupoval jako edukační kanál pro širokou veřejnost v rámci osvěty ochrany osobních údajů (Historie úřadu, c2024).



Obrázek 2 – Organizační struktura ÚOOÚ (Organizační struktura, c2024).

ÚOOÚ je výhradním dozorovým úřadem s obecnou působností v ČR a dozorová činnost patří mezi jeho hlavní úkoly. Další činnosti ÚOOÚ jsou náprava chybných procedur při zpracování osobních údajů správci nebo zpracovateli. Tento úřad se také zabývá nedostačující ochranou osobních údajů, která zasahuje více subjektů neboli to, že při její nápravě bude mít prospěch více subjektů údajů. Mimo agendu ochranu osobních údajů je pilířem činnosti ÚOOÚ program svobodného přístupu k informacím, kde má tento úřad přidělenou působnost. V neposlední řadě se ÚOOÚ zabývá provozem informačního systému poskytující identifikátory fyzických osob (Postavení úřadu, c2024).

Primárním úkolem ÚOOÚ je ochrana osobních údajů. ÚOOÚ má své pravomoci a povinnosti vymezené v GDPR, konkrétně v čl. 57 jsou vymezeny povinnosti a v čl. 58. jsou uvedeny pravomoci. Čl. 46 GDPR stanovuje rovněž pravomoci ÚOOÚ pro oblast zpracování osobních údajů ve smyslu předcházení a odhalování trestné činnosti, výkonných opatření, sledování trestných činů a výkonů trestů a bezpečnostních opatření (Postavení úřadu, c2024).

4 BEZPEČNOST OCHRANY OSOBNÍCH ÚDAJŮ

V současné digitální době je podstatná nejenom ochrana osobních údajů neboli jak je s osobními údaji zacházeno, jak jsou zpracovávány a spravovány, ale také zabezpečení ochrany osobních údajů čili ochrana před neoprávněným přístupem nebo například krádeží či zneužití. Následující kapitola pojednává o zabezpečení a porušeni zabezpečení osobních údajů.

4.1 Zabezpečení osobních údajů

Kybernetická bezpečnost patří mezi důležitou součást ochrany osobních údajů. I když je možná stále značné množství osobních údajů sbíráno listinou formou, ve většině případů následně dochází k digitalizaci těchto údajů. Je proto důležité věnovat pozornost tomuto tématu, neboť právě bez dostatečné formy zabezpečení není možná ochrana osobních údajů (Nezmar, 2017).

Zabezpečení osobních údajů je podle Žůrka: *„pouze jednou z vrstev kybernetické bezpečnosti, kterou by správci či zpracovatelé měli zajišťovat, protože osobní údaje nejsou jediné informace, které chrání.“* Samotné zabezpečení údajů se dá považovat za předpoklad v souladu s GDPR pro dosažení zpracování osobních údajů. Spolehlivá zabezpečení tak musí zajistit správce i zpracovatel, neboť se osobní údaje dají považovat za aktiva, která jsou předmětem zabezpečení. Z důvodu existence mnoha rozdílných správců a subjektů údajů, neexistují stejné povinnosti přijímaných bezpečnostních opatření. Proto se uplatňuje přístup založený na možném riziku, kdy správci údajů a zpracovatelé dle čl. 32 GDPR přijímají bezpečnostní opatření, které odpovídá stavu technických zařízení, nákladů na provedení, povaze a rozsahu zpracování i možným pravděpodobnostem a hrozbám, které zajistí dostatečnou úroveň zabezpečení odpovídajícímu riziku včetně:

- pseudonymizace a zašifrování osobních údajů,
- schopnosti dodržet trvalou důvěrnost, integritu, dostupnost a odolnost systému a služeb během zpracování,
- schopnost obnovit přístup k osobním údajům a jejich dostupnosti v případě fyzických nebo technických incidentů,
- procesu častého otestování a posouzení bezpečnosti osobních údajů a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování (Žůrek, 2018).

Správci a zpracovatelé jsou ve své podstatě svobodní, co se týče volby zabezpečení. U provedení zpracování osobních údajů, mohou použít pseudonymizaci i šifrování, ale nejedná se, avšak o povinný způsob zabezpečení. Šifrování a pseudonymizace jsou tradiční způsoby zabezpečení, jelikož jejich použití může hrát roli v řešení problémů v případě úniku osobních údajů. Tímto způsobem zabezpečení se také zlepšuje postavení správce či zpracovatele, protože v případě úniku, v závislosti na vážnosti případu, nemusí hlásit bezpečnostní incident dozorovému úřadu (Zabezpečení osobních údajů, c2023).

V současném světě digitalizace je velmi žádoucí dbát důraz na zabezpečení, protože množství rizik spojené s digitalizací se mnohonásobně zvýšil oproti době, kdy byla většina osobních údajů zpracovávána v listinné formě. Zvýšenou pozornost se musí dbát také při likvidaci výpočetní techniky, která v sobě uchovávají paměťová zařízení. Zde je potřebné provést kroky ke zničení paměťových zařízení, aniž by šly zpětně obnovit (Žůrek, 2018).

Nový problém, který vyplynul také z digitálního zpracování osobních údajů, je neschopnost identifikovat krádeže osobních údajů, protože při listinné podobě je krádež zřejmá, nicméně u digitální podoby osobních údajů může dojít ke kopírování, což nemusí být na první pohled zcela viditelné. Je proto velmi žádoucí, aby správce či zpracovatel disponoval mechanismy, které dokáží zjistit neoprávněné přístupy či neobvyklé aktivity v síti. I když je drtivé množství osobních údajů vedeno v elektronické podobě, stále se nesmí opomenout fyzické vedení evidencí, papírovou formou. Takové dokumenty by neměly být volně přístupné neoprávněným osobám a měly by být zabezpečeny odpovídají formou dle jejich obsahu a rizika v případě úniku. V souvislosti s fyzickou bezpečnosti se také jedná o bezpečnost objektů a přijetí odpovídajících bezpečnostních prvků (Žůrek, 2018).

Nezbytnou dávku pozornosti je nutné také směřovat na lidský faktor, a to konkrétně na zaměstnance organizací, kteří jsou často zodpovědní za způsobení mnoha bezpečnostních incidentů. Na místě je proto uspořádání pravidelného školení pro zaměstnance, kterými lze předcházet významným bezpečnostním rizikům uvnitř organizací. Je vhodné, aby správci, kteří patří mezi ty větší správce, co se týče velikosti množství osobních údajů, měli zpracovanou koncepci či bezpečnostní směrnici uvnitř organizace ohledně ochrany osobních údajů. Dle čl. 32 GDPR je stanovena povinnost pro správce a zpracovatele, aby libovolná fyzická osoba, která má přístup k osobním údajům a bude jednat z pověření správce či zpracovatele, zpracovávala osobní údaje dle pokynů správce či zpracovatele (Žůrek, 2018).

4.2 Porušení zabezpečení osobních údajů

Podle čl. 4 GDPR se za porušení zabezpečení osobních údajů považuje náhodné nebo protiprávní zničení, ztráta nebo neoprávněné zpřístupnění osobních údajů. V případě porušení zabezpečení nastává pro správce nebo zpracovatele povinnost takové situace bezodkladně řešit (Žůrek, 2018).

Charakter porušení se může lišit a obecně může být velmi rozmanitý. Zde je přehled základního členění porušení zabezpečení osobních údajů:

- neoprávněný nebo náhodný přístup k údajům – porušení důvěrnosti,
- neoprávněná nebo náhodná změna údajů – porušení integrity,
- ztráta dat nebo ztráta přístupu k datům – porušení dostupnosti (Secure personal data, 2016).

V případě, že u správce dojde k případu porušení zabezpečení osobních údajů, má správce povinnost přijít s adekvátním opatřením a zhodnocením daného rizika. Zde je nutné si uvědomit, že riziko plynoucí z porušení zabezpečení se bude odvíjet především od kategorie dotčených osobních údajů. V tomto ohledu hraje podstatnou roli fakt, zda se jedná o zvláštní kategorie osobních údajů nebo o jiné formy bezpečnostního incidentu, protože se od těchto faktorů bude odvíjet dopad na práva a svobody fyzických osob (Žůrek, 2018).

Za porušení dostupnosti osobních údajů se bude považovat dočasná neschopnost správce přistupovat k osobním údajům. V případě dlouhodobé nemožnosti přístupu k osobním údajům, se již bude jednat o porušení zabezpečení. V tomto směru ale existuje možnost, že se nebude jednat o žádný bezpečnostní incident, neboť může být vytvořena záloha, kterou správce obnoví osobní údaje. Až se zjištěním, že by záloha nebyla funkční, by se jednalo o vysoce rizikové porušení zabezpečení osobních údajů (Žůrek, 2018).

Důležitým aspektem v posuzování rizika bude bezesporu míra zavinění neboli zda se bude jednat o úmyslné jednání nebo nedbalost. V případě úmyslného jednání se s největší pravděpodobností bude jednat vždy o tu horší variantu pro správce nebo zpracovatele, neboť cílená krádež údajů bude mít na svědomí větší hrozbu než neúmyslné zničení. Aby se předešlo co nejméně stresovým situacím dotčených pracovníků v případě porušení zabezpečení, je vhodné mít pro takové případy zpracovány pohotovostní plány, kontakty na odpovědné pracovníky v organizaci, postupy nebo adresy dozorových orgánu, které se využijí k ohlá-

šení incidentu. Postup řešení takové situace souvisí s výkonem pověřence pro ochranu osobních údajů, který by měl koordinovat následný postup na daný incident, zahrnující i plnění povinností k dozorovému úřadu nebo subjektům údajů. V případě, že z porušení zabezpečení osobních údajů vyplyne ohrožení práva a svobody fyzických osob, má správce povinnost neprodleně a nejlépe do 72 hodin od okamžiku, kdy se o porušení dozvěděl, informovat dozorový orgán. Určit přesný začátek stanovené lhůty není jednoduché, protože může existovat mnoho lidí uvnitř správce, kteří se o incidentu dozví. Je proto žádoucí, aby každý správce vybral konkrétní osoby, u kterých je největší pravděpodobnost možné identifikace bezpečnostních incidentů (Žůrek, 2018).

