Systémová analýza působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů

Zadavatel: **Česká republika – Ministerstvo vnitra**
Nad Štolou 936/3, Praha 7
IČ: 00007064

Zhotovitel: **Pražská znalecká kancelář, s.r.o.**
Na Bateriích 822/9
162 00 Praha 6 - Střešovice
IČ: 48910660

Manažerské shrnutí

Systémová analýza působnosti obcí je provedena z hlediska nařízení Evropského Parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), označované jako General Data Protection Regulation (dále jen „GDPR“), které bude přímo použitelné (vstoupí v účinnost) dne 25. května 2018. GDPR představuje nový právní rámec ochrany OÚ v evropském prostoru s cílem hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich OÚ.

S ohledem na tuto novou legislativu Evropské unie (dále jen „EU“) uzavřela Česká republika - Ministerstvo vnitra (dále jen „MVČR") s Pražskou znaleckou kanceláří s.r.o. (dále jen „Zhotovitel") smlouvu č.j. MV-143611-1/LG-2017 ze dne 8.1.2018 na vytvoření systémové analýzy působnosti obcí z hlediska GDPR (dále jen „Smlouva“).

Systémová analýza obsahuje dvě části, z nichž první část je zaměřena na obce s rozšířenou působností a druhá část je zaměřena na obce se základním rozsahem přenesené působnosti. Každá část systémové analýzy zohledňuje specifika dané kategorie obcí tak, aby výstup byl pro obce příslušného typu do nejvyšší možné míry přiléhavý a využitelný.

V rámci systémové analýzy bylo provedeno dotazníkové a místní šetření na reprezentativním vzorku obcí. Tyto informace byly vyhodnoceny a na jejich základě byly navrženy dva typy modelových obcí, a to obec se základním rozsahem přenesené působnosti a obec s rozšířenou působností.

Pro další rozhodování byla provedena analýza rizik v souladu s doporučeními GDPR. Tato analýza rizik se liší od dosud používaných metod tím, že je prováděna z pohledu subjektu údajů, zpracování jeho osobních údajů v kontextu informací, které jsou běžně používány v rámci činnosti obce, a z pohledu uplatnění práv subjektu údajů. Na základě výsledků analýzy rizik byly stanoveny problematické oblasti, a to v oblasti organizačně právní a v technické oblasti. Pro tyto oblasti byl zpracován komentář, který se zabývá aspekty dosažení předepsané úrovně ochrany osobních údajů.

Následně byl s využitím zkušeností z šetření na obcích doporučen vhodný postup zavedení navržených opatření do praxe.

Systémová analýza se taktéž zabývá problematikou pověřence pro ochranu osobních údajů co do kvalifikačních standardů, jeho podpory ze strany dalších zaměstnanců nebo útvarů a návrhu vzorového manuálu činností pověřence pro ochranu osobních údajů.

Věříme, že tato systémová analýza bude cenným příspěvkem k implementaci organizačních a technických opatření do běžné každodenní praxe obcí.

Obsah

Seznam použitých zkratek

AIS	Agendový informační systém
ČR	Česká republika
ČSN	Česká státní norma
DDoS	Distributed Denial of Service
DLP	Data loss protection
DMZ	Demilitarized Zone
ESLP	Evropský soud pro lidská práva
EU	Evropská unie
FDE	Full Disk Encryption
FES	File Encryption System
GDPR	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)
GPS	Global Positioning System
HTTPS	Zabezpečený Hypertext Transfer Protocol
IDS	Intruder Detection Systems
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPsec	IP security
IS	Informační systém
ISVS	Informační systém veřejné správy
IT	Informační technologie
ITIL	IT infrastructure Library
LAN	Local Area Network
MAC	Media Access Control
MDM	Mobile Device Management
OÚ	Osobní údaje
PIN	Personal Identification Number
Rada	Rada Evropské unie
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SSL	Secure Socket Layer
SÚ	Subjekt údajů
ÚOOÚ	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud
USB	Universal Serial Bus
WPA2	Wi-Fi Protected Access verze 2
WP29	Pracovní skupina zřízená podle článku 29 směrnice 95/46/ES
Zadavatel, MV či MVČR	Ministerstvo vnitra České republiky
Zhotovitel	Pražská znalecká kancelář, s.r.o.
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších přepisů (dále také jako „zákon o kybernetické bezpečnosti“ nebo „ZKB“)

1 Vymezení předmětu systémové analýzy

1.1 Problematika GDPR v kontextu obcí

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*.“

GDPR upravuje postupy a mechanismy sloužící k ochraně subjektů údajů. Obec je povinna přijmout vhodná opatření, aby s osobními údaji zacházela v souladu s GDPR, zejm. popsat a definovat procesy v souvislosti se zpracováním osobních údajů, tak aby dodržela zásady:

- zákonnosti (zpracování osobních údajů na základě stanoveného právního důvodu a v souladu s GDPR),
- korektnosti a transparentnosti (zejména ve smyslu plnění informační povinnosti ve vztahu k subjektu údajů),
- účelového omezení (vymezení důvodu, na jehož základě správce osobní údaje zpracovává),
- minimalizace osobních údajů (zpracovávání přiměřených a relevantních osobních údajů v nezbytném rozsahu),
- přesnosti (zpracovávání pouze přesných osobních údajů),
- omezení uložení (zpracovávání osobních údajů pouze po nezbytnou dobu),
- integrity a důvěrnosti (náležité zabezpečení osobních údajů).

GDPR zdůrazňuje, že smyslem a účelem těchto zásad je jejich osvojení a promítnutí do všech procesů zpracování osobních údajů, které podléhají režimu GDPR.

Platné právní předpisy ukládají obcím řadu právních povinností, k jejichž plnění je nezbytné zpracování osobních údajů. Mezi tyto právní předpisy spadá zejména zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů (dále jen „zákon o obcích“), který definuje postavení obce a jejích občanů. Aby obec mohla plnit úkoly v samostatné a přenesené působnosti, je nezbytné, aby k tomuto účelu vedla potřebnou evidenci; tuto potřebnou evidenci mohou upravovat zvláštní právní předpisy, např. zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů.

Obec vykonává činnosti, při nichž dochází ke zpracování osobních údajů, nejen v přímé souvislosti s výkonem samostatné nebo přenesené působnosti, ale rovněž např. z pozice zaměstnavatele nebo účastníka smlouvy.

Obec může být jak správcem, tak zpracovatelem osobních údajů. Obec je správcem v případě, kdy sama určuje účely a prostředky zpracování osobních údajů, resp. pokud tento účel a prostředky obci ukládá zákon. Zpracovatelem je obec za situace, kdy provádí činnosti zpracování pro jiného správce, který může být definován přímo zákonem.

1.2 Vymezení a definice obcí

Obecní zřízení je upraveno zákonem o obcích, který definuje obec jako základní územní samosprávné společenství občanů. Obec tvoří územní celek, který je vymezen hranicí území obce. Obec je veřejnoprávní korporací, má vlastní majetek, vystupuje v právních vztazích svým jménem a nese odpovědnost z těchto vztahů vyplývající, pečuje o všestranný rozvoj svého území a o potřeby svých občanů; při plnění svých úkolů chrání též veřejný zájem.

Zákon o obcích definuje samostatnou a přenesenou působnost obce. V rámci přenesené působnosti vykonává obec úkoly státní správy; dle rozsahu těchto úkolů rozeznáváme obce (I. stupeň), obce s pověřeným obecním úřadem dle § 64 zákona o obcích (II. stupeň), jejichž výčet je uveden v Příloze č. 1 k zákonu č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností, ve znění pozdějších předpisů, a obce s rozšířenou působností dle § 66 zákona o obcích (III. stupeň), jejichž výčet stanoví Příloha č. 2 k zákonu č. 314/2002 Sb.

Úkoly obce na úseku státní správy jsou dány zvláštními zákony, vztahují se např. na oblasti evidence obyvatel, vydávání cestovních a osobních dokladů, řidičských průkazů, technických průkazů, živnostenských oprávnění, výplat sociálních dávek, sociálně-právní ochrany dětí, péče o staré a zdravotně postižené, vodoprávní řízení, odpadové hospodářství a ochrana životního prostředí, státní správa na úseku lesů, myslivosti a rybářství, dopravy a silničního hospodářství. Tyto zvláštní zákony vymezují právní povinnosti obcí, zejména obcí III. stupně, při nichž dochází ke zpracování osobních údajů.

1.3 Definice pojmů Subjekt údajů, Správce a Zpracovatel

Subjekt údajů

Subjekt údajů je dle čl. 4 odst. 1 GDPR identifikovaná nebo identifikovatelná fyzická osoba; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Správce

Dle definice uvedené v čl. 4 odst. 7 GDPR je správcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem EU či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

Správcem je ta osoba, která rozhodla, že bude vykonávat určitou činnost, jejíž nezbytnou součástí je zpracování osobních údajů. Účelem se rozumí cíl dané činnosti a jeho smysl, např. ochrana práv subjektů údajů, ochrana majetku, ochrana zdraví. Prostředky se rozumí zvolené postupy pro konkrétní zpracování, tedy konkrétní nástroje, které budou pro zpracování údajů využity.

Zpracování osobních údajů za určitým účelem může být určitému subjektu rovněž uloženo přímo zákonem. Účel zpracování a prostředky zpracování v tomto případě určí zákonodárce, i tak je ale povinný subjekt v postavení správce osobních údajů.

Správce je osobou odpovědnou za realizaci GDPR, je povinen zavést vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s GDPR. Nezbytné je zejména dodržení povinnosti ve vztahu ke stanovení právního důvodu zpracování osobních údajů. Pokud správce nedisponuje právním důvodem pro zpracování osobních údajů, nemůže osobní údaje zpracovávat. Správce odpovídá za rozsah osobních údajů, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

GDPR požaduje, aby zpracování osobních údajů bylo prováděno v souladu se zásadami zpracování osobních údajů, jejichž dodržování musí být správce zároveň schopen doložit.

Zpracovatel

Dle definice uvedené v čl. 4 odst. 8 GDPR je zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Zpracovatelem je osoba, která jedná z pověření správce a má přístup k osobním údajům. Zpracovatel může osobní údaje zpracovávat pouze na pokyn správce, ledaže jejich zpracování ukládá právo EÚ nebo členského státu. Zpracovatelem je vždy osoba s vlastní právní subjektivitou odlišnou od správce.

Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva EÚ nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Další náležitosti smlouvy nebo jiného právního aktu stanoví čl. 28 odst. 3 GDPR.

1.4 Definice pojmu Zpracování osobních údajů

Zpracováním osobních údajů se dle čl. 4 odst. 2 GDPR rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

1.5 Dopady GDPR na obce

Obec v rámci samostatné i přenesené působnosti musí analyzovat, jakým způsobem nakládá s osobními údaji, jaké osobní údaje zpracovává, k jakým účelům zpracování a na základě jakého právního důvodu. Obec tedy musí primárně provést analýzu svých činností, při nichž dochází ke zpracování osobních údajů.

Obec dále musí vyhodnotit rizika spojená se zpracováním osobních údajů a podle tohoto vyhodnocení přijmout vhodná technická a organizační opatření za účelem zajištění toho, že zpracování bude prováděno v souladu s GDPR, přičemž i tuto skutečnost bude muset být obec schopna doložit (čl. 24 odst. 1 GDPR).

Obec musí plnit povinnosti stanovené GDPR pro zabezpečení osobních údajů, vést záznamy o činnostech zpracování dle (čl. 30 GDPR), posoudit vliv určitého druhu zpracování na ochranu osobních údajů v případech, kdy to je třeba (čl. 35 GDPR) nebo jmenovat pověřence pro ochranu osobních údajů (čl. 37 GDPR).

Obec především musí být připravena plnit informační povinnosti vůči subjektům údajů, neboť GDPR subjektům údajů dává možnost dotazovat se, vznášet námitky atd. GDPR klade důraz na transparentnost zpracování osobních údajů a na práva subjektů údajů, např. výmaz za podmínek stanovených GDPR. Obec musí být připravena plnit povinnosti vůči subjektům údajů vyplývající z GDPR. Především v souvislosti s touto povinností bude nutné upravit vnitřní procesy a přijmout vhodná technická a organizační opatření za účelem umožnění řádného uplatňování práv ze strany subjektů údajů.

1.6 Obce zapojené do systémové analýzy

Systémová analýza byla zpracována s využitím informací a posouzení skutečného stavu formou místních a dotazníkových šetření na reprezentativním vzorku obcí všech typů.

Do analýzy na základě požadavku MVČR byly zapojeny následující obce (dále také jako „Vybrané obce“) a to:

- Město Černošice;
- Město Děčín;
- Město Dobříš;
- Město Cheb;
- Město Karviná;
- Město Nymburk;
- Město Tábor;
- Město Velké Meziříčí;
- Město Vyškov;
- Městská část Praha 4;
- Městská část Praha – Zbraslav;
- Obec Kamýk nad Vltavou;
- Obec Mladý Smolivec;
- Obec Srbce;
- Obec Vysoké Pole.

Další původně zapojené obce nedodaly z technickoorganizačních důvodů požadovaná vstupní data, nicméně poskytly požadovanou součinnost alespoň v konzultační rovině.

2 Metoda zpracování systémové analýzy

V souladu s předmětem plnění Smlouvy provede Zhotovitel analýzu v členění na obce se základním rozsahem přenesené působnosti a na obce s rozšířenou působností. Ačkoliv budou tyto dvě oblasti posuzovány separátně, bude na analýzu nahlíženo jednotnou metodikou. Zhotovitel bude k analýze obou oblastí přistupovat takovým způsobem, aby byly respektovány jejich specifické aspekty a aby výstupy byly pro obě oblasti relevantní a smysluplné.

Ačkoliv bude v daných oblastech analyzováno více obcí, závěry a výstupy budou obsahovat vždy agregované informace za celou oblast. Jednotlivé obce nebudou adresně zmiňovány, vždy bude pracováno s celou množinou obcí, jelikož hledání adresných problémů jednotlivých obcí není pro splnění účelu dokumentu podstatné. Pro tento anonymizovaný přístup se Zhotovitel rozhodl také z toho důvodu, že tento materiál bude popisovat potenciální nedostatky a dílčí zranitelnosti obcí, které by mohly být zneužity.

Cílem systémové analýzy působnosti obcí je identifikovat úroveň naplnění GDPR. Tato analýza bude realizována v několika etapách. První etapa je zaměřena na rychlé a efektivní zmapování agend a informačních systémů obcí na základě předpřipravených formulářů. Druhá etapa spočívá v sekundární analýze poskytnutých informací a předaných podkladových materiálů z jednotlivých úřadů a v realizaci místních šetření, které slouží k validaci poskytnutých informací a zjištění dalších skutečností, které nebylo možné zjistit pomocí formulářů. Poslední etapa je zaměřena na syntézu zjištění a vyhodnocení předchozích etap. Detailní způsob realizace jednotlivých etap analýzy je popsán v následujících podkapitolách.

2.1 Metoda mapování obcí

Zhotovitel nejdříve provede mapování Vybraných obcí, mezi které patří 11 obcí s rozšířenou působností (z toho jedna městská část – Praha 4) a 6 obcí se základním rozsahem výkonu přenesené působnosti, popřípadě s pověřeným obecním úřadem. Obce byly vybrány MVČR a poskytnuty Zhotoviteli. Úplný výčet zapojených obcí je uveden v kapitole č. 1.6.

Na Vybrané obce zašle Zhotovitel formuláře společně s metodikou pro vyplnění dotazníků, kde jsou popsány všechny dílčí položky včetně informací o způsobu jejich vyplnění. Na každý vybraný úřad budou zaslány 2 formuláře. První formulář s označením F01 slouží pro zmapování všech agend v rámci jednotlivých obecních či městských úřadů, které zpracovávají osobní údaje ve smyslu článku čl. 4 GDPR. Druhý formulář s označením F02 slouží ke zmapování informačních systémů sloužících k výkonu agend uvedených ve formuláři F01. Oba formuláře budou před odesláním schváleny Zadavatelem a následně odeslány spolu s metodickým pokynem.

Elektronická podoba dokumentů k mapování je obsažena v Příloze č. 8.

2.1.1 Formulář F01 – Dotazník pro provedení inventury osobních údajů

Tento formulář je zaměřen na získání přehledu o agendách vykonávaných dotazovaným úřadem, osobních údajích sbíraných v rámci výkonu této agendy a způsobu jejich uložení.

Následující tabulka č. 1 obsahuje všechny položky formuláře F01:

Tabulka 1 Detailní popis formuláře F01

Položka	Popis
Hlavička dotazníku	Hlavička dotazníku obsahuje údaje o pracovišti, kontaktní osobě

Položka	Popis
	odpovědné za vyplnění dotazníku a datum vyplnění dotazníku.
Oblast zpracování osobních údajů	Zde se uvádí agenda, oblast či proces odpovídající příslušné oblasti působnosti, při níž jsou zpracovávány osobní údaje. Může se jednat o agendy v přenesené působnosti státu (např. stavební povolení, evidence obyvatel, cestovní doklady, rybářské lístky, vedení obecní kroniky atd.), Samostatná působnost (např. Správa bytových fondů, pronájem nebytových prostor, těžba a prodej dřeva), Interní procesy úřadu (např. personalistika, zúčtování mezd, kamerové systémy, GPS lokace vozidel pracovníků). Níže uvedené části dotazníku bude odpovědná osoba vyplňovat pro každou agendu, proces či oblast samostatně.
Oblast působnosti agendy či procesu	Možnost výběru z již předefinovaných možností, a to: • Přenesená působnost státu (státní správa), jedná se o přenesenou působnost státu dle Hlavy III zákona č. 128/2000 Sb. o obcích; • Samostatná působnost (samospráva), jedná se o samostatnou působnost dle Hlavy II zákona č. 128/2000 Sb. o obcích; • Interní procesy úřadu.
Zpracovávané kategorie osobních údajů	Položka slouží k výběru kategorií zpracovávaných osobních údajů týkající se uvedené agendy. • Osobní údaje - osobní údaje dle čl. 4 Nařízení Evropského parlamentu a Rady (EU) 2016/679 jsou definovány takto "veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, sítový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby."; • Zvláštní kategorie osobních údajů – zvláštní kategorie osobních údajů je charakterizovány článkem č. 9 GDPR takto: " Osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stravu či o sexuálním životě nebo sexuální orientaci fyzické osoby." • Genetické údaje – Nařízení evropského parlamentu a Rady (EU) 2016/679 definuje genetické údaje takto "Osobní údaje týkající se zděděných nebo

Položka	Popis
	získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby"; • Biometrické údaje – biometrické údaje dle čl. 4 Nařízení evropského parlamentu a Rady (EU) 2016/679 jsou definovány takto "Osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje"
Výčet položek osobních údajů	Zde se uvádí taxativní výčet druhu zpracovávaných osobních údajů, např. Jméno, Příjmení, Rok narození, Telefon atd. U kategorie zvláštních osobních údajů, dle článku č. 9 GDPR, se jedná o následující prvky: • rasový či etnický původ; • politické názory; • náboženské vyznání; • filozofické přesvědčení; • členství v odborech; • genetické údaje; • biometrické údaje za účelem jedinečné identifikace fyzické osoby; • údaje o zdravotním stavu; • údaje o sexuálním životě; • údaje o sexuální orientaci.
Vztah subjektu údajů ke správci či zpracovateli osobních údajů	Uvedení vztahu subjektu údajů ke správci či zpracovateli osobních údajů nebo kategorie subjektů osobních údajů. Zhotovitel uvádí vybrané kategorie subjektu údajů: • Občan – přenesená působnost; • Občan – samostatná působnost; • Zaměstnanec; • Dodavatel; • Kategorie zvláště zranitelných subjektů údajů – nezletilý.
Právní základ zpracování osobních údajů	Uvedení právního základu zpracování osobních údajů, na základě článku č. 6 GDPR. Zhotovitel uvádí příklady právních základů a to: • Oprávněný zájem správce; • Plnění právní povinnosti; • Plnění smlouvy nebo jednání o jejím uzavření; • Souhlas se zpracováním osobních údajů pro jeden či více konkrétních účelů;

Položka	Popis
	• Veřejný zájem, výkon veřejné moci; • Ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.
Účel nakládání s osobními údaji	Popis důvodu, na základě, něhož dochází ke zpracování osobních údajů. Uvedení výčtu právních předpisů, na jejichž základě dochází ke zpracování osobních údajů. Jedná se o zákony, vyhlášky či případně interní akty řízení.
Úložiště osobních údajů	Vybrané obce vyplní druh úložiště osobních údajů. Zhotovitel předefinoval následující úložiště osobních údajů: • Elektronické úložiště strukturované (databáze, informační systém); • Elektronické úložiště nestrukturované (lokální disky, email, sdílené disky); • Listinné úložiště; • Kombinace výše uvedených úložišť – prosím o upřesnění kombinace úložišť.
Specifikace listinného úložiště	Vyplnění způsobu vedení listinné evidence v jednotlivých procesech obsahující osobní údaje.
Specifikace elektronického úložiště	Uvedení názvu informačního systému, který vede evidenci osobních údajů v rámci uvedené oblasti či procesu.
Kategorie příjemců včetně příjemců mimo EU	Dle článku č. 4 GDRP je Příjemcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Uvedení všech kategorií příjemců osobních údajů a to: • Interní příjemce – uvedení rolí pracovníků úřadu; • Externí příjemce – uvedení všech možných externích příjemců osobních údajů včetně příjemců mimo EU.
Doba zpracování OÚ	Osobní údaje mají být uchovány pouze po dobu nutnou k účelu jejich zpracování. Uvedení doby zpracování OÚ (např. kontrola souhlasu k publikaci OÚ v obecním periodiku).
Doba uložení osobních údajů	Uvedení lhůt pro archivaci záznamů s osobními údaji (pokud je oprávněné osobě známa). Například lze uvést, že se archivuje a skartuje dle schváleného archivačního a skartačního řádu či jiného dokumentu. Nebo uvedení lhůt vyplývajících z legislativy na základě, které se osobní údaje ukládají.
Využívání spolupráce se zpracovatelem OÚ	Zpracovatel je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Jedná se zpravidla o třetí stranu, která poskytuje službu úřadu. Jedná se o typicky outsourcing. Může se jednat o vedení účetnictví, zpracování mezd apod.

Položka	Popis
Způsob kontroly zpracování OÚ	Popis způsobu kontroly zpracování OÚ - např. roční audit, kontrola třetí stranou.
Připravenost na uplatňování práv ze strany subjektů OÚ	Dle GDPR informace o přijatých opatřeních musí být poskytnuta bez zbytečného odkladu a do jednoho měsíce od obdržení žádosti. Činí se tak pouze v odůvodněných případech a bezplatně. Uvedení připravenosti vybraných obcí na uplatňování těchto práv.
Další požadované dokumenty	Zhotovitel si dále od vybraných obcí vyžádal předání dokumentů, které akcentují libovolným způsobem zpracování osobních údajů, a to jak v oblasti zpracování v informačních systémech, tak i nakládání v listinné podobě, jelikož informace obsahující osobní údaje mívá zpravidla dvojí interpretaci, a to listinnou a elektronickou, v rámci problematiky GDPR tomu není jinak. Zhotovitel uvádí příklady některých dokumentů: • Organizační struktura posuzovaného subjektu / úřadu; • Organizační řád; • Spisový a skartační řád včetně vnitřních předpisů v oblasti archivace listinných dokumentů (Směrnice o archivaci); • Vnitřní předpisy mající vztah k problematice osobních údajů a k problematice řízení bezpečnosti informací; • Vzorové smlouvy k problematice zpracování osobních údajů nebo k činnostem, jejichž předmětem je zpracování osobních údajů.

2.1.2 Formulář F02 – Přehled používaných aplikací, které zpracovávají OÚ

Formulář F02 je zaměřen na získání detailních informací o všech aplikacích a informačních systémech úřadu, ve kterých se vykonávají agendy uvedení v předchozím formuláři.

Následující tabulka č. 2 obsahuje všechny položky formuláře F02:

Tabulka 2 Detailní popis formuláře F02

Položka	Popis
Název aplikace	Uvede se název aplikace zpracovávající osobní údaje a její zaměření. Např. IS VERA – Spisová služba.
Výrobce aplikace	Uvedení názvu výrobce aplikace.
Seznam zpracovávaných agend	V této kolonce uveďte seznam všech agend či procesů, které jsou v dané aplikaci/informačním systému realizovány. Agendy jsou předmětem Formuláře č. 1 (viz předchozí kapitola č. 2). Veškeré agendy, které jsou zpracovávány v aplikacích, musí být v tomto výčtu uvedeny. Je pravděpodobné, že některé agendy budou

Položka	Popis
	zpracovávány ve více aplikacích.
Vede evidenci osobních údajů?	Výběr z předefinovaných možností ANO/NE.
Výčet položek osobních údajů	Uvedení celého výčtu položek osobních údajů např. Jméno, Příjmení, Rodné číslo, Telefon, Email atd.
Vede evidenci zvláštní kategorie osobních údajů?	Výběr z předefinovaných možností ANO/NE.
Výčet položek zvláštní kategorie osobních údajů	U kategorie zvláštních osobních údajů se jedná o následující informace: • rasový či etnický původ; • politické názory; • náboženské vyznání; • filozofické přesvědčení; • členství v odborech; • genetické údaje; • biometrické údaje za účelem jedinečné identifikace fyzické osoby; • údaje o zdravotním stavu; • údaje o sexuálním životě; • údaje o sexuální orientaci.
Oblast působnosti	Odpovědná osoba zde vybere z již předdefinovaných oblastí působnosti, jimiž jsou: • Přenesená působnost státu (státní správa); • Samostatná působnost (samospráva); • Interní procesy úřadu; • Kombinace výše uvedených možností – pokud ano prosím o upřesnění jejich kombinace.
Předávání dat	Výčet aplikací, kterým daná aplikace předává data a jejich popis.
Archivace a skartace	Popis archivace a výmazu dat z aplikace.
Přípravné realizace	Do dotazníku prosím uveďte ještě připravované realizace aplikací či IS, pokud jsou Vám známi.
Je aplikace ve vlastnictví posuzovaného subjektu nebo je provozována třetí osobou jako služba?	Odpovědná osoba provede výběr z předdefinovaných možností: • Ve vlastnictví posuzovaného subjektu; • Provozováno třetí osobou jako služba; • Jiný – pokud vyberete jiný, je potřeba upřesnit, o jaký vztah se jedná.

Položka	Popis
Otázky pro správce informačních a komunikačních technologií: ▪ Odpovídá zabezpečení aplikace platným bezpečnostním politikám úřadu? ▪ Máte analýzu rizik pro tuto aplikaci s ohledem na ochranu osobních údajů? ▪ Provozní vlastník IT infrastruktury aplikace ▪ Způsob zajištění aplikační podpory ▪ Využíváte v aplikaci pseudonymizaci OU/ COU? ▪ Využíváte v aplikaci šifrování OU/COU? ▪ Přístup k aplikaci pouze přes šifrovaný kanál? ▪ Má aplikace řízený přístup k OU/COU dle pracovní pozice uživatele? ▪ Vedete auditní záznamy k aplikaci? ▪ Používáte dvoufaktorové ověření? ▪ Je aplikace napojena na SIEM/SOC? ▪ Řídíte přístup k aplikaci pomocí FW, VLAN, DMZ? ▪ Je aplikace v HA (redundance, replikace)? ▪ Provádíte pravidelné zálohy aplikace? ▪ Máte k aplikaci disaster recovery plan (plán její obnovy)? ▪ Máte plán zálohování aplikace? ▪ Provádíte pravidelný test záloh aplikace? ▪ Provádíte pravidelné vyhodnocování incidentů? ▪ Provádíte pravidelný test disaster recovery plánu? ▪ Provádíte pravidelně test zranitelnosti / penetrační testy aplikace? ▪ Provádí se v aplikaci export dat obsahující OU/COU? Posílají se data z aplikace třetím stranám?	Následují dichotomické otázky určené Správci informačních technologií či jiné kompetentní osobě, které disponuje potřebnými znalostmi o aplikacích či informačních systémech úřadu.

Položka	Popis
▪ Je aplikace připravena na přenositelnost OU?	

V rámci formuláře F02 budou po Vybraných obcích vyžadovány další dokumenty, pokud je budou mít k dispozici. Mezi další dokumenty patří dokumentace k provozování informačních systémů úřadu dle ISO 2000x a ISO 2700x nebo zákon o kybernetické bezpečnosti.

Společně s výše uvedenými dotazníky byly na obce zaslány již vzorově předvyplněné dotazníky pro snazší orientaci či předejití sporným bodům.

2.2 Metoda analýzy zpracování a ochrany osobních údajů v informačních systémech

Dalším krokem je realizace místních šetření ve Vybraných obcích s cílem zjistit doplňující informace k již zaslaným dotazníkům a zjistit připravenost a vyspělost implementace technických a organizačních opatření pro zajištění souladu s GDPR.

V rámci místních šetření ve Vybraných obcích budou diskutována především následující témata:

Tabulka 3 Plánovaný obsah místních šetření

Téma	Popis
Vyplnění zaslaných formulářů	Zhotovitel se ujistí, že pověření pracovníci obce jsou schopni kvalifikované vyplnit zaslané formuláře. Veškeré otázky jsou srozumitelné, pracovníkům jsou zodpovězeny veškeré dotazy k vyplnění formulářů.
Zjištění současného stavu implementace GDPR v obci	Zhotovitel se informuje o stavu implementace GDPR v obci, o podniknutých krocích a přípravách na blížící se datum účinnosti GDPR. Zjištění aktuálních problémů, se kterými se obec v této oblasti potýká.
Informace o běžných agendách úřadu	Seznámení s běžným chodem úřadu, jakým způsobem probíhají rutinní činnosti zaměstnanců. Zhotovitel se zaměří na agendy s listinné i elektronické. Cílem je zmapovat běžný chod úřadu a pochopit jeho fungování.
Informace o specifických agendách úřadu	Seznámení s aspekty specifických obecních agend nakládajících s osobními údaji. Jedná se především o agendy bez zákonného titulu, které poskytují služby občanům na bázi dobrovolnosti. Cílem je pochopit a zmapovat specifické aspekty těchto agend a seznámit se způsobem podpůrné evidence osobních údajů (v listinné, elektronické či kombinované podobě).

Téma	Popis
Zjištění stavu organizačního zajištění ochrany osobních údajů	Zhotovitel se seznámí s rozsahem a strukturou interních aktů řízení, vyspělostí implementace procesního řízení, stavu a rozsahu zavedení systému řízení bezpečnosti informací apod. Cílem je zjistit vyspělost úřadu v oblasti organizačního zajištění ochrany osobních údajů a vyžádat si od úřadu veškerou relevantní dokumentace pro kvalitativní analýzu.
Zjištění stavu technických opatření pro zajištění ochrany osobních údajů	Zhotovitel se seznámí se stavem výpočetní techniky v obci. Jedná se zejména o následující okruhy: zabezpečení serverů, problematika vzdálených přístupů a jejich řízení, zajištění provozu webových stránek obce, používání sdílených disků v rámci úřadu, správa sociálních sítí obce, ochrana dat pomocí antivirových programů, ochrana komunikačních linek pomocí firewallu, zacházení se služebními mobilními telefony a notebooky a jejich ochrana, systémy na ochranu zcizení dat, poskytování veřejných Wi-Fi sítí občanům, logování uložených záznamů a auditních informací, povolení užití webových úložišť pracovníky úřadu, zajištění lokálních disků v počítačových sestavách v rámci úřadu, rezervační systémy, používání e-mailu, spisové služby, kamerové systémy, cloudová úložiště, elektronické podpisy, zabezpečení budov, využití flash disků a CD pracovníky úřadu a obce, služební automobily s využitím GPS sledováním pohybu. Cílem je zmapovat komplexní systém technických opatření k zajištění dostupnosti, důvěrnosti a integrity osobních údajů.
Zjištění stavu právních opatření pro zajištění ochrany osobních údajů.	Dotazy budou směřovat ke smluvnímu zajištění čerpání a poskytování služeb třetím stranám s ohledem na GDPR. Cílem je zjistit, zdali jsou smlouvy uzavřené mezi obcí a poskytovateli služeb opatřeny požadavky na zajištění bezpečnosti dat a tzv. „exit plány“ pro případ ukončení služby a zajištění ponechání dat v rukou obce.

2.3 Metoda analýzy dostupné dokumentace úřadu

Zhotovitel si v rámci realizace místních šetření vyžádá veškerou relevantní dokumentaci, která se dotýká problematiky GDPR. Mezi tuto dokumentaci patří zejména interní akty řízení včetně následující dokumentace či její ekvivalenty:

- Organizační řád;
- Pracovní řád;
- Směrnice pro nakládání s osobními údaji;
- Směrnice pro klasifikaci informací;
- Směrnice pro uživatele výpočetní techniky;
- Bezpečnostní politika;
- Směrnice pro přijímání a odcházení zaměstnanců;
- Spisový a skartační řád + spisový plán.

V případě, že by úřad měl vypracované ještě jiné relevantní dokumenty (například dokumentaci z certifikace ČSN ISO/IEC 27001, z certifikace ISVS apod.), budou i tyto vyžádány a podrobeny analýze.

Analýza dokumentace bude zaměřena na šíři pokrytí problematiky ochrany osobních údajů, vzájemnou koherenci uvedených informací, účelnost dokumentů a jejich aktuálnost. Veškeré poskytnuté dokumenty by měly reflektovat aktuální situaci v obci a napomáhat v oblasti zajištění bezpečnosti informací. Zejména se bude přihlížet k reflektování základních zásad GDPR a to:

- zásada zákonnosti, korektnosti a transparentnosti;
- zásada účelového omezení;
- zásada minimalizace údajů;
- zásada přesnosti;
- zásada omezení uložení;
- zásada integrity a důvěrnosti;
- zásada odpovědnosti.

Analýza dokumentace bude provedena vždy globálně za celou množinu obcí se základním rozsahem přenesené působnosti a množinu obcí s rozšířenou působností.

2.4 Metoda analýzy rizik

Řízení rizik je vykonáváno podle článku 25 a článku 32 GDPR. 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 nebo eliminaci rizik pro práva subjektu údajů vztahujících se k realizovanému zpracování.

Analýza rizik v kontextu GDPR je unikátní v porovnání s dosavadními postupy analýzy či jiného posuzování rizik[1], a to s ohledem na posuzování hodnoty aktiv, hrozeb a stanovení dalších

[1] Např. dle zákona o kybernetické bezpečnosti a jeho prováděcí vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále jen „vyhláška o kybernetické bezpečnosti“), v příloze č.1

parametrů analýzy rizik z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

S ohledem na předpoklad Zhotovitele, že v rámci obcí došlo či dochází k adaptaci principů a technik dle ZKB, zvolil Zhotovitel metodu analýzy rizika, která ze ZKB vychází, a doplnil ji o části posuzující a vyhodnocující problematiku z pohledu subjektu údajů a jeho práv.

Na základě identifikace primárních aktiv z kapitoly č. 4.1.3 Zhotovitel provede ohodnocení primárních aktiv dle jejich kritičnosti pro organizaci. GDPR nepředepisuje povinný formát analýzy rizik a taktéž nikterak neuvažuje hodnotu aktiva. Hodnota aktiv je z pohledu GDPR stejná, GDPR předepisuje chránit osobní údaje jako celek. V rámci ISO 27001 se tím způsobem řeší, zda aktivum vstoupí do analýzy rizik či nikoliv. Nicméně s ohledem na modelový charakter a prioritizaci opatření, kterou je vhodné zvolit s ohledem na implementační náklady s cílem harmonizace prostředí obce s požadavky GDPR, zvolil Zhotovitel následující kategorizaci aktiv, a to:

- Běžná hodnota aktiva – jedná se o osobní údaje zaměstnanců – bodová hodnota 1,
- Střední hodnota aktiva – obsahuje osobní údaje občanů – bodová hodnota 3,
- Vysoká hodnota aktiva – obsahuje citlivé osobní údaje.

Následně bude provedena definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u daného aktiva. V dalším kroku bude provedeno expertní posouzení zranitelnosti jednotlivých aktiv vůči hrozbám. Na závěr bude proveden výpočet celkové míry rizika.

Proces analýzy rizik obsahuje následující kroky:

- Určení a ohodnocení primárních aktiv,
- Identifikace pravděpodobnosti hrozeb,
- Identifikace zranitelnosti (rizikovosti),
- Výpočet celkové míry rizika.

Celý proces analýzy rizik obsahuje následující základní pojmy:

- Hrozba (threat) – jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva,
- Zranitelnost (vulnerability) – vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou,
- Celková míra rizika – pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti,
- Opatření (countermeasure) – technické nebo organizační opatření, které snižuje zranitelnost a chrání aktivum před danou hrozbou.

2.4.1 Metoda určení a ohodnocení aktiv

Zhotovitel určí primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení. Aktivum chápeme jako objekt (aplikace, informační systém, kartotéka, spisovna, portál, evidence či jiné listinné nebo elektronické úložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR.

Klíčovým krokem posouzení rizik, která primárním aktivům hrozí, je ohodnocení samotných primárních aktiv. To je provedeno posouzením požadavků na důvěrnost, integritu a dostupnost aktiv, případně dat v aktivech obsažených a služeb aktivy poskytovaných.

Jelikož žádná z posuzovaných obcí (tzn. obec se základním rozsahem přenesené působnosti či obec s rozšířenou působností) nemá zaveden registr aktiv, který by obsahoval skutečné hodnoty těchto aktiv, byla Zhotovitelem vytvořena následující stupnice hodnoty primárních aktiv, která vyjadřuje, nakolik jsou tato primární aktiva pro obce kritická:

Tabulka 4 Stupnice hodnocení aktiv

Stupeň	Hodnota	Kritérium
1	Velmi nízká	Ztráta, poškození, narušení bezpečnosti primárního aktiva má jen nepatrný nebo žádný vliv na ochranu osobních údajů v rámci organizace Objednatele. Z pohledu GDPR obsahuje aktivum osobní údaje zaměstnanců obce či úřadu.
2	Nízká	Ztráta, poškození, narušení bezpečnosti primárního aktiva má nízký dopad na zákonné povinnosti Objednatele v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí v rámci GDPR.
3	Střední	Ztráta, poškození, narušení bezpečnosti primárního aktiva má střední dopad na zákonné povinnosti Objednatele v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností nebude mít zásadní vliv na fungování organizace Objednatele jako celku. Z pohledu GDPR obsahuje aktivum osobní údaje občanů.
4	Vysoká	Ztráta, poškození, narušení bezpečnosti primárního aktiva je velmi významná, může vést k neakceptovatelnému porušení zákonných požadavků v rámci ochrany osobních údajů. Narušením primárního aktiva pravděpodobně dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít vliv na fungování organizace Objednatele jako celku.
5	Velmi vysoká	Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace Objednatele jako celku. Z pohledu problematiky GDPR aktivum obsahuje citlivé osobni údaje

Kvalifikace aktiv bude provedena na základě expertního posouzení Zhotovitelem, jelikož přesná hodnota aktiv pro obce nebyla stanovena. Tuto metriku je vhodné následně zavést a zařadit ji do pravidelného hodnocení v rámci jednotlivých obcí.

