Best practices ochrany osobních údajů vybraného subjektu

Bc. Martina Capitová

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Martina Capitová**
Osobní číslo:	**L19590**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Studijní obor:	**Rizikové inženýrství**
Forma studia:	**Kombinovaná**
Téma práce:	**Best practices ochrany osobních údajů vybraného subjektu**

Zásady pro vypracování

1. Zpracujte literární rešerši současného stavu v oblasti best practices ochrany osobních údajů.
2. Analyzujte proces posuzování ochrany osobních údajů u vybrané skupiny subjektů.
3. Specifikujte subjekt pro ochranu osobních údajů.
4. Na základě best practices posuďte ochranu osobních údajů vybraného subjektu.

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

Seznam doporučené literatury:

1. IT GOVERNANCE PRIVACY TEAM. *EU General Data Protection Regulation (GDPR)*. Second edition. United Kingdom: IT Governance Publishing, 2017. ISBN 978-1-84928-946-7.
2. JANEČKOVÁ, Eva. *GDPR: řešení problémů v praxi obcí*. Praha: Grada Publishing. Právo v praxi, 2019. ISBN 978-80-247-2925-1.
3. TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey PA: Information Science Reference, 2019. ISBN 9781522594901.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2020**
Termín odevzdání diplomové práce: **14. května 2021**

L.S.

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

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou 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 – diplomovou 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 diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 7. 5. 2021

Jméno a příjmení studenta: Bc. Martina Capitová

…….
podpis studenta

ABSTRAKT

Diplomová práce se zabývá problematikou ochrany osobních údajů v souvislosti s právní úpravou této oblasti na základě implementovaného obecného nařízení GDPR. Předkládaná práce se zabývá posouzením vlivu na ochranu osobních údajů fyzických osob, která úzce souvisí s oblastí zabezpečení osobních údajů. Následně zajistit eliminaci zjištěných rizik a zabezpečit tak lepší a efektivnější ochranu osobních údajů. Diplomová práce je zaměřena na oblast veřejné správy. Získané poznatky jsou využitelné při implementaci pravidel GDPR a dobré praxe ve veřejné správě. Teoretická část definuje základní pojmy, legislativní dokumenty a poznatky z odborné literatury, které souvisí s problematikou ochrany osobních údajů. Praktická část je zaměřena na zpracování osobních údajů v kontextu činností obce, posouzení vlivu na ochranu osobních údajů a návrhu opatření k zajištění technického a organizačního zabezpečení.

Klíčová slova: obecné nařízení, ochrana osobních údajů, posouzení vlivu na ochranu osobních údajů, riziko.

ABSTRACT

The diploma thesis deals with the issue of personal data protection in connection with the legal regulation of this area on the basis of the implemented general regulation GDPR. The presented work deals with the assessment of the impact on the protection of personal data of individuals, which is closely related to the areas of personal data security. Then eliminate the risks to ensure better and more effective protection of personal data. The diploma thesis is focused on public administration. The acquired knowledge is used in the implementation of GDPR rules and Best practices in public administration. The theoretical part defines the basic concepts, legislative documents and knowledge from the literature that are related to the issue of personal data protection. The practical part is focused on the processing of personal data in the context of the activities of the municipality, the assessment of the impact on personal data protection and the proposal of measures to ensure technical and organizational security.

Keywords: general regulation, personal data protection, personal data protection impact assessment, risk.

Poděkování

Ráda bych touto cestou poděkovala vedoucímu mé diplomové práce Ing. Petru Svobodovi, Ph.D., za jeho vstřícné vedení, spolupráci a cenné informace. V neposlední řadě patří veliké díky manželovi, který mě ke studiu na vysoké škole motivoval. Obětavým rodičům, kteří nám během studií byli velkou oporou při výchově a hlídání našich synů a zároveň významnou podporou v cestě za našim cílem. Odměnou jim budiž to, že na nás můžou být pyšní.

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

OBSAH

ÚVOD

Spolu s rozvojem informačních technologií se informace změnily v cenné aktivum. Rizika nevznikají z vnějších jevů, ale z lidských rozhodnutí a činů, které souvisejí s řízením a využívánímp informací sociálních skupin, vlád, podniků a jednotlivců. Internet jako technologická infrastruktura podpořil realizaci nové oblasti komunikace mezi sociálními entitami v kontextu soukromého života.

Diplomová práce je zaměřená na jedno z aktuálních témat v současném období, kterou bezpochyby ochrana osobních údajů je. Odborná, ale i laická veřejnost vlivem informací a dezinformací vnímá současnou právní úpravu v oblasti ochrany osobních údajů jako zbytečnou byrokratickou zátěž vymyšlenou Evropskou unií.

Obecné nařízení o ochraně osobních údajů vstoupilo v platnost v květnu 2018 a přineslo mnohé změny, ale i výhody pro jednotlivce, kteří poskytují své údaje při využívání různých služeb a činností běžného dne. Organizace zpracovávající osobní údaje byly přinuceny provést ve svém prostředí komplexní změny, a to v takovém rozsahu, aby bylo dosaženo úspěšné implementace General Data Protection Regulation (dále jen, „GDPR“) v rámci organizace. Cílem nové legislativy je navrátit fyzickým osobám kontrolu nad zpracováním osobních údajů.

Předkládaná diplomová práce je zaměřena na posouzení vlivu ochrany osobních údajů a Best practices v oblasti zpracování osobních údajů v kontextu činností vykonávaných v rámci agendy obce. Výstupy z Data Protection Impact Assessment (dále jen „DPIA“) slouží jako základ pro konzultaci se zainteresovanými stranami. Výhodami provedeného posouzení je identifikace rizik a vyhodnocení jejich potenciálního dopadu na subjekty údajů a správce, zajištění souladu s požadavky právních předpisů, prevence proti incidentům, snížení nákladů na realizaci opatření.

Téma diplomové práce jsem si zvolila protože se v prostředí obecní samosprávy pohybuji již sedmnáct let a osobní údaje nám pod rukami procházejí téměř denně a i když není ochrana osobních údajů zcela úplnou novinkou v naší legislativě přesto GDPR přineslo zásadní změny, které ochranu osobních údajů značně ovlivňují. Myslím si, že téma osobních údajů bude se stále se zvyšující kvalitou technologií v budoucnosti ještě hodně diskutováno.

CÍLE ZPRACOVÁNÍ PRÁCE A POUŽITÉ METODY

Hlavním cílem diplomové práce je zlepšení současného stavu informační bezpečnosti vybrané obce. Získané poznatky budou využitelné při implementaci pravidel GDPR a dobré praxe ve veřejné správě.

Dílčími cíli práce je identifikace a zhodnocení aktiv, identifikace a zhodnocení pravděpodobnosti hrozeb, identifikace a zhodnocení zranitelnosti, poté bude provedena analýza rizik a jako poslední budou navržena opatření pro zvýšení informační bezpečnosti vybraného subjektu. V závěru praktické části práce bude vytvořen přehled nejčastějších činností vykonávaných obcí v souladu s best practice.

Pro zpracování diplomové práce bude využita metoda vícezdrojového sběru informací, uplatnění zkušeností získaných z praxe za dobu působení ve veřejné správě, komunikace s pověřencem. Dále bude aplikována metoda komparace při sestavení rozdílů mezi původní a novou právní úpravou ochrany osobních údajů. V praktické části práce byly použity identifikační metody kontrolní seznam, vývojový diagram, jednoduchá bodová polokvantitativní metoda „PZH“.

Pro vybraná rizika budou navržena opatření k minimalizaci rizik formou technického a organizačního zabezpečení. Metody hodnocení a analýzy rizik budou hodnoceny a konzultovány prostřednictvím brainstormingu s pověřencem obce, správcem sítě, starostou obce a dvěma administrativními pracovnicemi, které zpracovávají osobní údaje.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMINOLOGICKÉ POJMY

Pro lepší orientaci v problematice jsou v následující kapitole vysvětleny nejpoužívanější pojmy, které souvisejí s ochranou osobních údajů v rámci EU.

Adaptační zákon – Zákon č. 110/2019 Sb., o zpracování osobních údajů, navazuje na obecné nařízení o ochraně osobních údajů. Jednotlivé členské státy EU si některé oblasti upravily a zpřesnily formou vlastního zákona. (Česko, 2019a)

Anonymizovaná data – jsou taková, která nepřímo nepomáhají v identifikaci určitého člověka a nejsou s ním nijak spojitelná. Je tedy možné s nimi volněji nakládat, protože nejsou regulovatelné přísnými pravidly obecného nařízení. (Základy IT gramotnosti)

Best practices – soubor pokynů, etiky nebo myšlenek, které představují nejúčinnější nebo nejuváženější postup. (2019)

Doprovodný zákon – Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. (Česko, 2019b)

GDPR – (General Data Protection Regulation), *„obecné nařízení o ochraně osobních údajů, 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, představuje právní rámec ochrany osobních údajů platný na celém území Evropské unie, který hájí práva jejich občanů proti neoprávněnému zacházení s jejich daty a osobními údaji*“. (Nezmar, 2017)

Obecné nařízení – „*Právní rámec ochrany osobních údajů v evropském prostoru platný od 25. května 2018. Stanovuje pravidla pro zpracování osobních údajů“*. Cílem přijetí obecného nařízení bylo zajištění jednotnosti pravidel. (Nezmar, 2017)

Osobní údaj – informace vztahující se k identifikované nebo identifikovatelné „*osobě (dále jen subjekt údajů); identifikovatelnou osobou je fyzická osoba, která je přímo či nepřímo identifikovatelná určitým identifikátorem. Například jméno, identifikační číslo, lokační údaje, elektronický identifikátor, zvláštní prvky fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity“*. (Evropská unie, 2016)

Pseudonymizace – znamená nahrazení identifikačních údajů osob bezvýznamovým identifikátorem, například číslem. Cílem je zamezit možnému spárování osobních údajů s konkrétními lidmi. (Pseudonymizace, 2016)

Skupina WP29 – pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995. (Janečková, 2019)

Souhlas – *„je svobodný, konkrétní, informovaný, jednoznačný projev vůle, kterým subjekt údajů dává prohlášením“,* či zjevným potvrzením své svolení ke zpracování osobních údajů. (Evropská unie, 2016)

Správce – *„fyzická nebo právnická osoba, orgán veřejné moci, agentura, jiný subjekt, který společně s jinými určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce zpracovává osobní údaje pro účely, které vyplývají z jeho činnosti ale i pro vlastní potřebu“.* (Česko, 2017)

Zpracovatel – *„fyzická nebo právnická osoba, orgán veřejné moci, agentura, jiný subjekt, který zpracovává osobní údaje pro správce. Zpracovatel je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Zpracovatel se liší od správce tím, že v rámci činnosti pro správce může provádět takové zpracovatelské operace, kterými jej správce pověřil a vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen“.* (Evropská unie, 2016)

Zpracování osobních údajů – dle obecného nařízení je jím *„jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které se provádějí za pomoci automatizovaných postupů. Jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření, omezení, výmaz, zničení“.* (Evropská unie, 2016)

Zvláštní kategorie osobních údajů – osobní údaje, které vypovídají o etnickém či rasovém původu, politických názorech, náboženském vyznání, genetické a biometrické údaje zpracované za účelem jedinečné identifikace. Taktéž údaje o zdravotním stavu a sexuální orientaci fyzické osoby. (Janečková, 2019)

2 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V KONTEXTU ORGANIZACE

Z jednotlivých zásad a principů vyplývají povinnosti pro správce i zpracovatele jakým způsobem by měly organizace spravovat osobní údaje.

2.1 Zásady zpracování osobních údajů

Dle čl. 10 odst. 3 Listiny základních práv a svobod má *„každý právo na ochranu před neoprávněným shromažďováním, zveřejňováním, nebo jiným zneužíváním údajů o své osobě“.* (Česko, 1992) Zásady jsou dle Žůrka (2017) pilíře na nichž je celé obecné nařízení postaveno. Jedná se především o zásadu zákonnosti, transparentnosti, korektnosti, omezení účelu, minimalizace údajů, přesnost, integritu a důvěrnost a zásadu odpovědnosti.

2.1.1 Zásada zákonnosti

Zásada zákonnosti dle Žůrka (2017) vyjadřuje tezi, že osobní údaje mohou být správcem zpracovány pouze k určitému účelu a za předpokladu, že správce má ke zpracování přinejmenším jeden právní argument. Jestliže není zákonný důvod nalezen nebo pomine, nastává povinnost osobní údaje zlikvidovat.

Zpracování je zákonné za předpokladu, že je splněna alespoň jedna z podmínek v odpovídajícím rozsahu uvedeným v čl. 6 odst. 1 a zpracování zvláštní kategorie osobních údajů v čl. 9 odst. 2 obecného nařízení (2016). Zásada zákonitosti nesmí být protiprávní, to znamená, že nemůže probíhat za nelegálním či nelegitimním účelem.

2.1.2 Zásada transparentnosti a korektnosti

Janečková (2018) uvádí, že správce nezastírá pravý účel, pro který jsou dané osobní údaje shromažďovány a zpracovávány. Dále platí povinnost neslučovat osobní údaje, které byly získány k odlišným účelům. Spojením informací vzniká nová kvalita osobního údaje, nad kterým by subjekt údajů ztratil přehled o zpracovávaných údajích. Což by nebylo dostatečně korektní a transparentní.

2.1.3 Zásada účelového omezení

„Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů po dobu delší, než je nezbytně nutné pro účely, pro které jsou zpracovávány“, jak je uvedeno v obecném nařízení. (Evropská unie, 2016)

Osobní údaje lze zpracovávat jen se stanovenými účely, za kterými byly nasbírány a způsoby či prostředky jimiž jsou účely slučitelné. Janečková (2019) dále uvádí, že je zcela nepřípustné, aby správce získal informaci k určitému účelu a následně ji použil k účelu jinému. Subjekt údajů by měl mít plnou informaci o zpracování údajů, které se týkají jeho osoby a rozhodovat o tom, jak s nimi bude dále zacházeno.

2.1.4 Zásada minimalizace údajů

Žůrek (2017) popisuje, že zpracování musí být *„přiměřené, relevantní, omezené na nezbytný rozsah ve vztahu k účelu pro, který jsou zpracovány“*. Janečková (2019) ve své publikaci uvádí, že rozsah osobních údajů je vymezen dvojím způsobem. Za prvé vyplívá ze zákonné úpravy, která vyjmenovává osobní údaje. A za druhé je jejich rozsah definován správcem dle stanoveného účelu.

Aby byla zásada minimalizace osobních údajů zcela dodržována je rozsah zpracování údajů nutné neustále přehodnocovat a nepotřebné údaje likvidovat.

Technologie umožňují orgánům veřejné moci využívat osobní údaje s ohledem na ústavní principy svého fungování zpracovávají osobní údaje na základě zákona a v zákonem stanoveném rozsahu. (Tzanou, 2019)

2.1.5 Zásada přesnosti

Zákon o ochraně osobních údajů neukládá povinnost zajištění správnosti a přesnosti osobních údajů, které organizace zpracovává. Dle Nezmara (2017) se údaje v případě potřeby následně aktualizují. Obecné nařízení stanovuje, jakým způsobem je tato povinnost zajišťována.

Dle Janečkové (2019) se proces stanovuje s ohledem na povahu, charakter a rozsah zpracování dále rozdělením odpovědnosti mezi jednotlivé zaměstnance správce s ohledem na jeho technické možnosti a na účel zpracování.

2.1.6 Zásada integrity a důvěrnosti

Zabezpečení osobních údajů před hrozbami uvnitř i vně organizace ve všech podobách zpracování. Základní povinností, jak uvádí Janečková (2018) je údaje zabezpečit prostřednictvím přiměřených technických a organizačních opatření. Technická opatření se týkají především zabezpečení osobních údajů. Z hlediska organizačních opatření jde především o vnitřní předpisy. Důvěrnost je vlastnost, kdy informace nejsou zveřejněny neoprávněným osobám, jednotlivci, subjektu. Integrita je vlastnost přesnosti a úplnosti. (IT Governance Privacy Team, 2017)

2.1.7 Zásada odpovědnosti

S přihlédnutím k povaze, rozsahu, kontextu, účelu zpracování i s různě pravděpodobným a závažným rizikem pro fyzické osoby. Správcem jsou zaváděna technická a organizační opatření, aby bylo možné doložit, že je zpracování prováděno v souladu s obecným nařízením, jak uvádí Janečková (2019).

Nonnemann (2018) popisuje zásadu odpovědnosti následovně. Správce musí být schopen doložit, že je zpracování od samého počátku koncipováno jako zákonné, že je jeho realizace monitorována a jsou nastaveny procesy a kontrolní mechanismy, aby zpracování probíhalo tak, jak má.

2.2 Porovnání dosavadní právní úpravy s obecným nařízením

Tabulka 1 obsahuje srovnání právních úprav mezi zákonem č. 101/2000 Sb., o ochraně osobních údajů a obecným nařízením.

Tabulka 1 Srovnání právní úpravy zákona č. 101/2000 Sb., o ochraně osobních údajů s GDPR (Capitová, 2019), (Česko, 2017a)

ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ	GDPR
Osobní údaje *– jakákoliv informace týkající určeného nebo určitelné fyzické osoby, jestliže ji lze přímo či nepřímo identifikovat zejména základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.*	***Osobní údaje*** *– veškeré informace o identifikované nebo identifikovatelné fyzické osobě; 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 jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*
Citlivý údaj *– osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě fyzické osoby a genetický údaj fyzické osoby; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci fyzické osoby.*	***Citlivé údaje*** *– jsou speciální kategorií, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob.*
Anonymní údaj – *takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určené nebo určitelné fyzické osobě.*	*GDPR se nevztahuje na anonymní data.*

Tabulka 2 Srovnání právní úpravy zákona č. 101/2000 Sb., o ochraně osobních údajů s GDPR, pokračování tabulky (Capitová, 2019), (Česko, 2017a)

ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ	GDPR
Oznamovací povinnost *– ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování je povinen tuto skutečnost písemně oznámit Úřadu pro ochranu osobních údajů před zpracováním osobních údajů.*	*Tato povinnost je zrušena.*
Likvidace osobních údajů *– správce, nebo na základě jeho pokynu, zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti fyzické osoby.*	***Právo být zapomenut*** *– subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se dané fyzické osoby týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat.*
Přístup subjektu údajů k informacím *– požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.*	***Právo na přístup*** *– fyzická osoba má právo získat od správce potvrzení, zda osobní údaje, které se jí týkají, jsou či nejsou zpracovány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům.*
Ochrana práv subjektu údajů *– je-li žádost fyzické osoby shledána oprávněnou, správce nebo*	***Právo na opravu*** *– fyzická osoba má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se jí týkají. S přihlédnutím k účelům zpracování má fyzická osoba právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.*
Toto právo není v zákoně upraveno.	***Právo na přenositelnost údajů*** *– fyzická osoba má právo získat osobní údaje, které se jí týkají, jež poskytla správci ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.*
Tato povinnost není v zákoně upravena.	***Posuzování vlivu na ochranu osobních údajů*** *– pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro právo a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.*
Tato povinnost není v zákoně upravena	***Pověřenec pro ochranu osobních údajů*** *– správce a zpracovatel jmenují pověřence pro ochranu osobních údajů.*
Tento časový údaj není v zákoně uveden.	***Porušení ochrany dat*** *– jakékoliv porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu.*
Sankce – max. do výše 10 000 000 Kč.	***Sankce*** *– 10 000 000 EUR nebo do výše 2 % celkového ročného obratu celosvětově za předchozí finanční rok, 20 000 000 EUR nebo do výše 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok.*

3 POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

Žůrek (2017) popisuje pověřence jako osobu, která má být nápomocná správcům při dosahování souladu se zpracováním osobních údajů. Povinnost jmenovat pověřence vzniká v následujících případech:

u soukromých subjektů:

- Za předpokladu, že dochází ke zpracování osobních údajů, které vyžadují *„rozsáhlé, pravidelné a systematické monitorování subjektu údajů“*.
- Jejichž činnost se zaměřuje na rozsáhlé zpracování citlivých údajů, které se týkají rozsudků v trestných věcech a trestných činů.

u veřejných subjektů:

- Je povinný pro orgány veřejné moci a „veřejné subjekty“ bez ohledu na rozsah zpracování. (Sešit k GDPR, 2018)

3.1 Povinnosti pověřence

K nejdůležitějším činnostem pověřence patří *„poskytování informací a poradenství správcům či zpracovatelům a zaměstnancům jejichž činnost souvisí se zpracováním údajů“*. Dohlížet na dodržování souladu s obecným nařízením, zvyšovat podvědomí a odbornou přípravu pracovníků. Poskytovat poradenství v oblasti posouzení vlivu na ochranu osobních údajů. V neposlední řadě působí také jako kontaktní místo jak pro subjekt údajů, tak i pro dozorový úřad. (Evropská unie, 2016), (Žůrek, 2017)

3.1.1 Kvalifikace pověřence

„Pověřenec na ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39“. (Evropská unie, 2016)

3.1.2 Jmenování pověřence

V souladu s čl. 37 odst. 3 obecného nařízení může být jmenován jediný pověřenec pro několik orgánů veřejné moci ovšem za předpokladu zohlednění jejich organizační struktury a velikosti. (Navrátil, 2018)

3.2 Práva subjektu údajů

Obecné nařízení obsahuje doplněná práva o ochraně osobních údajů, které může subjekt údajů kdykoliv realizovat a správce či zpracovatel je povinen je respektovat. Práva subjektů údaje lze rozdělit na následující kategorie. První kategorií jsou práva aplikovatelná automaticky, bez nutnosti jejich vyžádání ze strany subjektů údajů. Druhou kategorií jsou práva uplatnitelná výhradně na žádost subjektu údajů. (Průvodce pro přípravu obcí na požadavky GDPR, 2018)

3.3 Právo automaticky uplatnitelné

Do první kategorie automaticky uplatnitelných práv bez nutnosti vyžádání ze strany subjektů údajů lze přiřadit:

3.3.1 Právo na informace

Janečková (2019) uvádí, že informační povinnost byla dříve opomíjena a zejména orgánům státní správy a samosprávy chybělo povědomí o nutnosti ji plnit. Základní parametry správného plnění informační povinnosti jsou stanoveny v čl. 12 obecného nařízení a následné podrobnosti jsou doplněny čl. 13 a 14. Informace má být poskytnuta stručným, transparentním a srozumitelným způsobem, zdarma a bez poplatků. Údaje získané přímo od subjektu údajů jsou informace poskytnuté subjektem například při registraci, e-mailové komunikaci, na webových stránkách, v kontaktních formulářích. Údaje, které nejsou získány přímo od subjektu údajů jsou údaje získané z veřejné evidence základních registrů.