Ohlášení obsahuje povinné náležitosti, které pověřenec pro ochranu osobních údajů, nebo jiná pověřená osoba předává dozorovému orgánu:

- profil konkrétního případu, kategorie a množství dotčených subjektů údajů,
- jméno a kontaktní údaje na pověřence pro ochranu osobních údajů, byl-li ustaven, případně jiné komunikační spojení na kompetentní osobu,
- komentář pravděpodobných následků,
- popis opatření, které byla správcem přijata nebo navrhl k přijetí s cílem vyřešit daný incident, včetně všech opatření vedoucích ke zmírnění negativních následků (Buckbee, 2022).

Když se ukáže, že ohlášení dozorovému orgánu proběhlo v pořádku a v dané lhůtě, měl by se takový postup natrvalo aplikovat do všech směrnic a plánu pro řešení bezpečnostních incidentů. V tomto případě je navíc žádoucí sestavit seznam dílčích procesů, obsahujících popis rolí, odpovědností a kontrolních bodů (GDPR Top Ten #9: Security and breach notification, c2024).

V některých situací může nastat případ, kdy nebude možné zveřejnit a poskytnou veškeré informace o porušení zabezpečení. Je tedy možné předávat zjištěné skutečnosti dozorovému úřadu postupně, zde ale pořád platí povinnost oznámit bezpečnostní incident do 72 hodin. Z čl. 33 GDPR plyne povinnost pro správce každé porušení zadokumentovat, a to i případě, že nedojde k ohrožení práv a svobod fyzických osob v důsledku porušení zabezpečení osobních údajů. Toto opatření slouží ke zpětné kontrole správce pro případ, aby nedošlo k úmyslné bagatelizaci porušení zabezpečení osobních údajů a vyhnutí se dalším povinnostem ohlašování dozorovému orgánu (Žůrek, 2018).

5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část se v první kapitole věnuje historickému vývoji ochrany osobních údajů jak ve světě a Evropě, tak na území ČR. V další kapitole následuje důležitý výčet definic čl. 4 GDPR, které jsou zásadní pro komplexní pochopení problematiky ochrany osobních údajů a také jsou zde uvedeny právní normy, které upravují ochranu osobních údajů. Následující kapitola je věnována samotnému GDPR, postavení pověřence pro ochranu osobních údajů a také dozorovému orgánu pro problematiku ochrany osobních údajů. Čtvrtá kapitola se soustředí na bezpečnost ochrany osobních údajů, a to jak z pohledu zabezpečení, tak porušení zabezpečení ochrany osobních údajů.

V následující praktické části se práce zaměří na ochranu osobních údajů v oblasti ochrany obyvatelstva. K provedení komplexní analýzy na ochranu osobních údajů je vybrána základní složka integrovaného záchranného systému, a to poskytovatelé zdravotnické záchranné služby, konkrétně Zdravotnická záchranná služba Zlínského kraje, p.o.

Použité metody v práci:

- **Analýza** – slouží k identifikaci důležitých a podstatných vlastností a k zaznamenání současného stavu s cílem získat vědomosti o fungování systému.
- **Expertní rozhovor** – kvalitativní metoda, s cílem získání informací k řešené problematice od kompetentní osoby.
- **SWOT –** analýza SWOT, která analyzuje daný jev a umožňuje vymezení silných a slabých stránek, příležitostí a hrozeb vybrané organizace.
- **What-If** – tato analýza slouží k identifikaci možných hrozeb, které vedou k negativním následkům. Součástí jsou i návrhy jednotlivých opatření k minimalizaci identifikovaných hrozeb.

II. PRAKTICKÁ ČÁST

6 ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA ZLÍNSKÉHO KRAJE

Zdravotnická záchranná služba Zlínského kraje, p.o. (dále jen „ZZS ZK“) patří mezi příspěvkovou organizaci, kterou zřizuje Zlínský kraj. Činnosti, které zajišťuje ZZS ZK, jsou garantovány státem a Zlínský kraj patří mezi zajišťující samosprávný celek. Činnost ZZS ZK je v současnosti hrazena:

- z rozpočtu Zlínského kraje,
- v případě hrazených zdravotních služeb z veřejného zdravotního pojištění,
- ze státního rozpočtu (Základní informace, c2024).

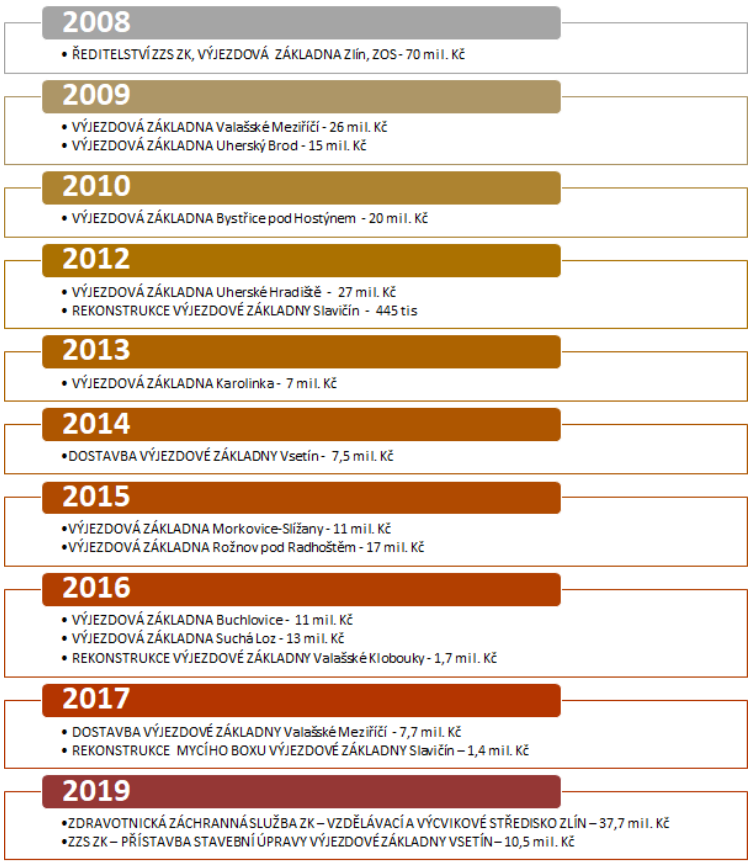
Obrázek 3 – Logo ZZS ZK (ZZS ZK, c2024).

Základním právním předpisem v činnosti ZZS ZK je zákon č. 374/2011 Sb., o zdravotnické záchranné službě, který stanovuje hlavní úkol ZZS ZK, a to poskytování přednemocniční neodkladné péče (dále jen „PNP“) osobám, které se nachází v přímém ohrožení života nebo s vážným poškozením zdraví (ČESKO, 2011).

6.1 Historie

Zřízení ZZS ZK proběhlo s účinností od 1. ledna 2004, kdy se ZZS ZK stala jednou ze 14 zdravotnických záchranných služeb v ČR. V roce 2003, konkrétně 31. prosince, byly zrušeny okresní úřady a vzniklo Územní středisko zdravotnické záchranné služby Zlínského kraje, které nahradilo dosud všechny organizace samostatných záchranných služeb v okresech Zlín, Uherské Hradiště, Kroměříž a Vsetín. Na současný název byla ZZS ZK změněna 1. dubna 2006 (Historie, c2024).

ZZS ZK se v rámci své organizace člení na 5 oblastí s 16 výjezdovými základnami.



Obrázek 4 – Přehled výjezdových základen (Historie, c2024).

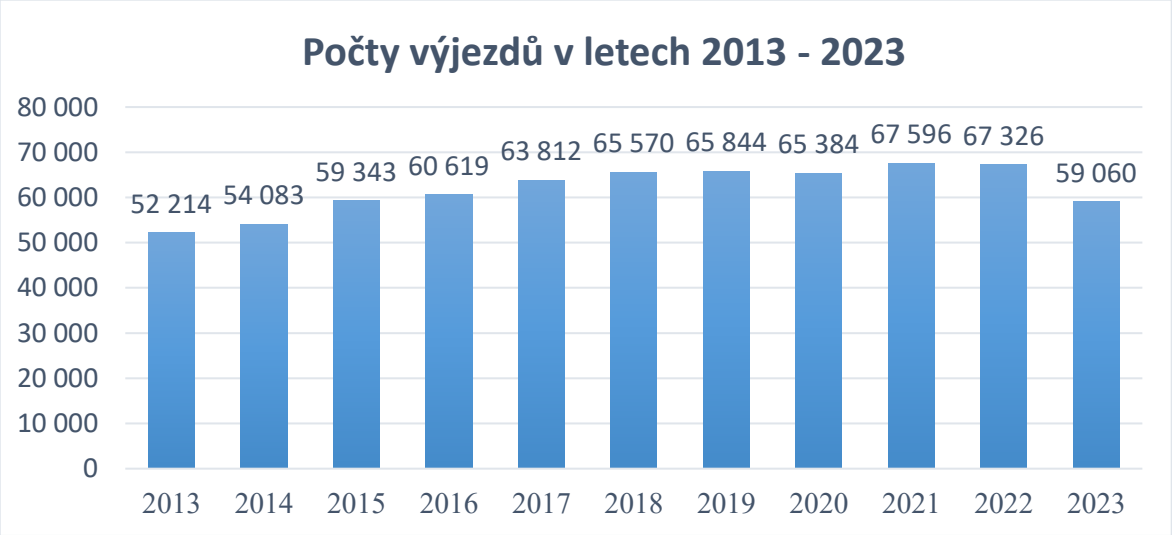
Tyto oblasti jsou členěny na Zlín, Uherské Hradiště, Kroměříž, Vsetín a Valašské Meziříčí.