Do hodnocení aktiv je taktéž vhodné promítnout povahu a charakter posuzovaného aktiva z celospolečenského pohledu. Unikátní aktivum s dlouhodobou tradicí, které nelze jinak nahradit a na kterém se podílely předchozí generace, bude mít větší hodnotu, než-li aktivum, které je reprezentováno elektronickou a listinnou formou a které vzniká zpravidla strojovým zpracováním dat. Jedná se např. o obecní kroniky či jiné materiály, sloužící k dokumentování kulturního či folklorního dědictví. Tyto informace je nezbytné uvést do vlastního hodnocení aktiva a z pohledu GDPR se jedná o skutečnosti, které je následně vhodné promítnout do případné formulace oprávněného zájmu.

2.4.2 Hrozby a identifikace pravděpodobnosti hrozeb

Prvním krokem hodnocení rizik je identifikace hrozeb a zranitelností. Východiskem tohoto hodnocení je seznam obvyklých hrozeb dle standardů a hrozeb týkajících se ochrany osobních údajů vycházejících z GDPR či vycházejících z dané problematiky.

Hrozba představuje vliv, jehož následkem je poškození analyzovaného systému IT a jeho aktiv. Cílem je identifikovat hrozby, kterým mohou být vystavena primární aktiva obcí v jejich správě nebo využívána v jejich činnosti a pravděpodobnosti výskytu této hrozby.

2.4.2.1 Osobnostní práva subjektu údajů

Dle čl. 10 Listiny základních práv a svobod má každý právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno. Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Právní stát je založen na představě o jednotlivci jako důstojné lidské bytosti, rovné v právech se všemi ostatními bytostmi. Lidská důstojnost je všem ostatním hodnotám nadřazena, a proto také musí být tyto hodnoty definovány a vykládány v hranicích vymezených lidskou důstojností. **Povinností veřejné moci je zajistit respekt a ochranu nedotknutelné důstojnosti člověka** (čl. 1 odst. 1 Listiny základních práv a svobod). Rovnost jednotlivce v důstojnosti a právech je základem uznání hodnoty každého člověka, a to bez ohledu na jeho další charakteristiky (jako např. schopnosti či znalosti) a užitečnost či prospěšnost pro celek (nález Pl. ÚS 83/06). V nálezu IV. ÚS 412/04 Ústavní soud zdůraznil, že těžištěm ústavního pořádku je jednotlivec a jeho práva garantovaná tímto pořádkem. **Proto je třeba vycházet z priority občana nad státem, a tím i z priority základních občanských a lidských práv a svobod** (nález Pl. ÚS 43/93). Stát má povinnost důstojnost každého respektovat, a je-li třeba, musí ji i chránit vůči třetím osobám, neboť každý člověk má nárok na respekt a uznání své osoby. Subjektivní právo na zachování důstojnosti je výslovně garantováno v čl. 10 odst. 1 Listiny základních práv a svobod. V nálezech IV. ÚS 412/04 a I. ÚS 557/09 propojil Ústavní soud důstojnost se základním právem na osobnost. Nedotknutelnost lidské důstojnosti umožňuje člověku plně užívat jeho osobnosti.

Z práva na důstojnost a čest se dovozuje respekt k vlastnímu životu, fyzické, psychické a duchovní integritě, soukromí, osobní svobodě a k vlastnictví.

Právo na život obsažené v čl. 6 Listiny základních práv a svobod v sobě v ústavněprávním kontextu zahrnuje základní východisko, že lidský život je hoden absolutní ochrany pro jeho hodnotu samotnou, a to bez ohledu na rasu, pohlaví, národnost, občanství jednotlivce.

Právo na psychickou a duchovní integritu vyjadřuje zásadní nepřípustnost jakýchkoli nedobrovolných zásahů do tělesné schránky člověka a jeho vědomí. **Z nedotknutelnosti osoby plyne, že jakýkoliv zásah do tělesné a duševní integrity je nepřípustný, pokud se tak neděje v rámci zákona, na základě svobodného a informovaného souhlasu dané osoby (s výjimkami, kdy souhlas není třeba, při současném absolutním zákazu mučení a ponižujícího zacházení).** Součástí tohoto práva je i právo rozhodovat o vlastní fyzické a psychické integritě, což se pojí s případy přerušení těhotenství[2], jakož i s právem na sexuální sebeurčení, včetně sexuální orientace[3].

[2] ESLP ve věci Vo proti Francii, body 79 a násl.
[3] ESLP ve věci Dudgeon proti Spojenému království nebo Schalk a Kopf proti Rakousku, kde se právo na sebeurčení prolíná s rodinným životem

Jednou z nejvýznamnějších složek osobnosti každé fyzické osoby od narození až do smrti je její **identita morální i fyzická, která ji zcela nezaměnitelně odlišuje od ostatních fyzických osob. Vážným zásahem do práva na ochranu osobnosti tak může být přiřazení osobních údajů určité osoby někomu, komu tyto identifikační údaje nepatří, nebo dokonce úmyslné zcizení něčí identity.**

Specifickým problémem dotýkajícím se práv dětí je oprávněný zájem na tom, aby dítě znalo svoji identitu, včetně svého původu, svých předků, o čemž má být citlivým způsobem ve vhodné době informováno.

Právo na soukromí obsahuje právo učinit neveřejným záležitosti svého rodinného a partnerského života a projevů osobní povahy, o kterých se člověk rozhodne, že je nechce učinit veřejnými. Toto právo platí i tehdy, kdy se soukromé jednání uskutečňuje ve veřejném prostoru. Součástí práva na soukromí je právo na respekt k soukromému a rodinnému životu, jakož i k obydlí a ke korespondenci. **Právo na soukromý život se v této dimenzi projevuje především jako negativní právo – svoboda, tj. jako právo bránící v první řadě veřejné moci ve vměšování (v zásazích) do tzv. osobní soukromé sféry. Nicméně lze z těchto práv dovodit i pozitivní závazek státu spočívající v takové právní úpravě, která zabrání i třetím, soukromým osobám zasahovat do osobní soukromé sféry. Zásahem do osobní soukromé sféry je i sběr a uchovávání údajů týkajících se soukromého života a také sledování, hlídání a pronásledování ze strany veřejné moci, a to i ve veřejném prostoru či na veřejně přístupných místech. Do soukromého života řadíme i aktivity profesní, obchodní či sociální[4]. ESLP ve své judikatuře k právu na respekt k soukromému životu dle čl. 8 Úmluvy o ochraně lidských práv a základních svobod označil za zásahy do soukromí jednotlivců mimo jiné i zásahy v podobě kontroly dat, obsahu pošty a odposlechu telefonních hovorů[5], zjišťování telefonních čísel telefonujících osob[6] či zjišťování údajů o telefonním spojení[7].**

Z toho pak také přímo pramení důraz na ochranu **před jakýmkoli nakládáním s osobními údaji**, které by bylo prosto respektu k lidské důstojnosti, ohrožovalo by **život, fyzickou, psychickou a duchovní integritu včetně její identity a také soukromí a další ústřední hodnoty, jako například osobní svobodu, nebo vlastnictví.**

Z principu rovnosti v důstojnosti vyplývá současně **zákaz diskriminace**.

Podle ustálené judikatury ESLP se diskriminací rozumí rozdílné zacházení s osobami nacházejícími se ve srovnatelné situaci, které nemá objektivní a rozumné odůvodnění.

Přítomnost diskriminace lze zjistit následujícím testem:

a) k vyčlenění srovnatelného jednotlivce nebo skupiny;

b) ze zakázaného („podezřelého, neospravedlnitelného") důvodu;

c) které mu je k tíži (uložením břemene nebo odepřením dobra); a

d) vyčleňování není možné ospravedlnit, tedy:

i) nesleduje žádný legitimní či akceptovatelný důvod (veřejného, legitimního zájmu) a

4 srov. Rozsudek ESLP - Niemietz proti Německu
5 viz. rozsudek Klass a další proti Německu, rozsudek Leander proti Švédsku, rozsudek Kruslin proti Francii či rozsudek Kopp proti Švýcarsku
6 viz. rozsudek P. G. a J. H. proti Spojenému království
7 srov. výše citované rozhodnutí ve věci Amman proti Švýcarsku

j) opatření je nepřiměřené (disproporční).

Základním imperativem při tvorbě jakéhokoli systému nakládání s osobními údaji proto je, že musí vždy vytvářet vysoký stupeň ochrany ústavních práv, tedy klást tomu odpovídajícím způsobem důraz na ochranu života, fyzické, psychické a duchovní integrity, soukromí, případně osobní svobody a vlastnictví osob.

Měřítkem dostatečnosti respektu systému nakládání s osobními údaji k základním ústavním hodnotám bude, že systém úspěšně projde výše popsaným testem diskriminace a testem proporcionality. Čím více se má zásah do soukromí jednotlivce dotýkat dat z jeho intimní sféry, tím přísnější nároky jsou kladeny na proporcionalitu takového zásahu.

Dále bude třeba vždy garantovat právo na informační sebeurčení, což je právo rozhodnout dle vlastního uvážení, zda, v jakém rozsahu a jakým způsobem a za jakých okolností mají být skutečnosti ze soukromého života zpřístupněny jiným subjektům (čl. 10 odst. 3 Listiny základních práv a svobod). Např. kamerové sledování veřejného prostoru nebo preventivní síťové či plošné sledování, musí být vždy testováno z hlediska proporcionality zásahu do práva na soukromí (jeho omezení), přičemž přísné nároky jsou kladeny již na hodnocení samotné nutnosti zásahu do práva na informační sebeurčení. ESLP dovodil z práva na soukromý život v podobě práva na informační sebeurčení i pozitivní povinnost státu, který má, ovšem jen za určitých okolností, povinnost umožnit jednotlivci získat data, která z jeho soukromé sféry stát shromáždil a zpracoval[8].

U práva na informační sebeurčení se současně uplatní určitá omezení u veřejně činných osob, které musí strpět větší míru invaze do soukromí v zájmu veřejné kontroly nad svým počínáním, která má souvislost s výkonem veřejné aktivity. Taktéž musí strpět veřejnou kritiku, nikoli však zveřejňování nepravdivých informací o sobě.

Informační sebeurčení dítěte je modifikováno vůlí nositelů rodičovské zodpovědnosti. Ti by měli dbát, aby se veřejnost nedozvídala informace ze soukromého života dítěte, které mohou být vnímány jako pro dítě ponižující, zesměšňující či jinak způsobilé narušit jeho řádný (rozuměno zejména psychický) vývoj. Rodiče vykonávají rodičovskou zodpovědnost s ohledem na zájem dítěte. Rozhodování třetích osob o nejlepších zájmech dítěte vychází z uspokojení základních potřeb dítěte (výživa, bydlení, zdraví, jeho rozvoje, názorů a přání dítěte, totožnosti dítěte, citového spojení, jeho zdraví, bezpečí, ochrany, zaopatření, péče, soudržnosti rodiny, trvalosti domova, vazeb dítěte na kamarády, ze školních vztahů, rizik náhradní péče, kulturního pozadí či náboženské víry). Samotné rozhodnutí pak musí sledovat cíl stabilního, a nikoliv přechodného řešení, které sleduje skutečně dlouhodobé zájmy dítěte.

Vedle práva na zachování cti a důstojnosti osob a práva na informační sebeurčení působí samostatně **právo na informace** upravené v článku 17 Listiny základních práv a svobod, kde garantuje právo na vyjádření názoru, tedy i přesvědčení a idejí, a to jakoukoliv formou; dále garantuje svobodu vyhledávat, přijímat a rozšiřovat ideje a informace, a to bez ohledu na hranice státu.

Při střetu základního politického práva na informace a jejich šíření s právem na ochranu osobnosti a soukromého života, tedy základních práv, která stojí na stejné úrovni, bude vždy věcí nezávislých soudů, aby s přihlédnutím k okolnostem každého jednotlivého případu pečlivě zvážily, zda jednomu právu nebyla nedůvodně dána přednost před právem druhým. Ústavní soud odepřel ochranu sdělování vědomě nepravdivých informací (nález I. ÚS 453/03). Přitom uvedl, že legitimitu zveřejnění informace nelze dovodit, pokud byla dominantně motivována touhou poškodit difamovanou osobu,

8 rozsudek Rotaru proti Rumunsku

pokud si šiřitel sám informaci neověřil, anebo pokud ji poskytl bezohledně, aniž by se řádně staral o to, zda je či není pravdivá.

Ústavní soud ve své judikatuře vychází z teze, podle níž jednotlivec musí mít k dispozici informace o fungování státní moci k utvoření si svobodného názoru za účelem toho, aby mohl případně iniciovat či participovat na veřejné diskusi, a tak státní moc kontrolovat (Pl. ÚS 2/10). V poslední době judikatura Ústavního soudu také brání zneužívání práva na informace a vyvažuje toto právo s oprávněnými zájmy subjektů dat (IV. US 1378/16).

Čl. 17 odst. 5 Listiny základních práv a svobod ukládá veřejné správě přiměřeným způsobem poskytovat informace o své činnosti, což se děje zejména v mezích správního řádu a zákona o svobodném přístupu k informacím.

2.4.2.2 Detailní popis relevantních hrozeb

V následující tabulce č. 5 jsou uvedeny hrozby, které jsou relevantní k posuzovaným primárním aktivům. Vždy je uvedena kategorie hrozeb a vysvětlení, co se pod jejich jednotným označením skrývá.

Tabulka 5 Popis hrozeb

Hrozby – kategorie	Popis
Vnější útoky	• Zneužití přístupu k PC s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ • Zneužití přístupu k počítačové síti s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ • Krádež nebo prolomení hesla do IS nebo aplikace s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ • Útok na IS nebo aplikace s cílem diskreditace či zcizení OÚ nebo omezení funkčnosti • Útok na web s možností zcizení nebo modifikace OÚ, která jsou na webové prezentaci uvedeny • Cílený útok na OÚ s motivem jejich odcizení a neoprávněného užití s možností cílené diskreditace organizace • Narušení referenčních OÚ v aplikacích nebo IS • Fyzické zcizení nebo poškození primárního aktiva včetně listinných evidencí s osobními daty • Průnik z vnější sítě do vnitřní sítě (prolomení perimetru) s cílem zcizení nebo kompromitace OÚ uložených v IS nebo aplikacích • Kompromitace dohledových prostředků nebo prostředků ke sledování a monitorování přístupu k OÚ • Kompromitace identity oprávněného uživatele Správce nebo Zpracovatele.
Technické chyby	• Chyby zálohování • Výpadek elektřiny • Výpadek hardwaru koncové stanice • Výpadek softwaru koncové stanice • Poškození nebo ztráta dat • Mechanické poškození listinné evidence osobních údajů • Narušení řádné čitelnosti listinné evidence osobních údajů • Poškození/selhání programového vybavení

Hrozby – kategorie	Popis
	• Nedostatečná ochrana vnějšího perimetru • Nedostatečná údržba informačního systému nebo aplikace, kde jsou evidovány OÚ • Nedostatečné postupy při identifikaci a odhalení incidentů • Dlouhodobé přerušení podpory dodavatele SW • Nedostatečná ochrana prostředků IS • Technické chyby ochrany úložišť listin obsahující OÚ
Lidský faktor	• Obecná chyba uživatele • Opomenutí uživatele • Nedostatečné školení nebo povědomí o nakládání s OÚ nebo jejich ochraně OÚ • Zkoušení prolomení zabezpečení uživatelem • Poškození fyzické vrstvy sítě • Zavlečení škodlivého SW • Porušení bezpečnostní politiky uživatelem • Zneužití oprávnění ze strany uživatelů • Zneužití oprávnění ze strany administrátorů • Narušení fyzické bezpečnosti – kancelář, serverovna • Nepřítomnost/zranění/smrt administrátora informačního systému • Nedostatečné vymezení bezpečnostních pravidel • Nedostatečná míra nezávislé kontroly • Nedostatečná ochrana úložišť listin obsahující OÚ
Narušení integrity OÚ	• Neoprávněné manipulování evidencemi OÚ na úrovni IS nebo aplikací pod správou Objednatele • Neoprávněné manipulování s listinnými evidencemi obsahující OÚ • Provedení neoprávněných činností • Zneužití vedených osobních údajů • Nevhodné či nesprávné nastavení přístupových oprávnění • Fyzické narušení listiny obsahující OÚ
Neoprávněný přístup	• K OÚ má přístup osoba, která k danému úkonu nemá oprávnění • Modifikace vedených OÚ • Nedostatečné monitorování činnosti uživatelů • Nedostatečné monitorování činnosti administrátorů
Narušení dostupnosti	• Nedostupnost osobních údajů z důvodu pochybení organizačního charakteru • Nedostupnost osobních údajů z důvodu technického pochybení
Ztráta osobních údajů	• Nevhodná manipulace s listinnou evidencí obsahující OÚ • Technické chyby v IS uchovávající osobní údaje • Úmyslné zcizení OÚ v listinné podobě z listinné evidence • Úmyslný export OÚ z IS nebo aplikací • Výmaz OÚ z IS nebo aplikací • Předání listinné evidence OÚ neautorizované osobě bez udání důvodu a bez dostatečné evidence a povinnosti navrátit předané OÚ
Narušení práv a svobod subjektu	• Narušení práva na soukromí

Hrozby – kategorie	Popis
údajů	• Narušení práva na ochranu cti a důstojnosti • Narušení práva na informační sebeurčení • Narušení práva na život • Narušení práva na duševní a tělesnou integritu • Narušení práva subjektu údajů na informace a přístupu k osobním údajům • Narušení práva subjektu údajů na výmaz (právo být zapomenut) • Narušení práva subjektu údajů na omezení zpracování OÚ • Narušení práva subjektu údajů na přenositelnost OÚ • Narušení práva na ochranu osobních údajů • Úmyslná kompromitace osobních údajů třetím subjektem • Narušení zákazu diskriminace • Narušení ochrany identity • Hmotné ztráty subjektu údajů • Neoprávněné zrušení pseudonymizace

Dále bude pro každé aktivum posouzena pravděpodobnost výskytu hrozby. Pro vlastní analýzu budou použita následující kritéria pro hodnocení pravděpodobnosti hrozby:

Tabulka 6 Stupnice hodnocení pravděpodobnosti hrozby

Stupeň	Četnost výskytu	Kritérium
1	Velmi nízká	Uplatnění hrozby je vysoce nepravděpodobné nebo nulová.
2	Nízká	Hrozba se může uplatnit méně než 1 x za rok, resp. se nebo kritické období.
3	Střední	Hrozba se může uplatnit zhruba 1x za rok, resp. hrozba se jednou uplatnila v průběhu kritického období.
4	Vysoká	Hrozba se může uplatnit zhruba 1x za měsíc, resp. hrozba se uplatnila jednou v průběhu více než 1x v kritickém období.
5	Velmi vysoká	Hrozba se může uplatnit zhruba 1x týdně, resp. hrozba se uplatnila denně v kritickém období.

2.4.3 Identifikace zranitelnosti (rizikovosti)

Odhad zranitelností zahrnuje slabá místa posuzovaných aktiv. Pro analýzu budou použita následující kritéria pro hodnocení zranitelností:

Tabulka 7 Stupnice hodnocení zranitelnosti aktiv

Stupeň	Zranitelnost aktiva	Kritérium
1	Velmi nízká	Hrozba se nemůže vůči aktivu uplatnit.
2	Nízká	Aktivum je chráněno, resp. je odolné velmi dobře proti uplatnění hrozby.

Stupeň	Zranitelnost aktiva	Kritérium
3	Střední	Aktivum je chráněno částečně resp. je mírně odolné proti uplatnění hrozby.
4	Vysoká	Aktivum je chráněno, resp. je odolné velmi nedostatečně proti uplatnění hrozby.
5	Velmi vysoká	Aktivum není chráněno vůbec.

Míra zranitelnosti a účinnost existujících ochranných opatření spolu úzce souvisí. Míra zranitelnosti určitou hrozbou je vlastností aktiva. Může být snížena jedině vhodným protiopatřením.

2.4.4 Celková míra rizika (riziková expozice)

Cílem identifikace míry rizika je zajištění optimálního výběru ochranných nebo nápravných opatření, která působí proti těmto rizikům.

Ohodnocení míry rizika se provádí jako kombinace (součin) tří hodnot:

- **Hodnota aktiva** na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.
- **Pravděpodobnost hrozby** na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.
- **Zranitelnost** na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.

Celková míra rizika je tak určena bezrozměrným číslem – rizikovým score. Bezrozměrné číslo je zvoleno, protože hodnocení je kalkulováno z heterogenních hodnot, které nelze převést na stejnorodé jednotky.

Rizikové skóre se vypočítává podle níže uvedené rovnice:

*Rizikové skóre = hodnota aktiva * pravděpodobnost * zranitelnost*

Rizikové skóre se pohybuje v rozmezí 0–125 bodů. Hranice akceptovatelného rizika je předmětem manažerského rozhodnutí na straně subjektu, u kterého je analýza rizik prováděna. Celková míra expozice pak doporučuje pořadí priorit při řešení a implementaci organizačních a technických opatření.

2.5 Metoda vyhodnocení systémové analýzy

Veškeré poznatky zjištěné v průběhu dílčích analýz popsaných v předchozích podkapitolách budou následně vyhodnoceny a budou adresovány nejzávažnější problémy **v právní, technické a organizační** oblasti.

Jakmile budou tyto problémy identifikovány, provede Zhotovitel jejich detailní popis a navrhne adekvátní opatření, která budou směřovat ke zlepšení současné situace.

Posledním navazujícím krokem byla příprava plánu implementace. Tento plán obsahuje doporučený postup obce pro implementaci opatření v oblasti technické, organizační a právní.

Zhotovitel pro potřeby této systémové analýzy sloučil rizika při jejich hodnocení do tří kategorií, a to nízká rizika, běžná a vysoká. Zbytkové riziko Zhotovitel s ohledem na modelový charakter analýzy rizik neuvažuje.

3 Analýza obcí se základním rozsahem přenesené působnosti

Zhotovitel provedl mapování pomocí dotazníků formuláři F01 a F02, které jsou blíže popsány v kapitole č. 2.1 Metoda mapování obcí. Tyto dotazníky byly rozeslány na kontaktní osoby jednotlivých obcí se základním rozsahem přenesené působnosti společně s metodikou pro vyplnění obou formulářů. Na základě rozeslaných dotazníků bylo následně u obcí se základním rozsahem přenesené působnosti domluveno a realizováno individuální místní šetření se zástupci obcí, kde byly řešeny aktuální stavy organizačních a technických opatření obcí se základním rozsahem přenesené působnosti. Místní šetření bylo převážně zaměřeno na tyto následující body:

- Shrnutí zaslaných dotazníků. Řešení problematiky, zda obec předala dotazníky a řešení problémů či bodů, kde si vyplňující osoby nebyly jisty ohledně vyplněných údajů;
- Zjištění současného stavu v implementaci organizačních a technických nařízení pro zajištění souladu s GDPR a zjištění aktuálních problémů s ochranou osobních údajů s ohledem na GDPR;
- Zjištění aktuálních technických opatření se zaměřením na ochranu elektronických a fyzických úložišť - zabezpečení serverů, problematiku vzdálených přístupů a jejich řízení, zajištění provozu webových stránek obce, používání sdílených disků v rámci úřadu, správa sociálních sítí obce, ochrana dat pomocí antivirových programů, ochrana komunikačních linek pomocí firewallu, zacházení se služebními mobilními telefony a jejich ochrana, služební notebooky a jejich používání, systémy na ochranu dat, poskytování Wi-Fi sítí, logování uložených záznamů a auditních informací, povolení užití webových úložišť pracovníky úřadu a obce, zajištění lokálních disků v počítačových sestavách v rámci úřadu, rezervační systémy, používání e-mailu, spisové služby, kamerové systémy, cloudová úložiště, elektronické podpisy, zabezpečení budov, využití flash disků a CD pracovníky úřadu a obce, služební automobily s využitím GPS sledováním pohybu;
- Zjištění aktuálního stavu organizačních opatření týkajících se ochrany osobních údajů. Identifikace klíčových směrnic a politik pro nakládání s osobními údaji, pro klasifikaci informací, pro chod spisové a skartační služby, bezpečnostních politik pro zacházení s informačními systémy úřadu, směrnici pro přijímání a odcházení pracovníků, organizační a pracovní řád úřadu, systemizaci pracovních míst a řízení přístupu do informačních systémů, další relevantní předpisy, které jsou závazné pro zaměstnance a definují komplexní rámec pro nakládání s osobními údaji;
- Problematika podpůrných evidencí osobních údajů a dalších agend úřadů, které nemají podporu informačních technologií.

3.1 Analýza zpracování a ochrany osobních údajů v informačních systémech

Zhotovitel provedl místní šetření v těchto obcích se základním rozsahem přenesené působnosti:

- Obec Kamýk nad Vltavou – místní šetření bylo provedeno dne 31. 1. 2018.
- Obec Mladý Smolivec – místní šetření bylo provedeno dne 24. 1. 2018
- Praha – Zbraslav – místní šetření bylo provedeno dne 5. 2. 2018
- Obec Srbce – místní šetření bylo provedeno dne 24. 1. 2018
- Obec Vysoké Pole – místní šetření bylo provedeno dne 25. 1. 2018

Poznatky zjištěné dotazníkovým a místním šetřením byly využity v rámci analýzy dostupné dokumentace obce se základním rozsahem přenesené působnosti a analýzy zpracování a ochrany osobních údajů v informačních systémech obcí se základním rozsahem přenesené působnosti. Postupy a výsledky těchto analýz jsou uvedeny v následujících kapitolách. Výsledky z místních šetření

v jednotlivých obcích se základním rozsahem přenesené působnosti jsou součástí přílohy č. 1 tohoto výstupu. Součástí přílohy č. 1 jsou také vyplněné dotazníky obcí společně s předanými dokumenty organizačního charakteru (řády, směrnice, politiky).

3.1.1 Analýza provedeného mapování obcí se základním rozsahem přenesené působnosti

Zhotovitel provedl analýzu zaslaných dotazníků F01 a F02 od obcí se základním rozsahem přenesené působnosti dle metody popsané v kapitole 2.1 Metoda mapování obcí.

Zhotovitel na základě analýzy vytvořil jednu vzorovou obec se základním rozsahem přenesené působnosti, u které vytvořil seznam všech agend, ve kterých obce prvního a druhého stupně zpracovávají osobní údaje; tento seznam je součástí Příloh č. 3 a č. 4.

Ke každé agendě Zhotovitel popsal následující položky:

- **Název agendy** – uvedení názvu agendy či jiného titulu zpracování osobních údajů;
- **Zpracovávané osobní údaje** – výčet všech osobních údajů, které jsou součástí dané agendy či titulu zpracování v kontextu obce nebo úřadu;
- **Právní základ zpracování** – uvedení legislativního předpisu upravující danou agendu nebo titulu zpracování;
- **Právní důvod zpracování** – uvedení právního důvodu zpracování osobních údajů úřadem (PP – právní povinnost, Souhlas – udělení souhlasu subjektu osobních údajů, Splnění smlouvy – zpracování osobních údajů na základě smlouvy);
- **Přenositelnost** – posouzení práva na přenositelnost údajů dle článku 20 GDPR;
- **Námitka** – posouzení práva vznést námitku dle článku 21 GDPR;
- **Archivní doba** – přiřazení spisového znaku, skartačního znaku a lhůty dle vzorového spisového plánu vydaného MV ČR (dostupné na *http://www.mvcr.cz/clanek/vzory.aspx*) nebo spisového a skartačního řádu posuzovaných obcí.

Na základě dotazníkového a místního šetření byla Zhotovitelem identifikována společná aktiva, která zpracovávají osobní údaje pro obce se základním rozsahem přenesené působnosti. K jednotlivým aktivům bylo Zhotovitelem přiřazeno označení, zda se jedná o listinné nebo elektronické úložiště osobních údajů (Elektronické úložiště - "E", Listinné úložiště - "L").

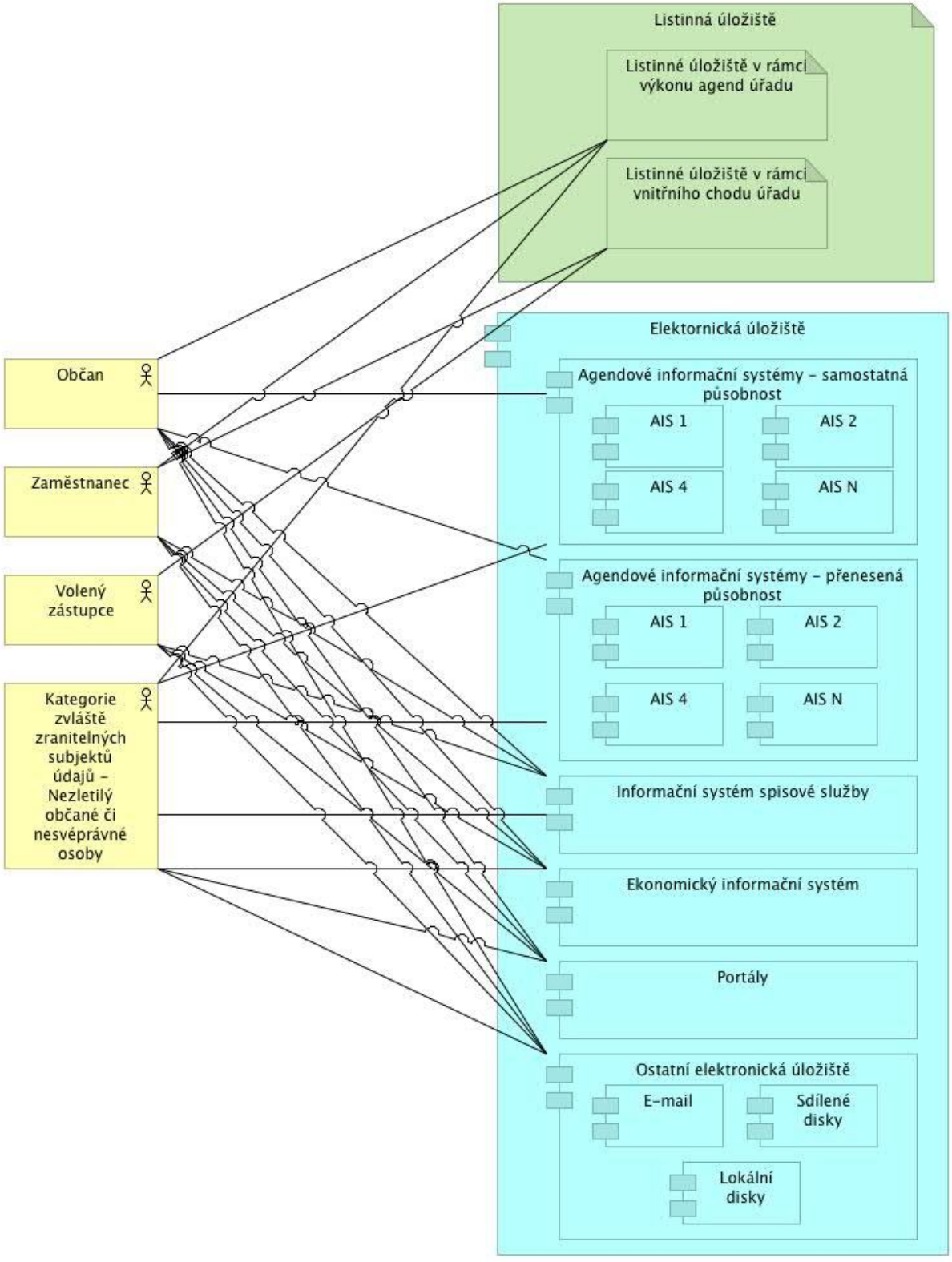
Zhotovitel určil na základě dotazníkového šetření a sběru souvisejících interních aktů řízení následující výčet identifikovaných aktiv:

- **Listinné úložiště v rámci výkonu agend úřadu (L)** – veškeré listiny, které jsou uloženy na úřadě a souvisí s výkonem agend úřadu;
- **Listinné úložiště v rámci vnitřního chodu úřadu (L)** – veškeré listiny, které jsou uloženy na úřadě a souvisejí s vnitřním chodem úřadu (příjem a propuštění zaměstnanců, účetnictví atd.);
- **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)** – e-mail, sdílené disky, lokální disky na počítačových sestavách.

Na základě podrobné systematické analýzy dotazníkového šetření byly Zhotovitelem identifikovány jednotlivé role subjektu údajů a následně k nim byla přiřazena odpovídající aktiva. Tyto vazby jsou uvedeny v Tabulce č. 8 a dále pak na Obrázku č.1.

Tabulka 8 Role subjektu osobních údajů

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 (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 (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 (E) • Ostatní elektronická úložiště (E)
Zvláště zranitelná kategorie subjektu údajů – Nezletilí občané či 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 (E) • Ostatní elektronická úložiště (E)



Obrázek 1 Role subjektu osobních údajů a přiřazená aktiva

3.1.2 Analýza dostupné dokumentace úřadu obce se základním rozsahem přenesené působnosti

Každá obec by měla mít sestaven alespoň základní okruh aktů řízení, který stanovuje základní pravidla chodu úřadu a oběhu úředních dokumentů. Při provádění místních šetření identifikoval Zhotovitel rozdílnou úroveň vyspělosti v přípravě a aplikaci těchto dokumentů do běžné praxe úřadu. Lze konstatovat, že každá z Vybraných obcí se základním rozsahem přenesené působností má vypracovány minimálně tyto dokumenty:

- Organizační řád
- Pracovní řád
- Spisový a skartační řád

Zhodnocení obsahu jednotlivých typů dokumentů z pohledu GDPR bude uvedeno dále.

Organizační a pracovní řád

Základní organizačnou normou obce je vždy Organizační řád, který stanovuje zásady činnosti úřadu. Pracovní řád blíže rozvádí práva a povinnosti zaměstnanců obecně vyplývající ze zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů (dále jen „zákoník práce“), a dalších pracovněprávních předpisů.

Poskytnuté Organizační řády obsahovaly co nejobecnější popisy organizační struktury úřadu včetně stručného výčtu jednotlivých odborů, oddělení a organizačních jednotek. U každé pozice byly definovány základní odpovědnosti a působnosti. Žádný Organizační řád neobsahoval roli pověřence pro ochranu osobních údajů.

Analyzované Pracovní řády byly vypracovány v souladu s § 306 zákoníku práce a bylo zřejmé, že nebyly aktualizovány pro zajištění souladu s GDPR. Systém řízení úřadu, který Organizační a Pracovní řád ustavuje, by měl obsahovat dostatečně detailně popsaná organizační opatření pro ochranu osobních údajů a citlivých osobních údajů, definice oprávnění pracovní role a způsob zpracování osobních údajů souvisejících s výkonem pracovních činností zaměstnance. Vhodné řešení je detailní popis pracovních rolí v Organizačním řádu tak, aby bylo zřejmé, které role přicházejí do styku s osobními údaji a citlivými osobními údaji, které role mají přístup do informačních systémů úřadu a jaká oprávnění v těchto informačních systémech mají mít přidělena. Zejména pokud pro tento účel nejsou vydány specializované interní akty řízení (směrnice). V obcích se základním rozsahem přenesené působnosti žádné další relevantní interní akty řízení, vyjma Spisového a skartačního řádu, nebyly.

Pracovní řád byl také jediným místem, kde byl alespoň náznakem nastíněn proces vzniku, změny a ukončení pracovního poměru. Tento proces je z pohledu implementace GDPR a systému řízení bezpečnosti informací klíčový a neměl by být ani na úrovni obcí se základním rozsahem přenesené působnosti opomínán. Rozsah zapracování v pracovních řádech byl z tohoto pohledu nedostatečný.

Spisový a skartační řád

Spisový a skartační řád je definován zejména následujícími právními předpisy:

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“).
- Nařízení 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).

- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.
- Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů.

Z analýzy předané dokumentace bylo zjevné, že obce využily vzorový skartační plán uvedený na webových stránkách Ministerstva vnitra ČR (viz http://www.mvcr.cz/clanek/vzory.aspx). Toto lze hodnotit jako dobrou praxi hodnou následování.

Na skartačních řádech bylo dále patrné, že mezi jednotlivými obcemi se základním rozsahem přenesené působnosti panují velké rozdíly v kvalitě a hloubce propracování. Z pohledu GDPR lze za velký nedostatek označit, že úřady neměly ani v jednom případě klasifikovány dokumenty s ohledem na obsah osobních či citlivých údajů. Tato klasifikace nebyla ustanovena žádným interním aktem řízení. Z absence klasifikace dokumentů vychází veškeré negativní důsledky – nemožnost definování specifických procesů a specifické ochrany dokumentů obsahujících osobní údaje a citlivé osobní údaje, nemožnost restrikce manipulace a zpracovávání osobních údajů či citlivých osobních údajů pouze na oprávněné účely apod.

S každým dokumentem v listinné i elektronické podobě je tedy formálně nakládáno stejně, dle totožných pravidel. V případě, že by minimální úroveň bezpečnosti informací byla nastavena dostatečně vysoko, aby pokryla alespoň požadavky plynoucí ze zákona o ochraně osobních údajů, bylo by možné tento přístup považovat za dostatečný. Toto se ovšem v průběhu místních šetření neprokázalo. Ochrana zejména listinných dokumentů obsahujících osobní údaje a citlivé osobní údaje na takto vytyčené úrovni nebyla.

Ve skartačních řádech či jiných interních aktech řízení chyběla záměrná a standardní ochrana dle GDPR, jejíž cílem je minimalizace rizik souvisejících se zpracováním již od návrhu systému. Prakticky se jedná například o striktní rozdělení oprávnění uživatelů dle principu „need to know“, aby se k dokumentům dostal pouze zaměstnanec, který je pro svou práci musí znát. V některých obcích existovala jistá míra benevolence v přiřazování uživatelských oprávnění a někteří uživatelé tak měli přístup ke všem uloženým dokumentům. Žádná obec taktéž neměla v žádném interním aktu řízení zdokumentovány procesy pseudonymizace osobních údajů, ačkoliv je v některých agendách pracovníci skutečně smysluplně využívali.

Z šetření bylo patrné, že skartační a spisové řády nebyly s ohledem na požadavky GDPR doposud novelizovány. Z místních šetření vyplynulo, že obce v tomto směru očekávají metodické kroky ze strany MV a publikování vzorových spisových a skartačních řádů, které již budou v souladu s GDPR.