V tabulce 3 je uveden souhrn informací, které by správce měl poskytnout jednotlivcům.

Tabulka 3 Právo být informován (Nezmar, 2017)

Jaké informace musí být sdělovány?	Údaje získané přímo od subjektu údajů	Údaje nejsou získány přímo od subjektu údajů
Identifikační údaje na správce a pověřence pro ochranu údajů	×	×
Účel zpracování a zákonné oprávnění pro zpracování	×	×
Oprávněné zájmy správce, případně třetí strany		×
Kategorie osobních údajů		×

Tabulka 4 Právo být informován, pokračování tabulky (Nezmar, 2017)

Jaké informace musí být sdělovány?	**Údaje získané přímo od subjektu údajů**	**Údaje nejsou získány přímo od subjektu údajů**
Každý příjemce, kategorie příjemců osobních údajů	×	×
Podrobnosti o přesunech do třetích zemí	×	×
Doba uchování nebo kritéria používaná k určení doby uchování	×	×
Existence jednotlivých práv subjektů údajů	×	×
Právo na odstoupení od smlouvy, kdykoli, je-li to relevantní	×	×
Právo podat stížnost dozorovému orgánu	×	×
Zdroj, od kterého pocházejí osobní údaje a zda pochází z veřejně přístupných zdrojů		×
Zda je poskytování osobních údajů součástí zákonného nebo smluvního závazku nebo požadavku a možné důsledky neposkytnutí osobních údajů.	×	
Informace o existenci automatizovaného rozhodování, včetně profilování a informace o procesu rozhodování, jeho význam a možné důsledky.	×	×

Nezmar (2017) následně uvádí, že v případě, kdy správce získává osobní údaje přímo od subjektu údajů je povinen informace poskytnou právě v okamžiku získání. Jestliže informace nezískal přímo od subjektu údajů, je povinností správce informace poskytnout:

- V přiměřené lhůtě, nejpozději však do 1 měsíce od získání údajů.
- Jestliže osobní údaje slouží pro účely komunikace, tak nejpozději v okamžiku této komunikace.
- V případě, že jsou osobní údaje poskytnuty jinému příjemci, tak nejpozději předtím, než jsou poskytnuty.

3.3.2 Právo nebýt předmětem automatizovaného individuálního rozhodování

Představuje pojistku proti automatizovanému rozhodování s právními účinky proti člověku. Žůrek (2017) popisuje, že automatizované individuální rozhodování je obecným nařízením umožněno, je-li nezbytné k uzavření nebo plnění smlouvy mezi zúčastněnými stranami.

3.3.3 Právo na výmaz

„Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají“. (Tzanou, 2019)

A to za předpokladu, že existuje některý z důvodu uvedených v čl. 17 obecného nařízení:

- *„Osobní údaje již nejsou potřebné pro účely, pro které byly zpracovávány.*
- *Subjekt údajů odvolá souhlas a neexistuje další právní důvod pro zpracování.*
- *Subjekt údajů vznese námitky proti zpracování.*
- *Osobní údaje byly zpracovány protiprávně.*
- *Osobní údaje shromážděné v souvislosti s nabídkou služeb informační společnosti“.* (Janečková, 2018)

3.3.4 Právo na opravu a aktualizaci údajů

V čl. 16 obecného nařízení (Evropská unie, 2016) se uvádí, že *„subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné údaje, které se týkají jeho osoby“*. Právo na opravu a povinnost osobní údaje opravit je spojováno se zásadou přesnosti. Osobní údaje mají být zpracovávány přesné a aktualizované.
Součástí tohoto práva je také právo na aktualizaci neúplných údajů formou dodatečného prohlášení. Jestliže subjekt údajů oznámí správci, že zpracovává nepřesné údaje a požaduje opravu. Je povinností správce se žádostí zabývat.

3.4 Právo subjektu údajů na žádost

Do druhé kategorie práv subjektu údajů uplatnitelné pouze na žádost lze přiřadit:

3.4.1 Právo na přístup k osobním údajům

Přístup k osobním údajům se rozumí oprávnění subjektu údajů na základě jeho aktivní žádosti získat od správce informaci, zda jsou jeho či nejsou jeho soukromé údaje

zpracovávány. V případě jejich zpracovávání má subjekt údajů právo získat zejména následující informace:

- Účel zpracování.
- Kategorii dotčených osobních údajů.
- Navrhovaná doba, po kterou budou osobní údaje uloženy.
- Požadovat od správce opravu nebo výmaz, právo vznést námitku.
- Podat stížnost u dozorového úřadu. (Navrátil, 2018)

Forma žádosti není stanovena, může být uplatněna písemně, ústně, prezenční formou nebo na dálku. Jen je nutné věnovat zvýšenou pozornost při identifikaci žadatele a jeho ztotožnění se se subjektem údajů. Článek 15 obecného nařízení odst. 3 také uvádí, *„že subjekt údajů má právo získat kopii“*, když říká že *„správce poskytne kopii zpracovávaných osobních údajů. Právem získat kopii nesmějí být nepříznivě dotčena práva a svobody jiných osob“.* (Evropská unie, 2016), (Navrátil, 2018)

3.4.2 Právo na omezení zpracování

Subjekt údajů má právo na omezení zpracování dle čl. 18 obecného nařízení v následujících případech.

- *„Subjekt údajů popírá přesnost osobních údajů a dobu potřebnou k tomu, aby správce měl možnost přesnost údajů ověřit.*
- *Zpracování je protiprávní a subjekt údajů odmítá výmaz, místo toho žádá omezení použití osobních údajů.*
- *Správce již nepotřebuje osobní údaje pro účely zpracování, subjekt údajů je požaduje pro určení, výkon, nebo obhajobu právních nároků.*
- *Subjekt údajů vznesl námitku proti zpracování“.*
  (Evropská unie, 2016), (Janečková, 2018)

3.4.3 Právo na přenositelnost

Je zcela novým právem subjektu údajů. Posiluje postavení subjektu údajů, umožňuje mu získat informace o zpracování a zároveň mu dovoluje za určitých okolností údaje získat a manipulovat jimi. V čl. 20 obecného nařízení (2016) není stanoven formát, ve kterém by měly být údaje předávány. Pouze uvádí, že by se mělo jednat o strukturovaný, běžně používaný a strojově čitelný formát, který poskytuje opakované použití. Strojově čitelný formát je formátem datového souboru se strukturou, která umožňuje programovému

vybavení nalézt, rozpoznat a získat konkrétní informace, včetně jednotlivých údajů a vnitřní struktury. Správce nese odpovědnost za veškerá bezpečnostní opatření, nejen z hlediska zajištění bezpečného přenosu na správné místo určení, ale také za nepřetržitou ochranu osobních údajů, které zůstaly v jeho systému. Správci taktéž posuzují jednotlivá rizika spojená s přenositelností údajů a přijmout odpovídající opatření ke zmírnění rizik.

4 MANAGEMENT RIZIK

Management rizik je soustavnou opakující se činností, jehož smyslem není identifikovat a ošetřit všechna rizika. Hlavním cílem tohoto procesu řízení rizik je umění včas rozpoznat, jestli se daným rizikem dále zabývat a věnovat následnou pozornost jeho ošetření.

4.1 Definice rizika

Riziko lze považovat za odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývající z hrozby a ze zranitelnosti zájmu, je možné posoudit na základě provedení analýzy rizik. Jenž zároveň vychází i z posouzení připravenosti čelit jednotlivým hrozbám. (Česko, 2016)

4.2 Proces managementu rizik

Zahrnuje systematické uplatňování všech politik, postupů a praktik na základě činností v komunikaci a konzultaci, kterými se stanovuje kontext, posouzení rizik, zvládání rizik, monitorování a přezkum procesu, jeho zaznamenávání a hlášení. V systémovém pojetí se rozdělují na soustavu činností a soustavu procesů. (Janíček, a další, 2013)

4.3 Rozsah, kontext a kritéria

Účelem procesu řízení rizik je stanovení rozsahu, kontextu a kritérií, tak aby bylo možné provést hodnocení rizik a odpovídající ošetření rizik. A dále zahrnují definování rozsahu procesu a pochopení vnitřního a vnějšího kontextu.

Stanovení rozsahu – organizace definuje rozsah činností v oblasti řízení rizik. Proces řízení rizik je aplikovatelný na různých úrovních (např. strategické, provozní, programové, projektové) je tedy důležité zvážit veškeré cíle a dát je do souladu s organizací.

Vnitřní a vnější kontext – je prostředí, ve kterém organizace definuje své cíle a zároveň se jich snaží dosáhnout. Pochopení kontextu má své opodstatnění, jelikož řízení rizik probíhá v kontextu cílů a činností organizace. Organizační faktory mohou být zdrojem rizika. Účel a rozsah procesu mohou být ve vzájemném vztahu s cíli organizace jako celku.

Kritéria – specifikují míru a typ rizika, které organizace může nebo nemusí podstupovat ve vztahu ke svým cílům. Definují kritéria pro hodnocení závažnosti rizika a pro podporu rozhodovacích procesů. (ČSN ISO 31000, 2018)

4.4 Posouzení rizik

Posouzením rizika rozumíme celkový proces identifikace, analýzy a hodnocení rizik. Proces posouzení je prováděn systematicky, opakovaně na základě získaných znalostí a ve spolupráci se zúčastněnými stranami. (ČSN ISO 31000, 2018)

4.4.1 Identifikace rizik

Účelem identifikace rizik je nalezení, rozpoznání, popis a zaznamenání rizika. Při identifikaci rizik je důležité mít k dispozici relevantní, vhodné a aktuální informace. V úvahu bychom měli vzít jednotlivé faktory a vazby mezi nimi:

- Hmotné a nehmotné zdroje rizika.
- Příčiny a události.
- Hrozby a příležitosti.
- Zranitelnosti a schopnosti.
- Změny ve vnitřním a vnějším kontextu.
- Ukazatele vznikajících rizik.
- Povahu a hodnotu aktiv a zdrojů.
- Důsledky a dopad na cíle.
- Omezení znalostí a spolehlivosti informací. (ČSN ISO 31000, 2018)

4.4.2 Analýza rizik

Janíček (2013) ve své publikaci uvádí, že analýza rizika je strukturovaným procesem pochopení povahy a stanovení úrovně rizika. Provádí se na základě vymezení předmětu analýzy rizika, rozpoznání či identifikace nebezpečí a odhadu rizika. Smyslem analýzy rizika je podrobné prozkoumání všech rizik, které mohou v rámci procesu vyvstat, získání podkladů pro komplexní posouzení, ošetření rizika a jeho snížení.

4.4.3 Hodnocení rizik

Hodnocení rizik zahrnuje srovnání výsledků analýzy rizik se stanovenými kritérii rizika, ze kterého následně vyplývá potřebné provedení opatření. Následující postup může vést k rozhodnutí:

- Rizikem se dále nezabývat.
- Zvážit možnosti ošetření rizik.

- Provést další analýzu.
- Zavést nebo zachovat stávající kontroly.
- Přehodnotit cíle.

Výsledky vyhodnocení rizik by měly být zaznamenávány a poskytnuty vrcholovému vedení organizace. (ČSN ISO 31000, 2018)

4.5 Ošetření rizik

Po provedení fáze posouzení rizik je následnou fází ošetření rizik. Fáze zahrnuje volby a odsouhlasení jedné či více variant, jak přeměnit pravděpodobnost výskytu a důsledku rizik. Po ošetření rizika následuje opakující se proces opětovného posuzování nové úrovně rizika. Možností, jak ošetřit rizika je provedení ošetření rizika, udržení rizika, vyhnutí se riziku a převod rizika. (Duricu, 2019)

4.6 Monitorování a přezkoumávání

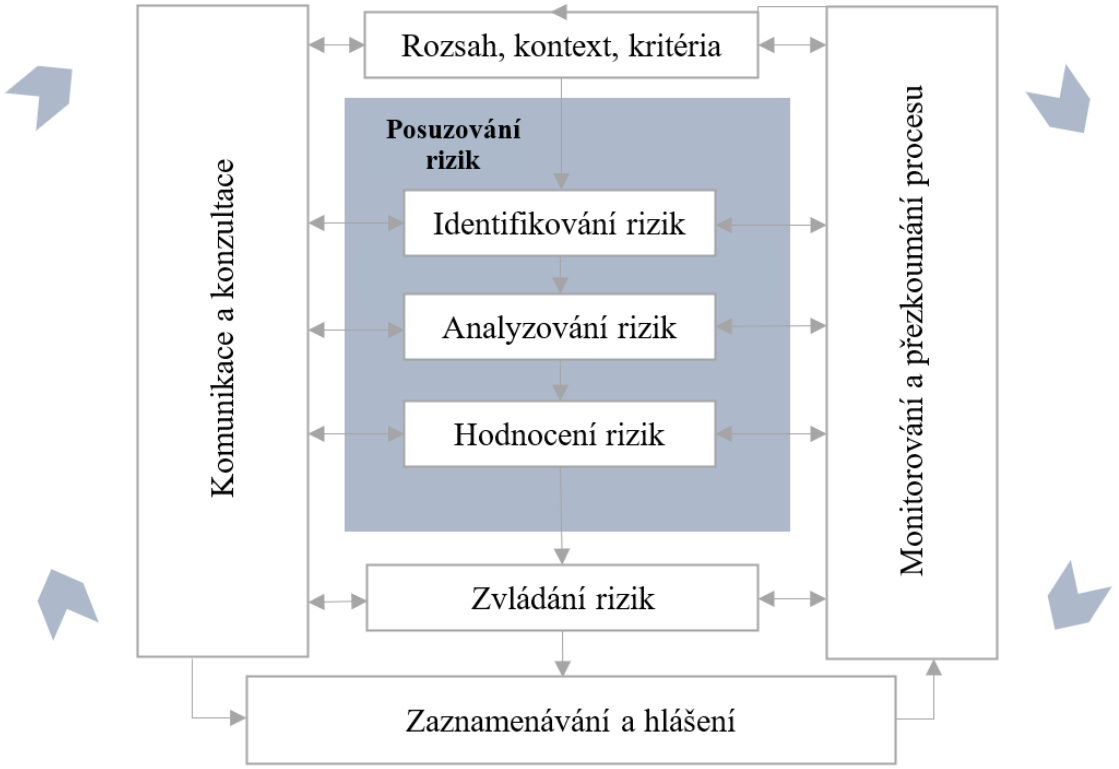
Cílem monitorování a přezkoumávání je zajistit a zlepšit kvalitu a efektivitu návrhu, implementace a výstupů procesu. Monitorování a kontrola zahrnuje plánování, shromažďování a analýzu informací, zaznamenávání výsledků a poskytování zpětné vazby. Včasná identifikace jakékoliv změny v kontextu organizace v rané fázi udržuje přehled o riziku. (Duricu, 2019)

4.7 Komunikace a konzultace

Komunikace a konzultace by dle Janíčka (2013) měla probíhat ve všech úrovních procesu řízení rizik za účasti všech zainteresovaných stran na daných rizicích. Komunikace dle normy (ČSN ISO 31000, 2018) podporuje podvědomí porozumění riziku. Konzultace zahrnuje získání zpětné vazby a informace na podporu rozhodování.

4.8 Zaznamenávání a hlášení

Proces řízení rizik a jeho výsledky jsou dle normy (ČSN ISO 31000, 2018) zdokumentovány a vykazovány prostřednictvím vhodných mechanismů. Podávání zpráv má za úkol zvyšovat kvalitu dialogu se zainteresovanými stranami a podporovat vrcholový management a orgány dohledu při plnění povinností.



Obrázek 1 Proces managementu rizik (ČSN ISO 31000, 2018)

V obecném nařízení (2016) se píše, že *„řízení rizik je prováděno s cílem určit vhodná technická a organizační opatření, která je nezbytné zavést pro zajištění bezpečnosti osobních údajů při jejich zpracování a pro zmírnění a eliminaci rizik. Tato opatření by měla zohledňovat povahu, rozsah, kontext a účely zpracování a riziko pro práva a svobody fyzických osob.“*

GDPR definuje porušení údajů jako *„porušení bezpečnosti vedoucí k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému vyzrazení nebo přístup k přenášeným, ukládaným, nebo jinak zpracovávaným údajům o osobě.“* (Brand, 2017)

5 POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

DPIA je procesem jehož hlavním záměrem je *„popsat zpracování, posoudit nezbytnost a přiměřenost zpracování, úspěšné zvládnutí rizik pro práva a svobody fyzických osob“,* která vyplývají ze zpracování osobních údajů. Nezmar (2017) ještě dodává, že ustanovení souvisí s požadavkem obecného nařízení na minimalizaci zpracovaných dat. Během DPIA analýzy můžeme zjistit, že jsou některá data pro účel zpracování zbytečná.

5.1 Kdy se DPIA provádí

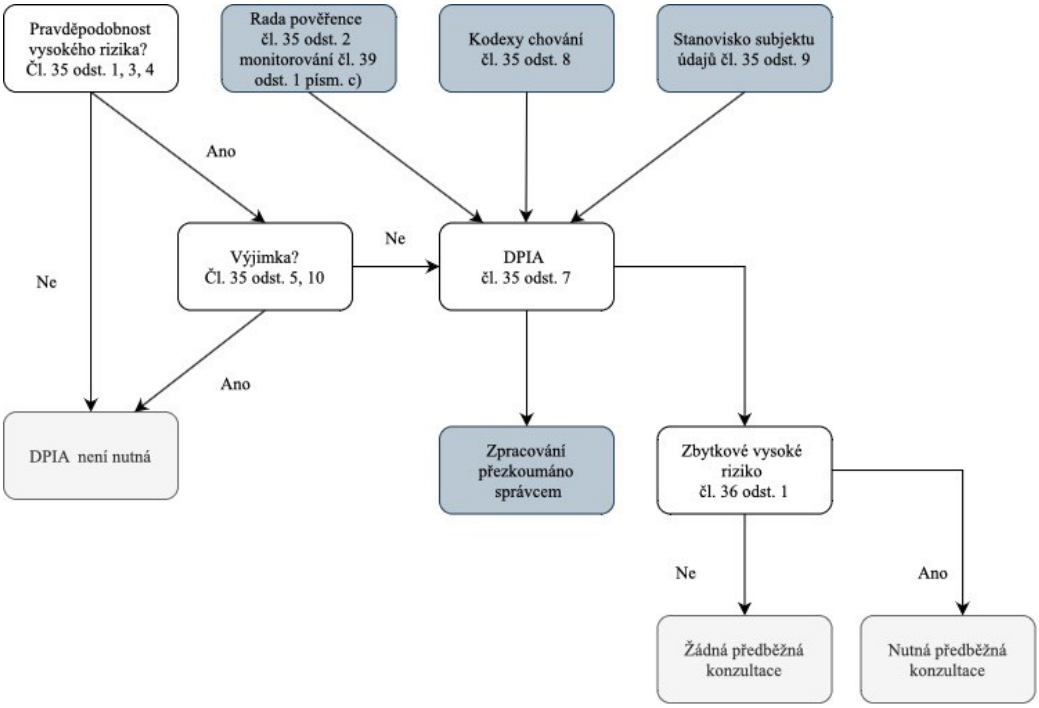
Navrátil (2018) ve své publikaci uvádí následující případy. V prvním případě se DPIA provádí tehdy, *„pokud je pravděpodobné, že určitý druh zpracování, zejména při použití nových počítačových a komunikačních technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování osobních údajů mít za následek vysoké riziko pro práva a svobody fyzických osob“*. Jedná se zejména o následující případy:

- Když dochází k systematickému a rozsáhlému vyhodnocování osobních aspektů, které se týkají fyzických osob, jsou založeny na automatizovaném zpracování, včetně profilování. Vznikají z rozhodnutí, která mají ve vztahu k fyzickým osobám závažný dopad, nebo vyvolávají k fyzickým osobám právní účinky.
- Kdy je prováděno rozsáhlé zpracování zvláštních kategorií údajů, jenž jsou uvedeny v čl. 9 odst. 1 obecného nařízení. Dále osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů uvedených v čl. 10 obecného nařízení.
- Kdy je provedeno rozsáhlé systematické monitorování veřejně přístupných prostorů. (Navrátil, 2018)

Operace zpracování údajů se vyvíjejí velmi rychle a vznikají tak nová slabá místa. Revize posouzení vlivu na ochranu osobních údajů není efektivní jen z pohledu zlepšování, ale má smysl i pro udržení úrovně ochrany osobních údajů v postupně měnícím se prostředí.

Změna může nastat i z důvodu změny organizačního a společenského kontextu, jelikož účinky automatizovaných rozhodnutí získají na významu, nebo dojde k ohrožení nových kategorií subjektů údajů diskriminací. (Belgium, 2017)

Obrázek 2 na následující straně zobrazuje posouzení vlivu na ochranu osobních údajů s pravděpodobností vysokého rizika pro subjekty údajů.