- Oblast Zlín – v této oblasti se nachází 5 výjezdových základen. Po uskutečněných rekonstrukcích a nezbytných opravách slouží v současnosti základny, a to ve Zlíně, Otrokovicích, Slavičíně a Valašských Kloboukách.
- Oblast Uherské Hradiště – oblast disponuje 4 výjezdovými skupinami, které se nacházejí v Uherském Brodě, Uherském Hradišti, Buchlovicích a Suché Lozi.
- Oblast Kroměříž – v oblasti jsou vybudovány výjezdové základny v Kroměříži, dále v Bystřici pod Hostýnem a nejnovější zřízená výjezdová základna v této oblasti v Morkovicích – Slížanech.
- Oblast Vsetín – tato oblast zahrnuje 2 výjezdové základny, základna po rozsáhlé rekonstrukci v Karolínce a po přístavbě také ve Vsetíně.
- Oblast Valašské Meziříčí – v oblasti se nachází 2 výjezdové základny ve Valašském Meziříčí a Rožnově pod Radhoštěm (Historie, c2024).

6.2 Současnost

ZZS ZK patří do systému zdravotnických služeb v ČR. Primárním úkolem ZZS ZK je zajišťování PNP. Právě k zajišťování PNP může dojít z několika situací, ať už se jedná o náhle vzniklé onemocnění, úrazy nebo zhoršení zdravotního stavu, kdy mohou tyto stavy způsobit dlouhodobé nebo doživotní následky a způsobit selhání životních funkcí (Základní informace, c2024).

Další činnost, kterou zajišťuje ZZS ZK je okamžitý příjem nepřetržitého volání na národní číslo tísňového volání 155 operátorem ze zdravotnického operačního střediska (dále jen „ZOS“) nebo pomocného operačního střediska. Dále probíhá vyhodnocení a rozhodování řešení tísňového volání a poslání výjezdových skupin na místo události. Nedílnou součástí činností ZZS ZK je i řízení PNP na místě zásahu a spolupráce s velitelem zásahu složek integrovaného záchranného systému (Základní informace, c2024).



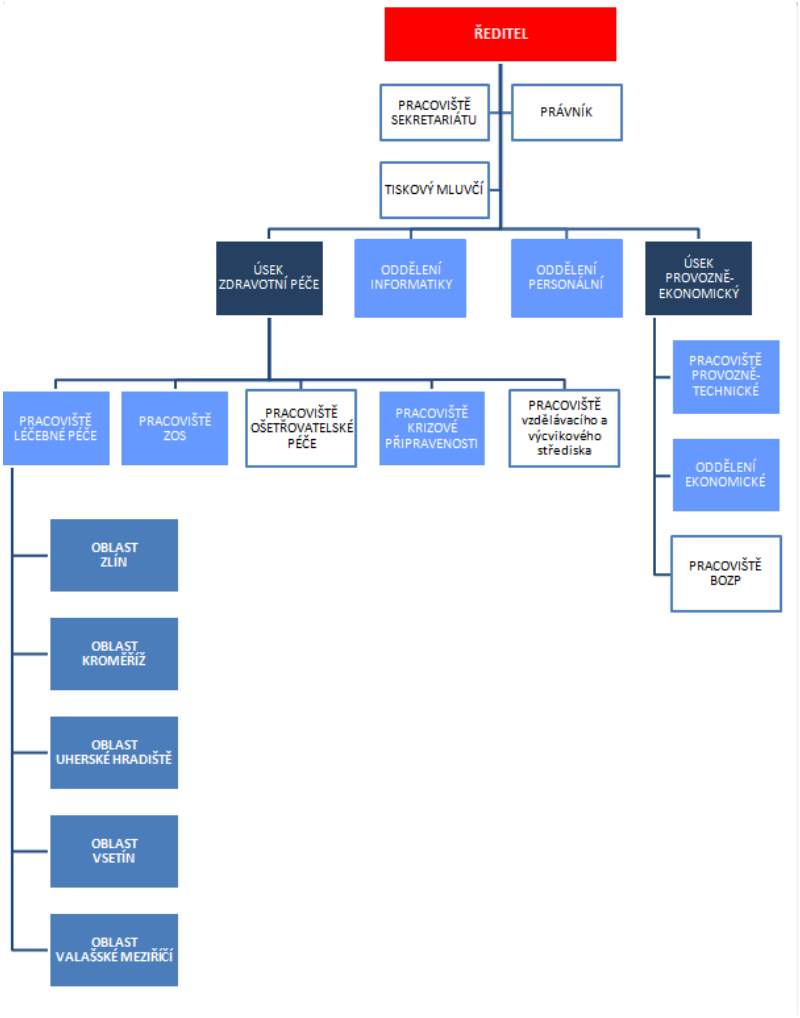
Obrázek 5 – Statistika výjezdů ZZS ZK (Statistika, c2024, vlastní zpracování).

ZZS ZK nedisponuje leteckou záchrannou službou, proto je v případě potřeby této služby využito letecké záchranné služby ze sousedních krajů, a to z Moravskoslezského, Olomouckého a Jihomoravského kraje (Základní informace, c2024).

6.3 Organizační struktura

V současnosti má ZZS ZK k dispozici až 34 výjezdových skupin v 16 výjezdových základnách. Nasazení výjezdových skupin závisí na vytížení jednotlivých směn, ať už denních, nočních nebo víkendových. Lokace jednotlivých výjezdových skupin se odvíjí od Plánu pokrytí území Zlínského kraje výjezdovými skupinami, kde je zajištěna zákonem stanovená

dojezdová doba 20 minut. Existují výjimky, kdy dojezdový doba nemusí být dodržena, a to v případě nenadálých nepříznivých klimatických nebo dopravních podmínek nebo případů zvláštního zřetele. Dojezdová doba se začíná počítat od momentu převzetí pokynu výjezdovou skupinou k výjezdu od operátora ZOS nebo pomocného operačního střediska (Základní informace, c2024).



Obrázek 6 – Organizační struktura ZZS ZK (Základní organizační struktura, c2024).

Součástí ZZS ZK je i ZOS, které patří mezi centrální pracoviště operační řízení, jenž běží v nepřetržitém režimu. Na ZOS pracuje 20 operátorů, 1 vedoucí operátor a vedoucí lékař ZOS. 4 operátoři zajišťují stálou činnost ZOS. Mezi hlavní úkoly ZOS patří především přijímání a vyhodnocování všech tísňových volání na linku 155 a následné předávání těchto informací výjezdovým skupinám, dále poskytování odborných instrukcí k zajištění první pomoci do příjezdu výjezdových skupin a spolupráce s dalšími operačními středisky (Zdravotnické operační středisko, c2024).

7 ANALÝZA OCHRANY OSOBNÍCH ÚDAJŮ U ZDRAVOTNICKÉ ZÁCHRANNÉ SLUŽBY ZLÍNSKÉHO KRAJE

V této kapitole se zaměřím na současnou ochranu osobních údajů u vybrané složky integrovaného záchranného systému a to ZZS ZK. Jelikož ZZS ZK vystupuje jako správce údajů, potřebuje k vykonávání své činnosti zejména osobní údaje osob – pacientů, potřebné pro vedení zdravotnické dokumentace a pro vykazování provedených úkonů zdravotním pojišťovnám, případně jiným subjektům.

Základním právním předpisem pro zpracování údajů o zdravotním stavu je GDPR, konkrétně čl. 9. odst. 2. písm. h), kde je uvedeno, že zpracování osobních údajů je nezbytné pro účely preventivního pracovního lékařství, pro hodnocení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování sociální i zdravotní péče, léčby nebo řízení systémů služeb ve zdravotní péči. Vše v souladu s právem EU nebo na základě smlouvy se zdravotnickým pracovníkem za předpokladu splnění podmínek a záruk uvedených ve čtvrtém odstavci (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