3.1.3 Modelová obec se základním rozsahem přenesené působnosti

Na základě mapování Vybraných obcí se základním rozsahem přenesené působnosti Zhotovitel stanovil vzorovou obec, ve které se spojují základní a společné věci vztahující se k agendám, informačním systémům, listinným a elektronickým úložištím obsahující osobní údaje a interním aktům řízení a dokumentace.

Agendy a činnosti

Úplný výpis vykonávaných agend a činností Vzorové obce jsou uvedeny v přílohách č. 3 a č. 4. Mezi společné agendy, které zpravidla vykonávají obce se základním rozsahem přenesené působnosti, patří:

- Agendy spojené s chodem úřadu či obce (účetnictví, personalistika, veřejné zakázky atd.);

- Czechpoint;
- Evidence obyvatel;
- Místní poplatky;
- Organizace či částečné spolupořadatelství společenských akcí;
- Poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů;
- Spisová služba;
- Vedení matriky;
- Vedení obecní kroniky;
- Volby a jejich agenda.

Informační systémy a portály

Vzorová obec se základním rozsahem disponuje těmito informačními systémy:

- Informační systém spisové služby – IS, který obsahuje nástroje pro vedení elektronické evidence dokumentů, průkaznou evidenci dokumentů, správu a vyřizování dokumentů v rámci obce či úřadu. Informační systém je poskytován od dodavatele jako hostovaná služba a obec tedy nedisponuje datovými centry s vlastními servery;
- Agendové informační systémy v rámci přenesené působnosti – vzorová obec je uživatelem IS, který se stará o agendu v rámci evidence obyvatel, volební agendy, legalizace a vidimace. Informační systém je poskytován od věcného gestora problematiky jako hostovaná služba a obec tedy nedisponuje datovými centry s vlastními servery;
- Agendové informační systémy v rámci samostatné působnosti – vzorová obec disponuje IS, který se stará o agendu v rámci místních poplatků. Informační systém je poskytován od dodavatele jako hostovaná služba a obec tedy nedisponuje datovými centry s vlastními servery;
- Ekonomický informační systém – vzorová obec disponuje Ekonomickým IS, který obsahuje účetnictví obce, obecní rozpočty, evidence zaměstnanců a správa mezd. Informační systém je poskytován od dodavatele jako hostovaná služba a obec tedy nedisponuje datovými centry s vlastními servery;
- Portály – vzorová obec disponuje jednou obecní webovou stránkou, která je spravována externím administrátorem.

Listinná úložiště obsahující osobní údaje

Vzorová obec nedisponuje pokročilou technologií na zabezpečení listinných úložišť jako jsou bezpečnostní dveře, bezpečnostní zámky, kamerovými systémy, docházkové systémy pro sledování přístupů do budov s listinnými úložišti. Listinné úložiště jsou umístěny v uzamykatelných místnostech, kdy zámky a dřevěné dveře nepředstavují zásadní překážku pro násilné vniknutí. Dokumenty jsou uloženy ve skříních, které buď nejsou uzamykatelné nebo zámky na skříních jsou lehce překonatelné.

Elektronická úložiště

Vzorová obec disponuje elektronickými úložišti, která jsou umístěna na počítačových sestavách zaměstnanců úřadu či obce. Počítače disponují základní ochranou před vnějšími útoky. Zálohy jsou prováděny na externí disk, který je uložen v uzamykatelné místnosti v budově úřadu či obce. Dále obec disponuje datovými úložišti pro sdílení dat a tento systém je umístěn v budově obce či úřadu a napojen na interní síť, která je oddělena od veřejné sítě. Obec dále nijak nechrání ethernetové vstupy, které jsou umístěny ve volně dostupných prostorách budovy obce.

Interní akty řízení a dokumentace

Vzorová obec disponuje těmito interními akty řízení a dokumentace:

- Organizační řád;
- Pracovní řád;
- Spisový a skartační řád.

Bližší popis těchto interních aktů řízení vzorové obce je uveden v kapitole č. 3.1.2 Analýza dostupné dokumentace úřadu.

Vzorová obec nedisponuje směrnicí pro ochranu osobních údajů a jejich zpracování, informační koncepcí, bezpečnostní politikou ISVS ani dalšími interními předpisy, které se zabývají ochranou a zpracováním osobních údajů.

Personální zajištění

Na správě obce se podílí malý tým, který je zpravidla složen z osob, které nemají dlouhodobou „úřednickou“ erudici. Obec zpravidla nemá kvalifikovaného správce IT, tyto služby jsou zajišťovány externě. Obec nemá dedikovaného archiváře. Osoby, podílející se na správě obce, povětšinou nemají kvalifikované právní vzdělání.

3.1.4 Rizika zpracování vzhledem k rozsahu, kontextu, povaze a účelům zpracování osobních údajů

Na základě definovaných primárních aktiv z kapitoly č. 3.1.1 Analýza provedeného mapování obcí se základním rozsahem přenesené působnosti Zhotovitel provede jejich ohodnocení, a to dle stupnice, která je definována v kapitole č. 2.4.1 Metoda určení a ohodnocení aktiv. Zhotovitel podotýká, že tato analýza rizik je prováděna z pohledu subjektu údajů dle GDPR. Hodnota aktiv a další stanovení parametrů analýzy rizik jsou stanoveny z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

Ohodnocení aktiv pro účely analýzy rizik je uvedeno v tabulce č. 9.

Tabulka 9 Hodnocení aktiv

Název aktiva	Stupeň hodnocení	Popis hodnocení
Listinné úložiště v rámci výkonu agend úřadu	**5**	Zhotovitel ohodnotil aktivum na nejvyšší stupeň, kdy v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění

Název aktiva	Stupeň hodnocení	Popis hodnocení
		sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Listinné úložiště v rámci vnitřního chodu úřadu	**3**	Zhotovitel ohodnotil aktivum na střední stupeň, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. Aktivum nedisponuje takovou širokou škálou osobních údajů jako v případě úložiště spojené s výkonem agend obce vůči občanům. Zhotovitel nepředpokládá, že v rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva by došlo k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít zásadní vliv na fungování obcí či úřadů.
Informační systém spisové služby	**5**	Zhotovitel ohodnotil aktivum na nejvyšší stupeň, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Agendové informační systémy – samostatná působnost	**5**	Zhotovitel ohodnotil aktivum na nejvyšší stupeň, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající

Název aktiva	Stupeň hodnocení	Popis hodnocení
		z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Agendové informační systémy – přenesená působnost	**5**	Zhotovitel ohodnotil aktivum na nejvyšší stupeň, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Ekonomický informační systém	**5**	Zhotovitel ohodnotil aktivum na nejvyšší stupeň a to s ohledem na skutečnost, kdy v tomto aktivu je vysoká koncentrace osobních údajů a dále osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto

Název aktiva	Stupeň hodnocení	Popis hodnocení
		aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Portály	**3**	Zhotovitel ohodnotil aktivum na střední stupeň, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. Aktivum nedisponuje takovou širokou škálou osobních údajů jako v případě úložiště spojené s výkonem agend obce vůči občanům. V rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva nedojde k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít vliv na fungování obcí či úřadů.
Ostatní elektronické úložiště	**1**	Zhotovitel ohodnotil aktivum na nízký stupeň, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. V rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva nedojde k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít vliv na fungování obcí či úřadů.

Zhotovitel v kapitole č. 2.4.2 Hrozby a identifikace pravděpodobnosti hrozeb uvedl seznam obvyklých hrozeb dle standardů a hrozeb týkajících se ochrany osobních údajů vycházejících z GDPR či z dané problematiky. Zhotovitel k jednotlivým hrozbám přiřadil pravděpodobnost uplatnění jednotlivých hrozeb, a to ke každému identifikovanému aktivu. Stupnice ohodnocení aktiv je uvedena v kapitole č. 2.4.2 Hrozby a identifikace pravděpodobnosti hrozeb. Zhotovitel uvedl do hodnocení výši stupně pravděpodobnosti uplatnění hrozby včetně popisu zvolení dané výše pravděpodobnosti. Hodnocení pravděpodobnosti uplatnění hrozeb na jednotlivá aktiva je uvedeno v tabulce č. 10.

Tabulka 10 Hodnocení pravděpodobnosti hrozeb k aktivům

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Listinné úložiště v rámci výkonu agend úřadu	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Obce se základním rozsahem působnosti nedisponují takovým objemem osobních údajů, proto vnější útoky nejsou u těchto obcí častým jevem.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Uplatnění této hrozby je nepravděpodobné, jelikož obce se základním rozsahem působnosti nedisponují technologiemi v zajištění listinných úložišť, které by byly náchylné na technické chyby, a tedy jejich pravděpodobnost výskytu je na nízké úrovni.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí se základním rozsahem na střední úrovni, jelikož tyto obce většinou nedisponují interními akty, které by upravovali procesy nakládání s osobními údaji a jejich úložišť, které by byly pro zaměstnance obcí a úřadů závazná.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí se základním rozsahem na střední úrovni, jelikož tyto obce většinou nedisponují interními akty, které by upravovali procesy nakládání s osobními údaji a jejich úložišť.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce se základním rozsahem mají zámky, které jsou lehce překonatelné, objektová bezpečnost je na nízké úrovni. Uzamykatelné skříně jsou dřevěné, vykazují vysoké opotřebení a známky nízkého odporu při překonávání. Zároveň Obce se základním rozsahem působnosti nedisponují takovým objemem osobních údajů, který by zapříčinil vysoký výskyt neoprávněných přístupů k osobním údajům.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Narušení dostupnosti osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Může dojít k narušení práv a svobod subjektu osobních údajů.
Listinné úložiště v rámci vnitřního chodu úřadu	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Obce se základním rozsahem působnosti nedisponují takovým objemem osobních údajů, proto vnější útoky nejsou u těchto obcí častým jevem.
	Technické chyby	1	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na velmi nízkou úroveň. Aktuální technická opatření obcí se základním rozsahem zamezují jakékoliv pravděpodobnosti vzniku technických chyb v rámci tohoto aktiva.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí se základním rozsahem na střední úrovni, jelikož tyto obce většinou nedisponují interními akty, které by upravovali procesy nakládání s osobními údaji a jejich úložišť, které by byly pro zaměstnance obcí a úřadů závazná.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí se základním rozsahem na nízké úrovni, jelikož manipulaci s tímto aktivem je v pravomoci úzkého okruhu

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
			zaměstnanců obce.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí se základním rozsahem na nízké úrovni, jelikož manipulaci s tímto aktivem je v pravomoci úzkého okruhu zaměstnanců obce.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Narušení dostupnosti osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to i z důvodu menšího počtu agend spojených s interním chodem obcí a jejich úřadů.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Může dojít k narušení práv a svobod subjektu osobních údajů, ale jen subjektů údajů, které jsou spojeny s vnitřním chodem úřadu (zaměstnanci, smluvní partneři atd.)
Informační systém spisové služby	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Informační systém spisové služby u obcí se základním rozsahem je většinou hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které mají obce se základním rozsahem k dispozici.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Střední úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu možného

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
			selhání technického zajištění IS spisové služby, tak i vnějších jevů jako je výpadek elektřiny apod., na obcích se základním rozsahem technické chyby nejsou častým jevem.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným IS.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Pravděpodobnost je na střední hodnotě, jelikož obce se základním rozsahem nedisponují takovými opatřeními, které by zamezovali neoprávněnému přístupu k OÚ, ale zároveň Zhotovitel nepředpokládá častější výskyt dané hrozby z důvodu menší atraktivity a objemu osobních údajů u obcí se základním rozsahem, které by se staly terčem neoprávněného přístupu, popřípadě zcizení.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to z důvodu vyspělosti IS spisové služby a úložiště IS spisové služby je hostováno u poskytovatele.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň je zde zapříčiněna vyspělostí IS spisové služby a jejich dlouhodobé používání.
Agendové informační systémy – samostatná působnost	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Agendový informační systém u obcí se základním rozsahem je většinou hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které mají obce se základním rozsahem k dispozici.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu nízké pravděpodobnosti selhání technického zajištění AIS – samostatná působnost. Na obcích se základním rozsahem technické chyby nejsou častým jevem.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce se základním rozsahem nemají pevně stanovené procesy prací s agendovými informačními systémy např. interními akty.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Přístupy do agendových informačních systémů jsou jen v úzkém kruhu zaměstnanců obcí či úřadu.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to z důvodu vyspělosti agendových informačních systémů a jejich úložišť.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň je zde zapříčiněna vyspělostí agendových IS a jejich používání jen úzkého kruhu zaměstnanců obcí či úřadů.
Agendové informační systémy – přenesená působnost	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Agendový informační systém u obcí se základním rozsahem je většinou hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které mají obce se základním rozsahem k dispozici.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu nízké pravděpodobnosti selhání technického zajištění AIS. Na obcích se základním rozsahem technické chyby nejsou častým jevem.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce se základním rozsahem nemají pevně stanovené procesy prací s agendovými informačními systémy např. interními akty.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
			uplatnění dané hrozby.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Přístupy do agendových informačních systémů jsou jen v úzkém kruhu zaměstnanců obcí či úřadu.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to z důvodu vyspělosti agendových informačních systémů a jejich úložišť.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň je zde zapříčiněna vyspělostí agendových IS a jejich používání jen úzkého kruhu zaměstnanců obcí či úřadů.
Ekonomický informační systém	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ekonomický informační systém u obcí se základním rozsahem je většinou hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které mají obce se základním rozsahem k dispozici.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Střední úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu možného selhání technického zajištění Ekonomického informačního systému, tak i vnějších jevů jako je výpadek elektřiny apod., na obcích se základním rozsahem technické chyby nejsou častým jevem.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce se

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
			základním rozsahem nemají pevně stanovené procesy prací s Ekonomickým informačním systémem např. interními akty.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Přístupy do Ekonomického informačního systému jsou jen v úzkém kruhu zaměstnanců obcí či úřadu.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to z důvodu vyspělosti Ekonomického IS a jeho úložišť.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň je zde zapříčiněna vyspělostí Ekonomického IS a jejich dlouhodobé používání.
Portály	**Vnější útoky**	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na vysokou úroveň. Využívané portály obcí se základním rozsahem nedisponují vyspělou ochranou a mohou se stát terčem vnějších útoků.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Technické zajištění portálů není na vysoké úrovni a může dojít k technickým

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
			chybám.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce se základním rozsahem nemají pevně stanovené procesy prací s Ekonomickým informačním systémem např. interními akty.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň.
Ostatní elektronické úložiště	**Vnější útoky**	1	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na velmi nízkou úroveň. Toto aktivum nedisponuje takovým rozsahem osobních údajů, aby bylo terčem vnějších útoků.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
			pravděpodobnosti byla Zhotovitelem stanovena z důvodu nízké pravděpodobnosti selhání technického zajištění ostatních elektronických úložišť.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce se základním rozsahem nemají pevně stanovené procesy prací s ostatními elektronickými úložišti např. interními akty.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na vysokou úroveň. Aktuální zabezpečení ostatních elektronických úložišť je příčinou vysoké pravděpodobnosti uplatnění této hrozby.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.

Zhotovitel na základě zjištěných informací z mapování obcí a vytvoření Vzorové obce přiřadil jednotlivým hrozbám zranitelnosti jednotlivých hrozeb, a to ke každému identifikovanému aktivu. Zhotovitel uvedl do hodnocení výši stupně zranitelnosti aktiv vůči hrozbám včetně popisu zvoleného stupně zranitelnosti. Hodnocení zranitelnosti aktiv vůči hrozbám je uvedeno v tabulce č. 11.

Tabulka 11 Zranitelnosti aktiv vůči hrozbám

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
Listinné úložiště v rámci výkonu agend úřadu	**Vnější útoky**	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Zabezpečení listinných úložišť je v obcích se základním rozsahem na nízké úrovni. Listiny nejsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy, nepředstavují zásadní překážku pro vnější útoky.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Ochrana před technickými chyby či vnějších vlivů nedosahuje u obcí se základním rozsahem působnosti takové úrovně, aby byla zranitelnost ohodnocena na nízké úrovni. Obce většinou nedisponují zabezpečovacími systémy obsahující např. tepelný detektor či kouřový detektor.
	Lidský faktor	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, popřípadě absence školení v rámci ochrany osobních údajů.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť včetně procesů jejich zabezpečení.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce se základním rozsahem mají zámky, které jsou lehce překonatelné, objektová bezpečnost je na nízké úrovni. Uzamykatelné skříně jsou dřevěné, vykazují vysoké opotřebení a známky nízkého odporu při překonávání. Obce se základním rozsahem působnosti nedisponují kamerovým systémem a většinou je budova úřadu volně přístupná.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Narušení dostupnosti osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Ztráta osobních údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, dále obce se základním rozsahem mají zámky, které jsou lehce překonatelné, objektová bezpečnost je na nízké úrovni. Uzamykatelné skříně jsou dřevěné, vykazují vysoké opotřebení a známky nízkého odporu při překonávání. Obce se základním rozsahem působnosti nedisponují kamerovým systémem a většinou je budova úřadu volně přístupná.
	Narušení práv a svobod subjektu údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů.
Listinné úložiště v rámci vnitřního chodu úřadu	**Vnější útoky**	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Zabezpečení listinných úložišť je v obcích se základním rozsahem na nízké úrovni. Listiny nejsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy nepředstavují zásadní překážku pro vnější útoky.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Ochrana před technickými chyby či vnějších vlivů nedosahuje u obcí se základním rozsahem působnosti takové úrovně, aby byla zranitelnost ohodnocena na nízké úrovni. Obce většinou nedisponují zabezpečovacími systémy obsahující např. tepelný detektor či kouřový detektor.
	Lidský faktor	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, popřípadě absence školení v rámci ochrany osobních údajů.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť včetně procesů jejich zabezpečení.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce se základním rozsahem mají zámky, které jsou lehce překonatelné, objektová bezpečnost je na nízké úrovni. Uzamykatelné skříně jsou dřevěné, vykazují vysoké opotřebení a známky nízkého odporu při překonávání. Obce se základním rozsahem působnosti nedisponují kamerovým systémem a většinou je budova úřadu volně přístupná.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Narušení dostupnosti osobních údajů v obcích se základním rozsahem působnosti je na nízké úrovni, a to i z důvodu menšího počtu agend.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Ztráta osobních údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, dále obce se základním rozsahem mají zámky, které jsou lehce překonatelné, objektová bezpečnost je na nízké úrovni. Uzamykatelné skříně jsou dřevěné, vykazují vysoké opotřebení a známky nízkého odporu při překonávání. Obce se základním rozsahem působnosti nedisponují kamerovým systémem a většinou je budova úřadu volně přístupná.
	Narušení práv a svobod subjektu údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů.
Informační systém spisové služby	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana informačního systému spisové služby je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele IS spisové služby, které je dostatečně zabezpečeno.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana informačního systému spisové služby je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele IS spisové služby, které je dostatečně zabezpečeno. IS spisové služby jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným IS.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným IS.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do IS spisové služby a nedochází k časté fluktuaci osob mající přístupy do IS spisové služby. Dané osoby mají již zavedené procesy užití IS spisové služby, takže by nemělo docházet k neoprávněným přístupům k IS spisové služby.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou před úmyslným exportem dat u IS či výmaz u IS spisové služby. Zároveň disponují obce alespoň základní ochranou před ztrátou dat.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Agendové informační systémy – samostatná působnost	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana Agendového informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana AIS je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno. AIS jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do AIS a nedochází k časté fluktuaci osob mající přístupy do AIS. Zároveň obce nedisponují aktivním řízením přístupů do AIS včetně monitoringu těchto přístupů.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou před úmyslným exportem dat z AIS či výmazem dat z AIS. Zároveň disponují obce alespoň základní ochranou před ztrátou dat.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Agendové informační systémy – přenesená působnost	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana Agendového informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana AIS je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno. AIS jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do AIS a nedochází k časté fluktuaci osob mající přístupy do AIS. Zároveň obce nedisponují aktivním řízením přístupů do AIS včetně monitoringu těchto přístupů.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou před úmyslným exportem dat z AIS či výmazem dat z AIS. Zároveň disponují obce alespoň základní ochranou před ztrátou dat.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Ekonomický informační systém	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana Ekonomického informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele Ekonomického informačního systému, které je dostatečně zabezpečeno.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Ze zjištěných informací Ekonomický informační systém je chráněn jen základním způsobem před technickými chybami.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb uživateli Ekonomického informačního systému, a to i z důvodu nezavedení interních aktů, které by řešili procesy užití Ekonomického IS.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb uživateli Ekonomického informačního systému, a to i z důvodu nezavedení interních aktů, které by řešili procesy užití Ekonomického IS. Dále je to také absence politiky přístupů obce či úřadu do Ekonomického IS.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do Ekonomického IS a nedochází k časté fluktuaci osob mající přístupy do Ekonomického IS. Zároveň obce nedisponují aktivním řízením přístupů do Ekonomického IS včetně monitoringu těchto přístupů.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou před úmyslným exportem dat z Ekonomického IS či výmazem dat z Ekonomického IS. Zároveň disponují obce alespoň základní ochranou před ztrátou dat.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Portály	**Vnější útoky**	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou portálů před vnějšími útoky.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Portály jsou zpravidla poskytovány externími subjekty a uloženy v rámci cloudového řešení, takže zranitelnost je na nízké úrovni.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb administrátory portálů obce.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb redaktory a administrátory portálů obce.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Zhotovitel nepředpokládá neoprávněných přístup na portály obce.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Portály disponují jen základní ochranou.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Ostatní elektronické úložiště	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce mají ostatní elektronická úložiště odděleny od veřejně dostupné sítě.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce provádějí zálohu dat.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb uživatelů ostatních elektronických úložišť, kdy dochází ke ztrátě či jinému znehodnocení dat obsahující osobní údaje.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb uživatelů ostatních elektronických úložišť, kdy dochází ke ztrátě či jinému znehodnocení dat obsahující osobní údaje.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem volný přístup do prostor budov obcí či úřadů, kde je v těchto prostorách možnost připojení do ethernetových výstupů, a tedy přístupu do sítě. Obce dále nedisponují interními akty pro řízení přístupů k počítačovým sestavám a jejich aktivní řízení.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.
	Ztráta osobních údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Obce nedisponují dostačující ochranou před ztrátou osobních údajů z ostatních elektronických úložišť.
	Narušení práv a svobod subjektu údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

V tabulce č. 12 jsou shrnuty úrovně pravděpodobnosti uplatnění jednotlivých hrozeb k vybraným aktivům.

Tabulka 12 Pravděpodobnost uplatnění hrozeb vůči aktivům

Aktivum	Hodnota aktiva	Pravděpodobnost							
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů
Listinné úložiště v rámci výkonu agend úřadu	5	2	1	3	3	2	3	3	3
Listinné úložiště v rámci vnitřního chodu úřadu	3	2	1	3	3	2	3	3	3
Informační systém spisové služby	5	2	5	3	4	2	3	4	3
Agendové informační systémy - samostatná působnost	5	2	4	4	3	3	3	3	3
Agendové informační systémy - přenesená působnost	5	3	2	2	4	3	2	2	3
Ekonomický informační systém	5	3	2	3	1	2	4	2	3
Portály	3	3	2	2	1	2	4	2	3
Ostatní elektronické úložiště	1	3	5	4	4	4	3	3	3

Následně byly Zhotovitelem stanoveny úrovně zranitelnosti jednotlivých aktiv vůči stanoveným hrozbám, které jsou uvedeny v tabulce č. 13

Tabulka 13 Zranitelnosti jednotlivých aktiv vůči hrozbám

Aktivum	Hodnota aktiva	Zranitelnosti							
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů
Listinné úložiště v rámci výkonu agend úřadu	5	3	3	4	3	3	2	4	4
Listinné úložiště v rámci vnitřního chodu úřadu	3	3	3	4	3	3	2	4	4
Informační systém spisové služby	5	2	2	2	2	2	3	3	3
Agendové informační systémy - samostatná působnost	5	2	2	2	2	3	3	3	3
Agendové informační systémy - přenesená působnost	5	2	2	2	2	3	3	3	3
Ekonomický informační systém	5	2	3	3	3	3	3	3	3
Portály	3	3	2	3	3	2	3	3	3
Ostatní elektronické úložiště	1	2	2	3	3	3	2	4	4

V tabulce č. 14 je uvedeno závěrečné rizikové skóre k jednotlivým aktivům včetně indikátorů:

- celková míra rizika hrozby – indikátor ukazuje celkové míry rizika hrozeb dle jejich výše. Dle výše indikátoru je tedy patrné, které hrozby jsou pro obec nejzávažnější a mohou zde směřovat technická a organizační opatření;
- celkové míra rizika aktiva – indikátor ukazuje celkové míry rizika aktiv dle jejich výše. Dle výše indikátoru je tedy patrné, která aktiva jsou nejnáchylnější a potřebují zvýšenou pozornost či ochranu ze strany obcí.

Tabulka 14 Rizikové skóre

Aktivum	Hodnota aktiva	Rizikové skóre								*Indikátor celkové míry rizika aktiva*
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů	
Listinné úložiště v rámci výkonu agend úřadu	5	30	15	60	45	30	30	60	60	330
Listinné úložiště v rámci vnitřního chodu úřadu	3	18	9	36	27	18	18	36	36	198
Informační systém spisové služby	5	20	50	30	40	20	45	60	45	310
Agendové informační systémy - samostatná působnost	5	20	40	40	30	45	45	45	45	310
Agendové informační systémy - přenesená působnost	5	30	20	20	40	45	30	30	45	260
Ekonomický informační systém	5	30	30	45	15	30	60	30	45	285
Portály	3	27	12	18	9	12	36	18	27	159
Ostatní elektronické úložiště	1	6	10	12	12	12	6	12	12	82
Indikátor celkové míry rizika hrozby	-	181	186	261	218	212	270	291	315	-

3.1.5 Vyhodnocení dosavadního postupu analýzy obcí se základním rozsahem přenesené působnosti

Zhotovitel provedl mapování obcí se základním rozsahem přenesené působnosti, zpracoval záznamy o činnostech na základě informací z Vybraných obcí, které jsou uvedeny v Přílohách. 3 a 4 a provedl analýzu rizik na modelové obci, jejíž rozsah je specifikován v kapitole 3.1.3 Modelová obec se základním rozsahem přenesené působnosti.

Na základě indikátoru celkové míry rizika aktiva stanovil Zhotovitel modelový rozsah organizačních a technických opatření pro jednotlivá aktiva v kontextu obvykle se vyskytujících situací. Detailní popis je uveden v následující kapitole.

3.2 Návrh opatření k zajištění plného souladu posuzovaných procesů s GDPR a dalšími právními předpisy a dosažení předepsané úrovně ochrany osobních údajů

Na základě provedené analýzy rizik pro modelovou obec jsme identifikovali obecné problematické situace v kontextu GDPR. K těmto situacím jsme zpracovali komentář, který diskutuje vhodné návrhy opatření vedoucí k dosažení souladu s požadavky GDPR.

V této kapitole jsou uvedeny situace, které Zhotovitel považuje za situace, které se zcela jistě vyskytují rovněž v obcích se základním rozsahem přenesené působnosti.

Jedná se o následující situace:

- Uveřejňování osobních údajů zaměstnanců na webových stránkách obce;
- Uveřejňování osobních údajů zaměstnanců/třetích osob na facebookovém profilu obce;
- Pořizování fotografií pro obec na akcích v obci;
- Uveřejňování informací a fotografií pořízených na akcích uskutečněných v obci na webových stránkách obce;
- Vydávání obecních novin – zpravodajská licence;
- Vedení vlastních agendových informačních systémů/přístup do agendových informačních systémů vedených jinými orgány veřejné moci;
- Souhlas zaměstnanců jako právní důvod pro zpracování osobních údajů zaměstnavatelem;
- Doba uchovávání kamerových záznamů;
- Kdo může a nemůže být pověřenec pro ochranu osobních údajů;
- Podřízené organizace a povinnost jmenovat pověřence pro ochranu osobních údajů;
- Zpracovatelská smlouva a její atributy;
- Školy a školská zařízení;
- Kdy se jedná o zpracování osobních údajů pro správce ze strany zpracovatele;
- Uveřejňování dokumentů;
- Provozování veřejné telekomunikační služby (Wi-Fi) a povinnost provozovatele uchovávat záznamy;
- Vedení a uveřejňování kronik;
- Vedení pomocných evidencí;
- Zpracování osobních údajů na základě právního důvodu „veřejný zájem“;
- Rozsah osobních údajů stanovený zákonem;
- Vydávání obecně závazných vyhlášek v kontextu ochrany osobních údajů;
- Vedení spisové služby;
- Uchovávání osobních údajů v souvislosti se zadávacím řízením;
- Uchovávání osobních údajů v souvislosti se zadávacím řízením

Správce, který vystupuje v roli zadavatele ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, je dle § 216 odst. 1 téhož zákona povinen uchovávat dokumentaci o zadávacím řízení, kterou tvoří všechny dokumenty v listinné nebo elektronické podobě a výstupy z ústní komunikace, jejichž pořízení v průběhu zadávacího řízení, popřípadě po jeho ukončení, vyžaduje tento zákon, včetně úplného znění originálů nabídek všech dodavatelů. Archivační doba je stanovena jednotně v délce 10 let ode dne ukončení zadávacího řízení nebo od změny závazku ze smlouvy na veřejnou zakázku, pokud jiný právní předpis (tj. zejména zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, může jím být též vnitřní předpis zadavatele či požadavky poskytovatelů dotací) nestanoví lhůtu delší. Obsah dokumentace o zadávacím řízení, kterou je nutné uchovávat, tedy tvoří mj. nabídky všech dodavatelů, resp. všech účastníků zadávacího řízení, a to i těch, kteří jsou v zadávacím řízení neúspěšní (tedy těch, s nimiž zadavatel neuzavřel smlouvu). Součástí těchto nabídek přitom mnohdy bývají též

životopisy, doklady o vzdělání či odborná osvědčení členů realizačního týmu, které zadavatel musí uchovávat.

Uchovávání dokumentace o zadávacím řízení je povinností, kterou správci/zadavateli ukládá zákon. Důvodem uložené povinnosti uchování dokumentace o zadávacím řízení je možnost provedení průběžné i následné kontroly postupu zadavatele a dodavatelů ve vztahu k předmětnému zadávacímu řízení. Nepořízení nebo neuchování dokumentace o zadávacím řízení po stanovenou dobu podle § 216 předmětného zákona je považováno za přestupek, ze nějž lze uložit pokutu ve výši 10 % ceny veřejné zakázky, nebo až do výše 20 mil. Kč, nelze-li celkovou cenu veřejné zakázky zjistit (§ 268 zákona).

DOPORUČENÍ:

Správce v roli zadavatele je povinen uchovávat dokumentaci o zadávacím řízení nejméně po dobu 10 let, pokud jiný právní předpis nestanoví archivační lhůtu delší. Dokumentaci o zadávacím řízení tvoří mj. též osobní údaje subjektů údajů uvedené v nabídkách účastníků zadávacího řízení (např. osobní údaje uvedené v životopisech, dokladech o vzdělání či odborných osvědčeních členů realizačního týmu). Při uchovávání osobních údajů v rámci dokumentace o zadávacím řízení je tedy nutné dodržet povinnosti stanovené GDPR, např. z hlediska zabezpečení či přístupových oprávnění k uchovávaným osobním údajům.

- Využití firemního resp. obecního e-mailu;
- Využití a problematika freemailů;
- Omezení přístupu na stránky se škodlivým obsahem;
- Webové stránky obce – problematika formulářů;
- Webové stránky obce – problematika záznamů a fotografií;
- Facebook a sociální sítě;
- Notebooky – šifrování;
- Chytré telefony - ochrana;
- Chytré telefony – soukromé vlastnictví;
- Počítačové sestavy v rámci úřadu a jejich ochrana;
- Interní ochrana sítě LAN;
- Segmentace interní sítě LAN;
- Problematika sítí LAN mezi více budovami úřadu;
- Externí správa IT infrastruktury;
- Problematika sledování přístupů a monitoring činností (tzv. logování;
- Problematika sdílených disků;
- Problematika využití flash pamětí a USB portů pracovníky úřadu;
- Problematika využití DVD/CD pracovníky úřadu.

Pod bodem DOPORUČENÍ u každé posuzované problematické situace je uveden návrh opatření k zajištění plného souladu posuzovaných procesů s GDPR a dalšími právními předpisy a dosažení předepsané úrovně ochrany osobních údajů.

Zhotovitel této systémové analýzy v této souvislosti upozorňuje, že závěry a doporučení u níže uvedených situací vycházejí ze systémové analýzy provedené na vzorku Vybraných obcí. Míru dopadu uvedených závěrů a doporučení musí posoudit každý správce osobních údajů ve smyslu čl. 4 odst. 7 GDPR, který vykonává činnosti spadající do věcné působnosti GDPR (čl. 2 odst. 1 GDPR), případ od případu a dle konkrétních okolností, zejména se zohledněním stanovených účelů, podmínek zpracování osobních údajů a úrovně zavedených organizačních a technických opatření. Odpovědný za zpracování osobních údajů v souladu s GDPR je totiž vždy správce, přičemž správce zároveň musí být schopen toto dodržení souladu doložit (čl. 5 odst. 2 a čl. 24 odst. 1 GDPR).

3.2.1 Uveřejňování osobních údajů zaměstnanců na webových stránkách obce

Podle § 5 odst. 2 písm. f) zákona o ochraně osobních údajů může správce zpracovávat osobní údaje bez souhlasu subjektů údajů, pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení. Mezi osobní údaje funkcionářů a zaměstnanců veřejné správy, které lze na základě komentovaného ustanovení zpřístupnit (např. na webu či facebookovém profilu obce), patří jméno a příjmení a základní kontaktní údaje (pracovní e-mailová adresa, pracovní telefonní číslo) v případě, že jejich pracovní pozice předpokládá jednání či nějaký jiný způsob kooperace s veřejností (např. zaměstnanec pracující v oddělení místních poplatků, opačným případem by mohl být zaměstnanec, který zastává pracovní pozici řidiče).

Výše uvedený právní důvod ke zpracování není obsažen v GDPR, nicméně dle návrhu doprovodného zákona k chystanému zákonu o zpracování osobních údajů přinese náhradu novelizovaný zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, který by měl v § 8a odst. 2 obsahovat ustanovení, podle kterého povinný subjekt poskytne osobní údaje o veřejně činné osobě, funkcionáři nebo zaměstnanci veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti nebo o jeho funkčním nebo pracovním zařazení.

Uveřejnění soukromé e-mailové adresy či telefonního čísla zaměstnance nepřichází u obce jako správce osobních údajů v úvahu, ledaže by pro takové zpracování bylo možné specifikovat legitimní účel a získat od zaměstnance souhlas s tímto zpracováním. S ohledem na zásady zákonnosti a minimalizace údajů lze správcům z oblasti veřejné správy doporučit neuveřejňovat fotografie zaměstnanců bez jejich souhlasu prostřednictvím webových stránek, byť by tento postup byl veden dobrým úmyslem či zájmem např. na vyšší vstřícnosti vůči občanům. Dle odborné literatury[9] není takové uveřejnění možné, pokud neexistuje nějaký významný veřejný zájem na tomto postupu, tím by např. mohlo být uveřejnění fotografie nového strážníka městské policie, aby se s ním mohli občané obce seznámit, nikoliv však např. fotografie všech zaměstnanců oddělení životního prostředí. Nicméně ani v případě fotografie strážníka uveřejnění nebude žádoucí, pokud se bude jednat o menší obec či konkrétní oblast, kde lze za vhodnější postup považovat například letáky s fotografií roznášené do schránek.[10]

Uveřejňuje-li obec na svých webových stránkách u identifikačních a kontaktních údajů zaměstnance informaci o tom, zda tento konkrétní zaměstnanec je přítomen na svém pracovišti, jedná se o zpracování osobního údaje. Pro tento druh určité formy veřejného monitoringu polohy fyzické osoby, tj. zpracování osobních údajů však s velkou mírou pravděpodobnosti nebude mít zaměstnavatel jako správce zákonný důvod. Jedná se sice do jisté míry o údaj vypovídající o úřední činnosti ve smyslu výše uvedeného ustanovení zákona o ochraně osobních údajů, nicméně toto ustanovení je nutné vykládat i s ohledem na článek 10 Listiny základních práv a svobod, který zaručuje právo na ochranu před neoprávněným zasahováním do soukromého života a před shromažďováním, uveřejňováním nebo jiným zneužíváním osobních údajů. K tomuto lze dále odkázat na nález Ústavního soudu sp. zn. IV. ÚS 1378/16 ze dne 17. 10. 2017, který konstatoval, že ustanovení článku 17 odst. 5 Listiny základních práv a svobod zavazuje státní orgány a orgány územní samosprávy poskytovat informace o své činnosti „*přiměřeným způsobem*“ s tím, že podmínky a provedení tohoto závazku, resp. jemu odpovídajícího práva, stanoví zákon. Právo na informace ve veřejném zájmu není absolutní; pokud jeho výkon zasahuje do práva na ochranu soukromého života, chráněného článkem 10 Listiny základních práv a svobod a článkem 8 Úmluvy o ochraně lidských práv a základních svobod, je nutno

[9] Viz Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha : C. H. Beck, 2012, s. 99 – 174.
[10] Srov. Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíček, J. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Praha: Wolters Kluwer ČR, 2017. s. 130 – 131.

v každém jednotlivém případě všechna tato práva poměřovat a zajistit mezi nimi spravedlivou rovnováhu. Ústavní soud dále nepřímo uvedl, že je nutné definovat účel, k jakému mají být požadované osobní údaje užity ve veřejném zájmu, a v čem tento veřejný zájem má spočívat, aby bylo možné posoudit, zda sledovaného účelu není možné dosáhnout i jinak, tj. při šetření ústavně chráněných základních práv dotčených osob.

DOPORUČENÍ:

S ohledem na shora uvedené lze doporučit, aby obec uveřejňovala na svých webových stránkách jméno a příjmení, pracovní e-mail a telefonní číslo zaměstnance pouze v případě, že jejich pracovní pozice předpokládá jednání či nějaký jiný způsob kooperace s veřejností. Uveřejnění soukromé e-mailové adresy či telefonního čísla zaměstnance by se obec, i v situaci, kdy obdrží od zaměstnance souhlas k takovému uveřejnění, měla raději vyvarovat.