Obrázek 2 Posouzení vlivu na ochranu osobních údajů (Nezmar, 2017)

5.2 Nejčastější nedostatky v DPIA v rámci vnitřních předpisů jsou:

- Nedostatečný nebo nesprávný popis.
- Chybějící posouzení přiměřenosti/nezbytnosti prováděných operací.
- Chybějící nebo nedostatečné DPIA pro práva a svobody subjektů.
- Nekonkrétní nebo nedostatečná specifikace technických a organizačních opatření, jejich úkolem je redukovat rizika zpracování osobních údajů na přijatelnou úroveň. (ÚOOÚ, 2020)

5.3 Úřad pro ochranu osobních údajů – dozorový úřad v ČR

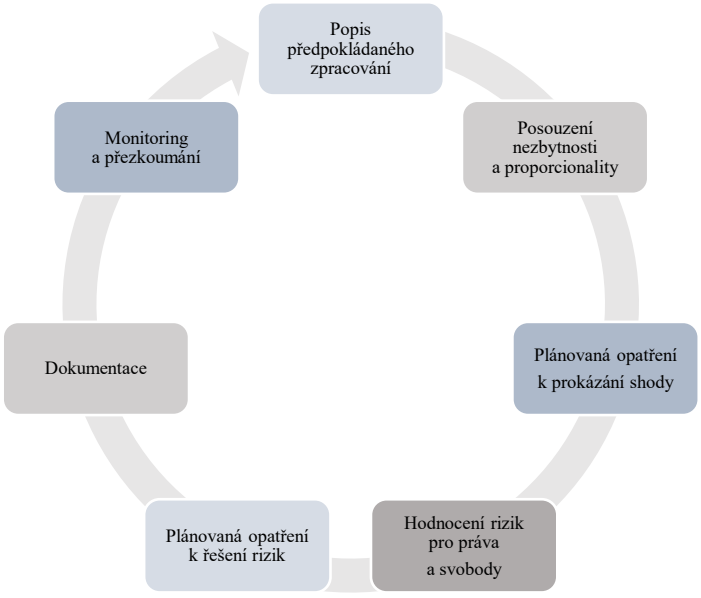
Významnou roli při DPIA zastává i Úřad pro ochranu osobních údajů jako orgán dozoru je vládní organizací, která je odpovědná za vymáhání GDPR. (IT Governance Privacy Team, 2017) V rozšířenějším významu popisuje Báča a kol. (2020) v praktickém komentáři: *„ÚOOÚ je nezávislý ústřední orgán státní správy, který má však mezi ostatními správními úřady specifické postavení. Jako vhodné se nabízí srovnání s regulačními úřady, kterými jsou například ÚOHS či Energetický regulační úřad, jejichž úkolem je ochrana určitého sektoru jednotného trhu. ÚOOÚ vedle toho nechrání žádnou část nebo vlastnost trhu,*

ale základní lidské právo, kterým je právo na ochranu osobních údajů ve smyslu práva na informační sebeurčení fyzických osob.“ a dále pak uvádí: *„jeho pravomoc se nevztahuje jenom na veřejnou správu, ale také na soukromý sektor.“*

Oblast ochrany osobních údajů je hlavní podstatou činnosti ÚOOÚ. ÚOOÚ se řídí obecným nařízením a nově Adaptačním zákonem, kterým byl nahrazen zákon č. 101/2000 Sb., o ochraně osobních údajů. Jeho působnost je jasně vymezena čl. 55 až 59 obecného nařízení, tak i v Adaptačním zákoně. Další působnost ÚOOÚ spočívá v kompetenci projednávat správní delikty, které se týkají neoprávněného zpracování.

5.4 Pokyny pracovní skupiny WP29

Pracovní skupina pro ochranu fyzických osob zřízená podle čl. 29 směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, byla s účinností obecného nařízení nahrazena Evropským sborem pro ochranu osobních údajů složeným ze zástupců dozorových členů členských států. Jedná se o nezávislý evropský poradní orgán. V dokumentu WP248 *„Pokyny pro posouzení vlivu na ochranu osobních údajů“* a ustanovení, zda *„je pravděpodobné, že zpracování bude mít za následek vysoké riziko“* pro účely nařízení 2016/679, uvádí východiska pro určení rizikovosti. (Belgium, 2017)
Obrázek 3 znázorňuje proces, který popisuje postup provedení posouzení dle výkladových stanovisek WP29. Zobrazený proces je opakovaný, je tedy pravděpodobné, že se před dokončením jednotlivých etap DPIA, budeme muset k některým etapách vracet opakovaně.



Obrázek 3 Proces provádění DPIA (Nezmar, 2017)

5.5 Sankce a pokuty

Žůrek (2017) popisuje, že účelem hrozby sankce je přimět adresáta chovat se podle normou vymezených pravidel. Obecné nařízení v čl. 83 stanovuje podmínky pro uložení pokut, včetně jejich možné výše.

Sankce jsou rozvrženy do dvou kategorií, a to z hlediska výše sankce a dopadu porušení. Společně pro obě kategorie platí, že v případě porušení souvisejících operací zpracování poruší správce nebo zpracovatel více ustanovení obecného nařízení*, „nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení“*.

Současně Žůrek (2017) uvádí, že *„pokuty ukládané veřejné moci a veřejným subjektům plynou z veřejných rozpočtů a bylo by neúčelné ponechat pro tyto subjekty nejvyšší možnou pokutu“.* Při rozhodování, zda uložit pokutu a v jaké výši může dozorový úřad přihlížet k následujícím okolnostem:

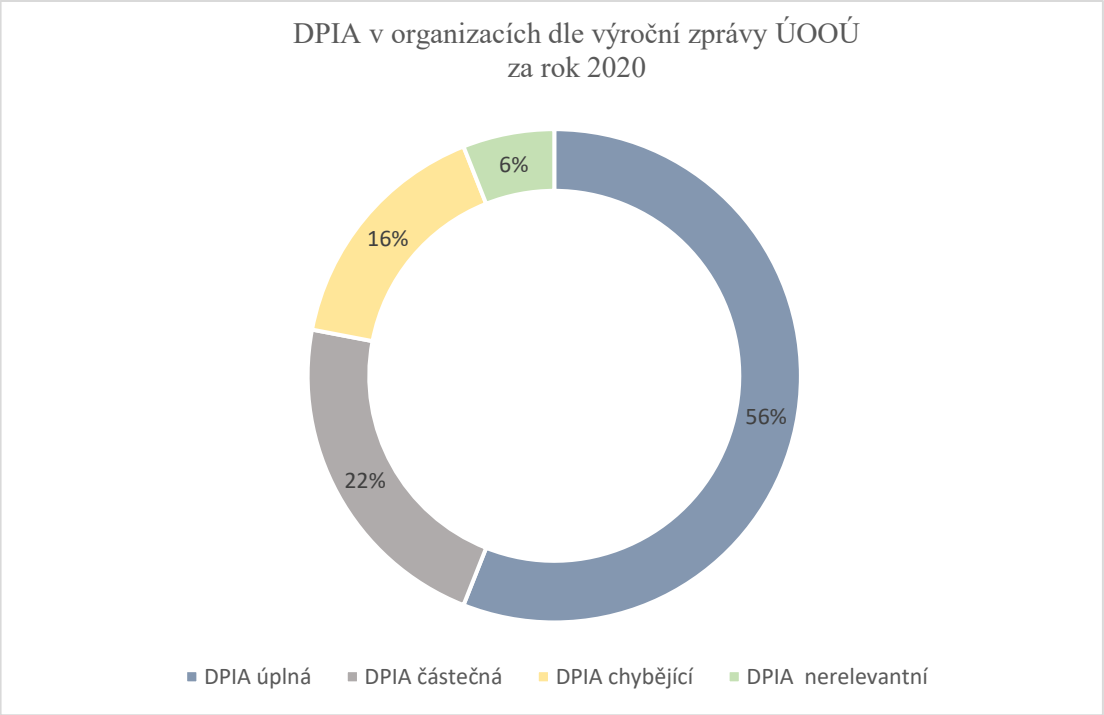
- Povaze, závažnosti a délce trvání porušení s přihlédnutím k povaze, rozsahu, účelu dotčeného zpracování, k počtu dotčených subjektů údajů, míře škody, jež byla způsobena.
- Zda došlo k úmyslnému či nedbalostnímu porušení a jaké byly podniknuty kroky ke zmírnění škod způsobených subjektům údajů.
- Míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením.
- Předešlé porušení správcem či zpracovatelem, dodržování navržených kodexů chování.
- Jakým způsobem se dozorový úřad o porušení dozvěděl, zda správce či zpracovatel porušení oznámil.

Čeští zákonodárci v Adaptačním zákoně č. 110/2019, o zpracování osobních údajů, který vešel v platnost skoro po roce účinnosti obecného nařízení rozhodli, že sankce za porušení GDPR pro orgány veřejné moci a veřejné subjekty budou nulové. (Česko, 2019a)

5.6 Audit GDPR

ÚOOÚ je oprávněný kontrolovat organizaci z hlediska plnění obecného nařízení. Organizace musí prokázat, jaká data jsou o subjektech údajů ukládána a zpracovávána v jakých IT systémech a jak vyhověla požadavkům subjektů na transparentnost, odvolání souhlasu, výmaz nebo přenositelnost jejich údajů. Dále je prokazována bezchybnost procesů

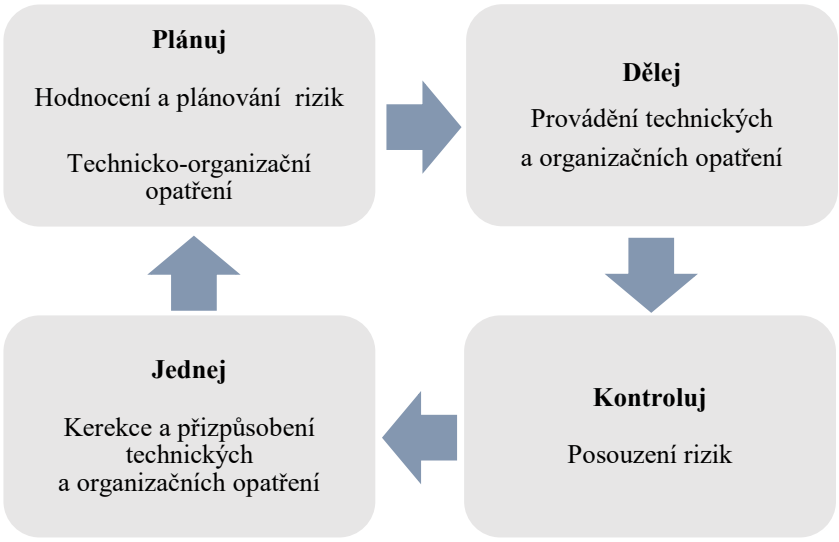
souvisejících s ochranou osobních údajů. Forma a rozsah samotného auditu záleží na tom, zda půjde o plánovanou kontrolu, kde se provádí kontrola v rámci organizace jako celku. Nebo kontrolu některého z aspektů založenou na konkrétní žádosti či problému. (Navrátil, 2018) Graf 1 znázorňuje zjištěné výsledky kontrol ÚOOÚ z hlediska plnění obecního nařízení.



Graf 1 DPIA v organizacích dle výroční zprávy ÚOOÚ za rok 2020 (ÚOOÚ, 2020)

5.7 Implementace úrovně ochrany pomocí systému řízení

Systém řízení by měl být také základním procesem neustálého zlepšování. Kontinuální proces zlepšování hodnotí stávající procesy a jejich výstupy, tak aby byl zajištěn soulad se zákony, předpisy a jinými požadavky. Cyklus Plan – Do – Check – Act (dále jen „PDCA“) nazývaný také jako Demingův cyklus, rozděluje standartní procesy a postupy pro systém řízení nebo vývojový proces do čtyř fází: plánuj, dělej, ověř, jednej. Jako cyklický proces se každá fáze zapojuje do následující v pořadí a umožňuje neustálé zlepšování. (IT Governance Privacy Team, 2017) Obrázek 4 na následující straně znázorňuje PDCA cyklus.



Obrázek 4 PDCA cyklus (Bitkom, 2017)

Soulad organizace s obecným nařízením vyžaduje implementaci technického i organizačního opatření. V čl. 32 odst. 1 písm. d) obecného nařízení popisuje zákonodárce požadavky na monitorování technických a organizačních opatření, která jsou pro bezpečnost informací uplatňována pomocí systémů řízení Information Security Management Systém (dále jen „ISMS“). Cílem ISO 27001 je chránit důvěrnost, dostupnost a integritu informací, proces řízení poskytuje zainteresovaným stranám důvěru v to, že rizika v rámci organizace jsou adekvátně řízena. (IT Governance Privacy Team, 2017)

V tabulce 5 je souhrnné porovnání požadavků ISO 27001:2015 a Obecného nařízení.

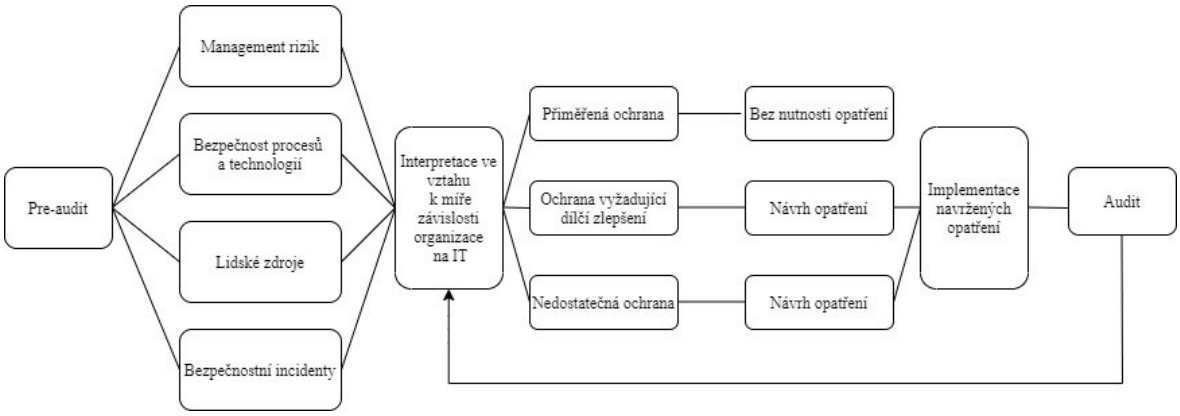
Tabulka 5 Porovnání požadavků ISO 27001:2015 a Obecného nařízení (vlastní zpracování, Česko, 2017b)

Fáze v ISMS	**Čl. 32 - Zabezpečení zpracování**
Posouzení rizik Vhodná technická a organizační opatření zahrnují: • náklady na implementaci; • povahu, rozsah, kontext, účel zpracování.	*„S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku“.*

Tabulka 6 Porovnání požadavků ISO 27001:2015 a Obecného nařízení, pokračování tabulky (vlastní zpracování, Česko, 2017b)

Fáze v ISMS	**Čl. 32 - Zabezpečení zpracování**
Hodnocení standardů • důvěrnost • integrita • dostupnost	*„Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim“.*
Opatření splňující kritéria: • pseudonymizace • šifrování • důvěrnost • integrita • dostupnost	Opatření zahrnují také: a) *„pseudonymizaci a šifrování osobních údajů;* b) *schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování*; c) *schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů*“.
Interní audit a postupy pro opravu/přizpůsobení přijatých opatření.	Opatření zahrnují: d) *„postup pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování“.*

Obrázek 5 znázorňuje zajištění informační bezpečnosti v organizaci.



Obrázek 5 Vyvážené informační bezpečnosti v organizaci (Král, 2010)

5.8 Povinnost zabezpečit osobní údaje

Povinnost zabezpečit osobní údaje není pro správce a zpracovatele novinkou. V předchozí právní úpravě byla povinnost zabezpečení osobních údajů stanovena § 13 zákona o ochraně osobních údajů. *„Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů“.* (Česko, 2000b)

Současně vznikla správcům i zpracovatelům povinnost dokumentovat přijatá a provedená opatření v souladu se zákonem a jinými právními předpisy.

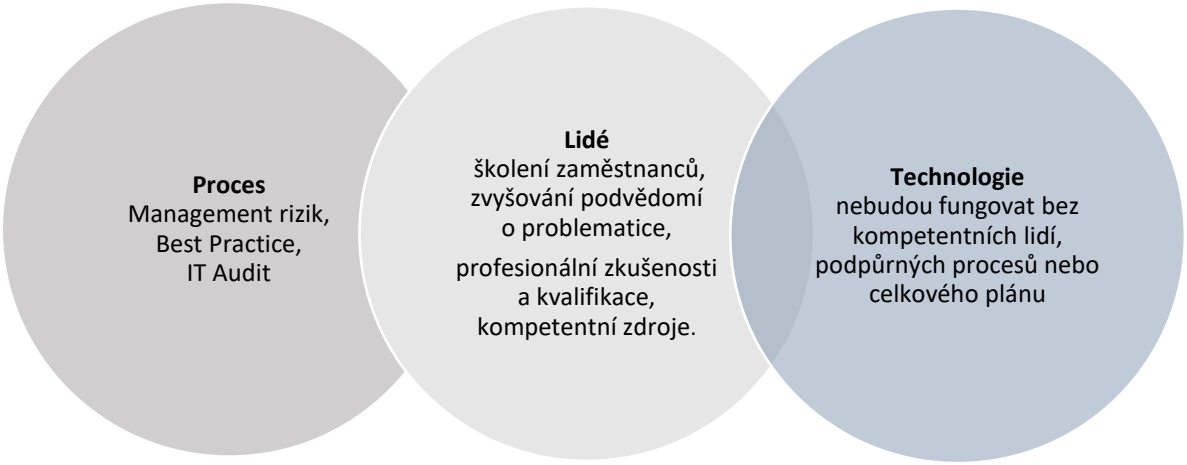
Obecné nařízení ukládá povinnost zabezpečit osobní údaje již v základních zásadách, týká se především o zásadu integrity, důvěrnosti a odpovědnosti. Odpovědnost správce je upřesněna ve článcích 24 a 25 obecného nařízení.

Janečková (2019) uvádí, že záleží na správci a zpracovateli jaký zvolí způsob, podobu a formu adekvátní ochrany, musí ovšem zohlednit základní oblasti:

- **Fyzickou bezpečnost** – souvisí s organizační bezpečností i objektovou bezpečností.
- **Organizační bezpečnost** – zajišťuje mimo jiné i administrativní bezpečnost, prostřednictvím, které lze zajistit, aby dokumenty obsahující osobní údaje, měly své místo, zaměstnanci měli k dispozici dostatek uzamykatelných prostor a v neposlední řadě dodržovali pravidlo „prázdného stolu“. To znamená, že před odchodem ze zaměstnání nezůstanou na stolech dokumenty s údaji. Samotný přístup k dokumentům by měl mít svá omezení.
- **IT bezpečnost** – i následující oblast má svá pravidla. Svěřenou výpočetní techniku používají zaměstnanci pouze v rámci pracovních povinností. Zachovává se jedinečnost a důvěrnost přístupového hesla. Při přihlašování k operačním systémům nebo aplikacím se dbá na to, aby nebylo heslo možné odpozorovat. Před opuštěním počítače zabezpečí zaměstnanec výpočetní techniku uzamčením pracovní plochy. Zaměstnancům není dovolené používat soukromé datové nosiče a podobně.

- **Personální bezpečnost** – zaměstnanci jsou seznámení s bezpečnostní dokumentací a jsou poučení o odpovědnosti za ochranu zpracovávaných informací a bezpečnostních opatřeních souvisejících s výkonem práce a prokazatelnou formou. Při zpracování bezpečností dokumentace praxe ukázala, že by dokumentace měla obsahovat výčet povinností s ohledem na postavení osob v procesu zpracování osobních údajů**.**

Technická opatření zahrnují konkrétní postupy, proškolení zaměstnanců, audity, příslušné technické i fyzické bezpečnostní kontroly, které tvoří součást efektivního systému řízení bezpečnosti rizik. Tyto procesy, zásady a kontroly mohou nastínit, jak organizace řídí komunikaci a rizika v souladu s předpisy. Obrázek 6 znázorňuje, které tři kategorii činností se vzájemně prolínají a souvisejí dodržováním předpisů.



Obrázek 6 Dodržování předpisů zahrnuje i následující kategorie činností
(IT Governance Privacy Team, 2017)

5.9 Porušení zabezpečení osobních údajů

Dle čl. 4 odst. 12 obecného nařízení je porušení zabezpečení osobních údajů definováno, jako *„porušení zabezpečení, jenž vede k náhodnému eventuálně protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených a jinak zpracovávaných osobních údajů*“. (Evropská unie, 2016)

Porušení zahrnuje následující kategorie:

Porušení důvěrnosti – v případě neoprávněného nebo náhodného poskytnutí eventuálně zpřístupnění osobních údajů.

Porušení dostupnosti – v případě náhodné nebo neoprávněné ztráty přístupu nebo zničení osobních údajů.

Porušení integrity – v případě neoprávněného nebo náhodného pozměnění osobních údajů. (Janečková, 2019), (IT Governance Privacy Team, 2017)

V praxi obecních úřadů mezi vysoce riziková porušení náleží fyzické zničení údajů, úmyslná modifikace většího rozsahu, prozrazení autentizačních údajů osobám, které nejsou kompetentními uživateli informačních systémů. Tabulka 7 představuje zjednodušený přehled řešení porušení zabezpečení osobních údajů, které slouží pro vnitřní potřebu úřadu.

Tabulka 7 Záznam o porušení zabezpečení osobních údajů
(vlastní zpravování, Janečková, 2019)

Záznam o porušení zabezpečení osobních údajů	
Informace o porušení zabezpečení	Následky porušení
Datum zjištění porušení zabezpečení u správce	
Popis události	
Kategorie a množství zasažených osobních údajů	
Kategorie a množství zasažených subjektů údajů	
Odhadované důsledky porušení zabezpečení osobních údajů	
Vyhodnocení míry rizika podle čl. 33 a 34 GDPR	a) bez rizika b) riziko c) vysoké riziko
Ohlášení dozorovému úřadu	a) ANO b) NE
Oznámení subjektu údajů	
Popis nápravných opatření	
Kontrola provedení nápravného opatření	

5.10 Ohlašování bezpečnostních incidentů

Ohlašování bezpečnostních incidentů je zcela novou povinností, kterou obecné nařízení zavádí. Články 33 a 34 obecného nařízení popisují za jakých podmínek se dozorovému úřadu ohlašují případy porušení zabezpečení osobních údajů. (Janečková, 2018)

Nedílnou součástí minimalizace bezpečnostních incidentů je důsledné a pravidelné informování a školení zaměstnanců, kteří mohou bezpečnostní incident zajistit. (Nonnemann, 2018) Ohlášení porušení zabezpečení osobních údajů musí obsahovat náležitosti obsažené v tabulce 7.

PRAKTICKÁ ČÁST

6 POPIS VYBRANÉ OBCE S OHLEDEM NA OBECNÉ NAŘÍZENÍ

Kapitola je zaměřena na charakteristiku obce a představení a popis posuzovaného objektu.