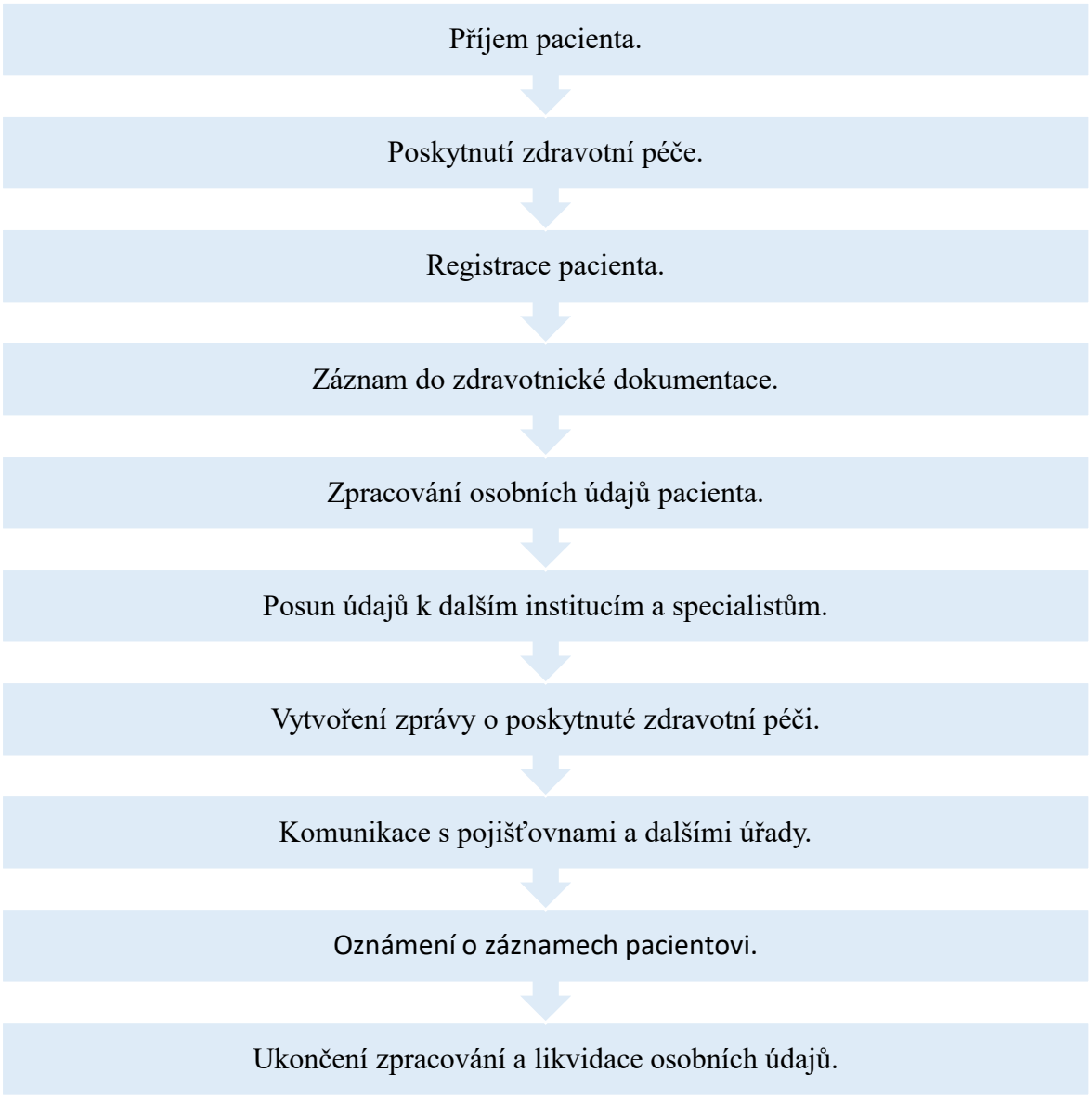
Během zpracování osobních údajů u ZZS ZK nedochází k profilování, což znamená, že nejsou u osob shromažďovány osobní údaje, které by mohl správce údajů využít k vytvoření jistého profilu osob neboli hodnocení osobních aspektů, který by mělo zasahovat do práv subjektů údajů.

Pro vedení zdravotnické dokumentace je účelem zpracování osobních údajů vedeno dle zákona č. 372/2011 Sb., zákon o zdravotních službách a podmínkách jejich poskytování. V tomto zákoně je zdravotnická dokumentace ustanovena v části šesté. Za příjemce osobních údajů jsou považováni poskytovatelé zdravotních služeb a také zdravotní pojišťovny pacientů (ČESKO, 2011).

V rámci lepší orientace v jednotlivých postupech zpracování osobních údajů je vytvořené následující schéma (viz obr. č. 7), které zobrazuje zpracování osobních údajů v rámci ZZS ZK.

V první fázi zaměstnanec ZZS ZK zaznamená základní údaje o pacientovi, po poskytnuté zdravotní péči je proveden záznam do zdravotnické dokumentace o provedených vyšetřeních a léčbě, následuje zapsání údajů do registračního systému. Dalším krokem je uchování osobních údajů pacienta při dodržování technických a organizačních opatření. Následuje předání zprávy o vykonaných úkonech ostatním institucím nebo specialistům. Následně je vytvořená

zpráva o vykonané zdravotní péči komunikována s pojišťovnami nebo dalšími úřady dle potřeby. Poté je pacientovi předána zpráva o vykonané péči a jeho údajích. Po uplynutí nezbytně dlouhé doby už nejsou osobní údaje zpracovávány a jsou odstraněny.



Obrázek 7 – Schéma zpracování osobních údajů (vlastní zpracování, 2024).

7.1 Expertní rozhovor

Pro komplexnější přehled současného stavu ochrany osobních údajů u ZZS ZK byl proveden expertní rozhovor s pověřencem pro ochranu osobních údajů ZZS ZK panem magistrem Michalem Chmelařem. Rozhovor se skládá z 12 otázek na téma ochrany osobních údajů u ZZS ZK, doplňující otázky na podrobnější zabezpečení osobních údajů nebylo možné zodpovědět z důvodu bezpečnosti.

1. **Jaké osobní údaje jsou shromažďovány a zpracovávány Zdravotnickou záchrannou službou Zlínského kraje?**

„Jedná se zejména osobní údaje pacientů pro účely vedení zdravotnické dokumentace v rozsahu vymezeném ve vyhlášce č. 98/2012 Sb., o zdravotnické dokumentaci, osobní údaje pacientů v rozsahu nezbytném pro vykazování úkonů zdravotním pojišťovnám a osobní údaje zaměstnanců nezbytné pro plnění povinností zaměstnavatele podle příslušných právních předpisů.“

Komentář: Z odpovědi vyplývá, že ZZS ZK shromažďuje jen osobní údaje pacientů, které nezbytně potřebuje k poskytování neodkladné přednemocniční péče a k výkonu své činnosti. Podle vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci, se jedná o údaje, které mohou být rozděleny do několika kategorií. Tyto kategorie se mohou rozdělit na identifikační údaje, kontaktní údaje, údaje, které se týkají citlivých údajů ohledně zdravotního stavu nebo popisné údaje. Do kategorie identifikačních údajů patří údaje, které jasně identifikují konkrétní subjekt údajů, a to například jméno, příjmení, rodné číslo, datum narození nebo adresu trvalého bydliště. Do kategorie kontaktních údajů patří telefonní číslo, kontaktní adresa nebo emailová adresa. Pod kategorii popisnou spadá například pohlaví nebo státní příslušnost pacienta. Údaje obsahující citlivé zdravotní údaje mohou obsahovat diagnózu nebo užívané léky. Celkově vyhláška č. 98/2012 Sb., o zdravotní dokumentaci pojednává o správném nakládání s potřebnými informacemi a o tom, aby byly zdravotní dokumentace efektivně a správně vedeny.

2. **Jakým způsobem je zajištěna ochrana osobních údajů pacientů během poskytování zdravotnických služeb v rámci záchranné služby?**

„Ochrana osobních údajů spočívá v návrhu vhodných technických a organizačních opatření stanovených před zahájením vlastního zpracování a zavedení a udržování přiměřených technických a organizačních opatření po celou dobu trvání zpracovatelské operace založených na výsledcích analýzy informačních rizik a s přihlédnutím k různě pravděpodobným a různě závažným rizikům pro práva a svobody subjektů údajů.

K ochraně osobních údajů přispívá také realizaci zásady minimalizace, tedy omezení rozsahu zpracovávaných osobních údajů pouze na ty skutečně nezbytné.“

Komentář: Tato odpověď se zabývá způsobem, jakým ZZS ZK zajišťuje ochranu osobních údajů pacientů během poskytování zdravotnických služeb. Je zde zmínka o návrhu vhodných

technických a organizačních opatření. Tato opatření jsou zásadní pro zajištění ochrany osobních údajů pacientů, a to po celou dobu trvání zpracovatelské operace. Tato opatření jsou založena na výsledcích analýzy informačních rizik, což je důležitý krok, který umožňuje identifikovat potencionální hrozby. Pro doplnění ochrany osobních údajů je také uplatňována zásada minimalizace dat, což je podstatné pro omezení rozsahu zpracovaných osobních údajů.

3. **Jak dlouho jsou osobní údaje pacientů uchovávány a jaký je postup jejich odstranění po uplynutí příslušné doby?**

„Osobní údaje jsou zpracovávány pouze na dobu nezbytnou podle příslušných právních předpisů, přičemž u osobních údajů pacientů se doby uchovávání řídí zejména vyhláškou č. 98/2012 Sb., o zdravotnické dokumentaci (příloha 3) a u osobních údajů zaměstnanců pak ustanoveními příslušných právních předpisů z oblasti pracovního práva a práva sociálního zabezpečení.

Postupy odstranění se řídí skartačním řádem ZZS ZK.“

Komentář: Doba úschovy osobních údajů jsou stanoveny dle platných právních předpisů. Jednotlivé lhůty úschovy se mohou lišit v závislosti na druhu zpracování osobních údajů. ZZS ZK má zpracovaný skartační řád, který stanovuje jednotlivé kroky, jak odstranit osobní údaje, a to je důležité pro bezpečnost osobních údajů, aby nedošlo k jejich úniku a zneužití.

4. **Jaký postup máte pro shromažďování a uchovávání citlivých zdravotních údajů pacientů v souladu s požadavky GDPR?**

„Údaje o zdravotním stavu pacientů jsou shromažďovány a zpracovávány na základě čl. 9, odst. 2 písm. h) GDPR pro účely poskytování zdravotní péče. ZZS ZK se řídí pravidly pro zpracování zvláštních kategorií osobních údajů podle nařízení GDPR. Údaje o zdravotním stavu jsou získávány od pacientů nebo jejich zákonných zástupců přímo, případně také ze záznamů hovorů na tísňové lince 155 a jsou zpracovávány v listinné a elektronické podobě při dodržování nastavených technických a organizačních opatření.“

Komentář: Postupy shromažďování a zpracování zdravotních údajů jsou v souladu s právním předpisem GDPR. Také jsou zmíněny způsoby získání údajů o zdravotním stavu pacientů nebo zákonných zástupců.