3.2.2 Uveřejňování osobních údajů zaměstnanců/třetích osob na facebookovém profilu obce

Uveřejňování osobních údajů o zaměstnancích na facebookovém profilu obce vychází ze stejných pravidel jako uveřejňování na webových stránkách obce. Osobní údaje ve vztahu k soukromí zaměstnanců a osobní údaje třetích osob lze uveřejnit jen na základě uděleného souhlasu (viz *Uveřejňování osobních údajů zaměstnanců na webových stránkách obce*). Fotografie zaměstnanců či třetích osob např. z akcí pořádaných obcí lze uveřejnit pouze se souhlasem dotčených osob, a to i například formou konkludentního souhlasu (viz *Uveřejňování informací a fotografií pořízených na akcích uskutečněných v obci na webových stránkách obce*). Dalším důvodem pro uveřejňování osobních údajů může být výkon tzv. zpravodajské licence (viz *Vydávání obecních novin – zpravodajská licence*). Nicméně vzhledem k obsahu smluvních podmínek definovaných společností Facebook lze doporučit se uveřejňování osobních údajů zaměstnanců vyvarovat. Součástí smluvních podmínek je totiž oprávnění, kterým správce účtu uděluje společnosti Facebook nevýhradní, přenosnou, převoditelnou, volnou (tj. bez nároku na autorský honorář) licenci na použití veškerého obsahu podléhajícího právu na duševní vlastnictví (fotografie a videa), které správce účtu uveřejní na Facebooku nebo v návaznosti na něj. Ze smluvních podmínek dále vyplývá, že po odstranění obsahu z uživatelského profilu odstraněný obsah může po přiměřeně dlouhou dobu existovat v záložních kopiích. Právě nedostatečná možnost kontroly nad uveřejněnými osobními údaji znamená, že není možné při získání osobních údajů subjektu údajů poskytnout veškeré informace o zpracování dle čl. 13 GDPR a dále po odvolání souhlasu se zpracováním a uplatněním práva na výmaz dle čl. 17 GDPR zajistit odstranění veškerých osobních údajů, které byly na základě uděleného souhlasu prostřednictvím sociálních sítí na profilu obce sdíleny.

DOPORUČENÍ:

Obec může uveřejňovat osobní údaje zaměstnanců a třetích osob na svém facebookovém profilu pouze na základě jimi udělených souhlasů se zpracováním osobních údajů. Nicméně vzhledem k nedostatečné kontrole nad uveřejněnými osobním údaji uveřejňování osobních údajů na Facebooku (či na jiných sociálních sítí) spíše nedoporučujeme.

3.2.3 Pořizování fotografií pro obec na akcích v obci

Právo k podobě člověka coby projevu osobní povahy je součástí osobnostních práv, jejichž ochranu na ústavní úrovni garantuje čl. 10 Listiny základních práv a svobod (viz kapitola 2.4.2.1 Osobnostní

práva subjektu údajů)[11]. Zákonnou úpravu práva člověka na zachycení jeho podoby představuje ust. § 84 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník"). Předmětem práva na podobu je individualizovaná (identifikovatelná) podoba člověka jako jedna z významných hodnot osobnosti jednotlivce (NS 30 Cdo 936/2005). Obsahem tohoto práva je také výlučné oprávnění člověka rozhodovat o tom, zda a jakým způsobem může dojít k zachycení jeho vlastní podoby a k jejímu následnému použití. Zachycení podoby člověka tak, aby podle daného zobrazení bylo možné určit jeho totožnost, jakož i následné použití jeho podoby, je tedy dle občanského zákoníku primárně založeno na požadavku udělení svolení tohoto člověka. Zároveň však občanský zákoník upravuje několik výjimek z tohoto požadavku nezbytného získání svolení k zachycení a použití podoby člověka.

Předně se jedná o případy rozmnožování a rozšiřování podoby člověka, který poskytl souhlas k zobrazení své podoby. Ustanovení § 85 odst. 2 občanského zákoníku obsahuje nevyvratitelnou domněnku o existenci svolení (též) k rozmnožování a rozšiřování podoby v souvislosti s (prvotním) zachycením podoby člověka, to však jen tehdy, pokud jsou naplněny všechny podmínky daného ustanovení[12] – tj. kritérium obvyklosti rozmnožování a rozšiřování ve vztahu k účelu pořízení podoby člověka, které je nutné posuzovat vždy podle konkrétních okolností a za předpokladu, že člověk při udělení svolení k zobrazení své podoby mohl vzhledem k okolnostem rozumně předpokládat, že toto zobrazení bude dále šířeno.[13] Závěr o tom, zda v konkrétním případě lze tuto zákonnou nevyvratitelnou domněnku aplikovat, bude tedy vždy nutné učinit na základě konkrétních okolností případu.

Další výjimku představují tzv. bezúplatné zákonné licence, a to bezúplatná zákonná licence úřední (§ 88 občanského zákoníku) a bezúplatná zákonná licence vědecká, umělecká a zpravodajská (§ 89 občanského zákoníku). Úprava zákonná licence představuje zákonné omezení výkonu absolutního osobnostního práva člověka na ochranu projevů osobní povahy, resp. zákonný důvod, na jehož základě je legitimizován zásah do osobnostního práva, a to za účelem dosažení obecného zájmu, pokud tento obecný zájem převažuje nad zájmem jednotlivce.

Zákonná úřední licence je v občanském zákoníku upravena tradičně z důvodu veřejného zájmu na zajištění veřejného pořádku v úředních věcech (§ 88 odst. 2 občanského zákoníku); výslovně zahrnuje také veřejné vystoupení v záležitosti veřejného zájmu, je-li dán úřední účel takového vystoupení založený zákonem. Z tohoto titulu je možné pořídit nebo použít podobiznu, písemnost osobní povahy nebo zvukový či obrazový záznam člověka. Zákonná úřední licence se dále vztahuje také na zajištění výkonu a ochrany jiných subjektivních soukromých práv (ovšem jen) některou z přípustných forem soudního, správního či jiného úředního procesu (§ 88 odst. 1 občanského zákoníku), přičemž oprávnění plynoucí z této licence se týká pořízení či použití podobizny nebo zvukového či obrazového záznamu (netýká se tedy písemností osobní povahy).

Použití zpravodajská licence je podrobněji popsáno v rámci kapitoly 3.2.5 Vydávání obecních novin – zpravodajská licence.

Shromažďování informací o společenských, sportovních nebo kulturních událostech pořádaných v obci a dokumentace těchto událostí prostřednictvím audiovizuálních nebo pouze vizuálních záznamů

[11] Na principu ochrany základních práv a lidských svobod je založeno též znění GDPR, které v úvodním recitálu 1 deklaruje, že právo na ochranu osobních údajů je základním právem každé fyzické osoby ve smyslu čl. 8 odst. 1 Listiny základních práv Evropské unie a čl. 16 odst. 1 Smlouvy o fungování Evropské unie. Znění recitálu 2 GDPR dále zdůrazňuje, že zásady a pravidla ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů by bez ohledu na jejich státní příslušnost nebo bydliště měly respektovat jejich základní práva a svobody, zejména právo na ochranu osobních údajů.

[12] § 85 odst. 2 občanského zákoníku: „*Svolí-li někdo k zobrazení své podoby* ***za okolností, z nichž je zřejmé, že bude šířeno****, platí, že svoluje i k jeho rozmnožování a rozšiřování* ***obvyklým způsobem****, jak je mohl vzhledem k okolnostem* ***rozumně předpokládat****.*"

[13] Srov. Občanský zákoník I. Obecná část (§ 1−654), 1. vydání, 2014, s. 506 - 508.

se považuje za zpracování osobních údajů za předpokladu, že tyto informace obsahují osobní údaje subjektů údajů. Typicky se tak jedná např. o fotografie, které zachycují podobizny jednotlivých fyzických osob, které se účastní akce pořádané v obci; naopak pořizování fotografií, které zachycují pouze průběh akce, ale nikoli podobizny jednotlivých fyzických osob, které nebudou ani jiným způsobem ztotožněny (např. uvedením jména), se za zpracování osobních údajů nepovažuje.[14]

Pro každé zpracování osobních údajů musí být stanoven zejména právní důvod, na jehož základě mohou být osobní údaje zpracovávány. V případě pořizování fotografií z jednotlivých akcí pořádaných v obci nelze tento právní důvod stanovit paušálně pro všechny možné v úvahu připadající situace. Ačkoli občanský zákoník je primárně založen na požadavku nezbytného udělení souhlasu subjektu údajů s pořízením fotografie jeho osoby, tento požadavek je „prolomen“ v případě výkonu bezúplatné zákonné licence (úřední či vědecké, umělecké a zpravodajské), kdy se svolení dotčené fyzické osoby nevyžaduje. Důležitým aspektem tohoto vyhodnocení bude též účel zpracování, resp. posouzení, zda konkrétního účelu nemůže být dosaženo i jinak.[15]

Za předpokladu, že na základě vyhodnocení konkrétní situace dospěje správce k závěru, že právním důvodem pro zpracování osobních údajů může být pouze souhlas subjektů údajů dle čl. 6 odst. 1 písm. a) GDPR, je nutné pro účely řádného získání souhlasu naplnit požadavky GDPR.

GDPR v čl. 4 odst. 11 definuje souhlas jako „*svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů*“. Souhlas dotčené osoby tedy nemusí být nezbytně písemný a ani (s ohledem na okolnosti konkrétního případu) výslovný. GDPR tedy obecně připouští možnost udělení tzv. konkludentního souhlasu.

V případě konkludentního souhlasu je k třeba klást vyšší nároky zejména na informovanost směrem k subjektům údajů, a to zejména ve vztahu k možnému vyjádření nesouhlasu s pořizováním fotografie. Subjekty údajů musí mít k dispozici ještě před udělením (konkludentního) souhlasu alespoň tyto informace:[16]

- Totožnost správce a jeho kontaktní údaje.
- Účel zpracování, pro který je žádáno o souhlas:
  - tedy proč budou osobní údaje zpracovávány a s jakým cílem,
  - pokud by měly být fotografie též uveřejněny, musí mít subjekty údajů informaci také o tom, kde a jakým způsobem budou fotografie uveřejněny.
- Jaké osobní údaje (druhy údajů) budou shromažďovány a používány:
  - např. zda bude pořizována pouze fotografie nebo zároveň budou k fotografii přiřazovány údaje jako jméno a příjmení dotčených osob apod.
- Existence práva odmítnout udělit souhlas s fotografováním a právo následně souhlas odvolat:
  - pro případy následného odvolání souhlasu musí být subjekty údajů zároveň informováni, jakým způsobem tak mohou učinit a kde mohou své právo uplatnit.

Fotografovaná osoba tedy musí být srozumitelným způsobem informována především o výše uvedených skutečnostech. Pouze v případě, že subjekt údajů je dostatečně o takovém zpracování poučen, může řádně posoudit a rozhodnout se, zda s ním bude souhlasit.

Výše uvedené informace musí mít subjekty údajů k dispozici především v místě konání akce (např. formou informačních tabulí). Rozmístění a počet těchto informačních tabulí pak musí odpovídat konkrétním okolnostem, zejména z hlediska typu, rozsahu nebo i umístění konkrétní akce. Např.

[14] Ke zveřejňování osobních údajů žáků na internetu, ÚOOÚ, dostupné z: https://www.uoou.cz/ke-zverejnovani-osobnich-udaju-zaku-na-internetu/d-1589.
[15] Viz recitál 39 GDPR: „Osobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky.“
[16] Pracovní skupina podle článku 29: Vodítka k souhlasu; WP 259 ze dne 28. 11. 2017.

v případě konání akce, na které se předpokládá účast velkého počtu osob, nepostačí umístění jedné informační cedule k hlavnímu vchodu do prostor, kde se má akce konat, informační tabule musejí být rozmístěny i v prostorech, kde se akce koná.

Informační povinnost je vedle rozmístění informačních tabulí vhodné doplnit rovněž např. sdělením v obecních novinách, na plakátech oznamujících konání akce, vyvěšením informace na webových stránkách obce, nebo také ze strany moderátora v průběhu konání akce apod.

Informační povinnost musí alespoň v nezbytné míře plnit také fotograf akce, a to jednak prostřednictvím viditelného označení, které bude mít na sobě, a dále poskytováním informací alespoň v takovém rozsahu, aby upozornil subjekty údajů na jejich právo odmítnout být fotografován, a v případě, že fotograf shledá, že konkrétní osoba nebyla s výše uvedenými informacemi např. skrze informační tabuli seznámena, tyto informace jim sdělit.

Zvláštní zřetel je nutné brát na děti, které GDPR považuje za zranitelné subjekty údajů. K pořizování fotografií dětí je nezbytný souhlas jejich zákonných zástupců.

Výše uvedenou informační povinností, kterou je nezbytné splnit ještě před udělením (konkludentního) souhlasu ze strany subjektu údajů, není dotčeno plnění informační povinnosti ze strany správce dle čl. 13 nebo 14 GDPR.

DOPORUČENÍ:

Stanovení právního titulu pro účely pořizování fotografií na akcích pořádaných v obci je nutné posoudit vždy v rámci konkrétního případu dle konkrétních okolností. Pokud správce dospěje k závěru, že zpracování osobních údajů je možné pouze se souhlasem subjektů údajů, souhlas může být udělen též konkludentně. Tento způsob získání souhlasu však klade vysoké nároky na splnění informační povinnosti vůči subjektům údajů ještě před zahájením zpracování osobních údajů, tedy před tím, než budou pořízeny fotografie subjektů údajů. Správce musí rovněž po celou dobu zpracování souhlasy evidovat, aby byl schopen udělení souhlasu kdykoliv doložit (v případě konkludentního souhlasu např. dokumentací obsahu a umístění informačních tabulí).

3.2.4 Uveřejňování informací a fotografií pořízených na akcích uskutečněných v obci na webových stránkách obce

Shromažďování informací o společenských, sportovních nebo kulturních událostech pořádaných v obci a dokumentace těchto událostí prostřednictvím audiovizuálních nebo pouze vizuálních záznamů se považuje za zpracování osobních údajů za předpokladu, že tyto informace obsahují osobní údaje subjektů údajů. Typicky se tak jedná např. o fotografie, které zachycují podobizny jednotlivých fyzických osob, které se účastní akce pořádané v obci; naopak pořizování fotografií, které zachycují pouze průběh akce, ale nikoli podobizny jednotlivých fyzických osob, které nebudou ani jiným způsobem ztotožněny (např. uvedením jména), se za zpracování osobních údajů nepovažuje.[17]

Pro účely takového shromažďování osobních údajů musí mít správce stanoven právní důvod pro zpracování osobních údajů (čl. 6 GDPR). Např. ustanovení § 36a zákona o obcích výslovně stanovuje, že obec může ocenit významné životní události svých občanů, přičemž za tímto účelem může obec získávat z evidence obyvatel osobní údaje jubilantů ve smyslu ust. § 4 odst. 2 a § 5 odst. 3 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů. V případě adresného blahopřání jubilantům nebo pozvání na vítání občánků jsou těmito nezbytnými údaji: jméno a příjmení, datum narození, a adresa

[17] Ke zveřejňování osobních údajů žáků na internetu, ÚOOÚ, dostupné z: https://www.uoou.cz/ke-zverejnovani-osobnich-udaju-zaku-na-internetu/d-1589.

místa trvalého pobytu jubilantů, novorozenců a jejich právních zástupců.[18] V tomto případě je tedy právním důvodem pro zpracování osobních údajů plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci (čl. 6 odst. 1 písm. e) GDPR). Z výčtu nezbytného rozsahu osobních údajů je patrné, že v něm není uvedena fotografie subjektů údajů. Pro pořízení fotografie tak bude nezbytný souhlas subjektu údajů dle čl. 6 odst. 1 písm. a) GDPR (viz *Pořizování fotografií pro obec na akcích v obci – konkludentní souhlas*).

Existence právního důvodu pro výše uvedený účel však automaticky neznamená, že na základě téhož právního důvodu je také možné shromážděné osobní údaje uveřejňovat na internetu. Za účelem uveřejnění osobních údajů na internetu obec potřebuje samostatný právní důvod. Tímto právním důvodem v případě uveřejnění osobních údajů jubilantů na webových stránkách obce je souhlas subjektů údajů dle čl. 6 odst. 1 písm. a) GDPR, jímž může být též konkludentní souhlas, budou-li splněny potřebné podmínky (viz *Pořizování fotografií pro obec na akcích v obci – konkludentní souhlas*).

Případy, kdy jsou osobní údaje zpracovávány v souladu s tzv. zpravodajskou licencí, viz *Uveřejňování osobních údajů v obecních novinách*.

Výše uvedené platí nejen pro činnosti vykonávané obcí po nabytí účinnosti GDPR, ale v souladu s GDPR budou muset být rovněž postupy správců, které byly provedeny před nabytím účinnosti GDPR.

Zvláštní zřetel je nutné brát na děti, které GDPR považuje za zranitelné subjekty údajů. Ke zpracování osobních údajů dětí je nezbytný souhlas jejich zákonných zástupců.

DOPORUČENÍ:

Obec při uveřejňování informací na internetu o akcích pořádaných v obci smí uvést osobní údaje subjektů údajů (typicky fotografie občanů obce z jednotlivých akcí) pouze s jejich souhlasem, a to i v případě udělení konkludentního *souhlasu (viz Pořizování fotografií pro obec na akcích v obci – konkludentní souhlas).* Dalším důvodem pro uveřejňování osobních údajů může být výkon tzv. zpravodajské licence *(viz Uveřejňování osobních údajů v obecních novinách).*

3.2.5 Vydávání obecních novin – zpravodajská licence

Vydávání obecních novin je možné považovat za výkon tzv. zpravodajské licence ve smyslu ust. § 89 občanského zákoníku za předpokladu, že vydávání obecních novin lze považovat za výkon zpravodajství. Zpravodajství přitom spočívá v činnosti, při níž je referováno o skutečnostech reálného světa, která je zaměřena na události politického, resp. společenského života a která slouží k „*informování veřejnosti o věcech oprávněného veřejného nebo obecného zájmu, a to zpravidla v mezích výkonu ústavního práva na poskytování a šíření informací*“[19].

O výkon zpravodajské licence se tak bude jednat především v případě vydávání periodického tisku územního samosprávného celku dle zákona č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), ve znění pozdějších předpisů (dále jen „tiskový zákon“). Periodickým tiskem územního samosprávného celku se dle ust. § 3 písm. g) tiskového zákona rozumí periodický tisk, jehož vydavatelem je obec, kraj nebo hlavní město Praha nebo jeho městská část (dále jen „územní samosprávný celek“) nebo právnická osoba zřízená či založená územním samosprávným celkem či společně více územními samosprávnými celky nebo

[18] K blahopřání jubilantům obcemi, ÚOOÚ, dostupné z: https://www.uoou.cz/k-nbsp-blahoprani-jubilantum-obcemi/d-20337.
[19] Lavický, P. a kol.: Občanský zákoník I. Obecná část (§ 1−654). Komentář. 1. vydání, Praha: C. H. Beck, 2014, 2400 s.

právnická osoba, kterou územní samosprávný celek sám nebo spolu s dalšími územními samosprávnými celky ovládá podle zvláštního právního předpisu, anebo periodický tisk, jehož obsah, vydání a veřejné šíření zajišťuje jiný vydavatel na základě smlouvy s územním samosprávným celkem či společně s více územními samosprávnými celky.

Zpracování osobních údajů subjektů údajů při výkonu zpravodajské licence lze považovat za plnění úkolu prováděného ve veřejném zájmu (čl. 6 odst. 1 písm. e) GDPR). Zpracovávat osobní údaje je však možné jen v nezbytném rozsahu. Obdobně též občanský zákoník v ust. § 89 připouští zpracování osobních údajů pouze přiměřeným způsobem, který je nutné posuzovat podle konkrétních okolností, zejména s přihlédnutím k formě, obsahu i rozsahu užití, a to pokud jde o podobiznu nebo zvukový či obrazový záznam týkající se fyzické osoby.

Např. v případě oceňování významných životních událostí Úřad pro ochranu osobních údajů považuje za přípustné v rámci místního tisku uveřejnit v určitém měsíci jména a příjmení jubilantů, jde-li o významná životní jubilea (to však neplatí pro každoroční uveřejňování jmen a příjmení v měsíci narození), a to i bez souhlasu těchto dotčených subjektů údajů. Uveřejnění jakéhokoli jiného osobního údaje, včetně podobizny konkrétní fyzické osoby, je však nutné učinit pouze se souhlasem subjektu údajů.[20] Naopak za přijatelné lze považovat, pokud budou uveřejněny fotografie zachycující pouze samotný průběh akce, ale nikoli podobizny jednotlivých fyzických osob, které nebudou ani jiným způsobem ztotožněny (např. uvedením jména).

DOPORUČENÍ:

Obec smí v rámci výkonu tzv. zpravodajské licence zpracovávat osobní údaje, zejména podobizny nebo zvukový či obrazový záznam týkající se fyzické osoby, i bez souhlasu subjektů údajů, vždy však pouze v rozsahu, který bude nezbytný, a vždy přiměřeným způsobem. V souladu s tímto postupem není uveřejnění fotografií novorozenců (nových občánků obce) v obecních novinách. K uveřejnění může dojít pouze se souhlasem subjektu údajů, resp. v tomto případě se souhlasem zákonných zástupců.

3.2.6 Vedení vlastních agendových informačních systémů/přístup do agendových informačních systémů vedených jinými orgány veřejné moci

Správcem se rozumí subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Tyto účely a prostředky mohou být též určeny přímo právním řádem.

Zpracovatelem se rozumí subjekt, který zpracovává osobní údaje pro správce. Zpracovatel tedy neurčuje účely ani prostředky zpracování osobních údajů.

V případě, že obec zpracovává osobní údaje ve vlastních agendových informačních systémech, zpracovává osobní údaje evidované v těchto informačních systémech v pozici správce.

V případě, že obec je pověřena zpracováním osobních údajů evidovaných v agendových informačních systémech vedených jinými orgány veřejné moci, vystupuje v pozici zpracovatele. Např. správcem evidence cestovních dokladů je dle ust. § 29 odst. 1 zákona č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů, Ministerstvo vnitra. Zpracovatelem údajů v evidenci cestovních dokladů je pro Ministerstvo vnitra orgán příslušný k vydání cestovního dokladu (§ 30 odst. 1 téhož zákona), kterým je v případě vydání cestovního pasu obecní úřad obce s rozšířenou působnosti (§ 12 odst. 1 téhož zákona).

Dle čl. 28 odst. 3 GDPR se zpracování osobních údajů zpracovatelem řídí smlouvou nebo jiným právním aktem, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání

[20] K blahopřání jubilantům obcemi, ÚOOÚ, dostupné z: https://www.uoou.cz/k-nbsp-blahoprani-jubilantum-obcemi/d-20337.

zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce, jakož i další náležitosti uvedené v daném ustanovení. GDPR tedy připouští, aby zpracování zpracovatelem bylo upraveno na základě zpracovatelské smlouvy, nebo aby podmínky zpracování byly stanoveny jiným právním aktem. Tímto jiným právním aktem může být zákon, ale i jiný podzákonný předpis. Podmínkou je, že smlouva či jiný právní akt musí mít písemnou formu, počítaje v to i elektronickou formu (čl. 28 odst. 9 GDPR).

DOPORUČENÍ:

V případě, že obec je jako zpracovatel pověřena zpracováním osobních údajů evidovaných v agendových informačních systémech vedených jiným orgánem veřejné moci – správcem, musí být takové zpracování osobních údajů pro správce upraveno smlouvou či jiným právním aktem, a to v písemné formě. Tímto jiným právním aktem může být zákon či podzákonný předpis. Odpovědnost za řádné zpracování osobních údajů prováděné zpracovatelem je na správci. Primárně by proto správce měl řešit úpravu vztahů se svými zpracovateli, a to prostřednictvím smluv či jiných právních aktů.

3.2.7 Souhlas zaměstnanců jako právní důvod pro zpracování osobních údajů zaměstnavatelem

Souhlas se zpracováním osobních údajů je jedním z právních důvodů, na základě kterého může správce osobní údaje zpracovávat. Souhlas subjektu údajů je jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Aby bylo možné dosáhnout svobodnosti, konkrétnosti, informovanosti a jednoznačnosti projevu vůle subjektu údajů, stanovuje GDPR v čl. 7 podmínky vyjádření souhlasu. Mezi ně patří jasná odlišitelnost souhlasu od jiného textu (např. by tak neměl být součástí smlouvy či všeobecných smluvních podmínek), nepodmíněnost (např. poskytnutí služby nesmí být podmiňováno poskytnutím souhlasu), určitost (souhlas musí být udělen pro „jeden nebo více konkrétních účelů“) a informovanost (subjekt údajů musí být informován o účelu a dalších podrobnostech zpracování předtím, než poskytne souhlas). Subjekt údajů má právo souhlas kdykoliv odvolat, a to stejně snadným způsobem, jakým svůj souhlas poskytl. Pokud je zpracování založeno na souhlasu, musí být správce schopen doložit jeho udělení subjektem údajů.

Podle výkladového stanoviska WP29[21] zaměstnanci nejsou téměř nikdy v postavení, aby mohli dát souhlas svobodně nebo souhlas odmítnout či odvolat, což je dáno závislostí vyplývající ze vztahu zaměstnavatel/zaměstnanec. Vzhledem k nerovnováze sil mohou zaměstnanci udělit svobodný souhlas jen za výjimečných okolností, kdy souhlas nebo odmítnutí nevyvolá žádné následky. Pro většinu zpracování osobních údajů na pracovišti tak nemůže a neměl by být právním důvodem souhlas zaměstnance.

Zpracování osobních údajů zaměstnance může být nezbytné pro plnění smlouvy (např. pracovní smlouvy nebo dohod o pracích konaných mimo pracovní poměr) v případech, kdy zaměstnavatel musí osobní údaje zpracovat, aby takovou povinnost splnil. Nejběžnějším právním důvodem ke zpracování osobních údajů bude splnění právních povinností, které pracovní právo zaměstnavateli ukládá.

Příklady užití souhlasů:

- Zveřejnění fotografií zaměstnance z propagačních či jiných účelů, které nesouvisí s jeho pracovněprávním vztahem, je podmíněno udělením souhlasu se zpracováním osobních údajů.

[21] Pracovní skupina podle článku 29: Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti; WP 249 ze dne 8. 6. 2017.

- Pro monitorování služebních vozidel zaměstnavatel jako správce nepotřebuje od zaměstnance souhlas se zpracováním osobních údajů, neboť zpracování provádí na základě plnění právní povinnosti (vedení knihy jízd pro daňové účely). Pokud však má zaměstnavatel v úmyslu využívat GPS i pro případ soukromých jízd svých zaměstnanců, je nutné získat od zaměstnance pro tyto účely jejich souhlas.

DOPORUČENÍ:

Vzhledem k nepoměru postavení mezi zaměstnavatelem a zaměstnancem lze doporučit se zpracování osobních údajů na základě udělení souhlasu zaměstnance spíše vyvarovat. Udělený souhlas lze považovat za svobodný jen za výjimečných podmínek, kdy udělení nebo odmítnutí souhlasu nebude mít pro zaměstnance nežádoucí účinek. V souvislosti s výše uvedenými příklady se tak např. jedná o situaci, kdy je používání vozidla pro soukromé účely benefitem – pokud zaměstnanec odmítne souhlas se sledováním soukromých jízd, ztratí možnost využívat vozidla nad rámec pracovního vztahu (nikoliv však v jeho rámci).

Správce by měl dále vzít v úvahu při rozhodování, zda zpracování osobních údajů provádět na základě poskytnutého souhlasu, několik skutečností, zejména že subjekt údajů souhlas může kdykoliv odvolat a správce pak musí ukončit další zpracování, což nemusí být vždy snadno technicky proveditelné. Dále je nutné v případě, kdy je zpracování založeno na souhlasu, souhlasy po celou dobu zpracování evidovat.

3.2.8 Doba uchovávání kamerových záznamů

Osobní údaje smí být uloženy pouze po dobu, která je nezbytná pro účely, pro které jsou osobní údaje zpracovávány. Jedná se o projev zásady omezení uložení ve smyslu čl. 5 odst. 1 písm. e) GDPR. Doba, po kterou jsou osobní údaje uchovávány, tedy musí být omezena na nezbytné minimum, a to z hlediska účelu zpracování osobních údajů.

Úřad pro ochranu osobních údajů se k době uchování záznamů z kamerového systému vyjádřil tak, že doba uchovávání by neměla přesáhnout limit přípustný pro naplnění účelu provozování kamerového systému. V případě trvale střeženého objektu by dle Úřadu pro ochranu osobních údajů měla být data uchovávána v rámci časové smyčky např. 24 hodin, případně po delší dobu, v zásadě ne však po dobu přesahující několik dnů.[22] Tato doba by neměla přesáhnout dobu potřebnou k tomu, aby zaznamenaný incident bylo možné dále prošetřit a zajistit další nezbytné informace, a to např. za účelem zpřístupnění záznamů orgánům činným v trestním řízení, soudu nebo pojišťovně. K tomuto účelu by dle Úřadu pro ochranu osobních údajů měla postačovat lhůta 7 dnů.[23] Obdobně se vyjádřila též pracovní skupina WP29, dle níž je nutné vždy řádně posoudit otázku přiměřenosti, kdykoli se považuje za nezbytné uchovat záznam po delší dobu, jež by však neměla přesahovat jeden týden.[24] Delší dobu uchování kamerových záznamů bude nutné vždy řádně odůvodnit.

DOPORUČENÍ:

Záznamy z kamerových systémů je možné uchovávat pouze po dobu nezbytnou pro účely, pro které jsou osobní údaje zpracovávány. Takovou dobu je nutné počítat v řádu několika dní, s tím, že pro účely možného prošetření zaznamenaného incidentu (např. za účelem zpřístupnění záznamů orgánům činným v trestním řízení) by dle Úřadu pro ochranu osobních

[22] Provozování kamerového systému z hlediska zákona o ochraně osobních údajů, ÚOOÚ, dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22294.
[23] Umístění kamerových systémů v bytových domech, ÚOOÚ, dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22428.
[24] Stanovisko č. 4/2004 ke zpracování osobních údajů prostředky kamerového sledování, WP29, dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22427.

údajů měla postačovat lhůta 7 dnů. Bude tedy nutné revidovat vnitřní postupy na straně správců osobních údajů tak, aby doba uchování záznamů z kamerových systémů odpovídala výkladové praxi.

3.2.9 Kdo může a nemůže být pověřenec pro ochranu osobních údajů

Ve smyslu čl. 37 odst. 5 GDPR musí být pověřenec jmenován na základě svých profesních kvalit, zejména na základě odborných znalostí práva a praxe v oblasti ochrany osobních údajů, a na základě své schopnosti plnit úkoly stanovené v čl. 39 GDPR. GDPR nijak neupravuje konkrétní náležitosti profesních kvalit (např. požadavky na vzdělání či certifikaci). Pověřenec by měl mít dostatečnou znalost interní struktury obce, postupů uplatňovaných při činnosti obce, prováděných operací zpracování, stejně jako informačních systémů[25], řízení procesů[26], bezpečnosti dat (jak znalost kybernetické bezpečnosti, tak ale i bezpečnosti dat v analogické podobě).

Pověřenec se nesmí dostat do střetu zájmů. WP29 ve svém výkladovém stanovisku[27] dovozuje, že **pověřenec nemůže zastávat pozici, na které by stanovoval účely nebo prostředky zpracování osobních údajů.** Osoby ve střetu zájmů budou ty, které se podílejí jak na koncipování, tak realizaci projektů zahrnujících činnosti v souvislosti se zpracováním osobních údajů.

Typické pozice ve střetu zájmů budou např.:

- tajemník obecního úřadu,
- ředitel finančního odboru,
- vedoucí IT oddělení apod.

Pověřenec může být zaměstnancem obce, nebo může jednotlivé úkoly plnit na základě smlouvy o poskytování služeb[28].

Externí zajišťování plnění povinností pověřence může poskytovat také právnická osoba, vždy však prostřednictvím konkrétní fyzické osoby fakticky vykonávající úlohu pověřence, která musí splňovat stanovené požadavky.

GDPR umožňuje, aby pro několik orgánů veřejné moci či veřejných subjektů byl jmenován jediný pověřenec.[29] V takovém případě však musí být zohledněna organizační struktura a velikost jednotlivých obcí, neboť každý správce nebo zpracovatel je odpovědný za zajištění, že tento jediný pověřenec bude vůči němu plnit své úkoly efektivně, přestože byl pověřenec jmenován pro několik subjektů najednou.

Úkoly pověřence:

- Monitoruje soulad zpracování osobních údajů s GDPR a dalšími relevantními právními předpisy.
- Zajišťuje udržování povědomí osob pracujících s osobními údaji o správném způsobu zpracování osobních údajů. Monitoruje, zda všechny osoby, které jsou zapojeny do operací souvisejících se zpracováním osobních údajů, jsou náležitě proškolovány v oblasti ochrany osobních údajů.

[25] Viz např. normy řady ISO 27000.
[26] Viz např. normy řady ISO 9000.
[27] Pracovní skupina podle článku 29: Vodítka k pověřencům pro ochranu osobních údajů, WP 243 rev. 01 ze dne 5. 4. 2017.
[28] Půjde o nepojmenovanou soukromoprávní smlouvu mezi správcem, případně několika správci, a pověřencem ve smyslu ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.
[29] Viz čl. 37 odst. 3 GDPR

- Poskytuje poradenství v oblasti zpracování osobních údajů, pomáhá posuzovat dopady zpracování na ochranu osobních údajů. Na vyžádání správce vyhotoví posudek na posouzení vlivu na ochranu osobních údajů dle čl. 35 odst. 2 GDPR.
- Je kontaktním místem pro subjekty údajů a dozorový úřad.
- Spolupracuje s dozorovým úřadem.

Činnosti, které pověřenec nesmí vykonávat:

- Nesmí se podílet na stanovování účelů nebo prostředků zpracování osobních údajů, tedy na výkonných činnostech v rámci obce.

DOPORUČENÍ:

Pověřenec musí být nezávislý na řídících funkcích obce. Doporučujeme ustanovit pověřence jako nezávislého kontrolora ochrany osobních údajů, který bude provádět kontrolu postupů obce ve věcech ochrany osobních údajů a bude zajišťovat roli konzultanta a poradce, přičemž tyto kompetence budou striktně odděleny od výkonných činností obce.

3.2.10 Podřízené organizace a povinnost jmenovat pověřence pro ochranu osobních údajů

Případná povinnost jmenovat pověřence se vztahuje pouze na ty podřízené organizace, které mají právní subjektivitu a nejsou přímo organizačními složkami obce. V případě podřízených organizací, jakožto organizačních složek obce bez právní subjektivity, se bude povinnost jmenovat pověřence vztahovat přímo na obec, jako orgán veřejné moci.

3.2.10.1 Školy a školská zařízení

Školy a školská zařízení budou mít povinnost jmenovat pověřence dle čl. 37 odst. 1 písm. a) GDPR.

Dle *Metodické pomůcky k aplikaci GDPR a zákona o zpracování osobních údajů v podmínkách školství* vypracované Ministerstvem školství[30] a rovněž dle *Metodického doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí* vypracovaného Ministerstvem vnitra[31], lze školy a školská zařízení označit za orgány veřejné moci ve smyslu GDPR, neboť v jistých situacích mají pravomoc rozhodovat o právech a povinnostech fyzických osob.

DOPORUČENÍ:

Školy a školská zařízení mají povinnost jmenovat pověřence dle čl. 37 odst. 1 písm. a) GDPR.

3.2.10.2 Poskytovatelé zdravotních služeb

Pokud bude takovouto podřízenou organizací nemocnice nebo poskytovatel zdravotnické záchranné služby, kde je zpracováváno rozsáhlé množství zvláštních kategorií osobních údajů, tedy zejména údaje o zdravotním stavu, genetické údaje, údaje o sexuálním životě či sexuální orientaci, budou tito poskytovatelé zdravotních služeb povinni jmenovat pověřence dle čl. 37 odst. 1 písm. c) GDPR.

[30] Metodická pomůcka k aplikaci GDPR a zákona o zpracování osobních údajů v podmínkách školství http://www.msmt.cz/file/44569/

[31] Viz http://www.mvcr.cz/sluzba/clanek/ministerstvo-vnitra-zverejnuje-metodicke-doporuceni-k-problematice-poverencu-pro-ochranu-osobnich-udaju.aspx

Při určování pojmu rozsáhlosti doporučuje výkladové stanovisko WP29[32] vzít v úvahu počet dotčených subjektů údajů, objem dat a rozsah různých datových položek, dobu trvání nebo nepřetržitost zpracování a územní rozsah zpracování.

Jako příklad zpracování, která jsou rozsáhlá uvádí výkladové stanovisko WP29 zpracování údajů o pacientech v rámci běžné činnosti nemocnice, naproti tomu jako zpracování, které není rozsáhlé, označuje zpracování údajů o pacientech jednotlivým lékařem.

DOPORUČENÍ:
Poskytovatelé zdravotních služeb, kteří provádějí rozsáhlé zpracování zvláštních kategorií údajů pacientů, mají povinnost jmenovat pověřence dle čl. 37 odst. 1 písm. c) GDPR.

3.2.10.3 Poskytovatelé sociálních služeb

Vzhledem k různorodosti poskytovatelů sociálních služeb, nelze obecně říci, zda všechny podřízené organizace v oblasti sociálních služeb budou povinny jmenovat pověřence. Bude nutné vždy posuzovat případ od případu, zda tyto organizace naplňují podmínky stanovené v čl. 37 odst. 1 GDPR. V případě, že poskytovatelé sociálních služeb provádějí rozsáhlé zpracování zvláštních kategorií osobních údajů (např. údaje o zdravotním stavu klientů), budou povinni jmenovat pověřence dle čl. 37 odst. 1 písm. c) GDPR – lze předpokládat, že se bude jednat např. o domovy pro osoby s chronickým duševním onemocněním nebo se závislostí na návykových látkách, domovy pro osoby se zdravotním postižením, domovy pro seniory.

V případě intervenčních center pracujících s odsouzenými osobami a v případě různých podobných prevenčních center, která zpracovávají ve velkém rozsahu údaje týkající se rozsudků v trestních věcech a trestných činů, lze rovněž předpokládat, že zde bude povinnost jmenovat pověřence dle čl. 37 odst. 1 písm. c) GDPR.

DOPORUČENÍ:

V případě poskytovatelů sociálních služeb bude vždy potřeba jednotlivě zhodnotit, zda je naplněna alespoň jedna z podmínek povinného jmenování pověřence ve smyslu čl. 37 odst. 1 GDPR.

3.2.10.4 Kulturní zařízení

Kulturní zařízení nelze považovat za orgány veřejné moci nebo veřejné subjekty ve smyslu čl. 37 odst. 1 písm. a) GDPR, a lze předpokládat, že neprovádějí rozsáhlé zpracování zvláštních kategorií osobních údajů nebo údajů o trestné činnosti subjektů údajů ani neprovádějí rozsáhlé pravidelné a systematické monitorování subjektů údajů, proto se na tyto instituce nebude vztahovat povinnost jmenovat pověřence.