6.1 Obec

Obce mají v rámci veřejné správy zcela specifické postavení. Jsou základními územními samosprávnými celky a jako jednotky místní samosprávy mají pevné postavení v Ústavě ČR. „*Ústavním pořádkem je garantováno právo občanů svobodně rozhodovat o záležitostech v rámci územního společenství. Obce jsou nezastupitelnou složkou lokální demokracie, která je výrazem práva a schopnosti místních orgánů, v mezích daným zákonem, řídit a regulovat část veřejných záležitostí. Obec je základní administrativní jednotkou státu a statistickou jednotkou.“* (MVČR, 2020)

Obcím plynou povinnosti zejména v souvislosti se zveřejňováním údajů ze své činnosti, s povinně zveřejňovanými informacemi na základě zákona o svobodném přístupu k informacím, musejí dodržovat příslušná ustanovení zákona č. 128/2000 Sb., o obcích a další právní předpisy. (Česko, 2000a)

Obce jsou dle ustanovení § 5 písm. a) a b) zákona o zpracování osobních údajů správci, mají povinnost dodržovat ochranu soukromí a principy transparentnosti.

6.2 Představení posuzovaného objektu

Obec Heršpice jejíž činností se práce zabývá se nachází v okrese Vyškov v Jihomoravském kraji. Celková katastrální rozloha obce činí 1802 hektarů. Pestré dějiny obce sahají až do roku 1237, kdy byla zaznamenána první písemná zmínka o obci. Do historie archeologie se obec zapsala rozsáhlým výzkumem zaniklé obce Konůvky. V současné době žije v obci 863 obyvatel. Učitel Emil Pátek popsal okolí ve dvacátých letech dvacátého století obec následujícím způsobem: *„Heršpice, katastrální a politická obec, leží v dolíku při okresní silnici a protéká jí potůček, jenž pramení v blízkých „Dvorcích“ a vtéká pak pode vsí Hodějicemi do Litavy. V údolí, asi čtvrt hodiny jihovýchodně obce je hájovna a panský dvůr Karlín, jinak Jalový též řečený; týmž směrem, asi jeden a půl hodiny od obce je druhá hájovna u Zlatého jelena. Jižně Heršpic, v krajině lesnaté při státní silnici (bývalé císařské) je myslivna u Bílého vlka. Nedaleko Jalového dvoru směrem východním je třetí hájovna Mušenice, od této pak směrem východním myslivna Vrčava.“* (Pátek, 1928)

6.3 Popis posuzovaného subjektu

Struktura úřadu a personální zajištění:

- Zaměstnanci obecního úřadu (starosta, místostarosta, účetní, referentka).
- Zaměstnanci obce, zpracovávající osobní údaje v rámci své činnosti (knihovnice, kronikářka, správkyně budovy).

Obecní úřad Heršpice je umístěn ve dvoupodlažní budově v řadové zástavbě se dvěma vchody, jež jsou zabezpečeny dveřmi s bezpečnostními zámky. Kanceláře obecního úřadu se nacházejí v 1. NP současně s prostory kulturního domu, do kterých je vstup umožněn samostatným vchodem.

V 1. NP je před samotným vstupem do kanceláří nutné projít chodbou s přepážkou, kde je referentkou vyřizována většina požadavků občanů. Občané se do prostor úřadu dostanou pouze v doprovodu referentky či starosty.

Ve 2. NP budovy se nachází obecní knihovna, spisovna, klubovna a komerční služby. Pro vstup do druhého patra je veřejností užíván vchod do kulturního domu.

Jednotlivé prostory kanceláří jsou zabezpečeny poplachovým zabezpečovacím systémem v rámci jedné zóny. Dálková signalizace je následně řešena prostřednictvím GMS pageru připojeným na komunikátor ústředny. Formou SMS je starostovi a místostarostce předána informace o poplachu. Dodavatel systému provádí pravidelné revize. Zaměstnanci obecního úřadu mají nastaveny vlastní přístupové kódy k poplachovému zabezpečovacímu systému. V rámci obecního úřadu je vedena jednoduchá evidence přístupových kódů a jejich uživatelů.

Každý zaměstnanec obecního úřadu obdržel při nástupu do pracovního poměru osobní svazek klíčů, který obsahuje klíč od vstupu do budovy a klíč do vlastní kanceláře. V kanceláři referentky jsou v uzamčené skříňce uloženy klíče od zbývajících prostor, které jsou jednotlivě označeny. (Capitová, 2019)

7 ETAPY POSOUZENÍ VLIVU

Pracovní skupina WP29 navrhla kritéria na základě, kterých mohou správci údajů určit, zda je provedení DPIA nutné či nikoliv. Tabulka 8 obsahuje základní obsahové náležitosti kontrolního seznamu, které jsou definovány v čl. 35 odst. 7 obecného nařízení.

Tabulka 8 Kontrolní seznam kritérií přijatelného DPIA dle WP29 (upraveno autorem, Belgium, 2017)

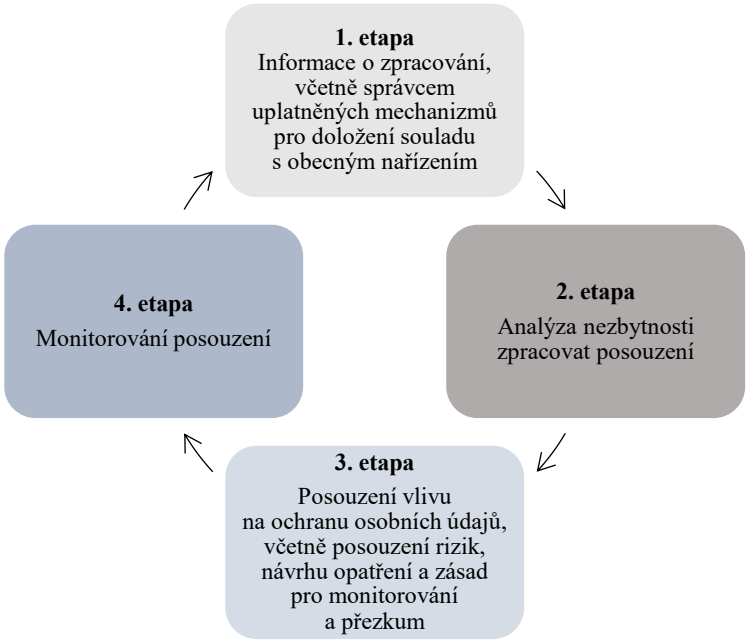
Kritéria přijatelného posouzení vlivu na ochranu osobních údajů		
Obsahové náležitosti	**Ano**	**Ne**
Systematický popis zpracování (čl. 35 odst. 7 písm. a)		
Přihlíží se k povaze, rozsahu, kontextu a účelům zpracování		
Zaznamenávají se osobní údaje, příjemce a doba, po kterou jsou osobní údaje uloženy?		
Uvádí se funkční popis operace zpracování?		
Stanovení prostředků, na nichž jsou osobní údaje závislé (hardware, software, sítě, lidé, tištěné dokumenty a jejich přenos)		
Soulad se schválenými kodexy chování (čl. 35 odst. 8)		
Posouzení nezbytností a přiměřenosti operací zpracování (čl. 35 odst. 7 písm. b)		
Jsou stanovena opatření určená k zajištění souladu s nařízením (čl. 35 odst. 7 písm. d) a 90 bodem odůvodnění		
Opatření za účelem přiměřenosti a nezbytnosti zpracování na základě:		
Stanovených, výslovně vyjádřených a legitimních účelu (čl. 5 odst. písm. b)		
Zákonnosti zpracování (článek 6)		
Údajů, které jsou přiměřené, relevantní a omezené na nezbytný rozsah (čl. 5 odst. 1 písm. c)		
Omezené doby uložení (čl. 5 odst. 1 písm. e)		
Opatření za účelem podpory práv subjektů údajů:		
Informace poskytnuté subjektu údajů (články 12, 13, 14)		
Právo na přístup a přenositelnost údajů (články 15 a 20)		
Právo na opravu a výmaz údajů (články 16, 17 a 19)		
Právo vznést námitku a na omezení zpracování (články 18, 19 a 21)		
Vztahy se zpracovatelem (článek 28)		
Ochrana týkající se předávání údajů mezinárodním subjektům		
Před konzultací (článek 36)		

Tabulka 9 Kontrolní seznam kritérií přijatelného DPIA dle WP29, pokračování tabulky (upraveno autorem, Belgium, 2017)

Kritéria přijatelného posouzení vlivu na ochranu osobních údajů		
Obsahové náležitosti	**Ano**	**Ne**
Zhodnocení původu, povahy, zvláštností a závažnosti rizik nebo přesněji pro každé riziko (nežádoucí přístup, nežádoucí úpravy a zánik dat) z hlediska subjektu údajů:		
Jsou zohledněny zdroje rizik		
Jsou určeny vlivy na práva a svobody subjektů údajů v případě události (nežádoucí přístup, nežádoucí úpravy a zánik dat)		
Hrozby, které mohou mít za následek neoprávněný přístup, nežádoucí úpravy, zánik dat		
Byl proveden odhad pravděpodobnosti a závažnosti?		
Byla stanovena opatření určená k řešení těchto rizik? (Čl. 35 odst. 7 písm. d) a bod 90. odůvodnění):		
Jsou zapojeny zúčastněné strany?		
Vyžádání posudku pověřence pro ochranu osobních údajů (čl. 35 odst. 2)		
Získání stanoviska subjektu údajů nebo jejich zástupců (čl. 35 odst. 9)		

7.1 Etapy DPIA

Každá z následující etapy obsahuje soubor kroků, které slouží k zajištění povinnosti provést posouzení vlivu. Obrázek 7 znázorňuje schéma postupu činností správce dle DPIA.



Obrázek 7 Schéma postupu činností správce dle jednotlivých etap DPIA (ÚOOÚ, 2020)

7.1.1 1. etapa – informace o zpracování

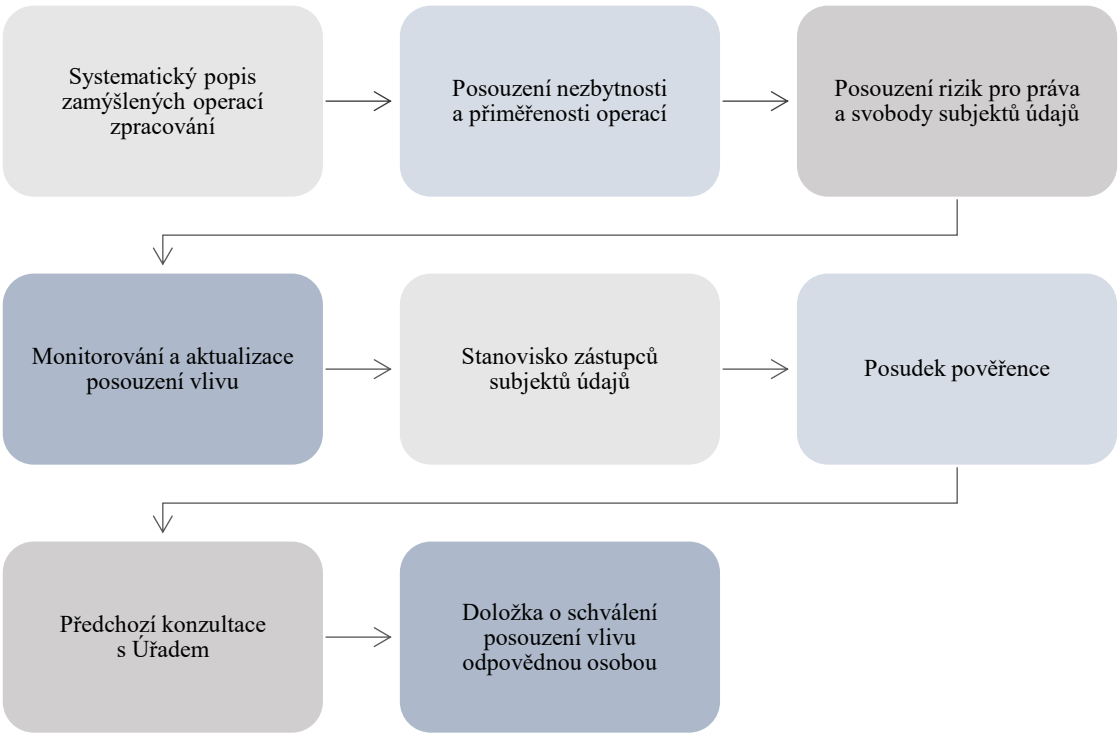
Pro provedení analýzy, zda je nutné provádět DPIA, je nezbytné mít k dispozici informace. V zásadě lze vycházet ze záznamů o činnostech zpracování, které musí každý správce vést, v souladu s čl. 30 obecného nařízení. (ÚOOÚ, 2020)

7.1.2 2. etapa – Analýza, zda je nezbytné provést DPIA

Povinnost posouzení vlivu je uložena správcům, kteří zpracovávají osobní informace mající za následek vysoká rizika pro práva fyzických osob. Určit, zda se na správce povinnost vztahuje lze uskutečnit nahlédnutím do seznamu operací zpracování, které nepodléhají posouzení vlivu. Pokud správce výjimku nenalezne, měl by provést vlastní hodnocení rizikovosti zpracování osobních údajů. (ÚOOÚ, 2020)

7.1.3 3. etapa – Provedení posouzení vlivu

Posouzení vlivu je možné rozdělit do osmi částí znázorněných v obrázku 8 v jejichž jednotlivých krocích provádí správce řadu úkonů.

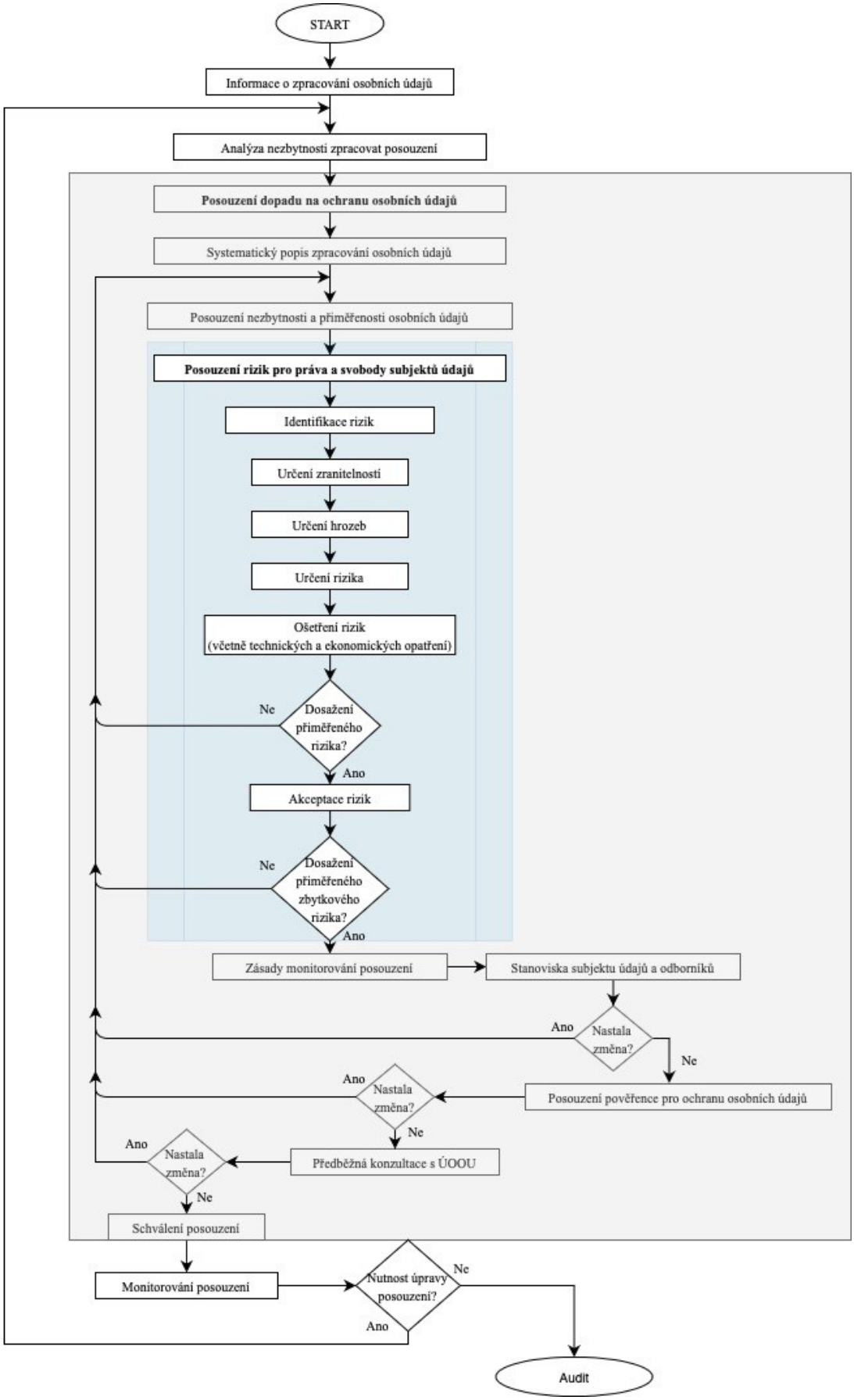


Obrázek 8 Provedení posouzení vlivu (vlastní zpracování, ÚOOÚ, 2020)

7.1.4 4. etapa – Monitorování dodržování opatření a pravidelné revize posouzení vlivu

Pravidelné monitorování a přezkoumávání rizik probíhá před začleněním nových aktiv do zpracování, vznikem nových hrozeb, vznikem synergických efektů hrozeb, identifikací nových zranitelností, po porušení zabezpečení osobních údajů. Využít lze nástroje pro monitorování zpracování osobních údajů, varování a informací vydávaných CERT/CSIRT. (ÚOOÚ, 2020)

Obrázek 9 na následují straně znázorňuje schéma postupu správce při provádění DPIA.



Obrázek 9 Postup správce pro provádění DPIA (vlastní zpracování, ÚOOÚ, 2020)

7.2 Vymezení technických a organizačních opatření

Technická opatření se zaměřují na:

- Zajištění fyzické bezpečnosti míst zpracování osobních údajů.
- Zabezpečení práce s mobilními zařízeními a vzdálené práce.
- Zabezpečení komunikačního prostředí/sítí.
- Správu a ověřování identity určených osob, řízení přístupových oprávnění.
- Monitorování a zaznamenávání činností určených osob.
- Detekci, řešení a vyhodnocení mimořádných událostí při zpracování osobních údajů, ochrana před škodlivými kódy.
- Ochranu identity subjektů údaj.
- Zajištění požadované úrovně dostupných osobních údajů.
- Zajištění zálohování a archivace.
- Zajištění aplikační bezpečnosti apod. (ÚOOÚ, 2020)

Organizační opatření se zaměřují na:

- Zajištění systému řízení ochrany osobních údajů.
- Zajištění řízení aktiv, zajištění řízení rizik, klasifikaci osobních údajů.
- Řízení dodavatelů/zpracovatelů.
- Organizační zajištění zpracování osobních údajů.
- Bezpečnost lidských zdrojů.
- Zajištění požadované dokumentace zpracování osobních údajů.
- Řízení monitorování zpracování osobních údajů a revize posouzení vlivu. (ÚOOÚ, 2020)

8 VYHODNOCENÍ RIZIK

Hodnocení rizik může mít různé podoby a postupy, závisí na získaných informacích, možnostech hodnotitelů, účelu posuzovaných rizik, druhu ohrožení apod. Metodu, kterou můžeme pro hodnocení rizik subjektů údajů a správců použít je jednoduchá bodová polokvantitativní metoda „PZH“. Pomocí metody vyhodnocujeme riziko ve třech složkách, a to s ohledem na pravděpodobnost (P), zranitelnost (Z) a výskytu hrozby (H). (Nezmar, 2017)

8.1 Aplikace jednoduché kvantitativní metody pro vyhodnocení rizika

Pomocí zvolené metody je riziko vyhodnocováno ve třech složkách s ohledem na:

- **pravděpodobnost uplatnění hrozby (P)** – hodnocení závažnosti události. Definují se pomocí hodnoty, jenž vyjadřuje závažnost dopadu pro subjekty údajů a správců. Hodnocení dopadů se provádí v závislosti na zpracovávaných informacích, druhu, rozsahu újmy způsobené fyzickým osobám a správci, jak je uvedeno v tabulce 11. Stupnice dopadu je stanovena vzestupně číslem od 1 do 4. (ÚOOÚ, 2020)
- **míra zranitelnosti (Z)** – Definuje se pomocí hodnoty vyjadřující využití zranitelnosti na základě přijatých opatření. V tabulce 12 je uvedena stupnice míry zranitelnosti vzestupně od 1 do 4. (ÚOOÚ, 2020)
- **míra hrozby (H)** – míra pravděpodobnosti výskytu hrozby. Definuje se pomocí hodnocení vyjadřující četnost výskytu hrozeb. V tabulce 13 je uvedena stupnice odhadu pravděpodobnosti výskytu hrozby stanovena je vzestupně od 1 do 4. (ÚOOÚ, 2020)

Pravděpodobnost vzniku hrozby a dopady z ní vyplývající jsou uvedeny v tabulce 11. Zranitelnost je vyjádřena v tabulce 12 a výskyt hrozby je uveden v tabulce 13.

Na základě stanovených koeficientů pro hodnocení pravděpodobnosti, zranitelnosti a hrozby se vypočte míra rizika „R“.

Vzorec pro výpočet celkového rizika

R = P x Z x H (1.1)

Bodové rozpětí v tabulce 19 vyjadřuje zbytkové riziko po přijetí vhodných opatření pro snížení rizika a prioritu bezpečnostních opatření.

Tabulka 10 Rizikové stupně (vlastní zpracování)

Rizikový stupeň	R	Míra rizika
I.	≥ 48	Kritické riziko
II.	18 ÷ 36	Vysoké riziko
III.	6 ÷ 17	Střední riziko
IV.	≤ 5	Nízké riziko

Analýza je provedena z pohledu daného subjektu údajů a správců dle obecného nařízení. Hodnota dopadu se odvíjí v závislosti na zpracovávaných údajích, druhu a rozsahu újmy způsobené fyzickým osobám a správci. Tabulkami 11, 12, 13 byla definovaná aktiva ohodnocena dle stupnic.