5. **Jak je zajištěn informovaný souhlas pacientů s ohledem na GDPR?**

„Informovaný souhlas pacientů je získáván za podmínek a v souladu se zákonem č. 372/2011 Sb., o zdravotních službách a tam, kde je jeho získání podle zákona nezbytné, je uchováván jako součást zdravotnické dokumentace při dodržování nastavených technických a organizačních opatření. Osobní údaje v informovaném souhlasu jsou zpracovávány za účelem poskytování zdravotní péče a ke splnění právních povinností ZZS ZK jako správce osobních údajů.“

Komentář: Získání informovaného souhlasu je důležité pro zachování práv pacientů na ochranu jejich osobních údajů. Pacienti mají právo vědět, jaké údaje jsou o nich shromažďovány a jak bude s těmito údaji zacházeno. Informovaný souhlas pacientů jako součást zdravotnické dokumentace je podstatný pro dodržení zákonných požadavků a udělení souhlasů.

6. **Jak jsou školeni zaměstnanci zdravotnické záchranné služby ohledně správy osobních údajů a zabezpečení proti jejich ztrátě či neoprávněnému přístupu?**

„Zaměstnanci jsou seznámeni s nezbytnými postupy a pravidly při zpracování a zabezpečení ochrany osobních údajů prostřednictvím povinného seznámení se s vnitřními předpisy ZZS ZK týkajícími se oblasti ochrany osobních údajů a rovněž podle potřeby při tematických školeních.“

Komentář: Seznámení zaměstnanců s vnitřními předpisy a pravidly je důležité pro zajištění správného dodržování postupů při zacházení s osobními údaji. Následná školení jsou nástrojem pro edukaci o nových trendech, hrozbách a postupech v oblasti ochrany osobních údajů.

7. **Máte vytvořený dokument, který popisuje, jaké konkrétní typy osobních údajů zpracováváte v rámci zdravotnické záchranné služby a jak s nimi zacházíte?**

„Ano, ZZS ZK má obsáhlé vnitřní předpisy týkající se ochrany osobních údajů a v jejich rámci jsou zpracovány rovněž příslušné záznamy o činnostech, které určují, jaké konkrétní druhy osobních údajů a v jakém rozsahu jsou zpracovávány, od jakých subjektů, jaký je právní základ pro jejich zpracování a další podmínky jejich zpracování.“

Komentář: Dokumenty přispívají k dodržování požadavků v souladu s GDPR. Tyto předpisy obsahují podrobné informace o zpracovaných osobních údajích v rámci ZZS ZK a způsobech, jakými jsou tyto údaje zpracovávány a chráněny.

8. **Jaká opatření jste přijali k zajištění transparentnosti a informovanosti pacientů o tom, jak jsou jejich osobní údaje zpracovávány?**

„Na svých webových stránkách zveřejnila ZZS ZK informace týkající se zpracování osobních údajů.“

Komentář: Zveřejnění informací týkající se ochrany osobních údajů přispívá k transparentnosti a zvýšení důvěry pacientů ohledně jejich osobních údajů. Zároveň mají lidé snadnější přístup k informacím ohledně kompetentních osob, na které se obrátit v souvislosti s ochranou osobních údajů.

9. **Máte uzavřené smlouvy s poskytovateli služeb, kteří mají přístup k osobním údajům pacientů, a zabezpečujete, aby i tito poskytovatelé dodržovali pravidla GDPR?**

„Ano, jsou uzavřeny smlouvy o zpracování osobních údajů podle čl. 28 GDPR s poskytovateli služeb, a to s poskytovateli IT služeb a s poskytovateli služeb v oblasti mzdového účetnictví.“

Komentář: Tyto smlouvy ukazují odpovědný přístup ZZS ZK k ochraně osobních údajů všech subjektů, a jsou také důležité pro stanovení práv a povinností třetích stran. To znamená, že i tito poskytovatelé služeb jsou povinni dodržovat pravidla a požadavky na ochranu osobních údajů dle GDPR.

10. **Jak často provádíte revize a aktualizace vaší politiky ochrany osobních údajů v souladu s aktuálními legislativními požadavky?**

„Revize a aktualizace jsou prováděny průběžně podle potřeby, v závislosti na vývoji právní úpravy a na vývoji rozhodovací praxe v oblasti ochrany osobních údajů.“

Komentář: Průběžná revize je podstatná pro reakce na změny v právní úpravě ochrany osobních údajů. Tím, že ZZS ZK reaguje na vývoj legislativních požadavků, je schopná reagovat na nové potřeby týkající se ochrany osobních údajů.

11. Jak reagujete na případné bezpečnostní incidenty, které mohou ohrozit bezpečnost osobních údajů pacientů a jaké jsou vaše postupy pro hlášení těchto incidentů dozorovým orgánům a dotčeným osobám?

„K takovému bezpečnostnímu incidentu dosud v naší praxi nedošlo. Máme zpracovány ve vnitřních předpisech postupy v souladu s nařízením GDPR pro případ výskytu bezpečnostních událostí a bezpečnostních incidentů a rovněž také postupy pro hlášení dozorovým orgánům a informování dotčených osob.“

Komentář: Z odpovědi vyplývá, že ZZS ZK má připravené postupy na možné bezpečnostní incidenty. Důležitý je také stanovený postup pro ohlašování incidentů dozorovým orgánům a v případě výskytu bezpečnostního incidentu, který musí být v souladu s GDPR. Významným prvkem je i vytvořený postup informování dotčených osob v případě bezpečnostního incidentu a případných dopadech na jejich osobní údaje.

12. Byly v minulosti nějaké problémy s ochranou osobních údajů u zdravotnické záchranné služby?

„Ne, nebyly.“

Komentář: I přes nezaznamenání problémů týkající se ochrany osobních údajů u ZZS ZK v minulosti je i nadále potřeba udržovat a zlepšovat opatření, která ZZS ZK uplatňuje. Tím bude moci ZZS ZK čelit novým výzvám a potencionálním hrozbám v ochraně osobních údajů.

7.2 SWOT analýza organizace

Na základě získaných informací z expertního rozhovoru a vlastního zjištění se nyní práce zaměří na metody analýzy rizik What-If a SWOT analýzu. První metodou bude SWOT analýza, která se zaměří na silné stránky (strenghts), slabé stránky (weaknesses), příležitosti (opportunities) a hrozby (threats). SWOT analýzu jsem využil pro systematické zhodnocení současného stavu ochrany osobních údajů u ZZS ZK s cílem identifikace důležitých parametrů, které slouží pro dosažení stanovených cílů.

Tabulka 1 – Prvky SWOT analýzy (vlastní zpracování, 2024).

Silné stránky:	**Slabé stránky:**
• Transparentnost • Profesionální personál • Postupy a směrnice • Důvěryhodnost • Bezpečnostní opatření	• Bezpečnostní incidenty • Zkušenosti • Finanční prostředky • Personální zabezpečení • Administrativa
Příležitosti:	**Hrozby:**
• Implementace nových technologií • Edukace veřejnosti • Tvorba strategií • Efektivita procesů • Externí spolupráce	• Kybernetické útoky • Nedostatečné školení zaměstnanců • Nekalost pacientů • Legislativa

Silné stránky

Transparentnost – Každá osoba má právo požadovat umožnění přístupu k osobním údajům, změnu nebo opravu nepřesných osobních údajů a žádat vymazání osobních údajů vůči ZZS ZK prostřednictvím pověřence pro ochranu osobních údajů.

Profesionální personál – Zaměstnanci jsou důsledně seznámeni s nejnovějšími postupy a směrnicemi uvnitř organizace pro ochranu a zabezpečení osobních údajů. Zaměstnanci taktéž absolvují školení týkající se ochrany osobních údajů.

Postupy a směrnice – Tyto dokumenty jasně stanovují nezbytné kroky, kterými se dodržují požadavky na ochranu osobních údajů a zajišťují bezpečnost během celé zpracovatelské operace osobních údajů.

Důvěryhodnost – Přesně stanovená pravidla pro ochranu osobních údajů spolu s transparentností vzbuzují u pacientů pocit důvěryhodnosti vůči ZZS ZK a tím přispívají k vzájemné lepší spolupráci během poskytování zdravotnických služeb a pacienti nemají strach o předávání svých osobních údajů.

Bezpečnostní opatření – Přijatá bezpečnostní opatření u ZZS ZK chrání před neoprávněnými přístupy nebo kybernetickými útoky. Tato bezpečnostní opatření minimalizují riziko spojené s výpadky systému, odcizením nebo ztráty osobních údajů pacientů.

Slabé stránky

Bezpečnostní incidenty – Bezpečnostní incidenty mohou způsobit vážné následky během ochrany osobních údajů. Při takovém bezpečnostním incidentu by mohlo dojít k úniku nebo zneužití osobních údajů pacientů.

Zkušenosti – U ZZS ZK dosud k bezpečnostnímu incidentu nedošlo, tudíž není v praxi vyzkoušen postup pro ohlašování bezpečnostních incidentů dozorovému orgánu. Je proto důležité v případě vyskytnutí takového problému postupovat dle daných vnitřních postupů organizace a dodržovat všechny směrnice a postupy.

Finanční prostředky – Omezené finanční prostředky z důvodu financování z veřejných rozpočtů mohou snížit množství financí vynakládané na ochranu osobních údajů. Organizace také může čelit porušení právních předpisů, a tudíž i nákladům na náhradu škod, což může vést k pokutám a soudním sporům.