Ministerstvo vnitra v důvodové zprávě k návrhu zákona o zpracování osobních údajů výslovně uvádí, že v příspěvkových organizacích s běžným rozsahem zpracování údajů, jako jsou například divadla a knihovny, nemá zřízení pověřence žádnou přidanou hodnotu a bylo by pouze zbytečnou administrativní zátěží.

DOPORUČENÍ:

Lze předpokládat, že na kulturní zařízení se nebude vztahovat povinnost jmenovat pověřence.

[32] Vodítka k pověřencům pro ochranu osobních údajů č. WP 243 rev. 01, ze dne 5. 4. 2017 vypracovaná Pracovní skupinou podle článku 29 (https://www.uoou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju/d-21750)

3.2.10.5 Oblast dopravní obslužnosti

Jak podle výkladového stanoviska WP29, tak podle důvodové zprávy k návrhu zákona o zpracování osobních údajů nelze subjekty zřizované obcí k výkonu činností v oblasti dopravní obslužnosti označit za orgány veřejné moci nebo za veřejné subjekty. V této oblasti tedy není jmenování pověřence povinné za předpokladu, že nebudou naplněny další podmínky ve smyslu čl. 37 odst. 1 písm. b) nebo c) GDPR, zejména pokud jde o rozsáhlé pravidelné a systematické monitorování subjektů údajů. Tuto podmínku budou s největší pravděpodobností splňovat provozovatelé městské hromadné dopravy, kteří provádí evidenci cestujících[33].

DOPORUČENÍ:

V oblasti dopravní obslužnosti bude potřeba vždy případ od případu zkoumat, zda je naplněna některá z podmínek ve smyslu čl. 37 odst. 1 GDPR, zejména pokud jde o rozsáhlé pravidelné a systematické monitorování subjektů údajů. Např. provozovatelé městské hromadné dopravy, kteří provádí evidenci cestujících, budou povinni pověřence jmenovat, pokud tento druh zpracování osobních údajů provádí ve velkém rozsahu.

3.2.10.6 Správa lesů, technické služby, správa bytového fondu

Jak podle výkladového stanoviska WP29, tak podle důvodové zprávy k návrhu zákona o zpracování osobních údajů nelze subjekty zřizované obcí k výkonu těchto činností označit za orgány veřejné moci nebo za veřejné subjekty. V těchto oblastech tedy není jmenování pověřence povinné za předpokladu, že nebudou naplněny další podmínky ve smyslu čl. 37 odst. 1 GDPR, zejména pokud jde o rozsáhlé pravidelné a systematické monitorování subjektů údajů.

DOPORUČENÍ:

V těchto oblastech činností bude potřeba vždy případ od případu zkoumat, zda je naplněna některá z podmínek ve smyslu čl. 37 odst. 1 GDPR, zejména pokud jde o rozsáhlé pravidelné a systematické monitorování subjektů údajů.

3.2.11 Zpracovatelská smlouva a její atributy

Správce může ke zpracování osobních údajů přibrat externí subjekt, který pro něj bude osobní údaje jakýmkoliv způsobem zpracovávat. Typicky se jedná o situaci, kdy externí subjekt správci poskytuje služby v souvislosti s elektronickým systémem. V takovém případě je tento externí subjekt zpracovatelem a je nutné, aby dostál požadavkům čl. 28 GDPR.

Mezi správcem a zpracovatelem musí být uzavřena písemná smlouva (považuje se za ni i jiný právní akt), v níž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce a dále povinnost, aby zpracovatel zejména:

- zpracovával osobní údaje pouze na základě doložených pokynů správce;
- zajistil, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
- přijal všechna opatření požadovaná podle čl. 32 GDPR;
- dodržoval podmínky pro zapojení dalšího zpracovatele;

[33] Viz Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí ze dne 10. 8. 2017, dostupné na: http://www.mvcr.cz/sluzba/clanek/ministerstvo-vnitra-zverejnuje-metodicke-doporuceni-k-problematice-poverencu-pro-ochranu-osobnich-udaju.aspx

- zohledňoval povahu zpracování a byl správci nápomocen, jde-li o žádosti subjektu údajů, jehož osobní údaje jsou zpracovávány;
- byl správci nápomocen při zajišťování souladu s povinnostmi vyplývajícími z čl. 32 až 36 GDPR;
- v souladu s rozhodnutím správce osobní údaje vymazal nebo vrátil správci (a zničil existující kopie);
- poskytoval správci informace potřebné k doložení toho, že byly splněny příslušné povinnosti;
- umožnil správci provádět audity či inspekce.

DOPORUČENÍ:

Vzhledem k tomu, že správce je vůči subjektu údajů nadále odpovědný i v případě, kdy zpracováním pověří externí subjekt, je v zájmu správce věnovat výběru zpracovatele a sjednání podmínek s ním náležitou pozornost a zapojit do zpracování pouze takového zpracovatele, který je schopen zajistit dostatečnou ochranu práv subjektu údajů v souvislosti se zpracováním osobních údajů. Není nutné, aby mezi správcem a zpracovatelem byla uzavřena samostatná smlouva, náležitosti požadované GDPR lze zakomponovat i do jiné smlouvy, kterou správce se zpracovatelem uzavírá v rámci např. obchodního či jiného vztahu. Co se stávajících smluv týče, nejsou-li v souladu s GDPR, bude nutné je včas revidovat (např. uzavřít dodatek).

3.2.12 Kdy se jedná o zpracování osobních údajů pro správce ze strany zpracovatele

Podle článku 4 GDPR je zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Na rozdíl od správce zpracovatel neurčuje účely a prostředky zpracování osobních údajů. Zpracovatel zpracovává osobní údaje pro správce na základě pověření (správce rozhodne o zapojení zpracovatele sám) či na základě zákona (zapojení zpracovatele stanovuje právní předpis).

V případě, že se správce rozhodne sám o zapojení zpracovatele, je povinen s ním uzavřít písemnou smlouvu, která bude splňovat náležitosti dle čl. 28 GDPR. Správce může na zpracovatele přenést jak pouze část jím prováděného zpracování osobních údajů, např. svěřit mu vedení mzdové agendy nebo získávání nových klientů a jejich údajů, tak více částí zpracování (např. shromažďování, třídění a předávání osobních údajů dle pokynů a potřeb správce) nebo i zpracování celé, pokud se mu to jeví hospodářsky i jinak výhodné.

Zpracovatelem nemůže být zaměstnanec správce ani jeho vnitřní útvar, ale vždy odlišná osoba. Zpracovatelem tak nebude např. oddělení marketingu správce, nicméně pokud bude marketing zajišťován externím subjektem, o zpracovatele se již jednat bude. Mezi další typické příklady zpracovatelů patří externí mzdové účetní, které namísto správce zpracovávají osobní údaje zaměstnanců v souvislosti se mzdovou agendou. Dále např. dodavatel IT řešení, pokud toto bude sloužit ke zpracovatelským operacím s osobními údaji nebo bezpečnostní agentura obsluhující kamerový systém správce určený k ochraně jeho majetku. Zpracováním bude i např. likvidace údajů, resp. nosičů s osobními údaji, pokud je zajišťuje další subjekt jako dodavatel.

DOPORUČENÍ:

Obec musí rozlišovat, kdy při zpracování osobních údajů vystupuje jako správce a kdy jako zpracovatel. V případě, že část nebo celé zpracování osobních údajů pro obec provádí externí subjekt, je nutné, aby v rámci písemné smlouvy s tímto subjektem byl stanoven předmět a doba zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce a další náležitosti dle čl. 28 odst. 3 GDPR.

3.2.13 Uveřejňování dokumentů

Obec při zpracování dokumentů musí dokumenty uveřejňovat na základě různých typů povinností. V případě, že dokumenty obsahují osobní údaje, je potřeba vždy posoudit, zda se povinnost uveřejnění vztahuje též na tyto osobní údaje, které dokument obsahuje, a to z hledisek GDPR i souvisejících právních předpisů. V případě, že obec dospěje k závěru, že osobní údaje uveřejněny být nemohou, je potřeba přijmout odpovídající technické řešení, které umožní uveřejnění dokumentu, aniž by zároveň došlo k uveřejnění osobních údajů (tj. je nutné osobní údaje znečitelnit). Zvolení konkrétního technického prostředku, s přihlédnutím k povaze dokumentu (formátu dokumentu), pak předurčuje to, zda v daném případě lze hovořit o provedené anonymizaci[34] či pseudonymizaci[35] osobních údajů.

DOPORUČENÍ:

Obec by měla od svého dodavatele technického řešení v oblasti anonymizování údajů požadovat informaci, zda poskytnuté řešení spočívá v anonymizaci či pseudonymizaci osobních údajů ve smyslu GDPR, a na základě tohoto zjištění přijmout odpovídající technické a/nebo organizační opatření, které nastaví podmínky provádění tohoto procesu.

Dále uvádíme typické situace spojené s uveřejňováním dokumentů.

3.2.13.1 Registr smluv

Obec je povinna v rámci své činnosti uveřejňovat různé dokumenty, které mohou obsahovat osobní údaje. Takovou povinnost obci například ukládá zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „zákon o registru smluv“). Ve vztahu k osobním údajům je nicméně obec povinna zpracovávat osobní údaje pouze na základě stanoveného legitimního účelu a právního důvodu dle čl. 6 odst. 1 GDPR. Pokud ke zveřejnění osobních údajů v registru smluv žádný zákonný důvod neexistuje, je nezbytné je v daném rozsahu ve smlouvě znečitelnit. Zákonným požadavkem uveřejnění prostřednictvím registru smluv podle zákona o registru smluv je identifikace smluvních stran. Tím je jméno a příjmení a IČO fyzické osoby jako smluvní strany. Další osobní údaje, které smlouva může obsahovat, jdou nad rámec účelu ztotožnění fyzické osoby (např. bydliště, sídlo, identifikační údaje osob jednajících za právnickou osobu, kontaktních osob, e-mail, telefon, číslo účtu, podpis apod.).

DOPORUČENÍ:

V případě uveřejnění smlouvy prostřednictvím registru smluv, je zveřejněný dokument nutné upravit tak, aby mimo výše uvedené identifikační údaje fyzické osoby jako smluvní strany neobsahoval další podrobné informace o smluvní straně či jakékoliv další osobní údaje.

3.2.13.2 Pořizování a zveřejňování obrazových a zvukových záznamů ze zasedání zastupitelstva a zápisů ze zasedaní zastupitelstva

Pořízení, uchovávání a zveřejnění zvukového nebo audiovizuálního záznamu z jednání zastupitelstva obce lze považovat za zpracování osobních údajů tehdy, pokud obsahuje informace týkající se identifikované nebo identifikovatelné fyzické osoby. V takovém případě bude obec v postavení správce osobních údajů.

---

[34] Výstupem anonymizace jsou osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným (srov. recitál 26 GDPR).

[35] Článek 4 odst. 5 GDPR pseudonymizací rozumí *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě*". Osobní údaje, na něž byla uplatněna pseudonymizace a jež by mohly být přiřazeny fyzické osobě na základě dodatečných informací, by měly být považovány za informace o identifikovatelné fyzické osobě (recitál 26 GDPR).

Podle stanoviska Úřadu pro ochranu osobních údajů[36] lze identifikovat dva účely zpracování. Prvním je pořízení záznamu jako podkladu pro pozdější vyhotovení zápisu za zasedání zastupitelstva, druhým účelem je informování veřejnosti o činnosti obce a zastupitelstva, typicky prostřednictvím jeho zveřejnění na internetových stránkách obce.

Jaký však bude mít obec právní důvod ke zpracování osobních údajů osob, které se na záznamech objevují? V případě členů zastupitelstva a dalších úředních osob se v současné době uplatní ust. § 5 odst. 2 písm. f) zákona o ochraně osobních údajů, které umožňuje zpracovávat bez souhlasu osobní údaje veřejně činných osob, funkcionářů či zaměstnanců veřejné správy, pokud vypovídají o jejich veřejné anebo úřední činnosti, o jejich funkčních nebo pracovních zařazeních.

Přestože uvedený právní důvod není obsažen v GDPR, jak vyplývá z návrhu doprovodného zákona k chystanému zákonu o zpracování osobních údajů, měl by být v budoucnu promítnut do novelizovaného zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Podle citovaného stanoviska Úřadu pro ochranu osobních údajů osobní údaje osoby z veřejnosti, která aktivně na jednání zastupitelstva vystoupí k některému z bodů, lze zpracovávat bez jejího souhlasu, neboť takové vystoupení je projevem politického práva konkrétního občana, který již z povahy věci není a nemůže být anonymní. U osob z veřejnosti, které budou přítomny (bez aktivního zapojení), není třeba osobní údaje na záznamu odstranit, pokud budou tyto osoby zachyceny přiměřeným způsobem (např. pouze krátkým záběrem do prostoru pro veřejnost). Naopak možnost uveřejnění se již netýká osobních údajů třetích osob, jejichž záležitosti jsou na záznamu projednávány.

V případě písemných zápisů se pak uplatní stejný přístup.

DOPORUČENÍ:

Obec nesmí v uveřejňovaných zvukových či audiovizuálních záznamech ze zasedání zastupitelstva ani v zápisech ze zasedání zastupitelstva uvádět osobní údaje o třetích osobách, jejichž záležitosti jsou na zastupitelstvu projednávány. Tato povinnost se nevztahuje na osobní údaje členů zastupitelstva či jiných úředních osob a dále ani osobní údaje osob, které se aktivně vyjadřují na zasedání zastupitelstva obce k projednávaným věcem.

3.2.14 Provozování veřejné telekomunikační služby (Wi-Fi) a povinnost provozovatele uchovávat záznamy

Byť z ustanovení § 1 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o elektronických komunikacích“), by šlo dovodit, že předmět úpravy tohoto zákona se týká pouze podmínek podnikání a výkonu státní správy, včetně regulace trhu, v oblasti elektronických komunikací, který dopadá především na činnost podnikatelů a orgánů vykonávajících v dané oblasti státní správu, lze tento zákon aplikovat i na některé činnosti obcí, a to zejména ty spojené s provozováním veřejné telekomunikační služby (Wi-Fi).

Obce mohou ve svých budovách, na svém území zprostředkovávat občanům veřejné telekomunikační služby např. veřejné Wi-Fi připojení na úřadech (obecní, městské, magistráty) a jejich odděleních, odborech, v sídlech příspěvkových organizací, knihovnách, muzeích, sportovištích.

Provozování veřejného Wi-Fi připojení lze ve smyslu ustanovení § 2 písm. o) zákona o elektronických komunikacích chápat jako veřejně dostupnou službu elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen. Z obsahu tohoto ustanovení lze dovodit, že i obce mohou vykonávat

[36] Stanovisko č. 2/2013 Úřadu pro ochranu osobních údajů z června 2013.

komunikační činnost. V průběhu provozování veřejného Wi-Fi připojení dochází ke zpracování osobních údajů subjektů údajů, mezi něž mohou patřit tyto osobní údaje:

- u služby přístupu k internetu z mobilního připojení
  - telefonní číslo uživatele, identifikátor mobilního zařízení, adresa IP a číslo portu, ze kterých bylo připojení uskutečněno;
- u služby přístupu ke schránce elektronické pošty
  - adresa IP a číslo portu, ze kterých bylo připojení uskutečněno, identifikátor uživatelského účtu, identifikátor protokolu elektronické pošty;
- u služby přenosu zpráv elektronické pošty
  - adresa IP a číslo portu zdroje a cíle přenášené zprávy, adresa elektronické pošty odesílatele, adresy elektronické pošty příjemců, identifikátor protokolu elektronické pošty.

Jelikož obce vykonávají jak komunikační činnost, tak zpracovávají osobní údaje, je nutné, aby při zpracování osobních údajů a zejména při jejich archivaci vycházely z dotčených právních předpisů. Doba archivace osobních údajů vyplývá z ustanovení § 97 odst. 3 zákona o elektronických komunikacích, dle kterého se provozní a lokalizační údaje (osobní údaje) uchovávají po dobu 6 měsíců.[37]

DOPORUČENÍ:

Chápeme-li obec jako právnickou osobu zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací v případech, kdy umožňuje veřejné připojení k Wi-Fi, je nutné si uvědomit, že na obec se bude vztahovat i mnoho dalších povinností vyplývající ze zákona o elektronických komunikacích. Lze tedy doporučit, aby obec plnila i ostatní povinnosti ze zákona o elektronických komunikacích vyplývající, např. aby vedla povinnou evidenci o:

- **počtu případů, ve kterých na základě žádosti poskytla provozní a lokalizační údaje orgánům oprávněným k jejich vyžádání,**
- **době, která v jednotlivých případech uplynula ode dne, kdy zahájila uchovávání provozních a lokalizačních údajů do dne, kdy o tyto údaje oprávněný orgán požádal, a**
- **počtu případů, kdy nemohla žádosti o poskytnutí provozních a lokalizačních údajů vyhovět.**

Obec zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna předávat Českému telekomunikačnímu úřadu evidenci uvedenou v předchozím odstavci souhrnně vždy za uplynulý kalendářní rok, a to v elektronické formě, nejpozději do 31. ledna následujícího kalendářního roku. Předávaná evidence nesmí obsahovat osobní a identifikační údaje. Rovněž je vhodné upozornit, že porušení povinností podle ustanovení § 97 zákona o elektronických komunikacích je správním deliktem podle ustanovení § 118 odst. 14 písm. c) téhož zákona s hrozbou sankce až do výše 20 mil. Kč.

3.2.15 Vedení a uveřejňování kronik

Vedení kronik je upraveno v zákoně č. 132/2006 Sb., o kronikách obcí, ve znění pozdějších předpisů (dále jen „zákon o kronikách“). Dle tohoto zákona je každá obec povinna vést kroniku obce, do níž se

[37] Dle ustanovení § 97 odst. 3 zákona o elektronických komunikacích je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací.

zaznamenávají zprávy o důležitých a pamětihodných událostech v obci pro informaci i poučení budoucím generacím.

Kronika je dle ustanovení § 2 zákona o kronikách vedena jako ručně psaná kniha s číslovanými listy nebo v elektronické podobě s následným tiskem číslovaných listů po uzavření každého kalendářního roku na trvanlivém papíře určeném pro dokumenty, které se zajistí vazbou.

Nahlížení do kroniky je dle ustanovení § 4 zákona o kronikách umožněno každému ve vymezené době na obecním úřadě.

DOPORUČENÍ:

S ohledem na obsah zákona o kronikách nelze doporučit zveřejňování obsahu kronik jiným způsobem než v zákoně uvedeným. Kronika musí být vedena jako ručně psaná kniha, nelze tedy její obsah uveřejňovat prostřednictvím webového portálu příslušné obce či jakýmkoliv jiným způsobem umožňujícím dálkový přístup.

3.2.16 Vedení pomocných evidencí

Při činnosti obcí může docházet ke vzniku tzv. pomocných evidencí osobních údajů subjektů údajů, typicky se může jednat např. o situaci, kdy v rámci vyřizování určité agendy sdělí subjekt údajů příslušnému úředníkovi svůj telefon nebo e-mailovou adresu.

Rozhodne-li se úředník obce takový osobní údaj zpracovat, je nutné si uvědomit, že právním důvodem zpracování osobních údajů bude v takovém případě souhlas subjektu údajů ve smyslu článku 6 odst. 1 písm. a) GDPR. Nejedná se o právní důvod zpracování ve smyslu článku 6 odst. 1 písm. c) GDPR – splnění právní povinnosti.

K naznačené situaci může docházet např. při zpracování agend občanských průkazů, cestovních dokladů, řidičských průkazů nebo živnostenských agend (např. vyřizování žádosti o živnostenské oprávnění).

Pokud je zpracování osobních údajů založeno na souhlasu, musí být obce schopny doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů. Toto lze nejlépe doložit písemným souhlasem subjektu údajů se zpracováním osobních údajů.

DOPORUČENÍ:

Obce musí při zpracovávání svých agend rozlišovat, které osobní údaje zpracovávají na základě právního důvodu splnění právní povinnosti nebo právního důvodu splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci a které jim subjekt údajů poskytl na základě souhlasu. Udělil-li subjekt údajů ke zpracování určitých osobních údajů souhlas, mohou obce tyto osobní údaje zpracovat. Dále je rovněž nutné, aby obec i při tomto zpracování splnila informační povinnosti dle čl. 13 GDPR.

3.2.17 Zpracování osobních údajů na základě právního důvodu „veřejný zájem“

Zpracování osobních údajů ve veřejném zájmu je jedním ze zákonných důvodů zpracování osobních údajů uvedených v článku 6 odst. 1 GDPR. Toto zpracování osobních údajů je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce. Tento právní důvod slouží primárně pro zpracování osobních údajů orgány veřejné moci. Orgány veřejné moci budou v naprosté většině případů zpracovávat osobní údaje buď na základě právě tohoto právního důvodu, nebo na základě právního důvodu plnění právní povinnosti uvedeného v článku 6 odst. 1 písm. c) GDPR. Rozdíl mezi těmito dvěma právními důvody spočívá v tom, jak musí být formulován jejich právní základ, tedy ustanovení zvláštního předpisu, který jim ke zpracování dává zmocnění. Právní základ pro použití právního důvodu plnění právní povinnosti musí správci něco

vyloženě přikazovat a ten nesmí mít na výběr, jestli tak učiní nebo ne. **Právní důvod zpracování při plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci se použije v případech, kdy správci právní základ dává určitý úkol ve veřejném zájmu a pro jeho splnění je nutné zpracovávat osobní údaje.** Na rozdíl od právního důvodu plnění právní povinnosti není potřeba, aby správce zpracováním plnil konkrétní právní povinnost.[38]

Příkladem může být kontrolní činnost při zpracování agend živnostenského úřadu (kontrola živnostníků), vodní, lesní stráže nebo vedení disciplinárního řízení. Podle ustanovení § 60 odst. 1, 2 zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, jsou živnostenské úřady oprávněny kontrolovat dodržování povinností při značení lihu a nakládání s lihem podle zákona upravujícího povinné značení lihu, pokud porušení těchto povinností zjistí při výkonu své jiné působnosti, nebo kontrolovat dodržování povinností při značení tabákových výrobků podle zákona upravujícího spotřební daně. Zjistí-li živnostenské úřady, že došlo k porušení povinnosti, sdělí tuto skutečnost bezodkladně správci spotřební daně. Z uvedeného ustanovení lze dovodit, že zákonodárce svěřuje živnostenským úřadům za účelem splnění úkolu ve veřejném zájmu určitou diskreční pravomoc, kterou živnostenské úřady mohou a nemusí využít. Živnostenské úřady jsou tedy oprávněny k výkonu kontrol, nikoliv povinny k jejich provádění. Dojde-li v průběhu kontroly ke zpracování osobních údajů, bude se jednat o zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu.

DOPORUČENÍ:

Obce musí při zpracování svých agend rozlišovat mezi zpracováním osobních údajů z důvodu plnění právní povinnosti a z důvodu plnění veřejného zájmu. Toto rozlišování je důležité provádět zejména z toho důvodu, že správce musí o právním důvodu informovat subjekt údajů, který má v případě, že jsou jeho osobní údaje zpracovávány za účelem plnění veřejného zájmu, možnost proti zpracování vznést námitku (na rozdíl od zpracování za účelem plnění právní povinnosti).

3.2.18 Rozsah osobních údajů stanovený zákonem

GDPR v článku 5 odst. 1 písm. c) stanovuje zásadu minimalizace údajů, tj. povinnost zpracovávat osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány. Při stanovení účelu zpracování osobních údajů je nutné, aby správce vymezil přiměřený, resp. nezbytný rozsah zpracovávaných osobních údajů, které ve vztahu k tomuto účelu minimálně potřebuje.

Rozsah osobních údajů může být v zásadě vymezen dvojím způsobem. Jednak může vyplývat ze zákonné úpravy, která jednoznačně vyjmenovává osobní údaje, nebo (častěji) je rozsah definován rozhodnutím správce, které se odvíjí od jím stanoveného účelu (např. pro zpracování osobních údajů za účelem marketingu jsou nezbytné kontaktní údaje – jméno, příjmení, adresa, e-mail, telefon, ale již ne místo narození).

Zákonem vymezený rozsah osobních údajů se vztahuje především na zpracování osobních údajů orgány veřejné moci, které mohou s ohledem na ústavní principy svého fungování (čl. 2 odst. 2 Listiny základních práv a svobod[39]) a právo každého na informační sebeurčení (čl. 10 odst. 3 Listiny základních práv a svobod) zpracovávat osobní údaje pouze na základě zákona a v zákonem stanoveném rozsahu. Příkladem osobních údajů vymezených zákonem jsou např. údaje vedené

[38] Srov. Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíček, J. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Praha: Wolters Kluwer ČR, 2017. s. 130 – 131.

[39] Čl. 2 odst. 2 Listiny základních práv a svobod: „Státní moc lze uplatňovat jen v případech a v mezích stanovených zákonem, a to způsobem, který zákon stanoví."

o občanech dle ust. § 3 odst. 3 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů, nebo rozsah osobních údajů o žácích ve školní matrice v ust. § 28 odst. 2 a 3 zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání, ve znění pozdějších předpisů. Zásada minimalizace údajů však musí být zachována i v těchto případech, tedy že rozsah osobních údajů stanovený zákonem musí odpovídat účelu daného zpracování.

DOPORUČENÍ:

V případě, že obec zpracovává osobní údaje v rozsahu stanoveném zákonem, tento rozsah musí být přiměřený, relevantní a omezený ve vztahu k účelu zpracování. Existuje zde možnost, že rozsah osobních údajů, které obci nařizuje zpracovávat zákon, není v souladu se stanoveným účelem, a tedy zásadami GDPR. Pokud zákonný rozsah osobních údajů nevyhovuje požadavkům GDPR, je třeba rozvinout veřejnou debatu, která by mohla vést k potřebným legislativním změnám (např. prostřednictvím zákonodárné iniciativy zastupitelstev krajů).

3.2.19 Vydávání obecně závazných vyhlášek v kontextu ochrany osobních údajů

Obecně závazné vyhlášky jsou jednou z forem normotvorby obcí a jedním z projevů práva na samosprávu garantovaného článkem 104 Ústavy ČR. Musí obsahovat výlučně obecnou právní úpravu, nemohou obsahovat rozhodnutí v konkrétní věci. Obecně závazné vyhlášky nemohou upravovat věci, které jsou vyhrazené pouze zákonu, a nesmějí být v rozporu s právními předpisy vyšší právní síly.[40] Při vydávání obecně závazných vyhlášek se obec musí vždy pohybovat v mezích samostatné působnosti vymezených zákonem. Obecně závazné vyhlášky jsou tedy určitým výrazem rozhodovací autonomie obce, vzhledem k ústavně zakotvené samostatnosti při správě vlastních záležitostí.

Obsah obecně závazné vyhlášky si tak obec stanovuje sama, je omezena pouze právními předpisy vyšší právní síly, se kterými nesmí být v rozporu. Z toho tedy vyplývá povinnost obcí respektovat při vytváření obecně závazných vyhlášek také zásady a povinnosti stanovené GDPR. Obecně závazné vyhlášky by měly být formulovány tak, aby z nich jasně vyplýval účel zpracování osobních údajů a aby tento účel byl v souladu s GDPR vyjádřen dostatečně určitě, jednoznačně a aby byl legitimní. V souladu se zásadami GDPR by měl být rovněž stanoven rozsah vyhláškou požadovaných osobních údajů. Pokud tento rozsah není stanoven přímo zákonem, měly by být od subjektů údajů vyžadovány osobní údaje v souladu se zásadou „minimalizace údajů“. Tedy vyžadované osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu ke stanovenému účelu zpracování.[41]

Vzhledem ke skutečnosti, že obec může dle ust. § 10 zákona o obcích, ukládat v samostatné působnosti obecně závaznou vyhláškou též povinnosti, bude právním důvodem pro zpracování osobních údajů stanovené obecně závaznou vyhláškou kromě plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci dle čl. 6 odst. 1 písm. e) GDPR, také splnění právní povinnosti ve smyslu čl. 6 odst. 1 písm. c) GDPR.

DOPORUČENÍ:

Obce při tvorbě obecně závazných vyhlášek jako předpisů nižší právní síly musí respektovat také povinnosti a zásady stanovené GDPR.

[40] Hendrych, D. a kol.: Správní právo. Obecná část. 7. vydání. Praha: C. H. Beck, 2009, 875 s.
[41] Viz čl. 5 GDPR.

3.2.20 Vedení spisové služby

Zpracováním osobních údajů se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, za určitým účelem; za zpracování osobních údajů se mj. považuje shromáždění, zaznamenání či uložení osobních údajů (čl. 4 odst. 2 GDPR).

Vedení spisové služby v souvislosti s výkonem činnosti obce lze označit za jeden ze způsobů zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR. Obec při vedení spisové služby zpracovává osobní údaje za stanoveným účelem v roli správce nebo zpracovatele, a je proto povinna plnit související povinnosti stanovené v GDPR (např. v otázce uplatňování práv ze strany subjektů údajů).

Stejně tak pokud obec v souvislosti se svým účastenstvím ve správním řízení vytváří vlastní evidenci dokumentace obsahující osobní údaje, a to za účelem řádného uplatňování či bránění svých práv v daném řízení, pak tímto způsobem stanovuje nové účely a prostředky zpracování osobních údajů, osobní údaje subjektů údajů proto zpracovává v roli správce a je povinna plnit povinnosti stanovené v GDPR. Zároveň je povinna tuto dokumentaci evidovat v rámci spisové služby.

Vedení spisové služby přitom musí být prováděno v souladu s přijatým spisovým a skartačním řádem (mj. v souladu se stanovenými skartačními lhůtami), který bude GDPR compliance.

DOPORUČENÍ:

Obec musí revidovat spisový a skartační řád, zejména pokud jde o provedenou klasifikaci informací, které obsahují osobní údaje, a to tak, aby nakládání s takovými osobními údaji bylo prováděno v souladu s požadavky GDPR, zejména z důvodu splnění povinnosti zavést vhodná technická a organizační opatření za účelem zajištění a doložení toho, že zpracování je prováděno v souladu s GDPR (čl. 24 odst. 1 GDPR).

Vhodným vodítkem může být např. Vzorový spisový a skartační plán pro obce s rozšířenou působností (viz. Příloha č.1 k MV-94685-1/AS-2013).

3.2.21 Uchovávání osobních údajů v souvislosti se zadávacím řízením

Správce, který vystupuje v roli zadavatele ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, je dle § 216 odst. 1 téhož zákona povinen uchovávat dokumentaci o zadávacím řízení, kterou tvoří všechny dokumenty v listinné nebo elektronické podobě a výstupy z ústní komunikace, jejichž pořízení v průběhu zadávacího řízení, popřípadě po jeho ukončení, vyžaduje tento zákon, včetně úplného znění originálů nabídek všech dodavatelů. Archivační doba je stanovena jednotně v délce 10 let ode dne ukončení zadávacího řízení nebo od změny závazku ze smlouvy na veřejnou zakázku, pokud jiný právní předpis (tj. zejména zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, může jím být též vnitřní předpis zadavatele či požadavky poskytovatelů dotací[42]) nestanoví lhůtu delší. Obsah dokumentace o zadávacím řízení, kterou je nutné uchovávat, tedy tvoří mj. nabídky všech dodavatelů, resp. všech účastníků zadávacího řízení, a to i těch, kteří jsou v zadávacím řízení neúspěšní (tedy těch, s nimiž zadavatel neuzavřel smlouvu). Součástí těchto nabídek přitom mnohdy bývají též životopisy, doklady o vzdělání či odborná osvědčení členů realizačního týmu, které zadavatel musí uchovávat.

[42] Srov. *Dvořák, D., Machurek, T., Novotný P., Šebesta, M. a kolektiv.* Zákon o zadávání veřejných zakázek. Komentář. 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, 1320 s.

Uchovávání dokumentace o zadávacím řízení je povinností, kterou správci/zadavateli ukládá zákon. Důvodem uložené povinnosti uchování dokumentace o zadávacím řízení je možnost provedení průběžné i následné kontroly postupu zadavatele a dodavatelů ve vztahu k předmětnému zadávacímu řízení. Nepořízení nebo neuchování dokumentace o zadávacím řízení po stanovenou dobu podle § 216 předmětného zákona je považováno za přestupek, ze nějž lze uložit pokutu ve výši 10 % ceny veřejné zakázky, nebo až do výše 20 mil. Kč, nelze-li celkovou cenu veřejné zakázky zjistit (§ 268 zákona).

DOPORUČENÍ:

Správce v roli zadavatele je povinen uchovávat dokumentaci o zadávacím řízení nejméně po dobu 10 let, pokud jiný právní předpis nestanoví archivační lhůtu delší. Dokumentaci o zadávacím řízení tvoří mj. též osobní údaje subjektů údajů uvedené v nabídkách účastníků zadávacího řízení (např. osobní údaje uvedené v životopisech, dokladech o vzdělání či odborných osvědčeních členů realizačního týmu). Při uchovávání osobních údajů v rámci dokumentace o zadávacím řízení je tedy nutné dodržet povinnosti stanovené GDPR, např. z hlediska zabezpečení či přístupových oprávnění k uchovávaným osobním údajům.

3.2.22 Využití firemního resp. obecního e-mailu

Zaměstnanci úřadu používají pracovní emaily pro komunikaci v rámci úřadu i pro komunikaci mimo úřad, nezřídka ovšem tato komunikace obsahuje osobní údaje (žádosti občanů, vyplněné formuláře, návrhy smluv, smlouvy, podání apod.).

Emailové zprávy mohou být přenášeny otevřeným internetem bez šifrování či nějakého jiného zabezpečení proti odposlechnutí a přečtení.

Emailové servery jsou často hostovány u třetích stran a k emailovým schránkám mají přístup administrátoři těchto systémů.

DOPORUČENÍ:

Pro zabezpečení emailů je nutné přijmout adekvátní technická a organizační opatření.

Je doporučeno stanovit jasná organizační pravidla pro používání emailů a to:

- **Povolit užívání emailu pouze pro pracovní účely;**
- **Zakázat přístup k emailům z nechráněných zařízení.**

Kde používání emailové komunikace není nezbytně nutné pro realizaci agendy, zakázat formou organizačního opatření používání emailů pro odesílání osobních údajů a tento zákaz vhodnou formou monitorovat.

Pokud je to nutné pro výkon agendy, neodesílat emaily obsahující osobní údaje v nešifrované podobě. Osobní údaje je nutné umístit do zašifrované přílohy a hesla zasílat jiným kanálem, než je email (např. sms, telefonicky apod.). Pro šifrování lze použít i běžně dostupný komprimovací program Zip, který má podporu na všech rozšířených platformách.

V případě používání hostovaných emailových serverů doporučujeme také ošetřit smluvně otázku přístupu k datům s poskytovatelem služeb tak, aby byla zajištěna bezpečnost a důvěrnost poskytovaných emailových schránek.

Technická opatření představují výhradní používání zabezpečených šifrovaných protokolů pro odesílání a stahování emailů. Dále je možné podpořit bezpečnost instalací specializovaných programů, které dokáží plnit funkci Data loss prevention (dále „DLP“) – ochrana proti úniku dat způsobeným lidskou chybou. Tyto DLP programy mohou být buď nainstalovány na koncové stanice uživatelů (tuto funkci dokáží plnit i některé antivirové programy) nebo jako síťová řešení, která zabezpečí komunikaci celého úřadu na úrovni perimetru vnější komunikace.

3.2.23 Využití a problematika freemailů

Některé úřady využívají pro emailové služby tzv. freemailové účty. Jedná se o hostované mailové servery, které bezplatně poskytují emailové schránky všem zájemcům (email.cz, gmail.com apod.). Přístup k těmto schránkám mají vždy i administrátoři systému, kteří nejsou zaměstnanci úřadu. Úřad nemá kontrolu nad administrací těchto serverů a nemá pod kontrolou přístup k mailovým schránkám. Přístup k těmto schránkám je možný z jakéhokoliv zařízení připojeného do internetu, nelze ho omezit pouze na přístup ze zabezpečených prostředků, které má úřad pod kontrolou.

DOPORUČENÍ:

Pro zabezpečení emailů na freemailových serverech je nutné přijmout obdobná technická a organizační opatření jako v předchozím případě.

Je doporučeno stanovit jasná organizační pravidla pro používání takto nezabezpečených emailů:

Kde to není nezbytně nutné pro realizaci agendy, zakázat používání emailů pro odesílání osobních údajů.

Pokud je to nutné pro výkon agendy, neodesílat emaily obsahující osobní údaje v nešifrované podobě. Osobní údaje je nutné umístit do zašifrované přílohy a hesla zasílat jiným kanálem, než je email (např. sms, telefonicky apod.). Pro šifrování lze použít i běžně dostupný komprimovací program Zip, který má podporu na všech rozšířených platformách.

Technická opatření představují výhradní používání zabezpečených šifrovaných protokolů pro odesílání a stahování emailů mezi poštovním klientem a serverem (SSL šifrované spojení). Dále je možné podpořit bezpečnost instalací specializovaných programů, které dokáží plnit funkci Data loss prevention – ochrany proti úniku dat způsobeným lidskou chybou. Tyto DLP programy je vhodné nainstalovat na koncové stanice uživatelů freemailů spolu s antivirovou ochranou.

3.2.24 Omezení přístupu na stránky se škodlivým obsahem

Zaměstnanci úřadu mohou přistupovat na stránky obsahující škodlivý obsah. Škodlivý obsah může představovat nelegální obsah (dětská pornografie, stránky propagující nezákonné ideologie) či například stránky šířící škodlivý kód (různé formy malwaru), který může způsobit významné škody na infrastruktuře úřadu.

DOPORUČENÍ:

Organizační opatření představují stanovení pravidel pro užívání internetu. Zakázat zaměstnancům přístup na stránky, které nepotřebují pro výkon svých pracovních povinností. Zakázat používání stránek, na kterých lze publikovat či sdílet dokumenty nebo soubory (ulož.to, facebook.com, youtube.com). Zakázat přístup na stránky obsahující nebezpečný či nezákonný obsah (pornografie, propagace fašismu apod.).

Jako vhodné technické opatření je doporučeno omezení přístupu uživatelů internetu na úrovni DNS (např. pomocí opendns.com), zakázání nestandardních portů (povolit pouze porty pro http, https, dns, icmp ping, internetové bankovnictví a pro připojení do hostovaných systémů nutných pro výkon agend), blokování stahování nebezpečných typů souborů (.dll, .vbs, .wps, .pif, .msc apod.).