Tabulka 11 P – dopady pro subjekty údajů a správce, (vlastní zpracování, ÚOOÚ, 2020)

Dopady		**Dopady na subjekty údajů**	**Finanční újma subjektů údajů**	**Finanční náklady správce**	**Narušení běžných činností správce**	**Ztráta důvěryhodnosti správce**	**Dopad na zaměstnance správce**	**Mezinárodní vztahy (předávání)**
1	Nízké	Vede k nepohodlí subjektu údajů (podrážděnost, krátkodobé časové nároky pro opětovné zadávání údajů, komunikace se správcem)	Finanční újma nehrozí.	Vede přímo či nepřímo ke ztrátám menším než 0,05 % ročního rozpočtu.	K narušení běžných činností nedochází, spíše ke zvýšeným časovým nárokům při zpracování osobních údajů.	Může negativně ovlivnit vztahy s jinými částmi správce, jinými subjekty nebo vztahy s veřejností, negativní publicita bude omezena na bezprostřední okolí a nebude mít dlouhé trvání (nepříjemnosti se subjekty údajů, nutnost jednání a dalšími subjekty, negativní či veřejné reakce subjektů údajů).	Může docházet ke krátkodobě nepříjemnosti při zpracování osobních údajů (zdržení a podráždění zaměstnanců nebo členů správce, jiné zdravotní dopady nehrozí).	Potřeba jednání mezi správcem a zahraničním partnerem o charakteristikách zpracování osobních údajů.
2	Střední	Vede k menší újmě (stres, nepohodlí, drobné fyzické obtíže, nedostatek porozumění, omezení přístupu ke službám správce či jiných subjektů, časové nároky spojené s řešením dopadu).	Odhadovaná finanční újma do 5000 Kč/subjekt údajů.	Vede přímo či nepřímo ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu.	Omezuje provádění běžných činností, narušení řádného řízení nebo fungování části nebo celého správce, krátkodobý výpadek služeb správce.	Negativní ovlivnění vztahů s jinými subjekty nebo veřejností, negativní publicita se týká omezené zájmové skupiny nebo je široká, ovšem krátkodobá (krátkodobé omezení přístupu ke službám využívaným správcem).	Může negativně ovlivnit výkon zaměstnanců při zpracování osobních údajů (stres zaměstnanců a členů správce, drobné fyzické a zdravotní potíže).	Vytváří negativní obraz správce u zahraničních partnerů v jenom teritoriu, případně v jednom státě, vede k dočasnému omezení zahraniční participace na zpracování osobních údajů.
3	Vysoké	Vede k závažné újmě (napadení, nepříznivý zdravotní stav, deprese, ztížené ekonomické znevýhodnění (černé listiny), krádež identity, předvolání vyšetřujícími orgány).	Odhadovaná finanční újma od 5000 do 50000 Kč/subjekt údajů (zneužití finančních prostředků, údajů poškození majetku).	Vede přímo či nepřímo ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu.	Způsobuje dočasné zastavení nebo podstatné narušení běžných činností správce nebo poškodit rozvoj prosazování cílů a zájmů správce.	Závažně ovlivňuje vztahy s jinými subjekty nebo veřejností s následkem celostátní negativní publicity.	Může způsobit závažné, krátkodobé omezení výkonu při zpracování osobních údajů (zhoršení zdravotního stavu zaměstnanců, členů, krátkodobá pracovní neschopnost).	Vytváří negativní obraz správce u zahraničních partnerů ve světě, vede k dočasnému nebo trvalému omezení zahraniční participace na zpracování osobních údajů.
4	Kritické	Vede k velmi závažné újmě, případnému ohrožení či ztrátě života (smrt, invalidita, dlouhodobě nepříznivý zdravotní stav a pracovní neschopnost, ztráta zaměstnání, velmi ztížené uplatnění, vyloučení, omezení práv).	Odhadovaná finanční újma od 50000 Kč/subjekt údajů (neschopnost splácet dluh, ztráta majetku).	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu.	Může dlouhodobě a závažně ovlivnit vztahy s jinými subjekty nebo veřejností s následkem celostátní negativní publicity, s dlouhodobými účinky a újmou (soudní proces, likvidace, vznik nesplatitelného dluhu).	Závažně a dlouhodobě ovlivňuje vztahy s jinými subjekty nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky na přijetí odpovědnosti (černé listiny, ztráta konkurenceschopnosti, masivní, negativní, dlouhodobé ohlasy v médiích včetně zahraničních).	Může způsobit závažné dlouhodobé omezení výkonu při zpracování osobních údajů (útoky na členy nebo zaměstnance společnosti, odchod zaměstnanců, dlouhodobá pracovní neschopnost).	Vytváření negativního obrazu České republiky v oblasti zpracování a ochrany osobních údajů po celém světě, spojeného s dlouhodobým nebo trvalým omezením participace zahraničních subjektů nebo i států na zpracování osobních údajů.

Tabulka 12 Z – míra zranitelnosti (vlastní zpracování, ÚOOÚ, 2020)

Míra zranitelnosti		**Popis**
1	Nízká	Využití zranitelnosti se nejeví jako možné. Existují opatření, která jsou schopna včas detekovat pokusy o narušení integrity, dostupnosti a důvěrnosti osobních údajů; přijatá opatření jsou schopna zamezit pokusům o narušení integrity, dostupnosti a důvěrnosti osobních údajů; účinnost opatření je pravidelně kontrolována; opatření jsou pravidelně revidována.
2	Střední	Využití zranitelnosti se jeví jako obtížné. Existují opatření, která jsou jen omezeně schopna včas detekovat pokusy o narušení integrity, dostupnosti a důvěrnosti osobních údajů; přijatá opatření jsou schopna zamezit pokusům o narušení integrity, dostupnosti a důvěrnosti osobních údajů; účinnost opatření je pravidelně kontrolována; opatření jsou pravidelně revidována.
3	Vysoká	Využití zranitelnosti se jeví jako možné. Neexistují detekce pokusů o narušení integrity, dostupnosti a důvěrnosti osobních údajů; přijatá opatření jsou schopna zamezit pokusům o narušení integrity, dostupnosti a důvěrnosti údajů jen omezeně; účinnost opatření není kontrolována; opatření nejsou pravidelně revidována.
4	Kritická	Využití zranitelnosti se jeví jako snadné. Neexistuje detekce pokusů o narušení integrity, dostupnosti a důvěrnosti osobních údajů; nejsou přijata opatření k zamezení pokusů o narušení integrity, dostupnosti a důvěrnosti osobních údajů nebo je jejich účinnost velmi omezena; účinnost opatření není kontrolována; opatření nejsou revidována.

8.1.1 Zranitelnosti

- Zastaralost informačních a komunikačních technologií podporujících zpracování.
- Nedostatečná údržba informačních a komunikačních technologií podporujících zpracování osobních údajů.
- Nedostatečná fyzická ochrana míst zpracování osobních údajů.
- Nedostatečné podvědomí určených osob o postupech zpracování a zabezpečení osobních údajů.
- Nedostatečné řízení přístupu k osobním údajům.
- Nedostatečné postupy při identifikování a odhalení mimořádných událostí a nebezpečných jevů.
- Nedostatečné monitorování činností, neschopnost odhalit nežádoucí způsoby chování nebo pochybení určených osob.
- Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností a bezpečnostních rolí v rámci zpracování osobních údajů.

- Nedostatečná ochrana aktiv.
- Nevhodná bezpečnostní architektura.
- Nedostatečná kontrola. (ÚOOÚ, 2020)

Tabulka 13 H – výskyt hrozby (vlastní zpracování, ÚOOÚ, 2020)

Míra hrozby		**Popis**
1	Nízká	Frekvence výskytu hrozby není častější než jednou za pět let.
2	Střední	Frekvence výskytu hrozeb se pohybuje v rozpětí od jednoho roku do pěti let.
3	Vysoká	Frekvence výskytu hrozeb se pohybuje v rozpětí od jednoho měsíce do jednoho roku.
4	Kritická	Frekvence výskytu hrozeb se pohybuje v častějších intervalech než jednou za měsíc.

8.1.2 Hrozby

- Poškození nebo selhání technického nebo programového vybavení (HW, SW, nosiče osobních údajů).
- Neoprávněný přístup k osobním údajům.
- Zavedení škodlivého kódu.
- Narušení fyzické bezpečnosti.
- Přerušení poskytování služeb elektronických komunikací, komunikačních služeb nezbytných pro zpracování osobních údajů.
- Zneužití nebo neoprávněná modifikace údajů.
- Ztráta, odcizení či poškození aktiva s osobními údaji.
- Nesprávné řízení ochrany osobních údajů.
- Pochybení ze strany určených osob.
- Zneužití vnitřních prostředků.
- Úmyslné poškození, selhání prostředí, nedostatek zaměstnanců s potřebou odbornou úrovní.

- Sociální inženýrství, špionážní techniky, zneužití vyměnitelných technických a jiných nosičů dat, napadení komunikace. (ČSN ISO/IEC 27005, 2018), (Česko, 2018), (ÚOOÚ, 2020)

Na základě systematické analýzy dotazníkového šetření identifikoval zhotovitel Systémové analýzy působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů jednotlivé role subjektu údajů a přiřadil k nim příslušná aktiva. V tabulce 14 jsou uvedeny spojitosti mezi rolí a aktivem.

Tabulka 14 Role subjektu údajů (PZK s.r.o., 2018)

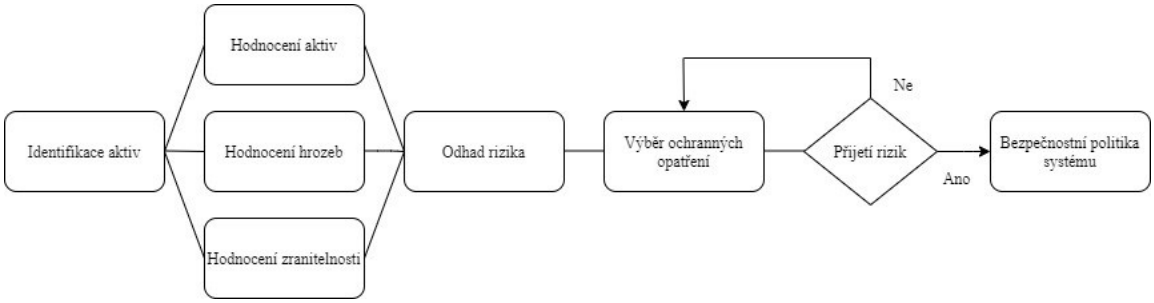
Role	Aktivum
Občan	• *Listinné úložiště v rámci výkonu agend úřadu (L)* • *Informační systém spisové služby (E)* • *Agendové informační systémy – samostatná působnost (E)* • *Agendové informační systémy – přenesená působnost (E)* • *Ekonomický informační systém (E)* • *Portály – veřejné i neveřejné webové portály (E)* • *Ostatní elektronická úložiště (E)*
Zaměstnanec	• *Listinné úložiště v rámci výkonu agend úřadu (L)* • *Listinné úložiště v rámci vnitřního chodu úřadu (L)* • *Informační systém spisové služby (E)* • *Ekonomický informační systém (E)* • *Portály – veřejné i neveřejné webové portály (E)* • *Ostatní elektronická úložiště (E)*
Volený zástupce	• *Listinné úložiště v rámci vnitřního chodu úřadu (L)* • *Informační systém spisové služby (E)* • *Ekonomický informační systém (E)* • *Portály – veřejné i neveřejné webové portály (E)* • *Ostatní elektronická úložiště (E)*

Tabulka 15 Role subjektu údajů, pokračování tabulky (PZK s.r.o., 2018)

Role	Aktivum
Zvláště zranitelné kategorie subjektu údajů - nezletilí občané, nesvéprávné osoby	• *Listinné úložiště v rámci výkonu agend úřadu (L)* • *Informační systém spisové služby (E)* • *Agendové informační systémy – samostatná působnost (E)* • *Agendové informační systémy – přenesená působnost (E)* • *Ekonomický informační systém (E)* • *Portály – veřejné i neveřejné webové portály (E)* • *Ostatní elektronická úložiště (E)*

8.2 Hodnocení aktiv

Aktivum tvoří základní zdroj řízení rizik. Aktivum lze chápat jako objekt (aplikaci, informační systémy, kartotéky, spisovny, portály, evidence nebo jiné elektronické úložiště). Hodnotu aktiva lze vyjádřit kvantitativně nebo kvalitativně. Hodnocení každého aktiva by měl provést správce a zároveň tak určit jaký dopad na organizaci by měla ztráta dostupnosti, důvěrnosti a integrita daného aktiva. (PZK s.r.o., 2018) Obrázek 10 znázorňuje identifikaci aktiv.



Obrázek 10 Identifikace aktiv (Král, 2010)

8.3 Míra rizik

Pro stanovení kategorie závažnosti vyhodnocení rizik je možné rozdělení do čtyř rizikových stupňů (I. až IV.). Výsledné hodnocení míry rizika (R) je poté následující:

I. **Kritické riziko** – riziko je nepřípustné a musí být bezodkladně zahájeny kroky k jeho eliminaci. Riziko je považováno za vysoké ve smyslu čl. 36 odst. 1 obecného nařízení. Hodnota kritického rizika je definovaná v rozmezí od 48 do 64.

II. **Vysoké riziko** – riziko je z dlouhodobého hlediska nepřípustné a musí být zahájeny systematické kroky pro jeho odstranění. Riziko je krátkodobě akceptovatelné pověřencem. Hodnota vysokého rizika je definovaná v rozmezí od 18 do 36.

III. **Střední riziko** – riziko je vhodné snížit finančně méně nákladnými opatřeními. Riziko akceptovatelné pověřence. Hodnota středního rizika je definovaná v rozmezí od 6 do 17.

IV. **Nízké riziko** – riziko je považováno za automaticky akceptovatelné. Hodnota nízkého rizika je definovaná v rozmezí od 1 do 5. (ÚOOÚ, 2020)

Z rizikové skóre před přijetím opatření v tabulce 16 lze vyčíst, které hrozby se budou pro obec jevit jako nejzávažnější a budou muset být zajištěny technickými a organizačními opatřeními. Současně která aktiva, mohou mít pro subjekt údajů a správce největší dopad a budou vyžadovat zvýšenou pozornost.

Tabulka 16 Přehledná analýza rizik před přijetím opatření (vlastní zpracování, PZK s.r.o., 2018)

Aktivum	Dopad	Pravděpodobnost uplatnění hrozby								Zranitelnost jednotlivých aktivit vůči hrozbám								Rizikové skóre před přijetím opatření							
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu
Listinné úložiště v rámci výkonu agend úřadu (L)	3	2	2	3	3	3	2	2	3	3	3	4	3	3	2	4	4	**18**	**18**	**36**	**27**	**27**	**12**	**24**	**36**
Listinné úložiště v rámci vnitřního chodu úřadu (L)	2	2	1	3	2	2	2	2	2	3	3	4	3	3	2	4	4	**12**	**6**	**24**	**12**	**12**	**8**	**16**	**16**
Informační systém spisové služby (E)	3	2	3	2	2	3	3	2	2	2	2	2	2	2	3	3	3	**12**	**18**	**12**	**12**	**18**	**27**	**24**	**24**
Agendové informační systémy – samostatná působnost (E)	3	2	2	3	2	2	3	2	2	2	2	2	2	3	3	3	3	**12**	**12**	**18**	**12**	**18**	**27**	**18**	**18**
Agendové informační systémy – přenesená působnost (E)	3	2	2	3	2	2	3	2	2	2	2	2	2	3	3	3	3	**12**	**12**	**18**	**12**	**18**	**27**	**24**	**24**
Ekonomický informační systém (E)	3	2	3	3	2	2	3	2	2	2	3	3	3	3	3	3	3	**12**	**27**	**27**	**18**	**18**	**27**	**24**	**24**
Portály – veřejné i neveřejné webové portály (E)	2	4	3	3	2	2	3	2	2	3	2	3	3	2	3	3	3	**24**	**12**	**24**	**12**	**8**	**24**	**12**	**12**
Ostatní elektronická úložiště (E)	1	1	2	3	2	4	2	3	3	2	2	3	3	3	2	4	4	**2**	**4**	**9**	**6**	**12**	**4**	**12**	**12**

8.4 Opatření navržená k zajištění technického a organizačního zabezpečení

Posouzení rizik lze zpracovat konzervativním postupem spojeným s formálním zjištěním informací, jejich vyhodnocením a dokumentací nebo prostřednictvím softwarových aplikací, které umožňují popsat charakteristiky DPIA, zdokumentovat jednotlivé kroky, které byly v procesu dodrženy, posoudit dopad na soukromí, identifikovat a spravovat rizika ochrany osobních údajů a zabezpečení Software nabízí například společnost Enactia Ltd., Acresia Consulting s.r.o., Vigilant Software Ltd.

Správce provádí sám hodnocení zpracování osobních údajů. Na základě sestaveného hodnocení pro určení hodnot u dopadů, zranitelnosti a hrozeb, které se provede za účasti určených odborníků, jež určí správce.

Ze seznamu zranitelností a hrozeb jsou odborníky sestaveny kombinace opatření jejichž cílem je minimalizovat dopady na práva a svobody fyzických osob a správce. Přijatá opatření jsou aplikovaná v tabulce 17.

Tabulka 17 Přijatá opatření připravená správcem
(vlastní zpracování, ÚOOÚ, 2020)

Přijaté opatření	Aktivum	Zranitelnost	Hrozba
1 Správa řízení identity	Aplikace	Nedostatečné řízení přístupu k osobním údajům.	Zneužití nebo neoprávnění modifikace osobních údajů.
2 Řízení přístupu	Server	Nedostatečné stanovení bezpečnostních pravidel.	Neoprávněný přístup k osobním údajům, zneužití.
		Nepřesné, nejednoznačné vymezení práv a povinností bezpečnostních rolí v rámci zpracování osobních údajů.	Neoprávněná modifikace osobních údajů, pochybení ze strany určených osob.

Tabulka 18 Přijatá opatření připravená správcem, pokračování tabulky (vlastní zpracování, ÚOOÚ, 2020)

Přijaté opatření	Aktivum	Zranitelnost	Hrozba
3 **Řízení aktiv**	Aplikace	Nedostatečné podvědomí zaměstnanců o postupech zpracování a zabezpečení osobních údajů, nedostatečné stanovení bezpečnostních pravidel.	Zneužití vnitřních prostředků, úmyslné poškození, pochybení ze strany zaměstnance.
4 **Zálohování a archivace dat**	Server	Zastaralost informačních a komunikačních technologií podporujících zpracování.	Poškození nebo selhání technického nebo programového vybavení (HW, SW, nosiče osobních údajů).
		Nedostatečná údržba informačních a komunikačních technologií podporujících zpracování osobních údajů.	Ztráta, odcizení či poškození aktiva s osobními údaji.
		Nedostatečná kontrola.	Úmyslné poškození, selhání prostředí, nedostatek zaměstnanců s potřebou odbornou úrovní.
			Selhání prostředí.

Tabulka 19 na následující straně obsahuje rizikové skóre po přijetí opatření technických a organizačních opařeních. Z jednotlivého bodového hodnocení dopadu, hrozeb a zranitelnosti lze vyčíst, kterým rizikům bude nutné věnovat zvýšenou pozornost.

Tabulka 19 Přehledná analýza rizik po přijetí opatření (vlastní zpracování, PZK s.r.o., 2018)

Aktivum	Přijatá opatření	Dopad	Pravděpodobnost uplatnění hrozby								Zranitelnost jednotlivých aktivit vůči hrozbám								Rizikové skóre po přijetí opatření							
			Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu
Listinné úložiště v rámci výkonu agend úřadu (L)	**2, 3**	3	1	2	2	2	2	2	2	2	2	2	3	2	2	1	3	2	**6**	**6**	**18**	**12**	**12**	**6**	**18**	**12**
Listinné úložiště v rámci vnitřního chodu úřadu (L)	**2, 4**	2	1	1	2	2	2	2	2	1	2	2	3	2	2	1	3	3	**4**	**4**	**12**	**18**	**8**	**4**	**12**	**6**
Informační systém spisové služby (E)	**1, 4**	3	1	2	1	2	2	3	2	1	1	1	1	1	1	2	2	2	**3**	**6**	**3**	**6**	**6**	**18**	**12**	**6**
Agendové informační systémy – samostatná působnost (E)	**1, 2, 4**	3	1	2	2	1	1	2	2	1	1	1	1	1	2	2	2	2	**3**	**6**	**3**	**3**	**3**	**12**	**12**	**6**
Agendové informační systémy – přenesená působnost (E)	**1, 2, 4**	3	1	2	2	1	1	2	2	1	1	1	1	1	2	2	2	2	**3**	**6**	**6**	**3**	**6**	**12**	**12**	**6**
Ekonomický informační systém (E)	**1, 2, 4**	3	1	3	3	1	1	3	2	1	1	2	2	2	2	2	2	2	**3**	**18**	**18**	**6**	**6**	**18**	**12**	**6**
Portály – veřejné i neveřejné webové portály (E)	**2, 3**	2	3	2	2	1	1	2	2	1	2	1	2	2	1	2	2	2	**12**	**4**	**8**	**4**	**2**	**8**	**8**	**4**
Ostatní elektronická úložiště (E)	**2, 3, 4**	1	1	2	3	2	3	2	2	2	1	1	2	2	2	1	3	3	**1**	**2**	**6**	**4**	**6**	**2**	**6**	**6**

Návrh opatření pro minimalizaci identifikovaných a hodnocených rizik zpracovaných metodou jednoduché bodové polokvantitativní metody „PZH“, bude řešena v následující kapitole práce. Jednotlivé bodové hodnocení dopadů, hrozeb a zranitelností jsou výstupem konzultace stanoveného týmu.

8.4.1 Řešení rizik a přijetí opatření

Závažnost některých rizik vyžaduje redukci míry rizika a zejména v případech kdy je riziko kritické. V takovém případě se nabízí možnost redukce rizika pro zpracovávané osobní údaje, jedná se zejména o:

- Snížení rizika – kdy, jsou na straně správce přijata opatření, tak aby míra rizika byla snížena na přijatelnou úroveň.
- Sdílení/přenesení rizika – správce má možnost přesunout opatření na jiný subjekt například zpracovatele, kdy dochází k pokrytí možných následků v případě mimořádných událostí, například tak že správce pokryje riziko pojistnou smlouvou, která správce ovšem nezbavuje odpovědnosti za zpracování osobních údajů případných negativních dopadů na subjekty údajů.
- Akceptace/podstoupení rizika – v případě, kdy míra rizika není kritická může správce riziko akceptovat/podstoupit bez dalších opatření.
- Vyhnutí se riziku – parametry zpracování jsou správcem modifikovány tak, aby vysokému nebo kritickému riziku nedocházelo.