Personální zabezpečení – Kvalifikované požadavky na osobu pověřence pro ochranu osobních údajů jsou velmi vysoké. Důležité tedy je zabezpečení této pozice odborníkem, který má dostatečné finanční ohodnocení, odbornost a nemá v organizaci střet zájmů.

Administrativa – Zpracování a uchovávání veškeré dokumentace s osobními údaji v souladu s právními předpisy je nutné osobně řešit a zvyšuje administrativní zátěž.

Příležitosti

Implementace nových technologií – Technologie, která by dokázala rychle a včas identifikovat možné bezpečnostní incidenty, včetně monitoringu a kontroly přístupu k osobním údajům pacientů.

Edukace veřejnosti – Pořádání workshopů nebo vytvoření informačních letáků pro širokou veřejnost, kde by se nacházeli informace a rady pro bezpečné zacházení s osobními údaji.

Tvorba strategií – Vytvoření komplexní strategie, která by analyzovala současnou situaci ochrany osobních údajů, zhodnotila by stav zabezpečení a identifikovala potencionální konkrétní možná rizika a hrozby pro ochranu osobních údajů.

Efektivita procesů – Digitalizace osobních údajů a s tím spojená automatizace, která by umožňovala bezpečnější a snadnější nakládání s osobními údaji a zároveň by dokázala rychlejší zpracování osobních údajů pacientů.

Externí spolupráce – Spolupráce s odbornými firmami pro provádění pravidelných auditů a využití firem pro implementaci bezpečnostních opatření.

Hrozby

Kybernetické útoky – Tyto útoky by mohly způsobit vážné následky, během nichž by mohlo dojít k úniku osobních údajů pacientů, dojít k výpadkům informačních systémů a tím omezit poskytování zdravotnické péče pacientům nebo poškodit či zničit zdravotní záznamy s údaji pacientů.

Nedostatečné školení zaměstnanců – Zaměstnanci ZZS ZK by mohli z důvodu nedostatečného školení při zacházení s osobními údaji porušovat právní předpisy, tím ohrozit bezpečnost těchto údajů a zvýšit riziko výskytu bezpečnostních incidentů.

Nekalost pacientů – Neochota nebo nespolupráce pacientů by mohla vést k omezení poskytované zdravotnické péče z důvodu neposkytnutí relevantních osobních údajů a tím ztížit možnosti léčby a správné diagnózy.

Legislativa – Dynamika v přijímání nových právních předpisů by mohla způsobit změnu dosavadních aplikovaných opatření a požadavků na ochranu osobních údajů a mohla by způsobit větší tlak na nové prostředky ochrany osobních údajů.

Nyní jsem shrnul rozbor všech parametrů v závislosti na jejich váze a bodech. Uvedené body jsou v rozmezí 1 až 5, přičemž čím nižší číslo, tím menší spokojenost s daným parametrem.

7.2.1 Parametry vnitřního prostředí

Tabulka 2 – Hodnocení silných stránek (vlastní zpracování, 2024).

Silné stránky	**Body**	**Váha**	**Výsledek**
Transparentnost	3	0,10	0,30
Profesionální personál	5	0,30	1,50
Postupy a směrnice	4	0,30	1,20
Důvěryhodnost	3	0,10	0,30
Bezpečnostní Opatření	4	0,20	0,80
	<1; 5>	**∑ 1**	**∑ 4,10**

Nejvyššího hodnocení ze silných stránek dosáhl profesionální personál, následovaly postupy a směrnice, bezpečnostní opatření, důvěryhodnost a transparentnost.

Tabulka 3 – Hodnocení slabých stránek (vlastní zpracování, 2024).

Slabé stránky	**Body**	**Váha**	**Výsledek**
Bezpečnostní incidenty	-3	0,20	-0,60
Zkušenosti	-4	0,30	-1,20
Finanční prostředky	-2	0,10	-0,20
Personální zabezpečení	-3	0,20	-0,60
Administrativa	-3	0,20	-0,60
	<-1; -5>	**∑ 1**	**∑ -3,20**

Nejvýše hodnocenou slabou stránkou jsou zkušenosti, následují bezpečnostní incidenty, personální zabezpečení, administrativa a finanční prostředky.

Celková hodnota parametrů vnitřního prostředí je 0,90, neboť silné stránky převyšují nad slabými stránkami.

7.2.2 Parametry vnějšího prostředí

Tabulka 4 – Hodnocení příležitostí (vlastní zpracování, 2024).

Příležitosti	Body	Váha	Výsledek
Implementace nových technologií	2	0,15	0,30
Edukace veřejnosti	4	0,40	1,60
Tvorba strategií	4	0,20	0,80
Efektivita procesů	3	0,15	0,45
Externí spolupráce	2	0,10	0,20
	<1; 5>	**∑ 1**	**∑ 3,35**

Nejvýše hodnocená příležitost je edukace veřejnosti, následuje tvorba strategií, efektivita procesů, implementace nových technologií a externí spolupráce.

Tabulka 5 – Hodnocení hrozeb (vlastní zpracování, 2024).

Hrozby	Body	Váha	Výsledek
Kybernetické útoky	-4	0,40	-1,60
Nedostatečné školení zaměstnanců	-3	0,30	-0,90
Nekalost pacientů	-2	0,20	-0,40
Legislativa	-2	0,10	-0,20
	<-1; -5>	**∑ 1**	**∑ -3,1**

Největší hrozbou jsou kybernetické útoky, následuje nedostateční školení zaměstnanců, nekalost pacientů a legislativa.

Celková hodnota parametrů vnějšího prostředí je 0,25, protože příležitosti převažují nad hrozbami.

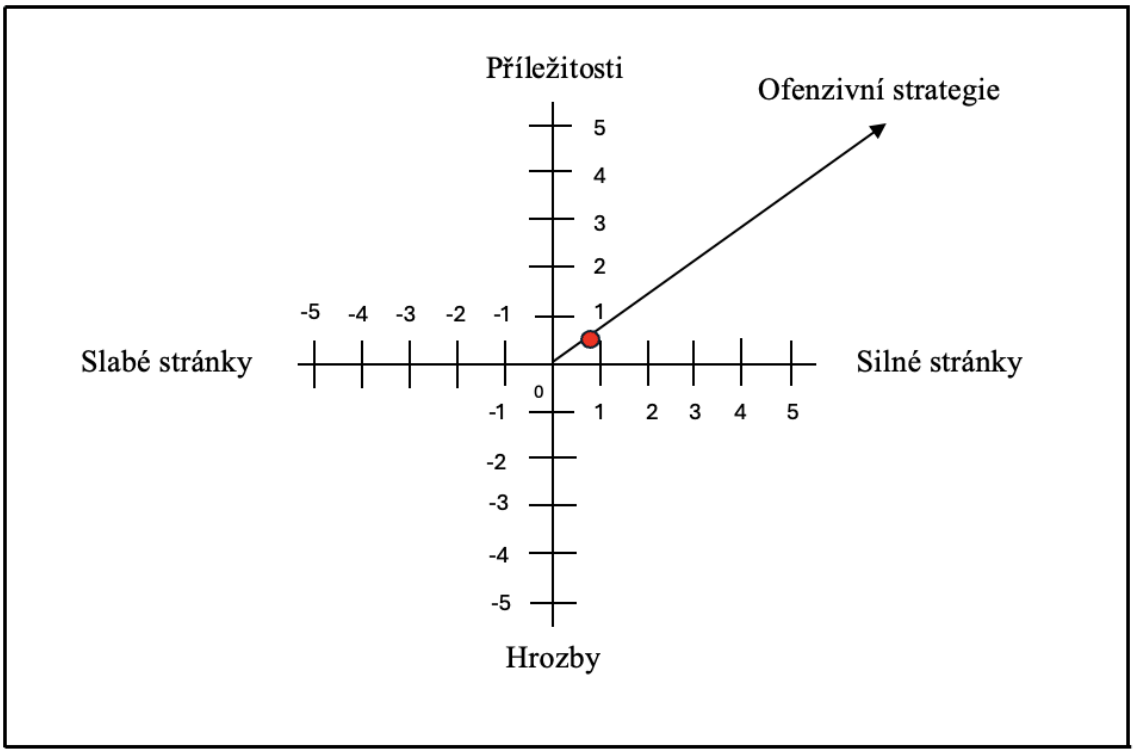
7.2.3 Zhodnocení SWOT analýzy

V následující tabulce jsou uvedeny nejsilnější parametry SWOT analýzy, které nejvíce ovlivňují výslednou strategii. Jelikož je součet parametrů vnitřního prostředí 0,90 a součet parametrů vnějšího prostředí 0,25, výsledná strategie vyšla jako ofenzivní.

Tabulka 6 – Nejsilnější parametry SWOT analýzy (vlastní zpracování, 2024).

	Pozitivní	**Negativní**
Vnitřní prostředí	• Profesionální personál	• Zkušenosti
Vnější prostředí	• Edukace veřejnosti	• Kybernetické útoky

Pro přehlednější výsledky SWOT analýzy byl vypracován následující graf, na kterém je zobrazen součet vnitřních a vnějších parametrů a výsledná strategie.



Obrázek 8 – Vyhodnocení SWOT analýzy (vlastní zpracování, 2024).

7.3 WHAT-IF analýza

Druhou analýzou bude metoda What-If (Co se stane, když...), která zhodnotí možné hrozby, následky a opatření pro ochranu osobních údajů u ZZS ZK. Tuto metodu jsem zvolil z důvodu identifikace možných hrozeb mířících na ochranu osobních údajů, odhadů následků a návrhů opatření k těmto hrozbám. Možné příčiny mohou být způsobeny jak lidskou chybou, tak technickými prostředky. Použitím této analýzy lze odhadnout jednotlivé následky a dopady konkrétních hrozeb, to zároveň umožňuje přijmout taková opatření, která budou sloužit k minimalizaci následků těchto hrozeb.