Pro zajištění těchto technických opatření je nutné používat vyspělejší síťové prvky, které výše uvedené funkčnosti umožňují.

3.2.25 Webové stránky obce – problematika formulářů

Některé obce mají na svých internetových stránkách formuláře pro přihlášení k poskytovaným službám, do kterých občané vyplní své osobní údaje a následně odešlou. Odesílání formulářů neprobíhá pomocí zabezpečeného protokolu. Dále jsou na těchto internetových stránkách umístěny analytické kódy, které slouží ke sběru dat o uživatelích.

DOPORUČENÍ:

Technická opatření spočívají v provozování webových stránkách na zabezpečeném protokolu HTTPS, který komunikaci mezi uživatelem a serverem šifruje. Dále je nutné zajistit, aby obsah formuláře nebyl přeposílán úředníkem v nezabezpečené podobě. Osobní údaje není vhodné umísťovat do těla emailu, ale pouze ve formě zašifrované přílohy, pokud úřad nepoužívá šifrování emailů pomocí certifikátů.

Analytické informace sbírané z webových stránek (pomocí Cookies, Google Analytics, Hotjar, Optimizely apod.) je nutné považovat za osobní údaje uživatelů a je nezbytně nutné se k nim takto chovat. To znamená, že musí být řádně chráněny jak samotným zpracovatelem, tak jeho dodavateli. Je doporučeno zanalyzovat, zdali je jejich sběr pro provoz služby nezbytný a zdali jsou účelně shromažďovány pouze nezbytně nutné údaje.

3.2.26 Webové stránky obce – problematika záznamů a fotografií

Obce publikují na svých webových stránkách fotografie zaměstnanců úřadu či telefonní kontakty na zaměstnance.

DOPORUČENÍ:

Problematika zveřejňování fotografií a osobních údajů zaměstnanců je již detailně diskutována v kapitole 3.2.1.

Lze doporučit, aby obec zveřejňovala na svých webových stránkách jméno a příjmení, pracovní e-mail a telefonní číslo zaměstnance pouze v případě, že jejich pracovní pozice předpokládá jednání či nějaký jiný způsob kooperace s veřejností.

Je nutné mít na zřeteli, že publikace těchto informací je v prostředí otevřeného internetu často nevratná a jakmile je něco umístěno, bez omezení přístupu pomocí jména a hesla či jiných prostředků, na internet, není tento obsah již dále pod plnou kontrolou. Ačkoliv bude informace z internetových stránek odstraněna, stejně po ní může zůstat tzv. digitální stopa. Například existují archivační servery, které se snaží obsah celého internetu archivovat, tudíž může být publikovaná informace přístupná a dohledatelná i neomezeně dlouhou dobu po jejím stažení z webových stránek obce. Dále existuje nepřeberné množství společností, které roboticky indexují obsah všech internetových stránek pro marketingové, výzkumné či jiné účely apod. Tyto společnosti nemusí vždy operovat z Evropské unie, neřídí se GDPR a není možné u nich ani uplatnit práva subjektu údajů na výmaz.

3.2.27 Facebook a sociální sítě

Obce zveřejňují na Facebooku a jiných sociálních sítích fotografie a osobní údaje zaměstnanců či třetích osob.

DOPORUČENÍ:

Problematika je diskutována již v kapitole 3.2.2.

Obec může zveřejňovat osobní údaje zaměstnanců a třetích osob na svém facebookovém profilu pouze na základě jimi udělených souhlasů se zpracováním osobních údajů. Nicméně vzhledem k nedostatečné kontrole nad zveřejněnými osobními údaji zveřejňování osobních údajů na Facebooku (či na jiných sociálních sítí) spíše nedoporučujeme.

Je nutné pamatovat, že každá zveřejněná informace na sociálních sítích přestává být pod kontrolou úřadu.

3.2.28 Notebooky – šifrování

Zaměstnanci úřadu používají služební notebooky, které vynášejí i mimo prostory úřadu. V případě ztráty či odcizení přenosného zařízení může nálezce či pachatel získat neoprávněný přístup k osobním údajům.

DOPORUČENÍ:

Organizační opatření může omezovat:

a) výskyt osobních údajů na přenosných zařízeních,

b) omezovat použití výpočetní techniky pouze na budovy úřadu.

Někdy je ovšem pro výkon agend nezbytné použití notebooku mimo prostory úřadu. V takovém případě je vhodné využít šifrování dat uložených v notebooku.

Toto může být provedeno buď přímo na úrovni celého disku (FDE - Full Disk Encryption) nebo na úrovni vybraných složek s daty (FES – File Encryption System). U první varianty není nutné sledovat a určovat, co a kdy se má šifrovat, jelikož se automaticky šifruje celý obsah pevného disku. Toto je významnou předností, jelikož celý proces šifrování nevyžaduje zásahy uživatele. Nevýhodou je, že uložené soubory nejsou chráněny při přenosu na výměnná média či při komunikaci emailem. Pro šifrování FDE je rozšířený nástroj BitLocker, který je dostupný na operačním systému Windows od verze Vista dále a jedná se o funkcionalitu operačního systému, která je nevyžaduje další dodatečné finanční náklady.

Druhá varianta – FES – vyžaduje přesné vymezení, které složky či soubory se mají šifrovat. Toto lze realizovat i pomocí zabudovaného šifrování přímo v operačním systému Windows nazvaného Encrypting File System.

Při nasazení šifrování je nutné pamatovat na zabezpečení vlastních šifrovacích klíčů, bez kterých se k zašifrovanému obsahu nikdo nedostane a které mohou být potřeba v případě technických problémů s notebookem nebo při reinstalaci.

3.2.29 Chytré telefony - ochrana

Současné „chytré“ mobilní telefony jsou například schopny přijímat emaily a mohou obsahovat i další osobní údaje uložené jako soubory, kontakty nebo v kalendáři. V případě jejich ztráty či odcizení může nálezce nebo pachatel získat neoprávněný přístup k osobním údajům.

DOPORUČENÍ:

Organizační opatření pro zajištění bezpečnosti mobilních telefonů spočívají ve stanovení jasných pravidel pro jejich používání a zabezpečení.

Veškeré SIM karty musí být chráněny kódem PIN. Přístup do mobilního zařízení musí být chráněn heslem nebo obdobnou soudobou technologií. Zařízení musí mít nastaveno automatické zamykání po stanovené době nečinnosti. Pokud to přístroj umožňuje, měl by být jeho obsah šifrován.

V případě služebních mobilních telefonů, ve kterých se počítá s příjmem emailů, ukládáním kontaktů a kalendářových událostí, může obec zohlednit jejich ochranu již ve fázi výběru vhodných modelů a vybrat takové modely, které podporují důsledné zabezpečení.

Mobilní telefony je v dnešní době možné ochránit obdobně jako přenosné notebooky. Pro správu mobilních telefonů se používají specializované softwarové nástroje MDM – Mobile Device Management. Pomocí těchto nástrojů lze řídit autorizovaný/neautorizovaný přístup do sítě, přidělení práv uživateli nebo vzdálené vymazání celého přístroje.

3.2.30 Chytré telefony – soukromé vlastnictví

Současné „chytré“ mobilní telefony jsou například schopny přijímat emaily a mohou obsahovat i další osobní údaje uložené jako soubory, kontakty nebo v kalendáři. V případě jejich ztráty či odcizení může nálezce nebo pachatel získat neoprávněný přístup k osobním údajům.

DOPORUČENÍ:

V předchozí situaci byly řešeny služební mobilní telefony, u kterých může obec ovlivnit jejich výběr, zaměstnanci ale často používají vlastní telefonní přístroje (někdy s dvěma SIM kartami).

Organizační opatření pro zajištění bezpečnosti mobilních telefonů i v tomto případě spočívají ve stanovení jasných pravidel pro jejich používání a zabezpečení.

Veškeré SIM karty musí být chráněny kódem PIN. Přístup do mobilního zařízení musí být chráněn heslem nebo obdobnou soudobou technologií. Zařízení musí mít nastaveno automatické zamykání po stanovené době nečinnosti. Pokud to přístroj umožňuje, měl by být jeho obsah šifrován.

U soukromých mobilních telefonů lze jen těžko nutit zaměstnance, aby si instalovali softwarové nástroje třetích stran, které by mohly monitorovat jejich užívání mobilního telefonu. V takovém případě je doporučeno stanovit, že do zařízení neopatřených nástroji MDM není možné stahovat data úřadu – emaily, kalendáře, kontakty apod. Tato data smí být ukládány pouze na zabezpečených zařízeních.

3.2.31 Počítačové sestavy v rámci úřadu a jejich ochrana

Počítačové stanice jsou vstupní branou do všech informačních systému úřadu a je nutné je adekvátně ochránit. Počítačové sestavy v rámci úřadu slouží k vykonávání agend s osobními údaji, shromažďování a zpracovávání osobních údajů, předávání osobních údajů apod. Zároveň jsou nejčastějším nástrojem pro neoprávněné získání osobních údajů, jejich zneužití, smazání či poškození a je proto nutné je co nejlépe zabezpečit.

DOPORUČENÍ:

Ochrana pracovních stanic zaměstnanců je fundamentální činností IT pracovníků. Skládá se z přiměřených organizačních a technických opatření.

Organizační opatření spočívají v definování pravidel užívání výpočetní techniky – nejlépe formou Směrnice pro uživatele výpočetní techniky.

Tato směrnice by měla obsahovat alespoň následující vymezení základního principu, a to že každá osoba (zaměstnanec, externí spolupracovník aj.) má povinnost chránit důvěrnost informací, které v rámci své činnosti využívá nebo zpracovává. Jakákoli informace má být poskytována pouze osobám, které z povahy své funkce nebo poslání s danou informací mají být obeznámeny, nebo ji potřebují pro výkon své pracovní činnosti (princip „need-to-know“). Původce informace musí zajistit její dostupnost pro všechny oprávněné osoby.

Je vhodné nadefinovat a implementovat obecná pravidla pro užívání výpočetní techniky, která obsahují následující pokyny:

- **Je zakázáno používat pracovní stanice jinak než k činnostem přímo souvisejícím s pracovní činností.**
- **Chránit data uložená v paměťových médiích koncových stanic před neoprávněným přístupem.**
- **Zamezit fyzickému přístupu ke koncové stanici neoprávněným osobám. Je zakázáno manipulovat s výpočetní technikou.**
- **Při krátkodobém opuštění pracoviště uzamknout koncovou stanici kombinací kláves CTRL+ALT+DELETE - volba „Uzamknout“.**
- **Při dlouhodobém opuštění pracoviště ukončit veškerý spuštěný software, uložit rozpracované dokumenty a koncovou stanici vypnout.**
- **Je zakázáno instalovat neschválené softwarové vybavení.**
- **Zdržet se konzumace jídla a pití v blízkosti hardware koncových stanic.**
- **Je zakázáno aktivně vytvářet nebo šířit škodlivý software a znemožňovat funkci ochranného softwaru.**
- **V případě poruchy, nefunkčnosti softwarového a hardwarového vybavení, podezření na nakažení svého počítače virem apod. neprodleně informovat odpovědné pracovníky.**
- **Je zakázáno vědomě využívat ilegální programové vybavení a data, případně takovéto programy či data nabízet jiným.**

Dobrým vodítkem pro tvorbu takové směrnice je zákon o kybernetické bezpečnosti a vyhláška o kybernetické bezpečnosti.

Technická opatření spočívají v nastavením skupinových politik pracovních stanic tak, aby reflektovaly výše uvedené požadavky. Přístup do počítače pouze po zadání přihlašovacího hesla a jména, nastavení automatického uzamykání obrazovek po nečinnosti, instalace antivirového programu na všech stanicích, monitorování chodu a užívání pracovních stanic, správa softwarových aktualizací stanic a další opatření.

Pro komplexní zajištění pracovních stanic doporučujeme použít vyhlášku o kybernetické bezpečnosti, která se celé problematice věnuje systematicky.

3.2.32 Interní ochrana sítě LAN

V kancelářích a na chodbách úřadů jsou volně přístupné ethernetové zásuvky, jejichž pomocí se může kdokoliv připojit do interní sítě úřadu. Obdobné nebezpečí představují síťové tiskárny umístěné na chodbách úřadu, u kterých lze přípojku rozpojit a vložit kabel přímo do notebooku a tím získat přístup do interní sítě úřadu.

DOPORUČENÍ:

Ochranu interní sítě lze realizovat pomocí vybraných technických opatření.

Základním bezpečnostním opatřením je vypnout všechny nepoužívané síťové zásuvky, aby je nebylo možné zneužít.

Pro aktivně používané zásuvky je nutné umožnění přístupu do sítě pouze schváleným zařízením (Network Access Control). Tento způsob slouží jako prevence před kybernetickými útoky a škodlivým chováním na síti. Kontrola přístupu může být řízena na úrovni povolování MAC adres zařízení na aktivních síťových prvcích. Zařízení, které nemá registrovanou MAC adresu, nebude do sítě připuštěno. Obdobně lze přístup řídit také pomocí vydaných bezpečnostních certifikátů, které bude vydávat pověřená osoba (správce IT) nebo pomocí protokolu IEEE 802.1x, který taktéž slouží k autentizaci uživatelů.

Tato bezpečnostní opatření musí podporovat aktivní síťové prvky.

3.2.33 Segmentace interní sítě LAN

Obec má pouze jednu nesegmentovanou počítačovou síť. Přístup k této síti mají i uživatelé veřejné Wi-Fi sítě. Důsledkem je možný přístup všech zařízení ke všem sdíleným prostředkům a v případě napadení jednoho počítače umožnění šíření útoku i na další zařízení.

DOPORUČENÍ:

Pokud všichni uživatelé mohou přistupovat na všechna zařízení a síťové služby, zvyšuje se významně bezpečnostní riziko. LAN musí být segmentovány dle úrovně důvěry a účelu. Pokud by se útočníkovi podařilo dostat na jedno síťové zařízení v sítí, mohl by z něj útočit na další cíle prakticky neomezeně. Nejde pouze o aparát jak izolovat útok či infekci, ale i různé provozní problémy na síti v rámci jedné domény. Segmentace LAN pomůže izolovat různá prostředí a umožní řídit přístup k prostředkům na síťové úrovni a to až na úrovni identit uživatelů.

Pokud obec provozuje veřejnou síť (Wi-Fi), je nezbytně nutné, aby tato byla galvanicky oddělena od vnitřní sítě úřadu. V jiném případě by mohl kdokoliv odposlouchávat provoz úřadu na síti, čímž by se mohl snadno dostat k osobním údajům a datům úřadu. Taktéž by mohl ohrozit chod informačních systémů obce, dostupnost a integritu dat na síťových úložištích apod.

3.2.34 Problematika sítí LAN mezi více budovami úřadu

Obec má umístěnu výpočetní techniku ve více lokalitách, je nutné zabezpečit komunikaci mezi jednotlivými lokalitami.

DOPORUČENÍ:

Realizace zabezpečení těchto propojení musí být adekvátní možnostem a potřebám obce.

V případě využití optického propojení, je nutné, aby provoz byl striktně oddělen od ostatního provozu například pomocí segmentace VLAN. Pro ještě větší zabezpečení je vhodné zvolit nějaký způsob šifrování a enkapsulace dat (IPSec).

Pokud je použito propojení pomocí bezdrátových pojítek (Wi-Fi), je bezpodmínečně nutné vždy zapnout šifrovaný přenos dat, aby byla síť zabezpečena proti odposlechnutí.

Obecně v případě použití šifrování je nutné sledovat situaci na trhu a v případě prolomení používané šifry implementovat opravu firmwaru nebo použít jiný typ šifrování. V roce 2017 byla například publikována chyba v šifrování WPA2, které patřilo k nejrozšířenějším v oblasti Wi-Fi.

3.2.35 Externí správa IT infrastruktury

Některé obce využívají pro správu infrastruktury externí správce. Tito správci mají přístup do všech interních systémů a tedy i k osobním údajům.

DOPORUČENÍ:

Řešení pomocí outsourcingu správy IT je legitimní, ale je nutné stanovit jasná pravidla. Outsourcing musí být řádně smluvně ošetřen. Smlouvy by měly obsahovat veškerá bezpečnostní opatření (viz. Příloha č. 7 návrhu nové vyhlášky o kybernetické bezpečnosti https://nukib.cz/cs/kyberneticky-zakon/legislativa/).

Přihlašování a aktivity externích správců IT musí být logovány a auditovány. Tyto záznamy musí být pravidelně dohledovány, zdali nedochází k nestandardním či neoprávněným úkonům.

Je nutné upozornit na skutečnost, že některé auditní logy obsahují detailní záznamy o změnách údajů v informačních systémech a tudíž obsahují osobní údaje, které je nutné řádně zabezpečit.

3.2.36 Problematika sledování přístupů a monitoring činností (tzv. logování)

Většina aplikací a informačních systémů umožňuje zaznamenávání sledování přístupů a monitoring činnosti formou logů, ve kterých jsou informace o sledovaných událostech v daném informačním systému nebo aplikaci. Tyto logy je zpravidla náročné sledovat a dohledovat. Jejich správné a včasné vyhodnocení však může vést ke zlepšení bezpečnostní situace v prostředí obce.

DOPORUČENÍ:

Pro řešení provozních i bezpečnostních incidentů je zásadní možnost chronologické rekonstrukce událostí zaznamenaných IT. Velmi často útočník manipuluje s logy a systémovým časem infikovaných zařízení tak, aby před administrátorem skryl své počínání. V jiném případě je historie pro uložení logů příliš krátká a není možné zajistit požadovanou retenci logů na všech systémech.

Pro účely bezpečného uložení auditních a systémových logů ze serverů a aplikací zajišťující kritické služby je doporučeno po analýze potřeb (zajištění integrity, důvěrnosti, podporované platformy a aplikace, uživatelsky přívětivé rozhraní pro vyhledávání v lozích atp.) a zdrojů dat nainstalovat a provozovat centralizovaný logovací server.

U menších obcí je možné používat i decentralizované řešení, jelikož množství zaznamenávaných informací je menší.

3.2.37 Problematika sdílených disků

Velmi rozšířenou praktikou je pro ukládání nestrukturovaných dat využití sdílených disků. Téměř každý úřad takový sdílený disk provozuje.

DOPORUČENÍ:

Problematika sdílených disků v sobě zahrnuje mnoho aspektů:

- **Sdílené disky je snadné implementovat. Jejich instalace může proběhnout pomocí systémových politik. Náklady na pořízení jsou velice nízké.**
- **Přístupová práva lze nastavovat na úrovni složek.**
- **Je náročné monitorovat a administrovat, kdo má přístup do kterých složek a zdali je přístup oprávněný.**
- **Sdílené disky jsou zranitelné vůči virovým nákazám a často slouží jako nástroj jejich šíření.**
- **Sdílené disky jsou zranitelné vůči ransomwaru (vyděračský software).**
- **Sdílené disky jsou náchylné na uživatelské chyby – nechtěným vymazáním či upravením obsahu souborů, nahráním souborů do jiných složek a tím možnosti zpřístupnění souboru dat i neoprávněným uživatelům apod.**

Pro zajištění souladu s GDPR doporučujeme omezit užívání sdílených disků pouze na nezbytně nutnou úroveň. Dále je nutné maximálně segmentovat diskový prostor (osobní data, data organizace / útvaru / oddělení). Řídit se pravidlem „need to know“ a povolit přístup pouze těm, kteří přístup potřebují. Cíleně omezit přístup zaměstnanců mimo oprávněné složky.

3.2.38 Problematika využití flash pamětí a USB portů pracovníky úřadu

DVD/CD média jsou na ústupu a jsou nahrazována přenosnými USB paměťmi. Kapacita těchto pamětí je totožná s velikostí pevných disků a není problém na ně zkopírovat celé počítačové systémy. Taktéž tyto paměti mohou být zdrojem škodlivého softwaru.

DOPORUČENÍ:

Využívání flash pamětí by mělo být zcela zakázáno. Rizika vyplývající z používání flash pamětí jsou následující:

- **Možnost zavlečení škodlivého softwaru;**
- **Umožnění úmyslného úniku obrovského množství dat;**
- **V případě ztráty hrozí opět únik dat.**

Pokud je nutné používat flash paměti pro zajištění pracovních agend, je nutné používat šifrované flash paměti, ze kterých není možné získat osobní údaje bez znalosti uživatelského hesla. V případě opakovaného chybného zadání hesla se data nevratně vymažou.

Stejná rizika plynou z povolení používání USB portů. Pomocí těchto portů lze připojit do počítačového systému nejrůznější zařízení, která mohou být pro ochranu osobních údajů závažnou hrozbou. USB porty by měly být povolené pouze zaměstnancům, kteří je potřebují pro výkon svých agend (například práce s digitálním fotoaparátem apod.).

3.2.39 Problematika využití DVD/CD pracovníky úřadu

Některé počítačové stanice jsou stále vybaveny vypalovací DVD/CD mechanikou. Na jedno médium se vejde obrovské množství osobních údajů. Přístup k ní není nijak omezen.

DOPORUČENÍ:

Možnost vypalovat data na DVD/CD by měla být výrazně omezena pouze na zdůvodnění případy, v ostatních případech by měla být technologicky zakázána, což všechny běžně používané operační systémy zvládají bez vynaložení významných nákladů.

3.3 Doporučení k možnostem personálního a organizačního obsazení pověřence pro ochranu osobních údajů

GDPR zakotvuje nový institut pověřence pro ochranu osobních údajů. Pověřenec je specifickou osobou, kterou musí jmenovat správci a zpracovatelé osobních údajů, kteří splňují podmínky stanovené v čl. 37 odst. 1 GDPR[43]. Každý správce a zpracovatel tak musí zvážit, zda se na něj povinnost jmenovat pověřence vztahuje.

Role pověřence spočívá zejména v dohlížení na soulad postupů správců a zpracovatelů s GDPR a v poskytování odborné podpory správcům a zpracovatelům v souvislosti s jejich povinnostmi souvisejícími s ochranou osobních údajů.

3.3.1 Kvalifikační standardy

V souladu s čl. 37 odst. 5 GDPR musí být pověřenec jmenován na základě svých profesních kvalit, zejména na základě odborných znalostí práva a praxe v oblasti ochrany osobních údajů, a na základě své schopnosti plnit úkoly stanovené v čl. 39 GDPR. GDPR nijak neupravuje konkrétní náležitosti profesních a odborných kvalit (např. požadavky na vzdělání či certifikaci). Vždy je však nutné dodržet podmínku, že musí jít o osobu, která bude schopná plnit úkoly pověřence stanovené v GDPR.

Pověřenec by zároveň měl mít dostatečnou znalost interní struktury správce nebo zpracovatele, postupů uplatňovaných při činnosti správce nebo zpracovatele či prováděných operací zpracování osobních údajů.

U každého správce nebo zpracovatele budou požadavky na osobu pověřence rozdílné, zejména s ohledem na organizační strukturu správce nebo zpracovatele a činnosti jimi prováděné. Vyšší nároky na kvalifikaci a praxi pověřence (zejména na podrobnou znalost právní úpravy, znalost problematiky kybernetické a fyzické bezpečnosti, řízení informačních systémů nebo schopnost monitorovat a auditovat činnosti správce nebo zpracovatele a dovozovat z tohoto monitoringu relevantní závěry) budou zcela jistě kladeny na pověřence, který bude vykonávat svou činnost jako společný pověřenec pro více obcí, neboť bude muset znát administrativní pravidla a postupy uplatňované při činnosti každé jednotlivé obce. Vyšší nároky budou kladeny také na pověřence podřízených organizací, které provádějí rozsáhlé zpracování zvláštních kategorií osobních údajů.

Pověřenec se nesmí dostat do střetu zájmů. Pracovní skupina WP29 ve svém výkladovém stanovisku[44] dovozuje, že pověřenec nemůže zastávat pozici, na které by stanovoval účely nebo prostředky zpracování osobních údajů. Osoby ve střetu zájmů budou ty, které se podílejí jak na koncipování, tak na realizaci projektů zahrnujících činnosti v souvislosti se zpracováním osobních údajů. Typickými pozicemi se střetem zájmů jsou například tajemník obecního úřadu, ředitel finančního odboru nebo vedoucí IT oddělení.

Pověřenec je dle čl. 38 odst. 5 GDPR v souvislosti se svou činností vázán povinností mlčenlivosti. Tato mlčenlivost se bude vázat zejména na osobní údaje subjektů údajů, ale také na aplikovaná bezpečnostní opatření a jiné důvěrné informace týkající se činnosti správce nebo zpracovatele.

---

[43] Viz čl. 37 odst. 1 GDPR:
„Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:
a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí,
b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, nebo
c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech uvedených v článku 10.“

[44] Pracovní skupina podle článku 29: Vodítka k pověřencům pro ochranu osobních údajů, WP 243 rev. 01 ze dne 5. 4. 2017

3.3.2 Organizační začlenění pověřence

Čl. 38 GDPR upravuje postavení pověřence z hlediska jeho zapojení do záležitostí souvisejících s ochranou osobních údajů. Toto ustanovení zakotvuje povinnost správce nebo zpracovatele zapojit pověřence do veškerých záležitostí souvisejících s ochranou osobních údajů a podporovat ho při plnění jeho úkolů a povinností dle čl. 39 GDPR. Pověřenec by měl být správcem nebo zpracovatelem brán jako diskuzní partner a měl by mít přístup do všech pracovních skupin zabývajících se ochranou osobních údajů v rámci správce či zpracovatele.

Čl. 38 GDPR rovněž zakotvuje požadavek nezávislosti výkonu funkce pověřence v rámci správce nebo zpracovatele, když v odstavci 3 stanoví, že „*správce a zpracovatel zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele*“. Pověřenec tedy dle GDPR má mít v rámci organizační struktury správce nebo zpracovatele specifické a do jisté míry nezávislé postavení. Pověřenec tedy není jen pouhým řadovým zaměstnancem správce nebo zpracovatele, který má na starosti ochranu osobních údajů.

Pověřenec nenese osobní odpovědnost za nedodržení pravidel stanovených GDPR, neboť dle čl. 24 odst. 1 GDPR správce odpovídá za to, že zpracování je prováděno v souladu s GDPR, a tuto skutečnost musí být správce rovněž schopen doložit. Pověřenec by měl v rámci správce nebo zpracovatele vždy zastávat svou funkci a plnit své povinnosti a úkoly nezávislým způsobem. Pokud správce nebo zpracovatel bude postupovat v rozporu s názorem pověřence a tento postup potenciálně povede k nesouladu s GDPR, není v kompetencích pověřence v tom správci nebo zpracovateli bránit. Pověřenec by ale měl mít vždy prostor pro vyjádření svých postojů a správce nebo zpracovatel by se s nimi měl odůvodněně vypořádat.[45]

Pověřenec může být zaměstnancem správce nebo zpracovatele, tedy interním pověřencem, nebo může jednotlivé úkoly plnit na základě smlouvy o poskytování služeb[46], a být pověřencem externím.[47]

Externím pověřencem může být také právnická osoba, to však za předpokladu, že bude předem označena konkrétní fyzická osoba, která bude splňovat požadavky stanovené GDPR a bude funkci pověřence fakticky vykonávat.

GDPR umožňuje, aby pro několik orgánů veřejné moci či veřejných subjektů byl jmenován jediný pověřenec. [48] V takovém případě však musí být zohledněna organizační struktura a velikost jednotlivých orgánů veřejné moci nebo veřejných subjektů, neboť každý takový správce nebo zpracovatel je odpovědný za zajištění, že tento jediný pověřenec bude vůči němu plnit své úkoly efektivně, přestože byl pověřenec jmenován pro několik subjektů najednou. Správce nebo zpracovatel má povinnost pověřence při plnění jeho úkolů podporovat a poskytovat mu zdroje k jejich plnění. S tím souvisí i skutečnost, že pověřenec musí mít dostatek času k plnění svých povinností. V souvislosti s tím, jak stanoví i výkladové stanovisko WP29, by měl mít pověřenec stanoven i pevný podíl času vyhrazený pro funkci pověřence u konkrétního správce nebo zpracovatele.[49]

---

[45] Obecné nařízení o ochraně osobních údajů (GDPR). Praktický komentář. Wolters Kluwer. Praha, 2017.

[46] Půjde o nepojmenovanou soukromoprávní smlouvu mezi správcem, případně několika správci, a pověřencem ve smyslu ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.

[47] Ke způsobu ustanovení interního nebo externího pověřence více viz Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních v podmínkách obcí vydané Ministerstvem vnitra dne 10. 8. 2017.

[48] Viz čl. 37 odst. 3 GDPR.

[49] K ustanovení společného pověřence více viz Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních v podmínkách obcí vydané Ministerstvem vnitra dne 10. 8. 2017.

3.3.3 Manuál činností pověřence

Dle ust. čl. 38 GDPR je správce nebo zpracovatel povinen zapojit pověřence do procesů souvisejících s ochranou osobních údajů, zajistit zdroje nezbytné k plnění jeho povinností a také k udržování jeho odbornosti, umožnit mu v otázkách ochrany osobních údajů přístup k nejvyššímu vedení správce nebo zpracovatele a zejména předejít případnému střetu zájmů.

Úkoly pověřence zakotvuje zejména čl. 39 GDPR, ze kterého plyne, že pověřenec by měl být osobou, která dohlíží na veškeré činnosti v oblasti ochrany osobních údajů v rámci správce nebo zpracovatele. Pověřenec dle výkladového stanoviska WP29 hraje klíčovou roli při rozvoji kultury ochrany osobních údajů uvnitř správce nebo zpracovatele a pomáhá zavádět základní prvky GDPR, jako jsou základní zásady zpracování osobních údajů (viz kapitola II GDPR), práva subjektů údajů (viz kapitola III GDPR), záměrná a standardní ochrana osobních údajů (viz čl. 25 GDPR), záznamy o činnostech zpracování (viz čl. 30 GDPR), zabezpečení zpracování (viz čl. 32 GDPR) a oznamování a ohlašování případů porušení zabezpečení ochrany osobních údajů (viz čl. 33 a 34 GDPR). Pověřenec zároveň dbá zejména na to, aby každé zpracování osobních údajů, které bude u správce nebo zpracovatele probíhat, bylo prováděno na základě některého ze zákonných důvodů vymezených v čl. 6 GDPR. Je zejména vhodné, aby pověřenec shromažďoval informace k preciznímu rozpoznání a vymezení zpracovávaných osobních údajů a analyzoval a kontroloval shodu vnitřní praxe správce nebo zpracovatele, včetně rozdělení odpovědnosti, s unijní a národní právní úpravou. V souvislosti s touto činností by měl pověřenec poskytovat správci nebo zpracovateli informace a poradenství, vydávat doporučení
a předkládat svá stanoviska.[50]

Pověřenec rovněž dle čl. 39 odst. 1 písm. b) GDPR dohlíží na to, aby všichni zaměstnanci správce nebo zpracovatele, kteří jsou zapojeni do operací souvisejících se zpracováváním osobních údajů a souvisejících auditů, byli proškolováni v oblasti ochrany osobních údajů.

Mezi další úkol pověřence, který je zakotven v čl. 39 odst. 1 písm. c) GDPR, patří poskytování poradenství a vypracovávání odborných stanovisek pro správce v souvislosti s posouzením vlivu na ochranu osobních údajů dle čl. 35 GDPR. Pověřenec by měl dle výkladového stanoviska WP29 zejména stanovit, zda je nutné provést posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR, jaká metodika při vypracování posouzení vlivu na ochranu osobních údajů by měla být správcem použita či zda bude třeba zpracování posouzení vlivu na ochranu osobních údajů zadat externímu subjektu. Pověřenec by měl dále doporučit, jaká jsou vhodná technická a organizační opatření pro zmírnění rizik pro zájmy a práva subjektů údajů. Součástí působnosti pověřence by mělo být též posouzení, zda bylo posouzení vlivu dle čl. 35 GDPR správce zpracováno dle GDPR formálně správně.

Důležitá je rovněž spolupráce pověřence s dozorovým úřadem. S tím se pojí také působnost pověřence coby kontaktního místa pro dozorový úřad. V případě potřeby by měl pověřenec poskytnout dozorovému úřadu veškerou potřebnou součinnost jménem správce nebo zpracovatele. Správce nebo zpracovatel nesmí pověřenci dávat pokyny, jak jednat v dané oblasti, například jakého výsledku se má dosáhnout, jak prošetřovat stížnost nebo zda a kdy kontaktovat dozorový úřad.

Pověřenec je rovněž dle čl. 38 odst. 4 GDPR kontaktním místem pro subjekty údajů, a to jak vně správce nebo zpracovatele, tak uvnitř správce (vůči zaměstnancům), a to za účelem poskytování informací
a poradenství subjektům údajů.

[50] Čl. 39 odst. 1 písm. a) a b) GDPR a bod 4.1. výkladového stanoviska WP29.

Jednou z nutných podmínek řádného výkonu povinností pověřence je rovněž jakási systematická kontrolní činnost. Z toho vyplývá, že správce, případně zpracovatel musí pověřenci umožnit přístup k veškeré dokumentaci a záznamům navázaným na zpracování osobních údajů (právo na přístup k záznamům a informacím, vč. auditních zpráv, nálezů regulačních orgánů apod.) a podle ustanovení čl. 38 odst. 2 GDPR by mu k tomu měl umožnit i vybudování přiměřeného administrativního aparátu.

Výčet úkolů a povinností pověřence stanovených v GDPR není dle čl. 38 odst. 6 GDPR taxativní. Je tedy možné, aby pověřenec plnil i jiné úkoly a povinnosti, než které nejsou výslovně v GDPR stanoveny, vždy ale musí být zohledněn princip zákazu střetu zájmů (viz výše).

Při poskytování informací a poradenství a v souvislosti s řešením dalších svých úkolů má pověřenec povinnost postupovat čestně a poctivě, ale zároveň zohledňovat také oprávněné zájmy správce nebo zpracovatele.

3.4 Plán

Zhotovitel zpracoval plán zavedení navržených opatření do praxe obce. Jedná se o komplexní plán, jehož činnosti není nutné realizovat v přesně předepsaném pořadí. Vybrané činnosti (např. ustanovení pověřence) může obec provést i bez dokončených činností v přípravné fázi.

Elektronická verze plánu je obsažena v Příloze č. 7.

Tabulka 15 Plán pro obce se základním rozsahem přenesené působnosti

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis	Výstup činnosti
1	Přípravná fáze	Sestavení projektového týmu		Čl. 24	Správce ustanoví projektový tým zahrnující nejméně starostu, účetní, archiváře.	Výstupem je zápis o sestavení týmu, určení odpovědností a stanovení kompetencí jednotlivých členů týmu.
2		Zpracování úvodní analýzy včetně mapování aktuálního zpracování osobních údajů		Čl. 5	Správce zajistí zpracování mapování osobních údajů alespoň v rozsahu definovaném touto systémovou analýzou včetně určení vztahů se zpracovateli.	Výstupem je zpracovaná analýza popisující věrně aktuální stav.
3		Zpracování záznamů o činnostech zpracování		Čl. 6, čl. 30	Správce vytvoří kvalifikované záznamy o činnostech zpracování na základě provedeného mapování.	Výstupem jsou záznamy o činnostech zpracování.
4		Nastavení interních procesů řízení rizik		Čl. 24	Správce ustanoví interní proces řízení rizik.	Výstupem je směrnice o řízení rizik.
5		Vymezení aktiv	Vymezení listinných úložišť	Čl. 5 a čl. 6	Správce detailně vymezí listinná úložiště v návaznosti na záznamy o činnostech zpracování. Součástí je revize práv přístupů k těmto úložištím a zhodnocení jejich stavu z pohledu fyzické a objektové bezpečnosti.	Výstupem je seznam listinných úložišť a zhodnocení jejich stavu.
6			Vymezení nástrojů užívaných pro zpracování osobních údajů ve strukturované		Správce detailně zhodnotí rozsah užívaných aplikací a IS, v rámci kterých zpracovává osobní údaje. Provede zhodnocení úrovně a kvality poskytované legislativní podpory ze strany dodavatele ve vztahu ke GDPR a provede revizi	Výstupem je seznam aplikací a IS zpracovávající OÚ a zhodnocení jejich stavu.

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis	Výstup činnosti
			(databáze) a nestrukturované formě (e-mail, sdílené disky apod.)		práv a oprávnění k aplikacím a IS. Správce provede revizi e-mailu a sdílených disků a odstraní neoprávněně zpracovávaná data s osobními údaji.	
7		Provedení analýzy rizik		Čl. 24	Správce provede analýzu rizik na základě nastavených interních procesů řízení rizik. Výstupem analýzy rizik je prioritizace oblastí, které následně správce řeší organizačními a technickými opatřeními.	Výstupem je analýza rizik. Správce zajistí, aby tato analýza rizik byla známa vedení obce a vedení obce je povinno se závěry analýzy rizik řídit.
8		Zpracování rozdílové analýzy		Čl. 5	Správce zpracuje rozdílovou analýzu s ohledem na závěry mapování a provedené analýzy rizik a to tak, aby v rozdílové analýze byly detailně popsány nedostatky současného stavu oproti cílovému stavu naplnění povinností správce dle GDPR. Správce si v rozdílové analýze určí ideální cílový stav souladu s GDPR.	Výstupem je rozdílová analýza. Správce zajistí, aby tato rozdílová analýza byla známa vedení obce.
9		Vyhodnocení přípravné fáze a určení interních projektů pro implementaci organizačních a technických opatření		Čl. 24 a čl. 25	Správce provede vyhodnocení přípravné fáze a připraví projekty implementace organizačních a technických opatření a zahájí jejich realizaci.	Výstupem je přehled projektů, jejich věcných garantů, detailní popis projektů včetně jejich rozpočtu.
10	Implementační	Ustanovit pověřence		Čl. 37	Správce ustanoví pověřence a	Výstupem je ustanovení pověřence

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis	Výstup činnosti
	fáze				informuje o tomto kroku obec.	včetně uzavření pracovně právního vztahu s pověřencem nebo jiného vztahu, na základě kterého bude pověřenec vykonávat svoji činnost.
11		Přijmout směrnici o ochraně osobních údajů nebo kodexu		Čl. 24	Správce přijme směrnici o ochraně osobních údajů nebo kodex a zajití jeho implementaci do organizace.	Směrnice o ochraně osobních údajů nebo kodex.
12		Proškolit zaměstnance		Čl. 24	Správce proškolí zaměstnance či jiné spolupracující osoby v oblasti ochrany a zpracování osobních údajů a interních pravidel a postupů pro dotčenou problematiku GDPR.	Výstupem je školení a záznam o proškolení zaměstnanců.
13		Implementace organizačních opatření		Čl. 25	Správce určí organizační opatření a provede jejich implementaci v souladu s definicí projektů v přípravné fázi.	Výstupem je zpráva o implementaci organizačních opatření.
14		Implementace technických opatření		Čl. 25	Správce určí technická opatření a provede jejich implementaci v souladu s definicí projektů v přípravné fázi. Správce provede ověření technických opatření např. formou penetračních testů či jiným testováním přijatých opatření s cílem vyhodnotit kvalitu přijatých opatření.	Výstupem je zpráva o implementaci technických opatření.
15		Implementace procesů k realizaci	Nastavení postupů	Čl. 15 až 22	Správce provede nastavení postupů pro zpracování žádostí	Zpráva o testu zpracování žádostí subjektů údajů.