V případě snížení a sdílení/přenesení rizika je návrh souboru opatření, jehož cílem je redukce míry rizika na přijatelnou úroveň. Technická a organizační opatření určená správcem či zpracovatelem lze rozdělit na preventivní a reaktivní/následná po mimořádné události, která mají za cíl minimalizovat pravděpodobnost opakování. (ÚOOÚ, 2020)

8.4.2 Fyzické zabezpečení osobních údajů a spravovaných dat v prostorách kanceláře

V uvedené oblasti lze využít následující opatření:

- Zaměstnanec zodpovídá za klíče od kancelářských prostor, které obdržel v den nástupu do pracovního poměru. Jejich ztrátu nebo odcizení je zaměstnanec povinen neodkladně nahlásit nadřízenému. Zaměstnanec si musí uvědomit, že ztrátou svěřených klíčů od kancelářských prostor může dojít k úniku citlivých informací a k ohrožení organizace.
- Odchází-li zaměstnanec ze zaměstnání jako poslední má povinnost zkontrolovat a zabezpečit: uzavření oken, zhasnutí světel, aktivovat alarm, uzamknout jednotlivé kanceláře a hlavní vchod do budovy obecního úřadu.

- Povinností zaměstnance je dodržovat zásadu „čistého stolu“, jelikož zaměstnanci při výkonu své činnosti disponují osobními údaji fyzických osob je zajištění bezpečnosti těchto informací žádoucí. Politika čistého stolu je nástrojem, jehož prostřednictvím lze zajistit, aby veškeré dokumenty, které obsahují osobní údaje fyzických osob a zaměstnanec je již nezpracovává, nebo zaměstnanec opustí pracovní místo, byly z pracovního prostoru odstraněny a uzamknuty.
- Povinností zaměstnance je neponechávat dokumenty po skončení scanování nebo kopírování v kopírovacím zařízení. Ponechání opomenutých dokumentů může mít za následek únik citlivých informací.
- Dokumenty v tištěné podobě, již nepotřebné pro výkon agendy zaměstnance je nutné skartovat.
- V neposlední řadě je důležitá i komunikace na pracovišti, v případě, kdy zaměstnanec neví, kam patřičné dokumenty s osobními údaji uschovat, zeptá se zodpovědné osoby.

8.4.3 Fyzické zabezpečení osobních údajů a spravovaných dat v elektronických zařízeních

V uvedené oblasti lze využít následující opatření:

- Zaměstnanec přebírá hmotnou odpovědnost za elektronická zařízení, která jsou mu přidělena v den nástupu do pracovního poměru. V případě ztráty nebo odcizení má zaměstnanec povinnost ohlásit skutečnost zodpovědné osobě. Ztráta fyzického zařízení není jedinou ztrátou, vezmeme-li v potaz i případnou ztrátu a zneužití citlivých údajů, které byly v elektronickém zařízení uloženy.
- Povinností zaměstnance je zabezpečit odpovídající fyzickou ochranu elektronických zařízení za které, převzal hmotnou odpovědnost a předejít tak odcizení nebo krádeži.
- Opouští-li zaměstnanec počítač musí zabezpečit výpočetní techniku uzamčením pracovní plochy či odhlášením.

8.4.4 Softwarové zabezpečení elektronických zařízení

V uvedené oblasti lze využít následující opatření:

- Povinností zaměstnance je zkontrolovat si, zda elektronické zařízení, které mu bylo přiděleno obsahuje nejaktuálnější verzi antivirového programu. Jestliže, elektronické

zařízení neobsahuje nejaktuálnější antivirový program je skutečnost ohlášena zodpovědné osobě, která neprodleně zajistí nápravu.

- Povinností zaměstnance je nastavení co nejvyšší úrovně zabezpečení elektronického zařízení.
- Zaměstnanec je povinný vytvořit heslo v rámci všech přístupů, které obsahuje předepsané náležitosti: minimální délka hesla je 8 znaků libovolné kombinace písmen a číslic, z nichž bude minimálně jedno velké písmeno a minimálně jeden z takzvaných speciálních znaků, například - # * ! .
- Při jakémkoliv podezření na kompromitaci hesla nebo jeho zneužití má zaměstnanec povinnost okamžitě heslo změnit.
- Zaměstnancům je zakázáno přeposílání dokumentů z pracovního emailu na soukromý email, aby se předešlo možnému úniku citlivých informací.
- Zaměstnanec si uvědomuje, že elektronické zařízení, které mu bylo svěřeno neslouží pro soukromé účely.
- Zaměstnanec si uvědomuje, že vstupem na nezabezpečené internetové stránky může být ohrožena bezpečnost elektronického zařízení. Přístup na nezabezpečené internetové stránky je zaměstnavatelem přísně zakázán. Pod nezabezpečenými internetovými stránkami si můžeme představit například: stránky s hazardními hrami nebo webové prohlížeče, které slouží ke stahování souborů.

9 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V KONTEXTU ČINNOSTÍ OBCE

Obce při své činnosti denně nakládají s osobními údaji občanů. Většina zpracovávaných údajů v obecních agendách vyplývá z plnění jiného právního předpisu, ze smlouvy, z výkonu veřejné moci, nebo při plnění úkolu ve veřejném zájmu.

Podmínky stanovení souhlasu jsou definovány čl. 4 odst. 11 obecného nařízení. Souhlas jako projev svobodné vůle musí být:

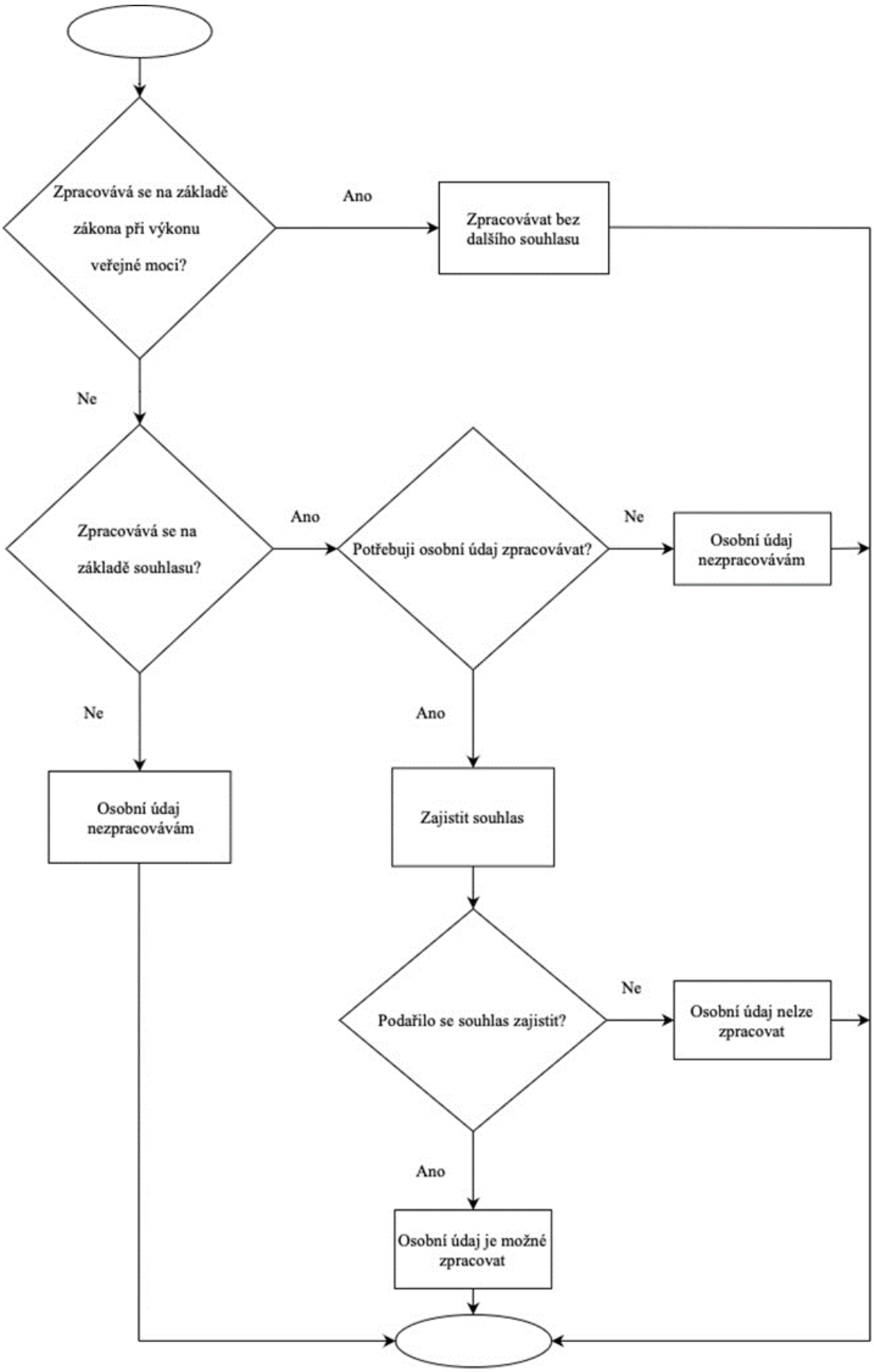
- Svobodný
- Konkrétní
- Informovaný
- Jednoznačný (Nezmar, 2017)

Uvedený souhlas musí být snadno udělitelný i odvolatelný. Občan nesmí být k udělení souhlasu donucen. Jeli zpracování založeno na souhlasu, musí správce doložit, že byl souhlas udělen. Souhlas je vhodné uchovávat v písemné či elektronické podobě. Odvoláním souhlasu o zpracování osobních údajů, mohou být údaje v budoucnu dále zpracovávány pouze za předpokladu, že správce disponuje jiným právním titulem.

9.1 Záznam o činnostech

Záznam o činnostech je písemným dokumentem, který vymezuje typ zpracování osobních údajů. Pro každý typ zpracování je veden samostatný záznam. Záznam musí splňovat obsahové náležitosti stanovené obecným nařízením jako například kontaktní údaje správce, účel zpracování, kategorie subjektu údajů. Vzorový záznam o činnostech zpracování – Místních poplatků je přílohou P I práce.

Obrázek 11 na následující straně znázorňuje postup zpracování osobních údajů na základě zákona při výkonu veřejné moci nebo na základě souhlasu.



Obrázek 11 Postup při zpracování osobního údaje (vlastní zpracování, MŠMT, 2019)

9.2 Vzorové dokumenty a modelové situace

Na webových stránkách Ministerstva vnitra České republiky byly postupně zveřejňovány v rámci metodické pomoci obcím vzorové dokumenty a modelové situace. V dubnu 2016 bylo GDPR schváleno a následně se mělo obecné nařízení implementovat do právní úpravy jednotlivých států EU. Již s koncem roku 2017 byly na webových stránkách MVČR uveřejněny vzorové dokumenty a modelové situace. Vzorové dokumenty obsahují záznamy o jednotlivých činnostech zpracování, které jsou správci povinni vést. (MVČR, 2021a), (MVČR, 2021b)

MVČR nechalo formou veřejné zakázky vypracovat Svazem průmyslu a dopravy v rámci projektu Akademie GDPR celkem 23 modelových situací, které vyvstávají z funkce obce. Modelové situace jsou současně doplněné konkrétními příklady, se kterými se setkáváme v praxi. Průvodce pro přípravu obcí následně rekapituluje nejzásadnější principy, práva a povinnosti ochrany osobních údajů ve vztahu k veřejné správě. Součástí je vymezení osob, které mají přístup ke zpracovávání osobních údajů v dané situaci. Výhodou modelových situací jsou i uvedené příklady dobré i nevhodné praxe při řešení problémů. V případě nutnosti souhlasu je modelová situace doplněná o účel souhlasu, rozsah a náležitosti souhlasu pro zpracování osobních údajů. (MVČR, 2018), (MVČR, 2021b)

Seznam modelových situací:

- Problematika souhlasů se zpracováním osobních údajů.
- Jak postupovat v případě žadatele, který požádá o zajištění všech relevantních informací, které o něm úřad vede.
- Jak postupovat v případě požadavku občana na výmaz záznamů.
- Jak postupovat v případě porušení zabezpečení osobních údajů.
- Kybernetická bezpečnost a ochrana osobních údajů.
- Požadavky na práce s daty uvnitř úřadu.
- Tvorba vnitřních předpisů a metodik.
- Postup s nakládáním osobních údajů v personální praxi a výběrových řízeních.
- Zveřejňování odměn zaměstnanců obcí.
- Platba místních poplatků.
- Uzavírání majetkových transakcí a jejich uveřejňování.
- Administrace výběrových řízení.
- Zveřejňování informaci na úředních deskách.

- Činnosti spojené s jednáním obecních zastupitelstev/rad měst – uveřejňování materiálů před jednáním/po jednání zastupitelstva/rady.
- Požadavky na uveřejňování informací na webu obce.
- Požadavky na uveřejňování informací v místních periodicích.
- Pořádání kulturních/společenských akcí.
- Činnost obecní knihovny.
- Správa bytového fondu.
- Fungování obecní policie.
- Správní řízení v prostředí obce.
- Kontrolní činnost.
- Výkon spisové služby, ukládání a skartace dokumentů. (MVČR,2021b)

9.3 Automaticky uplatnitelné právo subjektu údajů

Právo, které je aplikované automaticky bez nutnosti vyžádání ze strany subjektu údajů. Například právo na informace, právo na výmaz, právo na opravu a aktualizaci.

9.3.1 Uplatnění práva subjektu údajů na informace o zpracování údajů a práva na přístup k údajům v prostředí obce

Obec jako správce osobních údajů musí nejprve občana, který požádá o přístup ke svým osobním údajům, které o něm obec jako správce zpracovává, jednoznačně identifikovat, tak aby se nedopustila porušení zabezpečení osobních údajů. (MVČR, 2018)

Best practices: Pro poskytování informací subjektům údajů zpřístupnila obec na svých webových stránkách formulář, pomocí něhož mohou občané požádat o přístup ke svým osobním údajům. Pro identifikaci totožnosti občana slouží dodatečné ověření prostřednictvím SMS zprávy s přístupovým kódem, který občan zadá do formuláře. Druhou možností je požádat ústně na podatelně obecního úřadu, kde je protokol o podání žádosti o informace sepsán za pomoci referentky a totožnost žadatele je ověřena prostřednictvím nahlédnutí do občanského průkazu.

9.3.2 Uplatnění práva na výmaz osobních údajů v prostředí obce

Subjekt údajů je v případě podání žádosti o výmaz informován o skutečnosti, že jeho žádost, může být z důvodu jiného právního titulu zamítnuta. Zejména v případě, že je zpracování osobních údajů nezbytné pro plnění zákonné povinnosti správce v tomto případě znemožňují

jejich výmaz. Dle čl. 6 obecného nařízení (2016) se jedná zejména o úkony, které jsou prováděny ve veřejném zájmu, při výkonu veřejné moci, je-li zpracování nutné pro plnění smlouvy, jde-li o naplnění oprávněného zájmu správce. Také za předpokladu ochrany životně důležitých zájmů subjektů údajů a v neposlední řadě, jestliže subjekt údajů udělil ke zpracování svůj souhlas.

Best practices: Výmaz by obec měla realizovat až po konzultaci s pověřencem, který by měl být o každém výmazu informován. Doba, po kterou je uchování osobních údajů pomyslným limitem až po splnění zákonné povinnosti, naplnění smlouvy, úkolu ve veřejném zájmu nebo oprávněného zájmu správce. Výmaz osobních údajů, by obec jako správce údajů měla realizovat po skončeném skartačním řízení. Právo je uplatnitelné i na žádost v případě, že je z pohledu subjektu údajů již nezákonné. (MVČR, 2018)

9.4 Zabezpečení osobních údajů v rámci vnitřního chodu

V souvislostí s jednotlivými činnostmi obce můžou nastat situace, které budou vyžadovat zvláštní pozornost a v neposlední řadě také zavedení určitých opatření, aby k nežádoucím vnitřním pochybením obce docházelo v souvislosti s ochranou osobních údajů v co možná nejnižší míře.

9.4.1 Porušení zabezpečení osobních údajů v kontextu obce

Při výkonu činnosti obce může nastat situace, že se vyskytnou události, které mohou být klasifikovány jako bezpečnostní incidenty. Na takový typ bezpečnostního incidentu se vztahuje povinnost ohlašovat porušení dozorovému úřadu. Představuje-li únik informací vznik vysokého rizika pro práva a povinnosti fyzických osob platí povinnost oznámit incidenty i subjektům údajům. Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu je povinností, která vyplývá přímo z obecného nařízení. Nahlášení musí být uskutečněno bez zbytečného odkladu po zjištění bezpečnostního incidentu, nejpozději pak do 72 hodin. Specifikované náležitosti hlášení jsou uvedeny v čl. 33 obecného nařízení. (Evropská unie, 2016)

Má-li porušení za následek vysoké riziko pro soukromý subjektů osobních údajů, je povinností obce oznámit tuto skutečnost i samotným subjektům. Vypracování analýzy rizik a na základě zjištění klasifikace incidentů, které je nutné hlásit. Rozdělení odpovědnosti a vytvoření komunikačního schématu pro příklad ohlašování. (MVČR, 2018)

9.4.2 Informační bezpečnost a zabezpečení osobních údajů

Používání informačních systémů orgány veřejné moci je upraveno zákonem č. 365/2000 Sb., o informačních systémech veřejné správy. Vystupuje jako funkční celek nebo část, která zabezpečuje cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a nástroje umožňující výkon informačních činností. (Česko, 2000c)

Obce jsou povinny přijmout opatření, která odpovídají bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací. Dle čl. 32 obecného nařízení musí obec provést s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování vhodná technická a organizační opatření k zajištění zabezpečení daného rizika. (MVČR, 2018)

V tabulce 20 jsou shrnuty základní oblasti bezpečnosti osobních údajů, na které by se měla zaměřit každá organizace.

Tabulka 20 Základní oblasti bezpečnosti osobních údajů
(vlastní zpracování, MVČR, 2018)

Oblast	Opatření
Zajištění fyzické bezpečnosti	Jedná se především o listinnou podobu zpracování jejím obsahem je kontrola a zajištění bezpečnosti přístupu do prostor, kde je možné dostat se k nezabezpečeným datům. Jedná se zejména o zajištění uzamykatelnosti prostor, vymezení osob, které mají k dispozici klíč, kontrola přístupu do budovy, strategii čisté pracovní plochy.
Autorizace a autentizace	Uživatel má umožněný přístup pouze k osobním údajům, které potřebuje pro výkon své agendy. Přístupy jsou jasně organizačně a technicky zajištěny. Z pohledu autentizace je zásadní politika hesel.
Ochrana proti kybernetickým incidentům a jejich detekce	Ochrana před kybernetickými hrozbami pomocí bezpečnostních nástrojů. U detekce kybernetických bezpečnostních incidentů je možné napojení na dohledové centrum eGovermentu nebo externí firmu, jejímž úkolem je provádění monitoringu a bezpečnostních logů.
Zavedení sytému řízení informační bezpečnosti	Je především organizačním opatřením. Systém politik zajišťující výkon a dokumentaci agendy informační bezpečnosti v organizaci.

9.4.3 Požadavky na práce s daty uvnitř úřadu

Agenda obce obsahuje zpracovatelské operace počínaje uložením, přepisováním, výmazu, předání až po zveřejnění. Na veškeré interní procesy úřadu se vztahují povinnosti, které vyplývají z požadavků obecného nařízení. Účelem zpracování je zajištění činností obecního úřadu a jeho personální, mzdové a účetní, administrativní agendy spojené s výkonem samostatné či přenesené působnosti obce. V kontextu obce se jedná o základní účely zpracování jako:

- Vedení zaměstnanecké agendy.
- Správa účetnictví obce.
- Správa informačních systémů, sloužící k naplňování činnosti obecního úřadu. (MVČR, 2018)

9.4.4 Vnitřní předpisy a metodiky

Dokumenty jejichž charakter je určený pro vnitřní využití a zavazují organizaci a zaměstnance k jejich plnění. Vnitřní předpis je vydaný za účelem konkretizace úkolů a stanovení povinností zaměstnanců vyplývající z právních předpisů, nebo z podnětu obce a jejich vnitřních potřeb. Vnitřní předpis je na rozdíl od metodického doporučení vynutitelný, zaměstnanec může být za jeho nedodržování sankciován. Povinností zaměstnavatele je seznámit všechny stávající i budoucí zaměstnance s vnitřním předpisem, který musí být umístěn na přístupném místě. (SMO ČR, 2020)

Best practices: Proces pravidelné aktualizace současných i nových vnitřních předpisů. Centralizace vnitřních pokynů organizace na jedno místo, kde bude zajištěna dostupnost všem zaměstnancům. Součástí práce je příloha P II – Směrnice obce k ochraně osobních údajů dle GDPR.

9.4.5 Místní poplatky

Zákon č. 565/1990 Sb., o místních poplatcích definuje, jaké poplatky může obec zavést a vybírat. V rámci obce vybíráme místní poplatek ze psů, poplatek za užívání veřejného prostranství, poplatek za provoz sytému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů. (Česko, 1990) V Návaznosti na něj vydané obecně závazné vyhlášky obce.

S výběrem místních poplatků obcí dochází ke zpracování osobních údajů poplatníků či plátců poplatků. Mezi problematické poplatky se z hlediska obce zahrnuje poplatek ze psů a poplatek za odpad, kde dochází ke zpracování údajů o zdravotním stavu (například informace o zdravotním postižení či nevidomosti), které řadíme do zvláštní kategorie. (MVČR, 2018), (SMO ČR, 2020)

Best practices: Pracovnice obce zodpovědná za vyměřování a výběr poplatků, neposkytne třetí osobě informace o průběhu konkrétního daňového řízení s odkazem na zásadu neveřejnosti správy daní a poplatků, povinnost zachovat mlčenlivost správce daně současně se zajištěním ochrany osobních údajů a soukromí plátců daně. V tabulce 21 jsou uvedeny příklady aplikace všech zásad obecného nařízení.