Tabulka 7 – Analýza What-If (vlastní zpracování, 2024).

Pořadové číslo	Příčina	Následek	Návrh opatření k minimalizaci
1	Pacient odmítne poskytnout své osobní údaje	Omezení poskytované péče	Poučení pacientů o důležitosti poskytnutí osobních údajů
2	Pacient poskytne nepravé osobní údaje	Nesprávná zdravotní péče	Ověření osobních údajů pacienta
3	Neoprávněné osoby získají přístup k osobním údajům	Zneužití osobních údajů	Přístup k osobním údajům pomocí oprávnění
4	Neúplné odstranění osobních údajů	Porušení interních předpisů	Jasně stanovený způsob odstranění osobních údajů, (softwarový nástroj pro automatizované odstranění údajů)
5	Únik údajů zvláštní kategorie	Porušení důvěrnosti a soukromí	Zabezpečená komunikace (použití moderních šifrovaných metod)
6	Ztráta fyzického nosiče osobních údajů	Narušení bezpečnosti údajů	Fyzické zabezpečení nosiče osobních údajů (režimová opatření)
7	Nedostatečná znalost právních předpisů	Nedodržení zákonů	Pravidelná aktualizace interních předpisů
8	Nedostatečné finanční náklady na ochranu osobních údajů	Omezené prostředky vynakládané na zabezpečení osobních údajů	Efektivní využívání dostupných zdrojů financí
9	Únik osobních údajů poskytovatelům služeb	Vypovězení smlouvy s poskytovateli služeb	Smluvní závazky pro dodržování standardů ochrany údajů
10	Nedostatečné školení zaměstnanců	Nedodržení postupů při správě osobních údajů	Pravidelné školení pro všechny zaměstnance

11	Nedodržení bezpečnostních standardů	Narušení práv pacientů	Pravidelné audity a kontroly
12	Kybernetický útoky	Odcizení osobních údajů	Záloha údajů, monitoring bezpečnostních hrozeb, aktualizace softwaru
13	Nedostatečná odbornost pověřence pro ochranu osobních údajů	Špatné zhodnocení ochrany osobních údajů	Odborný rozvoj kompetencí pověřence a pravidelné sledování stavu ochrany osobních údajů

Příčiny – pomocí What-If analýzy byl zjištěn výčet možných scénářů hrozeb, které by mohly zasáhnout ochranu osobních údajů u ZZS ZK. Tyto příčiny se týkají nekalosti pacientů, špatného zacházení s osobními údaji, zneužití údajů, odcizení údajů nebo kybernetických útoků vedených proti ZZS ZK a nedostatečné edukace zaměstnanců.

Následky – prostřednictvím What-If byly identifikovány možné následky jednotlivých hrozeb a jejich dopady. Ať už se jedná o následky způsobené nekalostí pacientů, dále možné důsledky odcizení jako porušení právních předpisů nebo výpovědí smluv s jinými poskytovateli služeb. V neposlední řadě důsledky těchto hrozeb mohou být odcizené osobní údaje a jejich zneužití.

Návrhy opatření k minimalizaci – Pomocí What-If analýzy byla navrhnuta jednotlivá opatření ke konkrétním příčinám. Každá konkrétní příčina a její následek lze minimalizovat přijetím odpovídajícího návrhu, který bude dostatečně reflektovat významnost a dopad této hrozby. Jedná se především o oblasti edukace a pravidelného školení personálu, jasně stanovených postupů a pravidel, moderní technologie, přijaté bezpečnostní opatření a důslednost při zacházení s osobními údaji.

8 CELKOVÉ VYHODNOCENÍ A NÁVRHY NA ZLEPŠENÍ

V této kapitole jsou shrnuta zjištění z praktické části práce. Prostřednictvím expertního rozhovoru s pověřencem pro ochranu osobních údajů byl popsán a okomentován současný stav ochrany osobních údajů ZZS ZK. SWOT analýza sloužila k identifikaci silných a slabých stránek, příležitostí a hrozeb. Součtem vnitřních a vnějších parametrů byla zjištěna ofenzivní strategie. V této strategii převažují silné stránky nad slabými a příležitosti nad hrozbami. What-If analýza se zaměřuje na 13 možných hrozeb spojených s ochranou osobních údajů, přičemž je ke každé hrozbě přiřazen jeden následek a následné opatření k minimalizaci následků.

K případnému výskytu bezpečnostního incidentu by měl být vytvořen typ pohotovostního plánu pro řešení konkrétních bezpečnostních incidentů, který by obsahoval postupy a kompetence jednotlivých osob v rámci organizace pro minimalizaci škod a rychlé efektivní nápravě. Podstatné je, aby byl tento plán pravidelně, minimálně jednou ročně aktualizován, a byli s ním seznámeni všichni zaměstnanci. Dalším důležitým prvkem zabezpečení je průběžný systém kontrol bezpečnostních opatření a postupů, který může odhalit potencionální slabiny v zabezpečení osobních údajů. Tyto kroky by bylo vhodné otestovat v rámci uspořádaného cvičení, které by reflektovalo možné hrozby a tím vyzkoušelo jednotlivá přijatá bezpečnostní opatření. Vzhledem k omezeným finančním zdrojům je potřeba přijímat efektivní opatření v rámci organizace, a to investicí do moderních bezpečnostních technologií, které umožní kvalitní šifrování údajů při jejich přenosu jak v rámci ZZS ZK, tak s externími poskytovateli služeb a také včasnou detekci a prevenci bezpečnostních incidentů.

Další finanční prostředky by měly být směřovány do posílení pravidelného školení zaměstnanců, které je v tomto případě zásadní. Kvalitně a pravidelně školený personál může reagovat na možné hrozby, což v konečném důsledku může snížit náklady spojené s řešením bezpečnostním incidentů. Zároveň bude kvalitně vyškolený personál vystupovat vůči pacientům velmi profesionálně, což také zvýší důvěru veřejnosti během výkonů činností ZZS ZK.

Pro zajištění účinné ochrany osobních údajů je zásadní i z pohledu legislativy, zajistit odpovědnou osobu, v tomto případě pověřence pro ochranu osobních údajů, který svými kvalifikovanými schopnostmi dokáže implementovat a udržovat přijatá bezpečnostní opatření a zároveň včas identifikovat možné bezpečnostní incidenty. V rámci možných bezpečnostních incidentů v budoucnu, by bylo vhodné zřízení specializovaného bezpečnostního týmu,

který by se zaměřil na zabezpečení osobních údajů. Tento tým by měl za úkol i monitorování bezpečnostních hrozeb.

V rámci lepší administrativy by bylo vhodné zavést modernější informační systém, který by ukládal a spravoval osobní údaje. Zároveň by byl zabezpečených úložištěm osobních údajů a obsahoval by také správu oprávnění jednotlivých osob. Vytvoření takového systému by pomohlo administrátorům k lepšímu přehledu oprávnění a tím k vyšší bezpečnosti přístupu i minimalizaci neoprávněného přístupu. Například by se dala využít dvoufaktorová autentizace, při které by musela dotyčná osoba použít pro přihlášení dvě rozdílné informace z odlišných nezávislých zdrojů. Toto opatření by vedlo k omezení přístupových práv, například k citlivým osobním údajům ze zdravotní dokumentace a umožnilo přístup pouze oprávněným osobám.

Pro posílení ochrany před kybernetickými útoky cílenými na osobní údaje pacientů či zaměstnanců ZZS ZK by bylo vhodné stanovit pravidla v rámci prevence před možnými případy kybernetických útoků. Ať už by se jednalo o softwarové nebo hardwarové systémy, které pomohou k ochraně dat při jejich zpracování či přenosu.

ZZS ZK by mohla na svých internetových stránkách sestavit přehled pravidel, které by přispěly ke zlepšení a zabezpečení toho, že jsou pacienti informováni, komu a za jakým účelem budou jejich osobní údaje poskytnuty. Spolu s edukací pacientů o jejich právech a povinnostech během poskytování zdravotnických služeb, by vybudovaná větší důvěra přispěla k tomu, že pacienti budou přesvědčeni o důležitosti ochrany osobních údajů a důsledcích nezodpovědného nakládání s nimi.

Vytvoření pravidelných konferencí a vzdělávacích seminářů na problematiku ochrany osobních údajů ve zdravotnictví by mohlo povznést povědomí o ochraně osobních údajů u pacientů a různých zdravotnických zařízení napříč celou ČR. Tyto akce by mohla doprovodit online kampaň, kde by se uveřejňovaly články a tipy s doporučeními pro správné zacházení s osobními údaji.

ZÁVĚR

Bakalářská práce se zabývala problematikou ochrany osobních údajů v oblasti ochrany obyvatelstva. Práce se skládá ze dvou částí, teoretické a praktické. Teoretická část je tvořena pěti kapitolami. V první kapitole teoretické části byl popsán světový a evropský vývoj ochrany osobních údajů a také vývoj této problematiky na území ČR. Druhá kapitola se věnovala charakteristice odborné terminologie důležité pro pochopení celé problematiky a právního základu v oblasti ochrany osobních údajů. Třetí kapitola se zabývala Obecným nařízením o ochraně osobních údajů neboli GDPR, a přiblížila institut pověřence pro ochranu osobních údajů a dozorový orgán ÚOOÚ. Ve čtvrté kapitole byla popsána bezpečnost ochrany osobních údajů jak z pohledu zabezpečení, tak porušení zabezpečení osobních údajů. V poslední, páté kapitole, byl proveden dílčí závěr teoretické části a popsány použité metody.