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis	Výstup činnosti
		práv subjektů údajů	zpracování žádostí subjektů údajů		subjektů údajů např. o rozsahu zpracování, uplatnění "práva být zapomenut" a přenositelnosti. Správce připraví technické a organizační zázemí pro zpracování žádostí subjektů údajů včetně přidělení odpovídajících materiálních a lidských zdrojů. Správce je povinen identifikovat úložiště informací obsahující osobní údaje a to jak ve strukturované, tak i nestrukturované formě a v elektronické a listinné podobě a zajistí výkon zpracování žádostí subjektů údajů nad těmito úložišti. Úložiště měl správce určit v provedeném mapování a při zpracování záznamů o činnostech. Správce nesmí opomenout žádné úložiště osobních údajů (listinné archivy, kartotéky, aplikace, IS apod.).	Zdokumentované a zavedené nové procesy pro zpracování žádostí subjektů údajů.
16			Publikace postupů a případných podmínek k uplatnění práv subjektů údajů	Kap. 3	Správce může publikovat na veřejně dostupných zdrojích pokyny k uplatnění práv subjektů údajů.	Publikované pokyny např. formou životních situací na webových stránkách obce.

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis	Výstup činnosti
			na veřejně dostupných zdrojích			
17		Revize zpracovatelských smluv, pokud existují		Čl. 28	Správce s ohledem na provedené mapování a záznamy o činnostech zpracování provede revizi smluv se zpracovateli a zajistí odpovídající kvalitu zpracování osobních údajů včetně sankcí a dalších vhodných mechanismů (např. informační povinnost při kompromitaci zpracovávaných osobních údajů a způsobů řešení či eskalace těchto situací).	Zpráva o revizi zpracovatelských smluv.
18		Revize souhlasů subjektů údajů		Čl. 7	Správce provede revizi souhlasů subjektů údajů na základě provedeného mapování a záznamů o činnostech. Pokud je to nezbytně nutné, vyžádá si informovaný souhlas subjektu údajů ke zpracovávaným osobním údajům v již používaných evidencích a agendách.	Revidované informované souhlasy subjektů údajů.
19		Vyhodnocení implementace organizačních a technických opatření ve vztahu k rozdílové analýze		Čl. 24	Správce provede vyhodnocení implementace organizačních a technických opatření na základě výstupů přípravné fáze. Vedení obce vyhodnocení vezme na	Zpráva o stavu implementace organizačních a technických opatření.

P.č.	Fáze	Činnosti	Relevantní článek GDPR	Popis	Výstup činnosti
				vědomí.	
20	Provozní fáze (od 25. 5. 2018)	Úvodní posouzení stavu zpracování osobních údajů ze strany pověřence a průběžné monitorování stavu zpracování osobních údajů	Čl. 39	Pověřenec provede úvodní posouzení stavu každé situace či činnosti, kdy dochází k nakládání s osobními údaji a to na základě záznamů o činnostech zpracování.	Zpráva o posouzení stavu obsahující případné nálezy a postup jejich nápravy.
21		Pravidelné sebehodnocení Správce formou aktualizace analýzy rizik	Čl. 5	Správce s ohledem na přijaté procesy řízení rizik provede aktualizaci analýzy rizik.	Výstupem je aktualizace analýzy rizik.
22		Pravidelná aktualizace rozdílové analýzy (např. v ročním cyklu)	Čl. 5	Správce zajistí provádění pravidelné aktualizace rozdílové analýzy na základě postupu implementace organizačních a technických opatření zpravidla v ročním cyklu. Aktualizace rozdílové analýzy by měly správci ukázat vývoj a postup v implementaci opatření a vývoj jeho vyspělosti v oblasti zpracování osobních údajů dle požadavků GDPR.	Výstupem je aktualizovaná rozdílová analýza na základě dosavadního postupu implementace organizačních a technických opatření.
23		Aktualizace záznamů o činnostech při změnách nebo implementaci nových agend či povinností obce v porovnání se zpracovaným mapováním a zpracovaných záznamů o činnostech	Čl. 30	V případě, že dojde k úpravě určujícího právního předpisu, účelu nebo ke změně oprávněného zájmu při zpracování osobních údajů, provede správce neprodleně odpovídající aktualizaci záznamů o činnostech zpracování.	Výstupem jsou aktualizované záznamy o činnostech zpracování.

P.č.	Fáze	Činnosti	Relevantní článek GDPR	Popis	Výstup činnosti
24		Uplatňování práv subjektů údajů	Kap. 3	Na webových stránkách obce jsou publikovány pokyny a vzory žádostí k uplatnění práv subjektu údajů.	Výstupem jsou žádosti subjektů údajů a jejich zpracování v řádných termínech a deklarované kvalitě.
25		Vyhodnocení dosavadního průběhu interních projektů z přípravné fáze a jejich případná aktualizace a optimalizace	Čl. 24 a čl. 25	Správce provede vyhodnocení realizace projektů definovaných v přípravné fázi zaměřených na implementaci organizačních a technických projektů. Následně navrhne jejich ukončení, aktualizaci nebo optimalizaci. Toto vyhodnocení je vhodné provádět pravidelně a to alespoň jednou ročně.	Výstupem je zpráva o aktuálním stavu. Tato zpráva by měla být aktualizována nejméně jednou ročně či v závislosti na implementaci organizačních a technických opatření. Zpráva by měla též zhodnotit úroveň vyspělosti obce a měla by být vodítkem pro posuzování přiměřenosti implementovaných opatření.
26		Pravidelné každoroční školení zaměstnanců	Čl. 24	Správce zajistí pravidelné školení zaměstnanců v oblasti zpracování osobních údajů a jejich ochrany a to s cílem průběžného zvyšování povědomí o předmětné problematice.	Výstupem je záznam o proškolení zaměstnanců.

4 Analýza obcí s rozšířenou působností

Zhotovitel provedl mapování pomocí dotazníků formuláři F01 a F02, které jsou blíže popsány v kapitole č. 2.1 Metoda mapování obcí. Tyto dotazníky byly rozeslány na kontaktní osoby jednotlivých obcí společně s metodikou pro vyplnění obou formulářů. Na základě rozeslaných dotazníků bylo následně u obcí s rozšířenou působností domluveno a realizováno individuální místní šetření se zástupci obcí, kde byly řešeny aktuální stavy organizačních a technických opatření obcí s rozšířenou působností. Místní šetření bylo převážně zaměřeno na tyto následující body:

- Shrnutí zaslaných dotazníků. Řešení problematiky, zda obec předala dotazníky a řešení problémů či bodů, kde si vyplňující osoby nebyly jisty ohledně vyplněných údajů.
- Zjištění aktuálních technických opatřeních se zaměřením na ochranu elektronických a fyzických úložišť - zabezpečení serverů, problematika vzdálených přístupů a jejich řízení, zajištění provozu webových stránek obce, používání sdílených disků v rámci úřadu, správa sociálních sítí obce, antivir a firewall, služební mobilní telefony a jejich používání, služební notebooky a jejich používání, systémy na ochranu dat, Wi-Fi, logování uložených záznamů, povolení užití webových úložišť pracovníky úřadu a obce, lokální disky na počítačových sestavách v rámci úřadu a obce, rezervační systémy, E-mail, hostované spisové služby, kamerové systémy, cloudové úložiště, elektronické podpisy, zabezpečení budov, využití flash disků a CD pracovníky úřadu a obce, služební automobily s využitím GPS sledováním pohybu.
- Zjištění aktuálního stavu organizačních opatřeních týkající se ochrany osobních údajů. Zhotovitel zjistil, zda obec disponuje směrnicemi, řády či politikami, které aktuálně řeší problematiku ochrany osobních údajů, pokud úřad disponoval těmito dokumenty, tak Zhotovitel si vyžádal jejich předání k následné analýze.
- Seznam příspěvkových organizací, které spadají pod působnost úřadu a obce.
- Problematika podpůrných evidencí osobních údajů.
- Zjištění aktuálních problémů s ochranou osobních údajů s ohledem na GDPR.

4.1 Analýza zpracování a ochrany osobních údajů v informačních systémech

Zhotovitel provedl místní šetření u těchto obcí s rozšířenou působností:

1. Město Černošice – místní šetření bylo provedeno dne 24. 1. 2018
2. Město Děčín – místní šetření bylo provedeno dne 25.1.2018
3. Město Dobříš – místní šetření bylo provedeno dne 26. 1. 2018
4. Město Cheb místní šetření bylo provedeno dne 23.1.2018
5. Město Karviná – místní šetření bylo provedeno dne 29.1.2018
6. Město Nymburk – místní šetření bylo provedeno dne 31.1.2018
7. Město Tábor - místní šetření bylo provedeno dne 30.1.2018
8. Město Velké Meziříčí - místní šetření bylo provedeno dne 23.1.2018
9. Město Vyškov - místní šetření bylo provedeno dne 24.1.2018

Poznatky zjištěné dotazníkovým a místním šetřením byly využity v rámci analýzy dostupné dokumentace obce s rozšířenou působností a analýzy zpracování a ochrany osobních údajů v informačních systémech obcí s rozšířenou působností. Postupy a výsledky těchto analýz jsou uvedeny v následujících kapitolách. Výsledky z místních šetření na jednotlivých obcích s rozšířenou působností jsou součástí přílohy č. 1 tohoto výstupu. Součástí přílohy č. 1 jsou také vyplněné dotazníky od obcí společně s předanými dokumenty organizačního charakteru (řády, směrnice, politiky).

4.1.1 Analýza provedeného mapování obcí s rozšířenou působností

Zhotovitel provedl analýzu zaslaných dotazníků F01 a F02 od obcí s rozšířenou působností dle metody popsané v kapitole 2.1 Metoda mapování obcí.

Zhotovitel na základě analýzy vytvořil jednu vzorovou obec s rozšířenou působností, u které vytvořil seznam všech agend, ve kterých obce s rozšířenou působností zpracovávají osobní údaje; tento seznam je součástí Přílohy č. 5.

Ke každé agendě Zhotovitel popsal následující položky:

- **Název agendy** – uvedení názvu agendy či jiného titulu zpracování osobních údajů;
- **Zpracovávané osobní údaje** – výčet všech osobních údajů, které jsou součástí dané agendy či titulu zpracování v kontextu obce nebo úřadu;
- **Právní základ zpracování** – uvedení legislativního předpisu upravující danou agendu nebo titulu zpracování;
- **Právní důvod zpracování** – uvedení právního důvodu zpracování osobních údajů úřadem (PP – právní povinnost, Souhlas – udělení souhlasu subjektu osobních údajů, Splnění smlouvy – zpracování osobních údajů na základě smlouvy);
- **Přenositelnost** – posouzení práva na přenositelnost údajů dle článku 20 GDPR;
- **Námitka** – posouzení práva vznést námitku dle článku 21 GDPR;
- **Archivní doba** – přiřazení spisového znaku, skartačního znaku a lhůty dle vzorového spisového plánu vydaného MV ČR (dostupné na *http://www.mvcr.cz/clanek/vzory.aspx*) nebo spisového a skartačního řádu posuzovaných obcí.

Na základě dotazníkového a místního šetření byla Zhotovitelem identifikována společná aktiva, která zpracovávají osobní údaje pro obce se základním rozsahem přenesené působnosti. K jednotlivým aktivům bylo Zhotovitelem přiřazeno označení, zda se jedná o listinné nebo elektronické úložiště osobních údajů (Elektronické úložiště - "E", Listinné úložiště - "L").

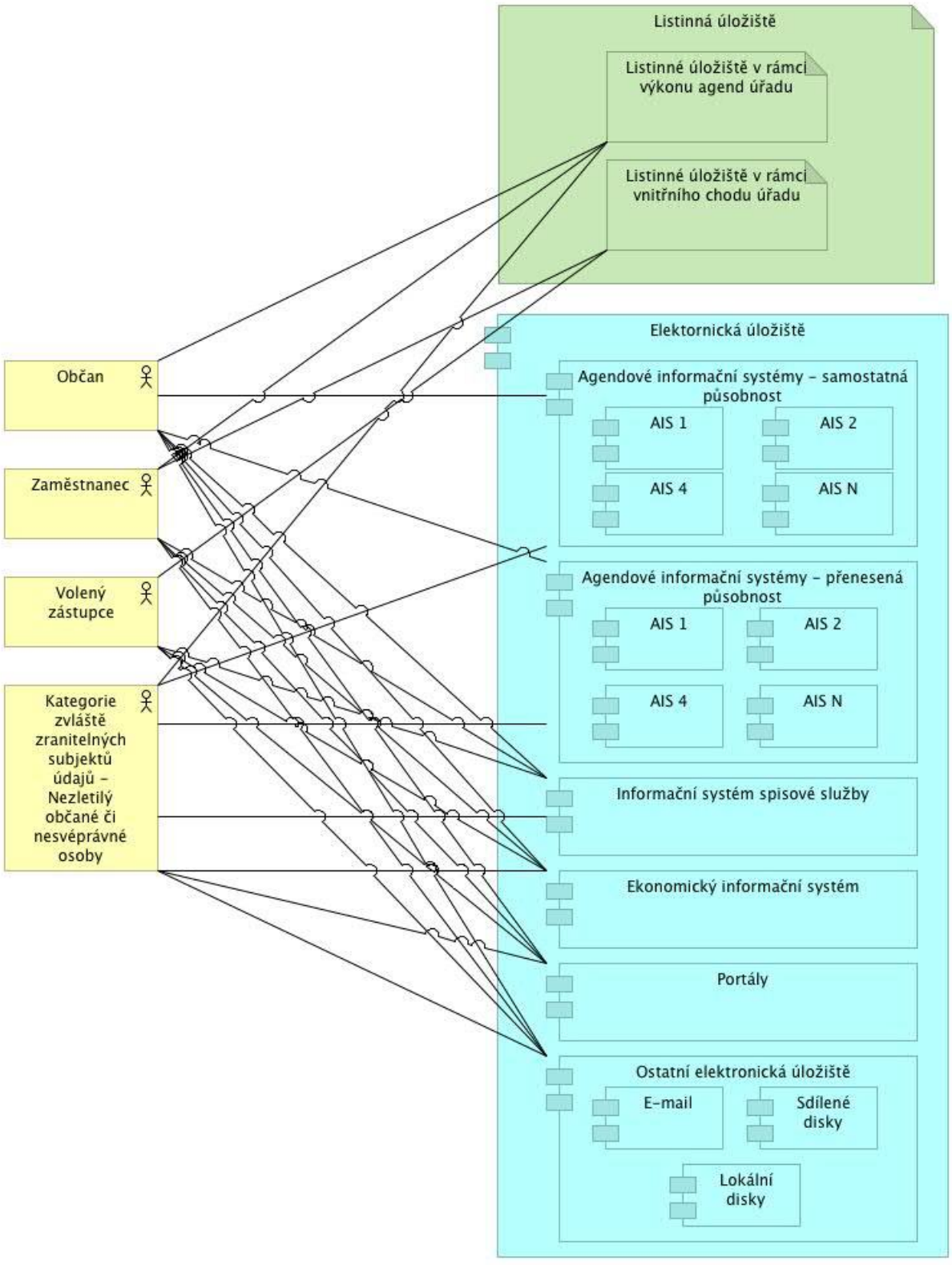
Zhotovitel určil na základě dotazníkového šetření a sběru souvisejících interních aktů řízení následující výčet identifikovaných aktiv:

- **Listinné úložiště v rámci výkonu agend úřadu (L)** – veškeré listiny, které jsou uloženy na úřadě a souvisí s výkonem agend úřadu;
- **Listinné úložiště v rámci vnitřního chodu úřadu (L)** – veškeré listiny, které jsou uloženy na úřadě a souvisejí s vnitřním chodem úřadu (příjem a propuštění zaměstnanců, účetnictví atd.);
- **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)** – e-mail, sdílené disky, lokální disky na počítačových sestavách.

Na základě podrobné systematické analýzy dotazníkového šetření byly Zhotovitelem identifikovány jednotlivé role subjektu údajů a následně k nim byla přiřazena odpovídající aktiva. Tyto vazby jsou uvedeny v tabulce č. 16 a dále pak na Obrázku č.2.

Tabulka 16 Role subjektu osobních údajů

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 (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 (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 (E) • Ostatní elektronická úložiště (E)
Zvláště zranitelná kategorie subjektu údajů – Nezletilí občané či 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 (E) • Ostatní elektronická úložiště (E)



Obrázek 2 Role subjektu osobních údajů a přiřazená aktiva

4.1.2 Analýza dostupné dokumentace úřadu obce

Poskytnutá dokumentace u obcí s rozšířenou působností byla na první pohled kvalitativně vyspělejší a obsáhlejší než u obcí se základním rozsahem přenesené působnosti. Obce s rozšířenou působností poskytly pro účely této analýzy následující dokumenty (název konkrétního dokumentu mohl být odlišný):

- Organizační řád;
- Pracovní řád;
- Skartační a spisový řád;
- Bezpečnostní politika ISVS;
- Informační koncepce ISVS;
- Směrnice na ochranu osobních údajů;
- Zásady pro používání výpočetní techniky.

Organizační a pracovní řád

Poskytnuté Organizační řády obsahovaly detailní informace o pracovních náplních jednotlivých odborů, úseků a oddělení. Žádný předaný organizační řád nebyl doposud aktualizován do souladu s GDPR a neobsahoval informace o roli pověřence pro ochranu osobních údajů.

Pracovní řády definují základní práva a povinnosti zaměstnanců úřadů, včetně důležitých atributů personální bezpečnosti. Taktéž tyto Pracovní řády obcí s rozšířenou působností stanovovaly procesy vzniku, změny a skončení pracovního poměru. Obsah těchto procesů nelze považovat za dostatečný tak, jak by bylo žádoucí pro zajištění ochrany bezpečnosti informací (viz vyhláška o kybernetické bezpečnosti). Lze konstatovat, že taktéž Pracovní řády bude nutné aktualizovat pro uvedení do souladu s požadavky GDPR. Zejména se jedná o činnosti pověřence pro ochranu osobních údajů, nové procesy implementující práva subjektů údajů a vylepšení procesů informační bezpečnosti (například procesy personální bezpečnosti – pravidelná školení zaměstnanců, procesy vzniku, změny a skončení pracovního poměru apod.).

Spisový a skartační řád

Obdobně jako obce se základním rozsahem přenesené působnosti i obce s rozšířenou působností využily vzorový skartační plán uvedený na stránkách MV. Skartační řády obcí s rozšířenou působností byly vypracovány kvalitně, dokonce obsahují i některé základní prvky ochrany osobních údajů (například procesy ochrany osobních údajů při umožnění nahlížení do dokumentů oprávněným žadatelům apod.)

V roce 2017 byla publikována na stránkách Ministerstva vnitra ČR novelizovaná verze Národního standardu pro elektronické systémy spisové služby (viz http://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx), která definovala nové požadavky na elektronické spisové služby a mohla mít tím pádem i dopad i do skartačních řádů. Žádný poskytnutý skartační řád nebyl po tomto datu novelizován, ačkoliv novela například zasahovala do základního názvosloví spisové služby (odstraněn pojem záznam, zaveden pojem koncept a zásilka).

Bezpečnostní dokumentace

Vybrané obce s rozšířenou působností měly vždy vypracovanou bezpečnostní dokumentaci ISVS. Z analýzy předaných podkladových materiálů je patrné, že se jedná o něco, co by se dalo označit jen jako „minimální úroveň bezpečnosti“. Rozhodně se nejedná o komplexní systém řízení bezpečnosti informací. Dokumentace neodpovídá svým rozsahem požadavkům zákona o kybernetické bezpečnosti a tedy ani rozsahu dle ČSN ISO/IEC 27001. Tento stav vychází z účelu dokumentů, kterým je především formální zajištění požadavků na provoz ISVS. Faktický dopad těchto bezpečnostních politik na chod úřadu je zpravidla minimální a pro systematickou ochranu informací by

bylo nutné je významně přepracovat. Nápomocným předpisem je již výše zmíněný zákon o kybernetické bezpečnosti.

V předmětných obcích byly též zavedeny směrnice pro ochranu osobních údajů. Tyto směrnice byly vytvořeny na základě zákona o ochraně osobních údajů a jsou dobrým základem pro implementaci GDPR do chodu úřadu. Obce si jsou vědomy, že je nutné tyto směrnice aktualizovat a dát do souladu s GDPR, ale vyčkávají a očekávají, že MV ČR poskytne na svých stránkách vzorovou Směrnici o ochraně osobních údajů, která bude nové požadavky GDPR implementovat.

Shrnutí

Obecně lze konstatovat, že v oblasti dokumentace jsou obce s rozšířenou působností připraveny na implementaci GDPR výrazně lépe než obce se základním rozsahem přenesené působnosti. Oproti obcím se základním rozsahem přenesené působnosti měla majorita Vybraných obcí implementovanou Směrnici na ochranu osobních údajů, dále základní Bezpečnostní politiky ISVS včetně informační koncepce ISVS a Směrnici pro užívání výpočetní techniky. Některé obce měly vypracovány i další detailní směrnice pro zvýšení bezpečnosti informačního systému ve vybraných oblastech – Směrnice pro užívání mobilních telefonů a přenosných zařízení, Využívání sítě internet, Využívání emailu, Řízení personálních změn apod.

Rozšířeným nedostatkem naopak byla chybějící systemizace pro přidělování uživatelských oprávnění v informačních systémech. Organizační řád nebyl dopracován v takovém detailu, aby u každé pracovní pozice bylo definováno, do kterého informačního systému má mít zaměstnanec přístup a v jaké roli. Přidělování práv neprobíhá automatizovaně na základě přidělení role zaměstnance, ale je nutné provést ruční přiřazení administrátory systémů.

4.1.3 Modelová obec s rozšířenou působností

Na základě mapování Vybraných obcí s rozšířenou působností Zhotovitel stanovil vzorovou obec, ve které se spojují základní a společné věci vztahující se k agendám, informačním systémům, listinným a elektronickým úložištím obsahující osobní údaje a interním aktům řízení a dokumentace.

Agendy a činnosti

Úplný výpis vykonávaných agend a činností Vzorové obce je uveden v příloze č. 5. Mezi společné agendy, které spojují obce s rozšířenou působností, patří tyto:

- Agenda stavebního úřadu;
- Agendy spojené s chodem úřadu či obce (účetnictví, personalistika, veřejné zakázky atd.).
- Cestovní doklady;
- Evidence obyvatel;
- Místní poplatky;
- Občanské průkazy;
- Poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů;
- Řidičské průkazy a evidence vozidel;
- Spisová služba;
- Vedení matriky;
- Volby a jejich agenda;
- Živnostenská agenda;

Informační systémy a portály

Vzorová obec s rozšířenou působností disponuje těmito informačními systémy a portály:

- Informační systém spisové služby – Úložiště IS je provozováno na vlastních serverech obce, která disponuje dvěma oddělenými datovými centry;
- Agendové informační systémy v rámci přenesené působnosti – Obec je uživatelem dvou typů informačních systémů a to systémů, které jsou hostovány v gesci věcného gestora (např. IS evidence obyvatel, IS pro výkon dopravně správních agend) a aplikací či IS, kde se obec přímo podílí na provozu těchto aplikací či IS (např. rybářské lístky, myslivost). Úložiště těchto aplikací a IS je provozováno na vlastních serverech obce, která může disponovat dvěma oddělenými datovými centry;
- Agendové informační systémy v rámci samostatné působnosti – Úložiště IS je provozováno na vlastních serverech obce, která disponuje dvěma oddělenými datovými centry;
- Ekonomický informační systém – Vzorová obec disponuje Ekonomickým IS, který obsahuje účetnictví obce, obecní rozpočty, evidence zaměstnanců a správa mezd. Úložiště IS je provozováno na vlastních serverech obce, která disponuje dvěma oddělenými datovými centry;
- Portály – Vzorová obec disponuje jednou obecní webovou stránkou, která obsahuje systém pro objednání občanů na jednotlivé agendy úřadu. Dále obec disponuje a spravuje webové stránky pro některé své příspěvkové organizace. Webové stránky jsou spravovány externím dodavatelem, se kterým má obec uzavřenou smlouvu.

Listinná úložiště obsahující osobní údaje

Vzorová obec disponuje docházkovým systém, který sleduje přístupy do budovy, kde jsou umístěny listiny a zároveň disponuje kamerovým systémem vně i uvnitř budov s listinnými úložišti. Listiny se nacházejí v uzamykatelných místnostech bez bezpečnostních dveřích a zámků. Skříně, kde jsou uloženy listiny, jsou opatřeny zámkem, který ale nepředstavuje zásadní odpor k možnému vnějšímu útoku. Místnosti nejsou opatřeny elektronickými zabezpečovacími systémy a bezpečnostními systémy.

Elektronická úložiště

Vzorová obec disponuje vlastními oddělenými datovými centry, které slouží jako úložiště pro některé IS a dále pro sdílené složky v rámci celého úřadu či obce. Přístupová práva do složek je řízen odborem IT, a to na úrovni jednotlivých odborů. Servery a datová centra nedisponují pokročilými systémy na ochranu dat včetně logování. Servery jsou chráněny základními antivirovými programy. Vnitřní síť úřadu je oddělena od veřejné sítě. Lokální úložiště na PC sestavách není nijak zálohováno a vnitřními předpisy není upraveno jeho používání. Úřad a obec poskytují pracovní notebooky, které disponují základní ochranou před počítačovými viry. Dále obec poskytuje mobilní telefony, které nejsou nijak důsledně chráněny ze strany úřadu či obce.

Interní akty řízení a dokumentace

Vzorová obec disponuje těmito interními akty řízení a dokumentace:

- Bezpečnostní politika ISVS;
- Informační koncepce ISVS;
- Organizační řád;
- Pracovní řád;
- Skartační a spisový řád;
- Směrnice na ochranu osobních údajů;
- Zásady pro používání výpočetní techniky.

Bližší popis těchto interních aktů řízení vzorové obce je uveden v kapitole č. 4.1.2 Analýza dostupné dokumentace.

Personální zajištění

Na správě obce se podílí profesionální tým. Obec má kvalifikovaného správce IT a dedikovaného archiváře.

4.1.4 Rizika zpracování vzhledem k rozsahu, kontextu, povaze a účelům zpracování osobních údajů

Na základě definovaných primárních aktiv z kapitoly č. 4.1.1 Zhotovitel provede jejich ohodnocení, a to dle stupnice, která je definována v kapitole č. 2.4.1 Metoda určení a ohodnocení aktiv. Zhotovitel podotýká, že tato analýza rizik je prováděna z pohledu subjektu údajů dle GDPR. Hodnota aktiv a další stanovení parametrů analýzy rizik jsou stanoveny z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

Ohodnocení aktiv pro účely analýzy rizik je uvedeno v tabulce č. 17.

Tabulka 17 Hodnocení aktiv

Název aktiva	Stupeň hodnocení	Popis hodnocení
Listinné úložiště v rámci výkonu agend úřadu	5	Zhotovitel ohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Listinné úložiště v rámci vnitřního chodu úřadu	3	Zhotovitel ohodnotil aktivum na střední stupeň, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. Aktivum nedisponuje takovou širokou škálou osobních údajů jako v případě úložiště spojené s výkonem agend obce vůči občanům. Zhotovitel nepředpokládá že v rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva by došlo k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít zásadní vliv na fungování

Název aktiva	Stupeň hodnocení	Popis hodnocení
		obcí či úřadů.
Informační systém spisové služby	5	Zhotovitel ohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Agendové informační systémy – samostatná působnost	5	Zhotovitel ohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Agendové informační systémy – přenesená působnost	5	Zhotovitel ohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů,

Název aktiva	Stupeň hodnocení	Popis hodnocení
		které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Ekonomický informační systém	**5**	Zhotovitel ohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Portály	**3**	Zhotovitel ohodnotil aktivum na střední stupeň, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. Aktivum nedisponuje takovou širokou škálou osobních údajů jako v případě úložiště spojené s výkonem agend obce vůči občanům. V rámci

Název aktiva	Stupeň hodnocení	Popis hodnocení
		ztráty, poškození a narušení bezpečnosti tohoto aktiva nedojde k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít vliv na fungování obcí či úřadů.
Ostatní elektronické úložiště	**3**	Zhotovitel ohodnotil aktivum na střední stupeň, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. V rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva nedojde k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít vliv na fungování obcí či úřadů.

Zhotovitel v kapitole č. 2.4.2 Hrozby a identifikace pravděpodobnosti hrozeb uvedl seznam obvyklých hrozeb dle standardů a hrozeb týkajících se ochrany osobních údajů vycházejících z GDPR či z dané problematiky. Zhotovitel k jednotlivým hrozbám přiřadil pravděpodobnost uplatnění jednotlivých hrozeb, a to ke každému identifikovanému aktivu. Stupnice ohodnocení aktiv je uvedena v kapitole č. 2.4.2 Hrozby a identifikace pravděpodobnosti hrozeb. Zhotovitel uvedl do hodnocení výši stupně pravděpodobnosti uplatnění hrozby včetně popisu zvolení dané výše pravděpodobnosti. Hodnocení pravděpodobnosti uplatnění hrozeb na jednotlivá aktiva je uvedeno v tabulce č. 18 na následující straně.

Tabulka 18 Hodnocení pravděpodobnosti hrozeb k aktivům

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Listinné úložiště v rámci výkonu agend úřadu	**Vnější útoky**	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce s rozšířenou působností disponují širokým objemem osobních údajů, proto je pravděpodobnost stanovena Zhotovitelem na střední úroveň.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Uplatnění této hrozby je nepravděpodobné, jelikož obce s rozšířenou působností disponují technologiemi v zajištění listinných úložišť, které zabraňují vzniku technických chyb, a tedy jejich pravděpodobnost výskytu je na nízké úrovni.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí s rozšířenou působností na střední úrovni, jelikož tyto obce sice většinou disponují interními akty, které jsou závazné a upravují procesy nakládání s listinami, ale počet zaměstnanců je daleko vyšší než u obcí se základním rozsahem působnosti, tak i fluktuace na jednotlivých pozicích v rámci úřadu těchto obcí je ve vyšší míře.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí s rozšířenou působností na střední úrovni, jelikož tyto obce sice většinou disponují interními akty, které jsou závazné a upravují procesy nakládání s listinami, ale počet zaměstnanců je daleko vyšší než u obcí se základním rozsahem působnosti, tak i fluktuace na jednotlivých pozicích v rámci úřadu těchto obcí je ve vyšší míře.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce s rozšířenou působností ne vždy disponují takovými opatřeními, které by znamenali výraznou překážku pro neoprávněných přístup třetích osob, a tedy i zneužití osobních údajů, proto je pravděpodobnost stanovena na střední úroveň.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Zhotovitel nepředpokládá výrazné překážky v rámci dostupnosti OÚ.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. U obcí s rozšířenou působností Zhotovitel předpokládá zpracování osobních údajů ve velkém objemu, a tedy pravděpodobnost ztráty je na střední úrovni.
	Narušení práv a svobod subjektu údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na vysokou úroveň. S ohledem na ostatní hrozby je velkou pravděpodobností, že by následně došlo k narušení práv a svobod subjektu údajů.
Listinné úložiště v rámci vnitřního chodu úřadu	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Zhotovitel nepovažuje informace o vnitřním chodu úřadu za tak atraktivní pro vnější útoky jako informace získané z úložiště pracující s informacemi spojené s výkonem agend úřadu.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Uplatnění této hrozby je nepravděpodobné, jelikož obce s rozšířenou působností disponují technologiemi v zajištění listinných úložišť, které zabraňují vzniku technických chyb, a tedy jejich pravděpodobnost výskytu je na nízké úrovni.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí s rozšířenou působností na střední úrovni, jelikož tyto obce sice většinou disponují interními akty, které jsou závazné a upravují procesy nakládání s listinami, ale počet zaměstnanců je daleko vyšší než u obcí se základním rozsahem působnosti, tak i fluktuace na jednotlivých pozicích v rámci úřadu těchto obcí je ve vyšší míře.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obcí s rozšířenou působností na nízké úrovni, jelikož manipulaci s tímto aktivem je v pravomoci úzkého okruhu zaměstnanců úřadu.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce s rozšířenou působností ne vždy disponují takovými opatřeními, které by znamenali výraznou překážku pro neoprávněných přístup třetích osob, a tedy i zneužití osobních údajů, proto je pravděpodobnost stanovena na střední úroveň.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Zhotovitel nepředpokládá výrazné překážky v rámci dostupnosti OÚ.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. U obcí s rozšířenou působností Zhotovitel předpokládá zpracování osobních údajů ve velkém objemu, a tedy pravděpodobnost ztráty je na střední úrovni.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. S ohledem na ostatní hrozby je pravděpodobnost, že by následně došlo k narušení práv a svobod subjektu údajů.
Informační systém spisové služby	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Informační systém spisové služby u obcí s rozšířenou působností je většinou dobře chráněn a má svojí dlouhou tradici.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Střední úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu možného selhání technického zajištění IS spisové služby, tak i vnějších jevů jako je výpadek elektřiny apod.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Pravděpodobnost je na střední úrovni, jelikož obce s rozšířenou působností nedisponují takovými opatřeními, které by zamezovali neoprávněnému přístupu k OÚ, např. aktivní řízení přístupů atd.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích s rozšířenou působnosti je na nízké úrovni, a to z důvodu vyspělosti IS spisové služby a jeho úložiště, které je většinou zálohováno do jiné lokality než je produkční server.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň je zde zapříčiněna vyspělostí IS spisové služby a jejich dlouhodobé používání.
Agendové informační systémy – samostatná působnost	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. AIS u obcí s rozšířenou působností je většinou dobře chráněn včetně elektronického úložiště dat. Obce mají většinou s dodavateli uzavřené servisní smlouvy.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu nízké pravděpodobnosti selhání technického zajištění AIS.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Obce s rozšířenou působností disponují příručkami popisující procesy v rámci AIS a aktivně probíhají školení nových i stávajících zaměstnanců.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Obce s rozšířenou působností disponují příručkami popisující procesy v rámci AIS a aktivně probíhají školení nových i stávajících zaměstnanců.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Přístupy do AIS jsou na obcích s rozšířenou působností zpravidla centrálně řízeny odborem IT.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích s rozšířenou působnosti je na nízké úrovni, a to z důvodu vyspělosti AIS a jeho úložiště, které je většinou zálohováno na server v jiné lokalitě, než je primární server.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň je zde zapříčiněna vyspělostí AIS a jejich dlouhodobé používání.
Agendové informační systémy – přenesená působnost	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. AIS u obcí s rozšířenou působností je většinou dobře chráněn včetně elektronického úložiště dat. Obce mají většinou s dodavateli uzavřené servisní smlouvy.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu nízké pravděpodobnosti selhání technického zajištění AIS.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Obce s rozšířenou působností disponují příručkami popisující procesy v rámci AIS a aktivně probíhají školení nových i stávajících zaměstnanců.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Obce s rozšířenou působností disponují příručkami popisující procesy v rámci AIS a aktivně probíhají školení nových i stávajících zaměstnanců.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Přístupy do AIS jsou na obcích s rozšířenou působností zpravidla centrálně řízeny odborem IT.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích s rozšířenou působnosti je na nízké úrovni, a to z důvodu vyspělosti AIS a jeho úložiště, které je většinou zálohováno na server v jiné lokalitě, než je primární server.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň je zde zapříčiněna vyspělostí AIS a jejich dlouhodobé používání.
Ekonomický informační systém	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ekonomický IS u obcí s rozšířenou působností je většinou dobře chráněn včetně elektronického úložiště dat. Obce mají většinou s dodavateli uzavřené servisní smlouvy.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Střední úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu možného selhání technického zajištění Ekonomického IS, tak i vnějších jevů jako je výpadek elektřiny apod.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce s rozšířenou působností disponují velkou zaměstnackou základnou a tudíž je pravděpodobnější, že dojde k této hrozbě.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích s rozšířenou působností Zhotovitel nepředpokládá častější uplatnění dané hrozby.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Přístupy do Ekonomického IS jsou na obcích s rozšířenou působností zpravidla centrálně řízeny odborem IT.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Ztráta osobních údajů v obcích s rozšířenou působnosti je na nízké úrovni, a to z důvodu vyspělosti Ekonomického IS a jeho úložiště, které je většinou zálohováno na server v jiné lokalitě, než je primární server.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň je zde zapříčiněna vyspělostí Ekonomického IS a jeho dlouhodobého používání.
Portály	**Vnější útoky**	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na vysokou úroveň. Využívané portály obcí s rozšířenou působností nedisponují vyspělou ochranou a mohou se stát terčem vnějších útoků.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Technické zajištění portálů není na vysoké úrovni a může dojít k technickým chybám.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce s rozšířenou působností nemají pevně stanovené procesy prací s Portály.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích s rozšířenou působností Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích s rozšířenou působností Zhotovitel nepředpokládá častější uplatnění dané hrozby.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň.
	Narušení práv a svobod subjektu údajů	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň.
Ostatní elektronické úložiště	**Vnější útoky**	1	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na velmi nízkou úroveň. Toto aktivum nedisponuje takovým rozsahem osobních údajů, aby bylo terčem vnějších útoků.
	Technické chyby	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na vysokou úroveň. Tato úroveň byla stanovena z důvodu možného technického selhání těchto úložišť.
	Lidský faktor	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na vysokou úroveň. Pravděpodobnost lidského faktoru je zde vysoká a může dojít k znehodnocení těchto úložišť.
	Narušení integrity OÚ	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na vysokou úroveň. Pravděpodobnost narušení integrity je zde vysoká a může dojít k znehodnocení těchto OÚ.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
	Neoprávněný přístup	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na vysokou úroveň. Aktuální zabezpečení ostatních elektronických úložišť je příčinou vysoké pravděpodobnosti uplatnění této hrozby.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň.

Zhotovitel na základě zjištěných informací z mapování obcí a vytvoření Vzorové obce přiřadil jednotlivým hrozbám zranitelnosti jednotlivých hrozeb, a to ke každému identifikovanému aktivu. Zhotovitel uvedl do hodnocení výši stupně zranitelnosti aktiv vůči hrozbám včetně popisu zvoleného stupně zranitelnosti. Hodnocení zranitelnosti aktiv vůči hrozbám je uvedeno v tabulce č. 19.