Tabulka 21 Aplikace zásad obecného nařízení v kontextu místních poplatků (zpracování vlastní, MVČR, 2018)

Zásada	**Aplikace obecného nařízení**
Zákonnosti, korektnosti a transparentnosti	Obec musí mít pro zpracování osobních údajů právní důvod, platnou obecní vyhlášku, kterou se zavádí příslušný poplatek, a upravuje náležitosti stanovené zákonem. Obec zpracovává osobní údaje plátců a poplatníků korektně a zákonným a transparentním způsobem.
Účelového omezení zpracování osobních údajů	Osobní údaje jsou zpracovávány za účelem správného zajištění, stanovení a zabezpečení úhrady poplatku.
Minimalizace údajů	Dodržení rozsahu zpracovávaných osobních údajů předepsaných zákonem o místních poplatcích, místní obecnou vyhláškou zavádějící poplatek.
Přesnost	Přesné zpracování osobních údajů jejich případná aktualizace. Nepřesné osobní údaje mají být opraveny, vymazány.
Omezení uložení	Zpracovávání osobních údajů jen po dobu nezbytně nutnou pro konkrétní zpracování, kterou udává lhůta pro vyměření a placení daně.
Integrita, důvěrnost, dostupnost	Zabezpečení osobních údajů a jejich ochrana před neoprávněným zpracováváním. Obec musí být schopna doložit dodržení souladu.

9.5 Zveřejňování povinných a nepovinných informací

Orgány samosprávy mají informační povinnost přiměřeným způsobem poskytovat některé informace ve vztahu k veřejnosti.

9.5.1 Zveřejňování informací na úřední desce

Při zveřejňování informací na úřední desce rozlišujeme, zda se jedná o zveřejňování povinné či nepovinné. Obce mají ze zákona o obcích povinnost zveřejňovat informace o konání zasedání zastupitelstva obce, a to včetně návrhu programu, obecně závazné vyhlášky a doručování veřejnou vyhláškou dle správního řádu. Zákon o rozpočtových pravidlech územních rozpočtů zase obci ukládá povinnost zveřejnit veřejnoprávní smlouvu na základě, které poskytla dotaci. (Česko, 2000b)

Mezi nepovinně uveřejňované informace patří informace zveřejňované ve snaze transparentnosti jednání obce. Příkladem jsou zápisy z jednání zastupitelstva obce, informace o společenském, kulturním a sportovním dění. (MVČR, 2018)

Obecní úřad by měl před vyvěšením dokumentu prověřit, zda je skutečně povinen v souladu s příslušným procesním předpisem doručený dokument na své úřední desce uveřejňovat. (SMO ČR, 2020)

Best practices: Písemnosti doručované obcí formou veřejné vyhlášky, která obsahuje osobní údaje i jiných osob než adresáta nebo osobní údaje zvláštních kategorií. Může obec zvolit možnost vyvěšení oznámení o možnosti převzít písemnost, ve které budou uvedeny pouze nevyhnutelné identifikační údaje osoby dotčené (jméno, příjmení, adresa případně datum narození).

9.5.2 Zveřejňování smluv, objednávek a faktur

Obce při výkonu své činnosti sjednávají nejrůznější druhy smluv, například smlouvy nájemní, kupní, smlouvy o dílo, pachty, vystavují objednávky a proplácejí faktury. Všechny výše zmíněné dokumenty obsahují osobní údaje, které podléhají ochraně na základě GDPR. Jestliže zveřejnění smlouvy, ukládá obci přímo zákon, postupuje se podle zákona. SMO ČR (2020) ve své publikaci uvádí, že v rámci zajištění vyšší míry transparentnosti svých rozhodnutí a informování občanů o činnosti obce zveřejňují dokumenty, musí zajistit anonymizaci osobních údajů, které se v nich nacházejí.

Best practices: Tabulka 22 může posloužit jako pomůcka při provádění anonymizace na zveřejňovaných dokumentech.

Tabulka 22 Příklady anonymizace osobních údajů (SMO ČR, 2020)

Údaj	Subjekt	Anonymizace	Komentář
Obchodní firma (název podnikajícího subjektu)	*PO*	*NE*	*Není osobním údajem. Slouží k identifikaci smluvní strany.*
	FOP	*NE*	*Je-li název podnikajícího subjektu tvořen jménem a příjmením, není nutné údaje anonymizovat.*
Jednající/Zastoupená	*PO*	*NE/ANO*	*U veřejnoprávních subjektů lze bez dalšího zpracovávat osobní údaje o veřejně činné osobě, funkcionáři nebo zaměstnanci veřejné správy nebo úřední činnosti nebo o jeho funkčním nebo pracovním zařazení. U soukromoprávních subjektů je možné neanonymizovat osobní údaje, které jsou na základě zákona přístupné, jedná se tedy o osobní údaje o osobách, které jsou statutárními orgány obchodních korporací.*
Sídlo firmy	*PO*	*NE*	*Není osobním údajem.*
Sídlo podnikatele	*FOP*	*ANO*	*Sídlo podnikatele se doporučuje anonymizovat. Pro ztotožnění subjektu je dostačující jeho identifikace názvem a identifikačním číslem. Vedle toho, podnikající fyzické osoby mají často místo podnikání v místě svého (soukromého bydliště), a v takovém případě by docházelo k zásahu do jejich soukromí.*
liště FO	*FO*	*ANO*	*Bydliště FO se nezveřejňuje, kromě případů, kdy jsou tyto osoby příjemci veřejných prostředků.*
IČO	*PO*	*NE*	*Není osobním údajem. Slouží k identifikaci smluvní strany.*
	FOP	*NE*	*Není nutné anonymizovat. Slouží k identifikaci smluvní strany. Právní titul čl. 6 odst. 1 písm. c) GDPR*
DIČ	*PO*	*NE*	*Není osobním údajem.*
	FOP	*ANO*	*Vzhledem k tomu, že DIČ fyzických osob je tvořeno identifikátorem „CZ“ a rodným číslem takové osoby, doporučuje se DIČ anonymizovat, a to i přesto, že DIČ lze vyhledat (podobně jako jiné údaje) např. v rejstříku živnostenských podnikatelů.*

Tabulka 23 Příklady anonymizace osobních údajů (pokračování tabulky, SMO ČR, 2020)

Údaj	Subjekt	Anonymizace	Komentář
Číslo bankovního účtu	*PO*	*NE*	*Není osobním údajem.*
	FOP/FO	*ANO*	*Anonymizovat, jelikož se jedná o osobní údaj.*
Osoba oprávněná za dodavatele jednat ve věcech technických	*PO*	*ANO/NE*	*U osoby jednající za veřejnoprávní subjekt lze zveřejnit, protože se jedná o informace vypovídající o veřejné či úřední činnosti a zásah do soukromí může být minimální.* *U zaměstnance dodavatele Soukromo-právního subjektu k tomu obvykle neexistuje právní titul a v úvahu přichází pouze souhlas.*
Osoba, která doklad (objednávku, fakturu) vystavila	*PO/FOP/FO*	*ANO*	*Na dokladu bývá často uvedeno jméno, příjmení, popř. kontakt osoby, která ho vystavila (např. účetní). Tyto údaje se doporučuje anonymizovat.*
Telefon	*PO/FOP/FO*	*ANO*	*Anonymizovat. Tyto údaje se nezveřejňují, jelikož může dojít k poškození práv osob (stalking). Čísla mobilních telefonů jsou zpravidla neveřejná.*
Email	*PO/FOP/FO*	*ANO*	*Anonymizovat. Tyto údaje se nezveřejňují, jelikož může dojít k poškození práv osob (spamming). Emaily jsou zpravidla neveřejné.*
Identifikátor datové schránky	*PO*	*NE*	*Není osobním údajem.*
	FOP/FO	*NE*	*Jedná se o otevřená data dle NV č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data.*
Obchodní tajemství	*PO/FOP*	*ANO*	*Anonymizovat.*
Podpis jednajících osob	*PO/FOP/FO*	*ANO*	*Anonymizovat.*

9.5.3 Uveřejňování materiálů ze zasedání zastupitelstva

Členové zastupitelstva disponují řadou materiálů k projednání, z nichž některé obsahují i osobní údaje. V rámci přípravy podkladů pro jednání zastupitelstva se zpracovávají údaje jen v potřebném rozsahu. Povinností obce je dle zákona o obcích alespoň sedm dní před zasedáním zastupitelstva zveřejnit na úřední desce a webových stránkách informace o konání zasedání zastupitelstva, které je veřejné, včetně programu jednání a doplňujících příloh. V průběhu zasedání je pořizován zápis, který je uložený na obecním úřadě a je dostupný k nahlédnutí. Smyslem uveřejňování je poskytnutí informací občanům o činnostech obce, nikoliv o osobách jejichž údaje mohou být předmětem jednání. (MVČR, 2018), (SMO ČR, 2020)

Best practices: Pro účely zveřejnění zvažujeme rozsah anonymizace údajů týkajících se osob o jejichž právech a povinnostech orgány obce jednají.

9.5.4 Uveřejňováni informaci na webu obce

U zveřejňování osobních údajů na webu ať už v podobě textu nebo fotografií je důležité rozlišovat, zda osobní údaje získávány a zpracovávány na základě legitimního účelu. Mezi nejčastější patří zejména – povinné zveřejňování informací plnění právní povinnosti, zveřejňování informací o aktualitách ve veřejném zájmu, při naplňování smluvních povinností obce, zveřejňování individuálních informací, jejichž zveřejnění lze v určitých případech odůvodnit jako oprávněný zájem obce. (MVČR, 2018), (SMO ČR, 2020)

Best practices: Zveřejnění pracovních kontaktních údajů volených činitelů obce je prováděno na základě veřejného zájmu. Zveřejnění kontaktních údajů nebo fotografií zaměstnanců obecního úřadu na základě veřejného zájmu, pouze za předpokladu, že je umožnění přímého kontaktu veřejnosti s pracovníkem považováno za žádoucí.

9.5.5 Zpravodaj obce

Ve zpravodaji obce jsou publikovány informace a články ze života obce, jedná se o využití účelu k informování veřejnosti v rámci naplňování veřejného zájmu na informovanosti o dění v obci. (MVČR, 2018), (SMO ČR, 2020)

Best practices: V rámci společenské rubriky není možné bez souhlasu subjektů údajů zveřejňovat soubory osobních dat občanů, které jako evidence spadají do působnosti GDPR. V případě uveřejnění blahopřání občana, se rozsah údajů minimalizuje, neuvádí se konkrétní věk ani přesná adresa bydliště. Ke zveřejnění jiných údajů musí mít obec písemný souhlas.

9.5.6 Obecní knihovna

Obecní knihovny nejsou orgánem veřejné moci ani veřejným subjektem ve smyslu zákona o zpracování osobních údajů, nemají tedy povinnost jmenovat pověřence. Na malé obci knihovny neplní pouze funkci místa, kde se půjčují knihy, ale i úlohu informačního, kulturního a společenského centra. Zaplacením evidenčního poplatku uzavřel uživatel služeb s obecní knihovnou smlouvu, která umožňuje uživateli využívat služby v rozsahu a podmínkách, které jsou v dané obci žádoucí. Přihláška čtenáře, kterou knihovna při své běžné činnosti využívá, by neměla obsahovat osobní údaje jiné, než je nezbytné pro účely realizace činností obecní knihovny. Při posuzování činnosti knihovny z pohledu ochrany

osobních údajů je nezbytné vymezit okruh odpovědných osob, které mají k údajům čtenářů přístup. (MVČR, 2018), (SMO ČR, 2020)

Best practices: Upomínky čtenářům jsou rozesílány emailem nebo písemně. Informace o čtenářích, kteří nedodržují výpůjční dobu se nikdy nezveřejňují.

Prostřednictvím e-mailu získávají čtenáři, kteří projevili zájem, informace o konání čtenářských akcí. Knihovnice se každého čtenáře ptá, jestli má o službu zájem. V případě, že čtenář projeví zájem o rozesílku informací, je zároveň informován, že přihlášení k odběru je zcela dobrovolné a lze je vzít kdykoli zpět.

9.5.7 Kontrolní činnost

Zaměřuje se na činnost v obci zejména pak na samotné hospodaření s majetkem obce, plnění usnesení zastupitelstva obce a dodržování právních předpisů a činností orgánů obce. Kontrolující přichází do styku s osobními údaji třetích osob. Zpracování osobních údajů a jejich ověřování je v průběhu samotné kontroly nevyhnutelné a realizují se v rámci plnění právních povinností kontrolujícího orgánu. Kontrolní orgán musí uvážit, zda je nezbytné jejich uvedení v kontrolní zprávě. Údaje třetích osob je vhodné anonymizovat, což má své opodstatnění zejména v situacích kdy, jsou závěry kontroly veřejně projednávány, například při zasedání zastupitelstva obce. (SMO ČR, 2020)

Best practices: Na malé obci nestačí anonymizovat pouze jména osob, vzhledem k tomu, že osoby je možné identifikovat i podle jiných znaků, například dle počtu dětí či zdravotního handicapu. Zveřejněné informace o provedené kontrole, by neměly obsahovat žádné osobní údaje včetně těch, které mohou vést k nepřímé identifikaci dotčených osob.

9.5.8 Spisová služba, ukládání a skartace

Obce vykonávají spisovou službu, jejímž cílem je zajištění odborné správy dokumentů vzniklých ze své činnosti. Spisová služba zahrnuje řádný příjem dokumentů, jejich evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, včetně kontroly uvedených činností. Spisová služba není nástrojem k zatěžování státní správy a samosprávy. Právě naopak je nástrojem průhledné, průkazné a účelné činnosti státní správy a samosprávy. Úkolem spisové služby je zajistit průkaznost a existenci v čase; od prvotního zaevidování v číselně posloupné řadě konkrétního roku a vazbou mezi podáním a vyřízením dokumentu. Zákon č. 499/2004 Sb., o archivnictví a spisové službě, výslovně uvádí jmenný rejstřík vyhledávání, ověřování a automatické zpracování údajů o adresách odesílatelů a adresátech dokumentů v evidenci

dokumentů spisové služby. V kontextu nové právní úpravy osobních údajů se provádí i revize spisového a skartačního plánu. Likvidace dokumentů se realizuje až po ukončeném skartačním řízení a pouze za předpokladu, že nebyly dokumenty vybrány za archiválie a následně odevzdány k archivaci příslušnému archivu. (Česko, 2004)

Činnosti spojené s vedením spisové služby musejí plnit zásady a požadavky obecného nařízení:

- Doložitelnost průběhu zpracování osobních údajů.
- Povinnost vést záznamy o zpracování osobních údajů.
- Povinnost zavést organizační opatření pro zajištění zabezpečení zpracování osobních údajů.
- Zajištění zabezpečení zpracování osobních údajů.

K dokumentaci obsahující osobní údaje by měla mít přístup pouze oprávněná osoba v rámci obecního úřadu.

Best practices: Ve spisovém řádu obce je vymezen vztah povinností obce v průběhu jejího uložení a při skartaci k realizaci práv subjektů údajů dle obecného nařízení, zejména právo na informace a přístup k údajům na výmaz údajů.

Dokumenty s osobními údaji vybrané v procesu skartačního řízení vybrané za archiválie, lze bez rizika uložit ve veřejném archivu, následně odpovědnost za správu a zabezpečení přechází na archiv.

9.5.9 Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Obecně nelze jednoznačně odpovědět na otázku jaké informace o fyzických osobách může či musí obec poskytnout. Vždy záleží na konkrétní informaci a individuálním požadavku fyzické či právnické osoby, která žádá o informaci. Test proporcionality spočívá v uvážení, zda nepřevažuje veřejný zájem na poskytnutí požadovaných informací, nebo právo na ochranu jednotlivce. (SMO ČR, 2020)

Best practices: V praxi se objevují žádosti dotazující se na výši platu, respektive odměny jednotlivých zaměstnanců obecních úřadů. Informace o výši platu konkrétní osoby, je osobním údajem. Platy a odměny pracovníků obcí jsou považovány za veřejné prostředky, a poskytování informací o nich spadá pod působnost zákona o svobodném přístupu. Obec provede test proporcionality a podle výsledku poskytne zveřejnění informace.

DÍLČÍ ZÁVĚR PRAKTICKÉ ČÁSTI

V praktické části diplomové práce je nastíněna charakteristika zájmové obce a představení posuzovaného objektu. Následně se práce zabývá postupem provedením DPIA, kde na základě daných kritérií bude správcem určeno, zda je provedení DPIA nutné či nikoliv. Formou kontrolního seznamu a vývojového diagramu je definován postup správce při provedení DPIA. Pro hodnocení rizik je použita jednoduchá bodová polokvantitativní metoda „PZH“, kde vyhodnocujeme riziko ve třech složkách s ohledem na pravděpodobnost, zranitelnost a výskyt hrozby. Součástí jsou opatření navržená k zajištění technického a organizačního zabezpečení. Kapitola devět je zaměřena na nejčastěji vykonávanou agendu obce v souvislosti se zpracováním osobních údajů v praxi a zároveň vysvětlit postupy konkrétního zpracování.

ZÁVĚR

Orgány veřejné správy za sebou mají fázi implementace obecného nařízení, které vešlo v účinnost 25. května 2018. Ochrana osobních údajů se vztahuje veřejnou správu, která osobními údaji fyzických osob také disponuje. Veřejná správa zpracovává obrovské množství osobních údajů, které jsou v rámci její činnosti potřebné a nezbytné. S postupnou modernizací veřejné správy se zvyšuje nejen množství zpracovávaných údajů, ale také zájem veřejnosti o přístup k nim. I když mají orgány veřejné správy dlouhodobé zkušenosti je nezbytné, aby v rámci prováděných úkonů zvyšovaly ochranu osobních údajů před zneužitím, a to neustálou kontrolou zaběhnutých postupů vyplývajících z činnosti správce.

Obecné nařízení obsahuje pokyny a postupy, které zajišťují shodu s předpisy a požadavky. Technická opatření zahrnují konkrétní postupy, stejně jako školení zaměstnanců, audity a zajištění příslušné technické a fyzické bezpečnostní kontroly, která tvoří součást efektivního řízení bezpečnostního informačního systému. Tyto procesy, zásady a kontroly jsou nastíněny v rámci předkládané práce. Organizační opatření vyplývají z vnitřních předpisů a směrnic obce.

Teoretická část práce je zaměřena na novou právní úpravu osobních údajů, popisuje zásady a práva pro subjekty údajů, správců a povinnost zajistit postupy, kontroly a opatření v rámci správy, které GDPR vyžaduje. Praktická část je zaměřena na posouzení vlivu na ochranu osobních údajů, identifikaci rizik a vyhodnocení potenciálního dopadu na subjekty údajů a správce. Po přijetí ošetření opatření hrozeb a zranitelnosti vybraných rizik nadále zůstává sedm krátkodobě akceptovatelných rizik, kterým je nutné věnovat následnou pozornost například formou modifikace technických, organizačních opatření a komunikace s pověřencem. Vzhledem k tomu, že neexistuje riziko spadající do kategorie s hodnotou kritického rizika, není nutné zahájit konzultaci s dozorovým úřadem.

Následně jsou navržena opatření pro fyzické zabezpečení osobních údajů a spravovaných dat v prostorách kanceláře, fyzické zabezpečení osobních údajů a spravovaných dat v elektronických zařízeních a v neposlední řadě i softwarové zabezpečení elektronických zařízení.

Snahou bylo vytvořit dokument, ve kterém budou jednoduše popsány nejčastější činnosti, při kterých dochází ke zpracování osobních údajů v praxi obcí a zároveň vysvětlit postupy konkrétního zpracování. Diplomová práce poslouží jako pomůcka pro snadnější uchopení dané problematiky pro spolupracující obce v rámci svazku Ždánický les a Politaví.

SEZNAM POUŽITÉ LITERATURY

BÁČA, Ján et al., 2020. *Zákon o zpracování osobních údajů: Praktický komentář*. Plzeň: Aleš Čeněk. ISBN 978-80-7380-804-4.

BELGIUM, 2017. *Guidelines on Data Protection Impact Assessment (DPIA)*. In: . European Commission, (wp 248 ev.01). Dostupné také z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Best practices Definition, 2019. *Investopedia* [online]. [cit. 2021-3-15]. Dostupné z: https://www.investopedia.com/terms/b/best_practices.asp

BITKOM, 2017. *Risk Assessment & Data Protection Impact Assessment: Průvodce* [online]. Bitkom e. V., s. 60 [cit. 2021-4-8]. Dostupné z: https://www.bitkom.org/sites/default/files/file/import/170919-LF-Risk-Assessment-ENG-online-final.pdf

BRAND, Wiley, 2017. *GDPR for dummies: MetaCompliance Special Edition*. West Sussex: John Wiley Sons. ISBN 978-1-119-41925-9.

CAPITOVÁ, Martina, 2019. *Řízení procesů na malé obci s ohledem na novou právní úpravu ochrany osobních údajů*. Zlín. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Slavomíra Vargová, PhD.

ČESKO, 1990. Zákon o místních poplatcích. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, ročník 1990, částka 92, číslo 565. Dostupné také z: http://data.atlascloud.cz/LCR/Rejstrik/Sb/1990/sb092-1990/565_1990/565_1990.pdf

ČESKO, 1992. Zákon č. 2/1993 ze dne 16. prosince 1992: Listina základních práv a svobod. In: *Sbírka zákonů České republiky*. Praha, ročník 1993, částka 1, s. 19. Dostupné také z: http://data.atlascloud.cz/LCR/Rejstrik/Sb/1993/sb001-1993/2_1993/2_1993.pdf

ČESKO, 2000a. Zákon o obcích. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, ročník 2000, částka 38, číslo 128. Dostupné také z: http://data.atlascloud.cz/LCR/Rejstrik/Sb/2000/sb038-2000/128_2000/128_2000.pdf

ČESKO, 2000b. Zákon o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra České republiky, částka 32, číslo 101. Dostupné také z: http://data.atlascloud.cz/LCR/Rejstrik/Sb/2000/sb032-2000/101_2000/101_2000.pdf

ČESKO, 2000c. Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra ČR, ročník 2000, částka 99, číslo 365. Dostupné také z: http://data.atlascloud.cz/LCR/Rejstrik/Sb/2000/sb099-2000/365_2000/365_2000.pdf

ČESKO, 2004. Zákon o archivnictví a spisové službě a o změně některých zákonů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra České republiky, ročník 2004, částka 173, číslo 499. Dostupné také z: https://www.zakonyprolidi.cz/cs/2004-499

ČESKO, 2016. *Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu*. In: Praha: Odbor bezpečnostní politiky a prevence kriminality, ročník 2016, číslo 1. Dostupné také z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

ČESKO, 2017a. *Nová pravidla ochrany osobních údajů*. In: Hospodářská komora České republiky, 19 s. Dostupné také z:https://www.ohkpv.cz/obrazky/PriruckaGDPR_final.pdf

ČESKO, 2017b. Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR - obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů. In: *Úplné znění předpisů*. Ostrava: Sagit, redakční uzávěrka 28.8.2017, číslo 1209. ISBN 978-80-7488-241-8.