Praktická část se skládá ze tří kapitol. Šestá kapitola se věnuje popisu ZZS ZK, a to její historii, současnosti a organizační struktuře. Sedmá kapitola práce je zaměřena na analýzu ochrany osobních údajů u ZZS ZK. Použité analýzy a metody byly expertní rozhovor, SWOT analýza a What-If. Expertní rozhovor s pověřencem pro ochranu osobních údajů obsahoval 12 otázek a sloužil ke komplexnějšímu přehledu o ochraně osobních údajů. Ve SWOT analýze, která sloužila pro identifikaci silných a slabých stránek, příležitostí a hrozeb, byly přiřazeny body a váhy jednotlivým parametrům u každého kvadrantu. Výsledná strategie této analýzy vyšla jako ofenzivní. Další analýzou byla What-If, ve které bylo vymezeno 13 možných hrozeb, které by mohly zasáhnout ochranu osobních údajů. Tato analýza následně přiřadila k těmto hrozbám následky a návrhy možných opatření k minimalizaci následků.

Hlavním cílem bylo na základě provedené analýzy vybrané složky integrovaného záchranného systému, konkrétně Zdravotnické záchranné služby Zlínského kraje, s důrazem na ochranu osobních údajů vyhodnotit dosažené výsledky a vypracovat návrhy na zlepšení. Dílčí cíle práce byly stanoveny jako popsat základní problematiku ochrany osobních údajů a provést komplexní analýzu ochrany osobních údajů u vybrané složky integrovaného záchranného systému. Hlavní i dílčí cíle práce byly splněny.

SEZNAM POUŽITÉ LITERATURY

BUCKBEE, Michael, 2022. *GDPR Data Breach Guidelines*. Online. Varonis. Dostupné z: https://www.varonis.com/blog/guide-eu-gdpr-breach-notification-rule. [cit. 2024-01-07].

ČESKO, 1993. Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky. In: *Sbírka zákonů České republiky*. 1/1993. Dostupné také z: https://www.e-sbirka.cz/sb/1993/2?f=lzps&zalozka=text.

ČESKO, 2011. Zákon o zdravotnické záchranné službě. In: *Sbírka zákonů*. 131/2011. Dostupné také z: https://www.e-sbirka.cz/sb/2011/374?zalozka=text.

ČESKO, 2011. Zákon o zdravotních službách a podmínkách jejich poskytování. In: *Sbírka zákonů*. 131/2011. Dostupné také z: https://www.e-sbirka.cz/sb/2011/372?zalozka=text.

GAL, Michal S a AVIV, Oshrit, 2020. The Competitive Effects of the GDPR. Online. *Journal of Competition Law and Economics*. 2020-09-09, roč. 16, č. 3, s. 349-391. ISSN 1744-6414. Dostupné z: https://doi.org/10.1093/joclec/nhaa012. [cit. 2023-12-19].

GDPR Top Ten #9: Security and breach notification, c2024. Online. Deloitte. Dostupné z: https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-security-and-breach-notification.html. [cit. 2024-01-09].

Historie Úřadu, c2024. Online. Úřad pro ochranu osobních údajů. Dostupné z: https://uoou.gov.cz/urad/historie-uradu. [cit. 2024-01-02].

Historie, c2024. Online. ZZS ZK. Dostupné z: http://www.zzszk.cz/historie/. [cit. 2024-03-09].

JANEČKOVÁ, Eva, 2020. *GDPR: řešení problémů v praxi škol*. Právo pro praxi. Praha: Grada Publishing. ISBN 978-80-271-2579-1.

KE, T. Tony a SUDHIR, K., 2023. Privacy Rights and Data Security: GDPR and Personal Data Markets. Online. *Management Science*. Roč. 69, č. 8, s. 4389-4412. ISSN 0025-1909. Dostupné z: https://doi.org/10.1287/mnsc.2022.4614. [cit. 2023-12-19].

Konsolidované znění Smlouvy o fungování Evropské unie, 2016. Online. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:12016E016.

Listina základních práv Evropské unie, 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:12016P008.

MELOTÍKOVÁ, Petra, 2020. *Osobní údaje v kontextu GDPR*. Teoretik. Praha: Leges. ISBN 978-80-7502-507-4.

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), 2016. Dostupné také

z: https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/gdpr-dokumenty/2017/11/Narizeni-EU-2016679_GDPR.pdf.

NAVRÁTIL, Jiří, 2018. *GDPR pro praxi*. Pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-807-3806-897.

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

Ochrana osobních údajů dle GDPR, 2021. Online. Businessinfo.cz. Dostupné z: https://www.businessinfo.cz/navody/ochrana-osobnich-udaju-ppbi/3/. [cit. 2024-01-2].

Organizační struktura, c2024. Online. Úřad pro ochranu osobních údajů. Dostupné z: https://uoou.gov.cz/urad/organizacni-struktura. [cit. 2024-01-03].

Postavení Úřadu, c2024. Online. Úřad pro ochranu osobních údajů. Dostupné z: https://uoou.gov.cz/urad/postaveni-uradu. [cit. 2024-01-03].

Pověřenec pro ochranu osobních údajů, c2023. Online. Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/gdpr/clanek/poverenec-pro-ochranu-osobnich-udaju-poverenec-pro-ochranu-osobnich-udaju.aspx. [cit. 2024-01-04].

Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?, 2018. Online. Epravo.cz. Dostupné z: https://www.epravo.cz/top/clanky/poverenec-pro-osobni-udaje-dle-gdpr-kdy-koho-a-jak-poverit-107265.html. [cit. 2024-01-12].

Právní předpisy, c2013. Online. Úřad pro ochranu osobních údajů. Dostupné z: https://uoou.gov.cz/pravni-ramec/ochrana-osobnich-udaju/pravni-predpisy. [cit. 2024-01-12].

Secure personal data, 2016. Online. European Data Protection Board. Dostupné z: https://edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en. [cit. 2024-01-08].

Statistika, c2024. Online. ZZS ZK. Dostupné z: http://www.zzszk.cz/statistika/. [cit. 2024-03-15].

Úvod do problematiky GDPR, GDPR pro e-shopy, 2018. Online. Businessinfo.cz. Dostupné z: https://www.businessinfo.cz/navody/uvod-do-gdpr-eshopy-ppbi/2/#subjekt-udaju. [cit. 2024-01-5].

VOIGT, Paul a BUSSCHE, Axel von dem, 2017. *The EU general data protection regulation (GDPR): a practical guide*. Cham: Springer. ISBN 978-3-319-57958-0.

Zabezpečení osobních údajů, c2023. Online. Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zabezpeceni-osobnich-udaju.aspx. [cit. 2024-01-12].

Základní informace, c2024. Online. Zdravotnická záchranná služba Zlínského kraje, p.o. Dostupné z: http://www.zzszk.cz/zakladni-informace/. [cit. 2024-03-08].
ZZS ZK, c2024. Online. ZZS ZK. Dostupné z: http://www.zzszlin.cz/. [cit. 2024-03-10].

ŽŮREK, Jiří, 2022. *GDPR v personalistice*. 2. doplněné vydání. Práce, mzdy, pojištění. Olomouc: ANAG. ISBN 978-80-7554-365-3.

ŽŮREK, Jiří, 2018. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Právo (ANAG). Olomouc: ANAG. ISBN 978-807-5541-529.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR	Česká republika
EU	Evropská unie
GDPR	Obecné nařízení o ochraně osobních údajů
LZPS	Listina základních práv a svobod
PNP	Přednemocniční neodkladná péče
ÚOOÚ	Úřad pro ochranu osobních údajů
ZOS	Zdravotnické operační středisko
ZZS ZK	Zdravotnická záchranná služba Zlínského kraje, p.o.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OTÁZKY PRO EXPERTNÍ ROZHOVOR

Otázky položené pověřenci pro ochranu osobních údajů Zdravotnické záchranné služby Zlínského kraje, p.o.:

1) Jaké osobní údaje jsou shromažďovány a zpracovávány Zdravotnickou záchrannou službou Zlínského kraje?
2) Jakým způsobem je zajištěna ochrana osobních údajů pacientů během poskytování zdravotnických služeb v rámci záchranné služby?
3) Jak dlouho jsou osobní údaje pacientů uchovávány a jaký je postup jejich odstranění po uplynutí příslušné doby?
4) Jaký postup máte pro shromažďování a uchovávání citlivých zdravotních údajů pacientů v souladu s požadavky GDPR?
5) Jak je zajištěn informovaný souhlas pacientů s ohledem na GDPR?
6) Jak jsou školeni zaměstnanci zdravotnické záchranné služby ohledně správy osobních údajů a zabezpečení proti jejich ztrátě či neoprávněnému přístupu?
7) Máte vytvořený dokument, který popisuje, jaké konkrétní typy osobních údajů zpracováváte v rámci zdravotnické záchranné služby a jak s nimi zacházíte?
8) Jaká opatření jste přijali k zajištění k zajištění transparentnosti a informovanosti pacientů o tom, jak jsou jejich osobní údaje zpracovávány?
9) Máte uzavřené smlouvy s poskytovateli služeb, kteří mají přístup k osobním údajům pacientů, a zabezpečujete, aby i tito poskytovatelé dodržovali pravidla GDPR?
10) Jak často provádíte revize a aktualizace vaší politiky ochrany osobních údajů v souladu s aktuálními legislativními požadavky?
11) Jak reagujete na případné bezpečnostní incidenty, které mohou ohrozit bezpečnost osobních údajů pacientů a jaké jsou vaše postupy pro ohlášení těchto incidentů dozorovým orgánům a dotčeným osobám?
12) Byly v minulosti nějaké problémy s ochranou osobních údajů u zdravotnické záchranné služby?