ČESKO, 2018. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o k. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra České republiky, ročník 2018, částka 43, číslo 82. Dostupné také z: http://data.atlascloud.cz/LCR/Rejstrik/Sb/2018/sb043-2018/82_2018/82_2018.pdf

ČESKO, 2019a. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. In: *111*. ročník 2019, částka 47, číslo 111. Dostupné také z: http://data.atlascloud.cz/LCR/Rejstrik/Sb/2019/sb047-2019/111_2019/111_2019.pdf

ČESKO, 2019b. Zákon o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. Praha, ročník 2019, částka 47, s. 890 - 911. ISSN 1211-1244. Dostupné také z: https://app.codexis.cz/doc/CR/118520/s/110%2F2019

ČSN ISO/IEC 27005, 2018. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 3. vydání. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN ISO 31000, 2018. *Management rizik: Směrnice 01 0351*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

DURICU, Alexandra, 2019. *Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation (GDPR): Information Security, master's level (120 credits) 2019*. Degree Project. Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering. Vedoucí práce John Lindström.

Enactia.com: Data Protection Impact Assessments (DPIAs) [online]. [cit. 2021-4-13]. Dostupné z: https://enactia.com/features/data-protection-impact-assessments

EVROPSKÁ UNIE, 2016. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Evropský věstník*. Evropská unie. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0679

EUROPEAN UNION, 2017. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. ISBN 9781849289450. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&an=1593800&scope=site

IT GOVERNANCE PRIVACY TEAM, 2017. *EU General Data Protection Regulation (GDPR)*. Second edition. United Kingdom: IT Governance Publishing, 377 s. ISBN 978-1-84928-946-

JANEČKOVÁ, Eva, 2018. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer. ISBN 978-80-7552-248-1.

JANEČKOVÁ, Eva, 2019. *GDPR: řešení problémů v praxi obcí*. Praha: Grada Publishing. Právo pro praxi. ISBN 978-80-247-2925-1.

JANÍČEK, Přemysl et al., 2013. *Expertní inženýrství v systémovém pojetí*. Praha: Grada. ISBN 978-80-247-8196-9.

KRÁL, David, 2010. *Informační bezpečnost podniku*. Brno. Zkrácená verze disertační práce. Vysoké učení technické v Brně, Fakulta Podnikatelská, Ústav Informatiky. Vedoucí práce Doc. Ing. MILOŠ KOCH, CSc.

MŠMT, 2019. Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracován osobních údajů v podmínkách školství. In: *Metodika GDPR* [online]. 88 st. [cit. 2021-4-3]. Dostupné z: https://www.msmt.cz/dokumenty-3/metodicka-pomucka-k-aplikaci-obecneho-narizeni-o-ochrane

MVČR, 2018. Svaz průmyslu a dopravy ČR, 2018. *Průvodce pro přípravu obcí na požadavky GDPR* [online]. In: . s. 16 [cit. 2021-3-15]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/modelove-situace.aspx

MVČR, 2020. Odbor strategického rozvoje a koordinace veřejné správy, 2020. *Meziobecní spolupráce v ČR: Příklady dobré praxe a doporučení pro realizaci meziobecní spolupráce* [online]. In: s. 59 [cit. 2021-3-17]. Dostupné z: https://www.mvcr.cz/clanek/verejna-sprava-publikace.aspx

MVČR, 2021a., *Vzorové dokumenty* [online]. [cit. 2021-3-14]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/vzorove-dokumenty.aspx

MVČR, 2021b., *Ministerstvo vnitra ČR: Modelové situace* [online]. [cit. 2021-3-15]. Dostupné z: https://www.mvcr.cz/

NAVRÁTIL, Jiří, 2018. *GDPR pro praxi*. Plzeň: Aleš Čeněk. ISBN 9788073806897.

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

NEZMAR, Luděk, 2017. *GDPR - Požadavky na dokumentaci* [online]. In: s. 28 [cit. 2021-4-13]. Dostupné z: https://docplayer.cz/108138670-Gdpr-pozadavky-na-dokumentaci-ludek-nezmar.html

NONNEMANN, František, 2018. *Příručka pověřence pro ochranu osobních údajů*. Praha: Klika. Otevřeno. ISBN 978-80-88-298-10-6.

Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR - obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů: redakční uzávěrka 28.8.2017, [2017]. Ostrava: Sagit. ÚZ. ISBN 978-80-7488-241-8.

PÁTEK, Emil, 1928. *Obec Heršpice u Slavkova: Příspěvek kulturně vzdělávací*. Slavkov u Brna: nákladem vlastním, tiskem Josef Šimka.

Pseudonymizace [online], 2016. ManagementMania.com [cit. 2021-4-16]. Dostupné z: https://managementmania.com/cs/pseudonymizace-pseudonymisation

PZK S.R.O., 2018. *Systémová analýza působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů* [online]. In: Praha: Ministerstvo vnitra ČR, s. 161 [cit. 2021-4-9]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/systemova-analyza-obci.aspx

SMO ČR, 2020. *Správa osobních údajů v praxi obcí a měst: Posilování administrativní kapacity obcí na bázi meziobecní spolupráce*. Praha. ISBN 978-80-88375-06-7.

Sešit k GDPR [online], 2018. In: Ministerstvo vnitra ČR. Praha, s. 15 [cit. 2018-10-5]. Dostupné z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj10_GR8OzvAhXV_ioKHdq5CaYQFjAAegQIBRAD&url=https%3A%2F%2Fwww.mvcr.cz%2Fgdpr%2Fsoubor%2Fgdpr-sesit-pdf.aspx&usg=AOvVaw3ah2rx_lwSpOzBzhYSqTtJ

TZANOU, Maria, 2019. *Personal data protection and legal developments in the European Union*. Hershey PA: Information Science Reference. ISBN 9781522594901.

ÚOOU, 2020. *Úřad pro ochranu osobních údajů: Metodika obecného posouzení vlivu na ochranu osobních údajů* [online]. [cit. 2021-3-22]. Dostupné z: https://www.uoou.cz/

Vigilant Software Ltd.: DPIA Tool – Conduct a data protection impact assessment in six simple steps [online]. [cit. 2021-4-13]. Dostupné z: https://www.vigilantsoftware.co.uk/topic/dpia

Výroční zpráva Úřadu pro ochranu osobních údajů z rok 2019 [online], 2020. Nakladatelství Munipress Brno [cit. 2021-4-27]. ISBN 978-80-210-9548-9. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=40546

Základy IT gramotnosti: Anonymizace [online]. Fakulta informatiky Masarykovy univerzity [cit. 2021-4-16]. Dostupné z: https://is.muni.cz/do/1492/el/sitmu/law/html/ch02s10.html

ŽŮREK, Jiří, 2017. *Praktický průvodce GDPR*. Olomouc: ANAG. Právo (ANAG). ISBN 978-80-7552-248-1.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
Č.	Číslo
Čl.	Článek
ČR	Česká republika
DPIA	Data Protection Impact Assessment
EU	Evropská unie
GDPR	General Data Protection Regulation
GMS	Globální systém pro mobilní komunikaci
HW	Hardware
MVČR	Ministerstvo vnitra České republiky
NP	Nad podlaží
NV	Nařízení vlády
Odst.	Odstavec
PDCA	Plan-Do-Check-Act
Písm.	Písmeno
IT	Informační technologie
Sb.	Sbírka zákonů
SMS	Služba krátkých textových zpráv
SW	Software
ÚOOÚ	Úřad pro ochranu osobních údajů
ÚOHS	Úřad pro ochranu hospodářské soutěže
WP29	Pracovní skupina zřízená dle článku 29 směrnice 95/46/ES

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: ZÁZNAM O ČINNOSTECH ZPRACOVÁNÍ – MÍSTNÍ POPLATKY

Záznam o činnostech zpracování – MÍSTNÍ POPLATKY ***(a jiná obdobná plnění – poplatek za komunální odpad)*** **čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů (GDPR)** **Správce:** … *(název, adresa, datová schránka)* … **Pověřenec pro ochranu osobních údajů:** … *(jméno, příjmení, e-mail)* …
I. Účely zpracování
ZAJIŠTĚNÍ AGEND OBCE PODLE ZÁKONA O MÍSTNÍCH POPLATCÍCH
Čl. 6 odst. 1 písm. e) GDPR - zpracování nezbytné pro výkon veřejné moci, kterým je obec pověřena: zákon č. 565/1990 Sb., o místních poplatcích, ve znění pozdějších předpisů zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů obecně závazná vyhláška obce o stanovení místního poplatku *V případě, že obec namísto stanovení místního poplatku za provoz systému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů stanoví poplatek za komunální odpad podle zákona č. 185/2001 Sb., o odpadech a o změně některých dalších zákonů, je pro rozsah zpracování osobních údajů rozhodný také:* *zákon č. 185/2001 Sb., o odpadech a o změně některých dalších zákonů* *obecně závazná vyhláška obce o stanovení systému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů vznikajících na katastrálním území obce*
II. Kategorie subjektů údajů
Poplatník poplatku, plátce poplatku
III. Kategorie osobních údajů
Údaje o poplatníkovi nebo plátci v rozsahu ohlašovací povinnosti podle § 14a zákona o místních poplatcích – základní identifikační údaje, údaje rozhodné pro stanovení výše poplatkové povinnosti, údaje rozhodné pro úlevy či osvobození od poplatků, údaje rozhodné pro prominutí poplatku nebo jeho příslušenství Údaje využívané pro účely řízení o místních poplatcích ze základního registru obyvatel, z informačního systému evidence obyvatel a z informačního systému cizinců v rozsahu podle § 16 zákona o místních poplatcích
IV. Kategorie příjemců
Nadřízený správce daně (krajský úřad), orgány finanční správy
V. Plánované lhůty pro výmaz kategorií osobních údajů
Údaje jsou zpracovávány po dobu trvání poplatkové povinnosti a po dobu běhu lhůty pro placení daně (§ 160 daňového řádu). Uplatní se skartační lhůty stanovené spisovým a skartačním řádem: *(doplní obec)*
VI. Obecný popis technických a organizačních bezpečnostních opatření
K osobním údajům mají přístup pouze osoby, které je potřebují využívat při plnění povinností obce jakožto správce daně, a to pouze v nezbytném rozsahu. Přístup k databázím s osobními údaji je zabezpečen hesly, listinná dokumentace je uzamykána.

PŘÍLOHA P II: SMĚRNICE K OCHRANĚ OSOBNÍCH ÚDAJŮ DLE GDPR

Obec Heršpice
Heršpice 91
684 01 Slavkov u Brna

Směrnice č. 7/2021

Směrnice k ochraně osobních údajů dle GDPR

1. Předmět úpravy

1.1.Ustanovení této směrnice upravuje pravidla k ochraně osobních údajů.

1.2.Tato směrnice je v souladu se

- zákonem č. 262/2006 Sb., zákoník práce, v platném znění,
- zákonem č. 89/2012 Sb., občanský zákoník, v platném znění,
- zákonem č. 435/2004 Sb., o zaměstnanosti, v platném znění,
- zákonem č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), v platném znění,
- zákonem č. 133/2000 Sb., o evidenci obyvatel,
- zákonem č. 110/2019 Sb., o zpracování osobních údajů,
- nařízením Evropského parlamentu a Rady (EU) 2016/679 z 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 "Obecné nařízení".

2. Vymezení účelu směrnice

2.1. Tato směrnice je aplikací ochrany fyzických osob a jejich soukromí v souvislosti se zpracováním jejich osobních údajů a o volném pohybu těchto údajů v naši organizaci, tak, aby bylo dosaženo požadované ochrany údajů u fyzických osob (zaměstnanců, žáků, osob ucházejících se o zaměstnání, současných i budoucích obchodní partnerů a dalších osob), jejichž osobní údaje získává naše organizace při své činnosti.

2.2.Touto směrnicí jsou povinni řídit se všichni zaměstnanci organizace.

3. Základní pojmy

3.1.**Osobní údaj** je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo

či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

3.2. **Subjekt údajů** je fyzická osoba, jíž se osobní údaje týkají. Osobní údaje mohou být pouze ve vztahu k žijící fyzické osobě. Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách.

3.3. **Zpracování osobních údajů** je jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Zpracování osobních údajů je nutné považovat za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky.

3.4. **Správce** je subjekt, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti, ale může je zpracovávat i pro vlastní určené účely.

3.5. **Zpracovatel** je subjekt, který zpracovává osobní údaje pro správce. Od správce se zpracovatel liší tím, že v rámci činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen. Zpracovatelem je pouze ve vztahu k osobním údajům poskytnutým správcem, nikoli osobních údajů, které zpracovává pro účely, které se jej přímo dotýkají.

3.6. **Pověřenec pro ochranu osobních údajů**. Jeho hlavním úkolem je monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z Obecného nařízení, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat a působí jako kontaktní osoba pro dozorový úřad.

3.7. **Souhlas** je jedním z právních důvodů, na základě, kterého může správce osobní údaje zpracovávat. Jde o aktivní a dobrovolný projev vůle subjektu údajů, ke kterému nesmí být nucen. Souhlas se vždy poskytuje k určitému účelu zpracování, který musí subjekt údajů znát. Dítě nabývá způsobilosti k udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti přímo jemu dovršením patnáctého roku věku.

3.8. **Anonymizace** je proces, při kterém se nevratně odstraní všechny osobní údaje, bez možnosti zpětné identifikace konkrétní fyzické osoby. Anonymizovaný soubor nejenom neobsahuje žádné údaje o fyzických osobách či identifikátory, ale také vylučuje možnost opětovného propojení s takovými údaji a konkrétní osobou.

3.9. **Pseudonymizace**. Jde o zpracování osobních údajů způsobem, který neumožňuje jejich přiřazení ke konkrétnímu člověku bez použití dodatečných informací. Ty musejí být uchovány odděleně s dostatečnou technickou a organizační ochranou.

4. Zásady zpracování osobních údajů a zákonnost zpracování

4.1. S osobními údaji je třeba zacházet na základě právního důvodu, transparentně, se zřetelem ke stanovenému účelu zpracování, a pouze v nezbytném rozsahu.

4.2. Osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely.

4.3. Osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,

4.4. Osobní údaje musí být přesné.

4.5. Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány.

4.6. Osobní údaje musí být zabezpečeny pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

4.7. Podmínka zákonnosti zpracování osobních údajů se považuje za splněnou, pokud ke zpracování dojde zejména na základě některého z těchto důvodů:

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

4.8. Správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést.

4.9. Pokud správce provádí zpracování osobních údajů při plnění právní povinnosti nebo výkonu působnosti a je povinen subjektu údajů poskytnout informace podle čl. 13 nebo čl. 14 odst. 1, 2 a 4 Obecného nařízení, může tyto informace v rozsahu odpovídajícím jím obvykle prováděnému zpracování osobních údajů poskytnout zveřejněním způsobem umožňujícím dálkový přístup.

5. Zpracování zvláštních kategorií osobních údajů (citlivých osobních údajů)

5.1. Zakazuje se, zpracování osobních údajů, které vypovídají o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborové organizaci, genetický údaj, biometrický údaj zpracovávaný za účelem jedinečné identifikace fyzické osoby, údaj o zdravotním stavu, o sexuálním chování, o sexuální orientaci a údaj týkající se rozsudků v trestních věcech a trestných činů nebo souvisejících bezpečnostních opatření.

5.2. Zvláštní kategorie osobních údajů lze zpracovávat v těchto případech:

- subjekt údajů udělil výslovný souhlas,
- zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,
- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů,
- zpracování je nezbytné z důvodu významného veřejného zájmu,
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče,
- zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků,
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.

5.3.Citlivé údaje, kdy je nutný výslovný písemný souhlas se v naši organizaci vyžadují v případech: *Např.*

- zjištění trestní bezúhonnosti – u zaměstnanců u nichž se vyžaduje odpovědnost za svěřené hodnoty,

- podrobné údaje o zdravotním stavu, zdravotní testy, vše nad rámec běžné vstupní zdravotní prohlídky – u podnikových řidičů, dalších zodpovědných a extrémně náročných profesí s rizikem vzniku škod.
- pro provádění srážek ze mzdy a poukazování odborových příspěvků zaměstnanců a poukazování odborových příspěvků zaměstnanců – organizace vede seznam zaměstnanců v konkrétní odborové organizaci a má pro tento případ písemný souhlas zaměstnance s prováděnou srážkou. Údaje jsou anonymizovány, protože v dohodě o srážkách je uvedeno číslo bankovního účtu a částka.

6. Evidence a způsob zpracování osobních údajů

6.1. Zpracováním osobních údajů na základě zákona nebo na základě souhlasu jsou pověřeni zaměstnanci jednotlivých odborů.

6.2. Přístup k údajům mají pouze pověření zaměstnanci jednotlivých odborů a zaměstnanci, kteří mají přímo v popisu práce styk s těmito údaji.

6.3. Na základě „dohody o mlčenlivosti" jsou zaměstnanci, kteří mají oprávněný přístup k údajům, povinni vyhýbat se jednání, které by mohlo být považováno za neoprávněné a při kterém by mohlo dojít k neoprávněnému zveřejnění osobních údajů.

6.4. Osobní údaje zaměstnanců (uchazečů o zaměstnání) jsou shromažďovány a zjišťovány z důvodu pracovněprávních, daňových, bezpečnostních, hygienických předpisů, vztahů k OSSZ a zdravotním pojišťovnám, z předpisů o zaměstnanosti. Pro interní potřeby jsou data zjišťována pro výběr, zvyšování kvalifikace zaměstnanců, přeřazování na jiné funkce atd. U uchazečů o zaměstnání jde o získávání údajů z důvodu zhodnocení vhodnosti na volnou pracovní pozici. Zaměstnanci poskytují údaje písemně (občanský průkaz, potvrzení o zaměstnání od předchozího zaměstnavatele, dotazníky, žádosti, životopisy atd.) nebo ústně (nahlašování změn). Ústní údaje jsou písemně zaznamenány.
Veškeré údaje v listinné podobě jsou uloženy ve spisech zaměstnanců u personálního útvaru, v elektronické podobě jsou uloženy u mzdové účetní a u personálního útvaru. Zálohování dat je zajištěno na druhý pevný disk a na CD, která jsou ukládána v archivu.

6.5. Osobní údaje fyzických osob v rámci obchodních partnerů jsou shromažďována z důvodu uzavírání obchodních smluv. Údaje jsou získávány formou odpovědí na inzeráty správce, prostřednictvím výběrového řízení, z předkládaných nabídek odběratelů atd. Z dokladů jako jsou živnostenské listy, obchodní smlouvy, výpisy z rejstříku a další evidence. Nakládání s údaji je obdobné jako u osobních údajů zaměstnanců. Externí nabídky doručené elektronickou poštou procházejí firewallem a antivirem.

6.6. Povinností dotčených zaměstnanců a dalších osob je řídit se touto směrnicí v rámci svých pracovních povinností. Pokud jsou údaje poskytnuty na základě smlouvy externím pracovníkům, ti se musí také řídit touto směrnicí. Smlouva upravuje účel, dobu platnosti smlouvy, zodpovědné osoby, technické a organizační zabezpečení ochrany osobních údajů při jejich předávání a zpracování.

7. Ochrana osobních údajů

7.1. Byla přijata technická, organizační a procesní opatření a zavedeny takové bezpečnostní prvky, abychom zajistili a byli schopni doložit, že zpracování je prováděno v souladu s Obecným nařízením.

7.2. Zásadním právem subjektu údajů je právo na to, aby byly jeho údaje vymazány a nebyly dále zpracovávány, pokud již nejsou potřebné pro účely, pro které byly zpracovány, případně pokud subjekt údajů odvolal svůj souhlas se zpracováním a neexistuje žádný další důvod pro zpracování, subjekt údajů vznesl námitku proti zpracování osobních údajů, které se ho týkají, nebo pokud je zpracování jeho osobních údajů v rozporu s nařízením.

7.3. Žádá-li subjekt údajů o provedení výmazu osobních údajů podle čl. 17 Obecného nařízení, pak původce musí zohlednit další povinnosti, které mu vyplývají ze zákona. Jsou-li dokumenty zpracovávány v informačních systémech spravujících dokumenty a dalších evidencích, žádající subjekt údajů upozorní, že výmaz z informačního systému, nebo odstranění z dokumentů v analogové podobě, ve smyslu ustanovení článku 17 Obecného nařízení je možné provést teprve po uplynutí skartačních lhůt dokumentů a jejich zařazení do procesu výběru archiválií, a to pouze u těch dokumentů, které nebudou příslušným archivem vybrány jako archiválie.

8. Předávání údajů do jiných států

8.1. Pokud správce chce předat jinému správci osobní údaje do země mimo Evropskou unii, musí k tomu mít nejen právní důvod, ale zároveň musí být zajištěna jejich institucionální ochrana, tj. nelze (až na výjimky) předávat osobní údaje do zemí, kde není zajištěna dostatečná právní ochrana osobních údajů, resp. správce nepřijal instrumenty, které tuto ochranu při předávání zajistí.

9. Kontrola

9.1.Kontrolu dodržování této směrnice vykonává pověřenec pro ochranu osobních údajů.

10.Účinnost

10.1. Účinnosti tato směrnice nabývá dnem 1.3.2021

V Heršpicích, dne 1.3. 2021

OBEC HERŠPICE

.....

Starosta obce