Tabulka 19 Zranitelnosti aktiv vůči hrozbám

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
Listinné úložiště v rámci výkonu agend úřadu	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Zabezpečení listinných úložišť je v obcích s rozšířenou působností na dostačující úrovni. Listiny jsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy, představují zásadní překážku pro vnější útoky. Dále obce disponují interními akty, které upravují procesy nakládání s listinami.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Ochrana před technickými chyby či vnějších vlivů nedosahuje u obcí s rozšířenou působností takové úrovně, aby byla zranitelnost ohodnocena na nízké úrovni. Obce většinou nedisponují zabezpečovacími systémy obsahující např. tepelný detektor či kouřový detektor.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce disponují interními akty, které popisují procesy nakládání s listinami, ale zároveň se jedná o velký objem listin v rámci agend obcí, kdy může dojít k této hrozbě.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce disponují interními akty, které popisují procesy nakládání s listinami, ale zároveň se jedná o velký objem listin v rámci agend obcí, kdy může dojít k této hrozbě.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Obce s rozšířenou působností disponují takovým technickým zajištěním, které monitoruje vstupy do budov obcí či úřadů.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Zabezpečení listinných úložišť je v obcích s rozšířenou působností na dostačující úrovni. Listiny jsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy, představují zásadní překážku pro vnější útoky. Dále obce disponují interními akty, které upravují procesy nakládání s listinami.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň, a to i s ohledem zranitelnosti aktiva vůči ostatním hrozbám.
Listinné úložiště v rámci vnitřního chodu úřadu	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Zabezpečení listinných úložišť je v obcích s rozšířenou působností na dostačující úrovni. Listiny jsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy, představují zásadní překážku pro vnější útoky. Dále obce disponují interními akty, které upravují procesy nakládání s listinami.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Ochrana před technickými chyby či vnějších vlivů nedosahuje u obcí s rozšířenou působností takové úrovně, aby byla zranitelnost ohodnocena na nízké úrovni. Obce většinou nedisponují zabezpečovacími systémy obsahující např. tepelný detektor či kouřový detektor.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce disponují interními akty, které popisují procesy nakládání s listinami, ale zároveň se jedná o velký objem listin v rámci agend obcí, kdy může dojít k této hrozbě.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce disponují interními akty, které popisují procesy nakládání s listinami, ale zároveň se jedná o velký objem listin v rámci agend obcí, kdy může dojít k této hrozbě.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Obce s rozšířenou působností disponují takovým technickým zajištěním, které monitoruje vstupy do budov obcí či úřadů.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Zabezpečení listinných úložišť je v obcích s rozšířenou působností na dostačující úrovni. Listiny jsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy, představují zásadní překážku pro vnější útoky. Dále obce disponují interními akty, které upravují procesy nakládání s listinami.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň, a to i s ohledem zranitelnosti aktiva vůči ostatním hrozbám.
Informační systém spisové služby	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana informačního systému spisové služby je na vysoké úrovni a úložiště jsou dostatečně zabezpečena.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. IS spisové služby jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS a dochází k proškolení zaměstnanců.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS a dochází k proškolení zaměstnanců.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Obce s rozšířenou působností aktivně řídí přístupy do IS spisové služby, kdy je vše centrálně řízeno odborem IT na základě žádostí vedoucích odborů.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou před úmyslným exportem dat u IS či výmaz u IS spisové služby. Zaměstnanci běžně mohou používat externí disky i cloudová úložiště. V rámci serverů obce disponují pokročilou ochranou dat.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Agendové informační systémy – samostatná působnost	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana AIS je na vysoké úrovni a úložiště jsou dostatečně zabezpečena.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana AIS je na vysoké úrovni a úložiště jsou dostatečně zabezpečena, AIS jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS a u obcí s rozšířenou působností nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS a u obcí s rozšířenou působností nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na aktivní řízení přístupů do AIS, ale zároveň se jedná o velký počet přístupů, které jdou napříč celou obcí či úřadem, které lze snadno zneužít.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou před úmyslným exportem dat u IS či výmaz u AIS. Zaměstnanci běžně mohou používat externí disky i cloudová úložiště. V rámci serverů obce disponují pokročilou ochranou dat.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
Agendové informační systémy – přenesená působnost	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana AIS je na vysoké úrovni a úložiště jsou dostatečně zabezpečena.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana AIS je na vysoké úrovni a úložiště jsou dostatečně zabezpečena, AIS jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na aktivní řízení přístupů do AIS, ale zároveň se jedná o velký počet přístupů, které jdou napříč celou obcí či úřadem, které lze snadno zneužít.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou před úmyslným exportem dat u IS či výmaz u AIS. Zaměstnanci běžně mohou používat externí disky i cloudová úložiště. V rámci serverů obce disponují pokročilou ochranou dat.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Ekonomický informační systém	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana Ekonomického IS je na vysoké úrovni a úložiště jsou dostatečně zabezpečena.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana Ekonomického IS je na vysoké úrovni a úložiště jsou dostatečně zabezpečena. Ekonomické IS jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici Ekonomických IS na obcích s rozšířenou působností, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným Ekonomickým IS.
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na aktivní řízení přístupů do Ekonomického IS, ale zároveň se jedná o velký počet přístupů, které jdou napříč celou obcí či úřadem, které lze snadno zneužít.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou před úmyslným exportem dat u IS či výmaz u Ekonomického IS. Zaměstnanci běžně mohou používat externí disky i cloudová úložiště. V rámci serverů obce disponují pokročilou ochranou dat.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Portály	**Vnější útoky**	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obce nedisponují ochranou portálů před vnějšími útoky.
	Technické chyby	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Portály jsou většinou spravovány přímo obcemi a nedisponují takovou ochranou před technickými chybami.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb administrátory portálů obce.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb redaktory a administrátory portálů obce.
	Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Zhotovitel nepředpokládá neoprávněných přístup na portály obce.
	Narušení dostupnosti	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.
	Ztráta osobních údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Portály disponují jen základní ochranou a je možné že dojde ke ztrátě dat.
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Ostatní elektronické úložiště	**Vnější útoky**	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Obce mají ostatní elektronická úložiště odděleny od veřejně dostupné sítě a aktivně řídí přístupy do jednotlivých úložišť.
	Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Obce provádějí zálohu dat.
	Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb uživatelů ostatních elektronických úložišť, kdy dochází ke ztrátě či jinému znehodnocení dat obsahující osobní údaje.

Název aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení integrity OÚ	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na možnost způsobení chyb uživatelů ostatních elektronických úložišť, kdy dochází ke ztrátě či jinému znehodnocení dat obsahující osobní údaje.
	Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem volný přístup do prostor budov obcí či úřadů, kde je v těchto prostorách možnost připojení do ethernetových výstupů, a tedy přístupu do sítě.
	Narušení dostupnosti	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň.
	Ztráta osobních údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Obce nedisponují dostačující ochranou před ztrátou osobních údajů z ostatních elektronických úložišť. Obce nedisponují funkcí logování záznamů atd.
	Narušení práv a svobod subjektu údajů	4	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká úroveň zranitelnosti tohoto aktiva byla Zhotovitelem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

V tabulce č. 20 jsou shrnuty úrovně pravděpodobnosti uplatnění jednotlivých hrozeb k vybraným aktivům.

Tabulka 20 Pravděpodobnost hrozeb k jednotlivým aktivům

Aktivum	Hodnota aktiva	Pravděpodobnost							
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů
Listinné úložiště v rámci výkonu agend úřadu	5	3	2	3	3	3	2	3	4
Listinné úložiště v rámci vnitřního chodu úřadu	3	2	2	3	2	3	2	3	3
Informační systém spisové služby	5	2	3	2	2	3	3	2	2
Agendové informační systémy - samostatná působnost	5	2	2	2	2	2	3	2	2
Agendové informační systémy - přenesená působnost	5	2	2	2	2	2	3	2	2
Ekonomický informační systém	5	2	3	3	2	2	3	2	2
Portály	3	4	3	3	2	2	3	2	2
Ostatní elektronické úložiště	3	1	4	4	4	4	3	3	3

Následně byly Zhotovitelem stanoveny úrovně zranitelnosti jednotlivých aktiv vůči stanoveným hrozbám, které jsou uvedeny v tabulce č. 21.

Tabulka 21 Zranitelnosti aktiva vůči hrozbám

Aktivum	Hodnota aktiva	Zranitelnosti							
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů
Listinné úložiště v rámci výkonu agend úřadu	5	2	3	3	3	2	2	3	3
Listinné úložiště v rámci vnitřního chodu úřadu	3	2	3	3	3	2	2	3	3
Informační systém spisové služby	5	2	2	2	2	2	2	3	3
Agendové informační systémy - samostatná působnost	5	2	2	2	2	3	2	3	3
Agendové informační systémy - přenesená působnost	5	2	2	2	2	3	2	3	3
Ekonomický informační systém	5	2	2	2	3	3	2	3	3
Portály	3	3	3	3	3	2	3	3	3
Ostatní elektronické úložiště	3	2	2	3	3	3	2	4	4

V tabulce č. 22 je uvedeno závěrečné rizikové skóre k jednotlivým aktivům včetně indikátorů:

- celková míra rizika hrozby – indikátor ukazuje celkové míry rizika hrozeb dle jejich výše. Dle výše indikátoru je tedy patrné, které hrozby jsou pro obec nejzávažnější a mohou zde směřovat technická a organizační opatření;
- celkové míra rizika aktiva – indikátor ukazuje celkové míry rizika aktiv dle jejich výše. Dle výše indikátoru je tedy patrné, která aktiva jsou nejnáchylnější a potřebují zvýšenou pozornost či ochranu ze strany obcí.

Tabulka 22 Rizikové skóre

Aktivum	Hodnota aktiva	Rizikové skóre								
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů	*Indikátor celkové míry rizika aktiva*
Listinné úložiště v rámci výkonu agend úřadu	5	30	30	45	45	30	20	45	60	305
Listinné úložiště v rámci vnitřního chodu úřadu	3	12	18	27	18	18	12	27	27	159
Informační systém spisové služby	5	20	30	20	20	30	30	30	30	210
Agendové informační systémy - samostatná působnost	5	20	20	20	20	30	30	30	30	200
Agendové informační systémy - přenesená působnost	5	20	20	20	20	30	30	30	30	200
Ekonomický informační systém	5	20	30	30	30	30	30	30	30	230
Portály	3	36	27	27	18	12	27	18	18	183
Ostatní elektronické úložiště	3	6	24	36	36	36	18	36	36	228
Indikátor celkové míry rizika hrozby	-	164	199	225	207	216	197	246	261	-

4.1.5 Vyhodnocení mapování obcí s rozšířenou působností

Zhotovitel provedl mapování obcí, zpracoval záznamy o činnostech na základě informací z Vybraných obcí, které jsou uvedeny v Příloze č. 5, a provedl analýzu rizik na modelové obci, jejíž rozsah je specifikován v kapitole 4.1.3 Modelová obec s rozšířenou působností.

Na základě indikátoru celkové míry rizika aktiva stanovil Zhotovitel modelový rozsah organizačních a technických opatření pro jednotlivá aktiva v kontextu obvykle se vyskytujících situací. Detailní popis je uveden v následující kapitole.

4.2 Návrh opatření k zajištění plného souladu posuzovaných procesů s GDPR a dalšími právními předpisy a dosažení předepsané úrovně ochrany osobních údajů

Na základě provedené analýzy rizik pro modelovou obec s rozšířenou působností jsme identifikovali obecné problematické situace v kontextu GDPR. K těmto situacím jsme zpracovali komentář, který diskutuje vhodné návrhy opatření vedoucí k dosažení souladu s požadavky GDPR. Řada situací je společných se situacemi zpracovanými v kapitole 3.2 Návrh opatření k zajištění plného souladu posuzovaných procesů s GDPR a dalšími právními předpisy a dosažení předepsané úrovně ochrany osobních údajů.

V této kapitole jsou uvedeny situace, které Zhotovitel považuje za situace, které se zcela jistě vyskytují v obcích s rozšířenou působností. Jejich výskyt v obcích se základním rozsahem přenesené působnosti je taktéž možný, nicméně pravděpodobnost výskytu těchto situací není velká.

Jedná se o další následující situace:

- Výpočetní infrastruktura;
- Problematika veřejné Wi-Fi sítě poskytované obcemi;
- Interní správa IT infrastruktury;
- Korelace logů;
- Připojení k internetu úřadu a jeho problematika;
- Antivirus/Antispam;
- Zálohování;
- Výmaz dat ze záloh při uplatňování práv subjektů údajů;
- Problematika vzdálených přístupů do sítě;
- Lokální disky na počítačových sestavách v rámci úřadu;
- Bezpečnost perimetru lokální sítě (LAN);
- Systémy na ochranu dat (DLP řešení).

Pod bodem DOPORUČENÍ u každé posuzované problematické situace je uveden návrh opatření k zajištění plného souladu posuzovaných procesů s GDPR a dalšími právními předpisy a dosažení předepsané úrovně ochrany osobních údajů.

Zhotovitel této systémové analýzy v této souvislosti upozorňuje, že závěry a doporučení u níže uvedených situací vychází ze systémové analýzy provedené na vzorku Vybraných obcí. Míru dopadu uvedených závěrů a doporučení musí posoudit každý správce osobních údajů ve smyslu čl. 4 odst. 7 GDPR, který vykonává činnosti spadající do věcné působnosti GDPR (čl. 2 odst. 1 GDPR), případ od případu a dle konkrétních okolností, zejména se zohledněním stanovených účelů, podmínek zpracování osobních údajů a úrovně zavedených organizačních a technických opatření.

4.2.1 Výpočetní infrastruktura

Fyzická bezpečnost výpočetní infrastruktury na úřadech není vždy adekvátní vůči hodnotě ochraňovaných aktiv.

DOPORUČENÍ:

Pokud úřad provozuje vlastní výpočetní infrastrukturu, musí být tato infrastruktura přiměřeně zabezpečena. V oblasti fyzické bezpečnosti serverových místností byly identifikovány významné nedostatky.

Serverové místnosti nebyly optimálně umístěny – někde se nacházely v záplavové oblasti pod hladinou řeky. Serverovou místností by neměl být veden rozvod plynu, vody ani kanalizace.

Pokud má tato vyhrazená místnost okna, měla by být zabezpečena proti vniknutí (bezpečnostní fólie, mříže). Vstup do místnosti by měl být zabezpečen buď elektronickým zařízením, nebo bezpečnostním zámkem. V serverovně by měla být protipožární čidla, bezpečnostní dveře a protipožární prostupy pro vedení pro serverovou místnost. Serverová místnost by neměla být používána pro další účely, není vhodné, aby byla zároveň skladem výpočetní techniky. Klimatizační jednotky by měly být redundantní, aby v případě výpadku jedné byla místnost chlazena tou druhou. Přívody elektrické energie by měly být taktéž redundantní. Pro případ přerušení elektřiny by měl být připraven dieselagregát.

Uvedená opatření nejsou sice předepisována GDPR, ale patří k obecným principům zajištění bezpečnosti informací. Je zřejmé, že obce by měly k zabezpečení serveroven přistupovat s rozvahou a volit taková opatření, která jsou v jejich finančních a technických možnostech tak, aby udělaly pro zabezpečení infrastruktury maximum.

V případě využívání hostované infrastruktury se problematika překlápí především do právní roviny, kdy klíčovou bezpečnostní pojistkou jsou kvalitně připravené smlouvy, které řádně ošetří všechny kritické oblasti. Užitečným vodítkem při tvorbě smluv s poskytovateli služeb je v době psaní tohoto dokumentu návrh nové vyhlášky o kybernetické bezpečnosti (viz https://nukib.cz/cs/nova-vkb/), která ve své příloze č. 7 definuje důležitá bezpečnostní opatření pro smluvní vztahy.

4.2.2 Problematika veřejné Wi-Fi sítě poskytované obcemi

Některé obce poskytují otevřené veřejné Wi-Fi sítě pro občany. Někdy je síť dostupná pouze v prostorách úřadu, v některých obcích bývá provozována i na větším geografickém prostoru.

DOPORUČENÍ:

Z právního hlediska byla tato problematika diskutována již v kapitole 3.2.14.

V případě provozování otevřené Wi-Fi sítě se na obce bude vztahovat mnoho povinností vyplývající ze zákona o elektronických komunikacích a lze jim tedy doporučit, aby plnily i ostatní povinnosti z tohoto zákona vyplývající, např. aby vedly povinnou evidenci o:

- **počtu případů, ve kterých na základě žádosti poskytla provozní a lokalizační údaje orgánům oprávněným k jejich vyžádání,**
- **době, která v jednotlivých případech uplynula ode dne, kdy zahájila uchovávání provozních**
  a lokalizačních údajů do dne, kdy o tyto údaje oprávněný orgán požádal, a
- **počtu případů, kdy nemohly žádosti o poskytnutí provozních a lokalizačních údajů vyhovět.**

Obce zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací jsou povinny předávat Českému telekomunikačnímu úřadu evidenci uvedenou v předchozím odstavci souhrnně vždy za uplynulý kalendářní rok, a to v elektronické formě, nejpozději do 31. ledna následujícího kalendářního roku. Předávaná evidence nesmí obsahovat osobní a identifikační údaje.

Z výše uvedeného vyplývá, že obce musí logovat používání služeb Wi-Fi a tyto logy po nezbytně dlouhou dobu uchovávat. Záznamy o provozu sítě podle §97 uvedeného zákona jsou osobními údaji a musí být také adekvátně chráněny. Uchovávání logů proto musí být řádně zajištěno, aby nebyla narušena jejich důvěrnost, dostupnost a integrita.

4.2.3 Interní správa IT infrastruktury

Způsob správy IT infrastruktury v obcích je často nedostatečný a nenaplňuje současnou dobrou praxi v oblasti řízení IT. Správa IT má přímý vliv na kvalitu celého systému informační bezpečnosti a nesprávné postupy mohou zvyšovat rizika úniku či zneužití osobních údajů.

DOPORUČENÍ:

V současné době existují standardně užívané profesionální metodiky a postupy správy IT (například ITIL – IT Infrastructure Library), které je za účelem ochrany osobních údajů vhodné implementovat. GDPR nenařizuje přesné postupy, ale očekává, že zpracovatel udělá vše pro to, aby s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování ochránil osobní údaje před narušením jejich důvěrnosti, integrity a dostupnosti.

Níže jsou popsána některá základní pravidla, která je doporučeno implementovat:

- **Nepoužívají se standardní přednastavené administrátorské účty. Tyto účty je doporučeno zbavit všech pravomocí.**
- **Každý administrátor má vlastní administrátorský účet, od kterého zná přihlašovací údaje pouze on.**
- **Jsou zřízeny administrátorské účty, jejichž přihlašovací údaje jsou bezpečně uchovány (například v trezoru) pro případ potřeby (při nedostupnosti administrátora).**
- **Činnost všech administrátorů je řádně auditována, aby bylo možné dohledat, k jakým prostředkům přistupovali a kdy. Tyto auditní záznamy jsou pravidelně dohledovány, aby bylo možné odhalit nestandardní a neoprávněné chování.**
- **Ke všem systémům je vedena aktuální dokumentace, aby bylo možné v případě nedostupnosti administrátora jeho zastoupení. Toto je obzvlášť důležité pro menší obce.**
- **Přihlašování uživatelů do systémů by mělo být logováno a auditováno, aby bylo možné dohledat nestandardní či neoprávněné chování.**

4.2.4 Korelace logů

Důležitou částí řízení IT infrastruktury je i trvalé sledování stavu zabezpečení ICT. Jelikož jsou tyto úkony značně procesně, organizačně a především technologicky náročné, je nutné k tomu použít vedle procesních a organizačních postupů i specializovaných technických prostředků.

DOPORUČENÍ:

Sada těchto prostředků je obecně shrnuta pod názvem Security Information and Event Management (SIEM).

Základními SIEM funkcemi jsou:

- **řízení logů (Log Monitoring / Management),**
- **řízení bezpečnostních událostí (Event Monitoring / Management),**
- **sledování síťového provozu (Flow Monitoring / Management / NBA),**
- **detailní analýza zajištěných dat,**
- **sledování bezpečnosti v reálném čase pomocí statistických výstupů,**
- **generování reportů k zajištění shody s regulativy.**

Logy, události a síťový provoz ze všech podstatných komponent sítě jsou centrálně sbírány, korelovány a vyhodnocovány. Vyhodnocení všech získaných dat se provádí v reálném čase

nebo zpětně např. pro potřeby forenzní analýzy, výstupy jsou dostupné přes grafické rozhraní bezpečnostního týmu a interního auditu.

Ačkoliv GDPR využití těchto technologií výslovně neuvádí, pro větší obce můžeme využití SIEM nástroje doporučit.

4.2.5 Připojení k internetu úřadu a jeho problematika

Každý úřad je připojen do internetu. Toto připojení je zdrojem neustálých bezpečnostních hrozeb.

DOPORUČENÍ:

Internetové připojení úřadu je místem neustálých kybernetických útoků. Pro zabezpečení konektivity
je proto vhodné toto připojení zabezpečit již na úrovni jejich poskytovatelů. Jenom tak se dá účinně bránit například útokům typu DDoS (Distributed Denial of Service).

Stejně tak je vhodné již u poskytovatele požadovat služby systému prevence průniku (IPS – Intrusion Prevention Systems) a detekce průniku (IDS – Intrusion Detection Systems). Tyto služby slouží k preventivní obraně a monitorování podezřelých aktivit. Jedná se velmi sofistikované systémy, jejichž pořízení je velmi nákladné. Proto je vhodnější tyto systémy pořídit jako služby.

4.2.6 Antivirus/Antispam

Jednou z nejčastějších hrozeb, se kterou se uživatel výpočetní techniky může setkat, jsou počítačové viry, spam a phishingové útoky.

DOPORUČENÍ:

Je nezbytné, aby každý počítač byl chráněn aktualizovaným antivirovým systémem. Stejně tak je vhodné aplikovat antivirové systémy jako moduly do mailových serverů, aby filtrovaly příchozí a odchozí emaily a eliminovaly šířící se viry a spam obsahující phishingové útoky.

Základním atributem těchto systémů musí být častá aktualizace, jelikož virové epidemie se šíří velice rychle a pouze aktualizované antivirové programy je dokáží včas zastavit.

Antivirové programy by měly být nainstalovány i na zranitelných mobilních zařízeních – mobilních telefonech, tabletech.

Některé antivirové programy dokáží poskytovat i další žádoucí služby – například osobní firewall, antimalware, vzdálenou centralizovanou správu počítače apod.

4.2.7 Zálohování

Pokud dojde k poškození primárních dat, jedinou rychlou možností nápravy bývá obnova systému ze záloh. Některé obce na tuto eventualitu nejsou připraveny a nemají dostupné zálohy všech dat.

DOPORUČENÍ:

Zálohování dat je jednou z nejdůležitějších bezpečnostních aktivit v rámci správy výpočetní techniky. V případě poškození originálních dat je záloha často jediný možný způsob, jak tato data obnovit.

Přesné postupy a intervaly GDPR striktně nedefinuje, proto je na každém úřadu, aby si vytvořil systém zálohování, který mu s ohledem na jeho možnosti nejvíce vyhovuje.

Doporučujeme tzv. pravidlo 3-2-1 – tedy mít alespoň 3 instance dat na 2 různých médiích s 1 instancí dat na geograficky vzdálené lokalitě.

Zálohy by měly být také pravidelně kontrolovány, aby se nestalo, že v okamžiku nejvyšší nouze správce IT zjistí, že zálohovací systém je dlouhodobě nefunkční a žádná data zálohována nebyla.

4.2.8 Výmaz dat ze záloh při uplatňování práv subjektů údajů

Při uplatňování práv subjektů údajů, a to zejména při uplatňování „práva na zapomnění“, může vlivem použité technologie (např. pásková zálohovací knihovna) dojít k situaci, kdy Správce nemůže realizovat práva subjektu údajů přesně ve Správcem stanovené skartační lhůtě (např. S/5 od data vytvoření dokumentu obsahující osobní údaje).

DOPORUČENÍ:

Správce uvede pro předmětnou oblast zpracování osobních údajů svůj oprávněný zájem spočívající v zajištění technických lhůt, které plynou z navrženého zálohovacího scénáře. Touto technickou lhůtou tedy dojde k rozšíření skartační lhůty, která je uvedena v záznamech o činnosti. Po uplynutí těchto technických lhůt dojde k uplatnění práva subjektu údajů. Jedná se zpravidla o lhůty v řádech týdnů. Tyto technické lhůty je nezbytné včas uvést a zahrnout do záznamů o činnostech a dalších dokumentovaných postupů.

4.2.9 Problematika vzdálených přístupů do sítě

Některé úřady umožňují přístupy do interní sítě pomocí vzdáleného přístupu. Toto může být z důvodu nutnosti zaměstnanců přistupovat k interním systémům úřadu, nebo, a to je častější, nutnost poskytovatelů informačních systémů tyto systémy vzdáleně administrovat. Vzdálený přístup do interní sítě sebou vždy nese riziko.

DOPORUČENÍ:

Základním předpokladem je, že vzdálený přístup podléhá stejným pravidlům a bezpečnostním politikám jako připojení do lokální sítě.

Vzdálený přístup do interní sítě musí být realizován pomocí zabezpečené technologie VPN či šifrovaným RDP protokolem.

Tento přístup mohou využívat pouze oprávnění uživatelé, kteří mají pro tento přístup povolení.

Osoby se vzdáleným přístupem je nutné evidovat, jejich přístupy musí být logovány, auditovány a dohledovány.

Každý uživatel přistupující do VPN či RDP se přihlašuje vlastním přihlašovacím jménem a heslem. Pokud je možné vázat přístup na statickou IP adresu, tak je vhodné toho využít.

4.2.10 Lokální disky na počítačových sestavách v rámci úřadu

Menší úřady využívají pro ukládání dat lokální počítačové disky. Tyto disky nelze centrálně spravovat a je složité sledovat, co se na nich s uloženými osobními údaji a daty úřadu děje.

DOPORUČENÍ:

Lokální disky by měly být využívány co nejméně.

Pokud je nutné vést nestrukturované osobní údaje, je vhodné tyto uložit na centrální sdílené disky, které je možné lépe dohledovat a jsou zpravidla i centrálně zálohované či obsahují

vlastní bezpečnostní opatření (zrcadlení disků, verzování souborů apod.). Je případně. Hodné použít nástroje pro indexování dat pro jejich rychlejší vyhledání s jejich odpovídajícím zabezpečením.

Nezálohovaná data není možné v případě znehodnocení v důsledku lidské chyby či vlivem bezpečnostního incidentu zachránit.

4.2.11 Bezpečnost perimetru lokální sítě (LAN)

Soudobý úřad se neobejde bez síťové komunikace. Počítače umístěné v lokální síti komunikující přes internet se tak stávají rizikovým bodem, který může být cílem či prostředníkem útoků.

DOPORUČENÍ:

Lokální počítačová síť by měla být adekvátně chráněna před útoky z internetu. Základní ochranou je tzv. firewall, který slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Základní firewall bývá součástí modemů či routerů, které slouží pro připojení lokální sítě do internetu.

Dále mohou být využity tzv. proxy servery, které slouží jako prostředník mezi klientem a cílovým serverem. Tyto servery překládají klientské požadavky a vůči cílovému serveru vystupují jako sám klient. Díky tomu dokáží skrýt pravou identitu klienta a tím ho chránit. Obdobnou funkci plní i systémy NAT (Network Address Translation), které pracují již na síťové vrstvě komunikace a taktéž dokáží skrýt celou lokální síť za jednu internetovou adresu.

Dalším důležitým prvkem ochrany lokální sítě je již dříve uvedená segmentace sítě, která slouží k logickému rozčlenění a omezení provozu.

Pro systémy a servery, které musí být přístupné z otevřeného internetu, je vhodné vytvořit samostatnou logickou podsíť tzv. DMZ (demilitarized zone), která je bezpečně oddělena od vnitřní důvěryhodné sítě.

IDS/IPS systémy a způsob ochrany před DDoS útoky již byly popsány v jiných situacích.

4.2.12 Systémy na ochranu dat (DLP řešení)

Pokud se správcům informačních technologií podaří opevnit informační systémy natolik, že budou odolné vůči útokům zvenčí, pořád ještě mohou být zranitelné vůči cíleným či nechtěným útokům zaměstnanců uvnitř perimetru.

DOPORUČENÍ:

Pro ochranu před ztrátou dat slouží tzv. DLP (data loss prevention) systémy. Tyto systémy mohou sloužit buď k ochraně na úrovni počítačové sítě, nebo na koncových stanicích. Princip ochrany spočívá v analýze komunikace, kontrole komunikace, kontrole emailových komunikací, kontroly přístupu na fyzická zařízení (DVD mechaniky, flash disky apod.) a fyzické komunikační porty.

Některé antivirové programy obsahují funkce DLP systémů a mohou být vhodným komplementem pro zvýšení úrovně bezpečnosti informací v organizaci.

4.3 Doporučení k možnostem personálního a organizačního obsazení pověřence pro ochranu osobních údajů

GDPR zakotvuje nový institut pověřence pro ochranu osobních údajů. Pověřenec je specifickou osobou, kterou musí jmenovat správci a zpracovatelé osobních údajů, kteří splňují podmínky stanovené v čl. 37 odst. 1 GDPR[51]. Každý správce a zpracovatel tak musí zvážit, zda se na něj povinnost jmenovat pověřence vztahuje.

Role pověřence spočívá zejména v dohlížení na soulad postupů správců a zpracovatelů s GDPR a v poskytování odborné podpory správcům a zpracovatelům v souvislosti s jejich povinnostmi souvisejícími s ochranou osobních údajů.

4.3.1 Kvalifikační standardy

V souladu s čl. 37 odst. 5 GDPR musí být pověřenec jmenován na základě svých profesních kvalit, zejména na základě odborných znalostí práva a praxe v oblasti ochrany osobních údajů, a na základě své schopnosti plnit úkoly stanovené v čl. 39 GDPR. GDPR nijak neupravuje konkrétní náležitosti profesních a odborných kvalit (např. požadavky na vzdělání či certifikaci). Vždy je však nutné dodržet podmínku, že musí jít o osobu, která bude schopná plnit úkoly pověřence stanovené v GDPR.

Pověřenec by zároveň měl mít dostatečnou znalost interní struktury správce nebo zpracovatele, postupů uplatňovaných při činnosti správce nebo zpracovatele či prováděných operací zpracování osobních údajů.

U každého správce nebo zpracovatele budou požadavky na osobu pověřence rozdílné, zejména s ohledem na organizační strukturu správce nebo zpracovatele a činnosti jimi prováděné. Vyšší nároky na kvalifikaci a praxi pověřence (zejména na podrobnou znalost právní úpravy, znalost problematiky kybernetické a fyzické bezpečnosti, řízení informačních systémů nebo schopnost monitorovat a auditovat činnosti správce nebo zpracovatele a dovozovat z tohoto monitoringu relevantní závěry) budou zcela jistě kladeny na pověřence vykonávající činnost v rámci obcí s rozšířenou působností (tedy obce III. stupně), které mají složitější strukturu a vykonávají působnost v širším okruhu agend než obce I. stupně (např. evidence obyvatel, vydávání cestovních dokladů, sociálně-právní ochrana dětí atd.). Vyšší nároky budou kladeny také na pověřence podřízených organizací, které provádějí rozsáhlé zpracování zvláštních kategorií osobních údajů.

Pověřenec se nesmí dostat do střetu zájmů. Pracovní skupina WP29 ve svém výkladovém stanovisku[52] dovozuje, že pověřenec nemůže zastávat pozici, na které by stanovoval účely nebo prostředky zpracování osobních údajů. Osoby ve střetu zájmů budou ty, které se podílejí jak na koncipování, tak na realizaci projektů zahrnujících činnosti v souvislosti se zpracováním osobních údajů. Typickými pozicemi se střetem zájmů jsou například tajemník obecního úřadu, ředitel finančního odboru nebo vedoucí IT oddělení.

Pověřenec je dle čl. 38 odst. 5 GDPR v souvislosti se svou činností vázán povinností mlčenlivosti. Tato mlčenlivost se bude vázat zejména na osobní údaje subjektů údajů, ale také na aplikovaná bezpečnostní opatření a jiné důvěrné informace týkající se činnosti správce nebo zpracovatele.

---

[51] Viz čl. 37 odst. 1 GDPR:
„Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:
a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí,
b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, nebo
c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech uvedených v článku 10.“

[52] Pracovní skupina podle článku 29: Vodítka k pověřencům pro ochranu osobních údajů, WP 243 rev. 01 ze dne 5. 4. 2017

4.3.2 Organizační začlenění pověřence

Čl. 38 GDPR upravuje postavení pověřence z hlediska jeho zapojení do záležitostí souvisejících s ochranou osobních údajů. Toto ustanovení zakotvuje povinnost správce nebo zpracovatele zapojit pověřence do veškerých záležitostí souvisejících s ochranou osobních údajů a podporovat ho při plnění jeho úkolů a povinností dle čl. 39 GDPR. Pověřenec by měl být správcem nebo zpracovatelem brán jako diskuzní partner a měl by mít přístup do všech pracovních skupin zabývajících se ochranou osobních údajů v rámci správce či zpracovatele.

Čl. 38 GDPR rovněž zakotvuje požadavek nezávislosti výkonu funkce pověřence v rámci správce nebo zpracovatele, když v odstavci 3 stanoví, že „*správce a zpracovatel zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele*“. Pověřenec tedy dle GDPR má mít v rámci organizační struktury správce nebo zpracovatele specifické a do jisté míry nezávislé postavení. Pověřenec tedy není jen pouhým řadovým zaměstnancem správce nebo zpracovatele, který má na starosti ochranu osobních údajů.

Pověřenec nenese osobní odpovědnost za nedodržení pravidel stanovených GDPR, neboť dle čl. 24 odst. 1 GDPR správce odpovídá za to, že zpracování je prováděno v souladu s GDPR, a tuto skutečnost musí být správce rovněž schopen doložit. Pověřenec by měl v rámci správce nebo zpracovatele vždy zastávat svou funkci a plnit své povinnosti a úkoly nezávislým způsobem. Pokud správce nebo zpracovatel bude postupovat v rozporu s názorem pověřence a tento postup potenciálně povede k nesouladu s GDPR, není v kompetencích pověřence v tom správci nebo zpracovateli bránit. Pověřenec by ale měl mít vždy prostor pro vyjádření svých postojů a správce či zpracovatel by se s nimi měl odůvodněně vypořádat.[53]

Pověřenec může být zaměstnancem správce nebo zpracovatele, tedy interním pověřencem, nebo může jednotlivé úkoly plnit na základě smlouvy o poskytování služeb[54], a být pověřencem externím.[55]

Externím pověřencem může být také právnická osoba, to však za předpokladu, že bude předem označena konkrétní fyzická osoba, která bude splňovat požadavky stanovené GDPR a bude funkci pověřence fakticky vykonávat.

GDPR umožňuje, aby pro několik orgánů veřejné moci či veřejných subjektů byl jmenován jediný pověřenec. [56] V takovém případě však musí být zohledněna organizační struktura a velikost jednotlivých orgánů veřejné moci nebo veřejných subjektů, neboť každý takový správce nebo zpracovatel je odpovědný za zajištění, že tento jediný pověřenec bude vůči němu plnit své úkoly efektivně, přestože byl pověřenec jmenován pro několik subjektů najednou. Správce nebo zpracovatel má povinnost pověřence při plnění jeho úkolů podporovat a poskytovat mu zdroje k jejich plnění. S tím souvisí i skutečnost, že pověřenec musí mít dostatek času k plnění svých povinností. V souvislosti s tím, jak stanoví i výkladové stanovisko WP29, by měl mít pověřenec stanoven i pevný podíl času vyhrazený pro funkci pověřence u konkrétního správce nebo zpracovatele.[57]

---

[53] Obecné nařízení o ochraně osobních údajů (GDPR). Praktický komentář. Wolters Kluwer. Praha, 2017.

[54] Půjde o nepojmenovanou soukromoprávní smlouvu mezi správcem, případně několika správci, a pověřencem ve smyslu ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.

[55] Ke způsobu ustanovení interního nebo externího pověřence více viz Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních v podmínkách obcí vydané Ministerstvem vnitra dne 10. 8. 2017.

[56] Viz čl. 37 odst. 3 GDPR.

[57] K ustanovení společného pověřence více viz Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních v podmínkách obcí vydané Ministerstvem vnitra dne 10. 8. 2017.

4.3.3 Manuál činností pověřence

Dle ust. čl. 38 GDPR je správce nebo zpracovatel povinen zapojit pověřence do procesů souvisejících s ochranou osobních údajů, zajistit zdroje nezbytné k plnění jeho povinností a také k udržování jeho odbornosti, umožnit mu v otázkách ochrany osobních údajů přístup k nejvyššímu vedení správce nebo zpracovatele a zejména předejít případnému střetu zájmů.

Úkoly pověřence zakotvuje zejména čl. 39 GDPR, ze kterého plyne, že pověřenec by měl být osobou, která dohlíží na veškeré činnosti v oblasti ochrany osobních údajů v rámci správce nebo zpracovatele. Pověřenec dle výkladového stanoviska WP29 hraje klíčovou roli při rozvoji kultury ochrany osobních údajů uvnitř správce nebo zpracovatele a pomáhá zavádět základní prvky GDPR, jako jsou základní zásady zpracování osobních údajů (viz kapitola II GDPR), práva subjektů údajů (viz kapitola III GDPR), záměrná a standardní ochrana osobních údajů (viz čl. 25 GDPR), záznamy o činnostech zpracování (viz čl. 30 GDPR), zabezpečení zpracování (viz čl. 32 GDPR) a oznamování a ohlašování případů porušení zabezpečení ochrany osobních údajů (viz čl. 33 a 34 GDPR). Pověřenec zároveň dbá zejména na to, aby každé zpracování osobních údajů, které bude u správce nebo zpracovatele probíhat, bylo prováděno na základě některého ze zákonných důvodů vymezených v čl. 6 GDPR. Je zejména vhodné, aby pověřenec shromažďoval informace k preciznímu rozpoznání a vymezení zpracovávaných osobních údajů a analyzoval a kontroloval shodu vnitřní praxe správce nebo zpracovatele, včetně rozdělení odpovědnosti, s unijní a národní právní úpravou. V souvislosti s touto činností by měl pověřenec poskytovat správci nebo zpracovateli informace a poradenství, vydávat doporučení a předkládat svá stanoviska.[58]

Pověřenec rovněž dle čl. 39 odst. 1 písm. b) GDPR dohlíží na to, aby všichni zaměstnanci správce nebo zpracovatele, kteří jsou zapojeni do operací souvisejících se zpracováváním osobních údajů a souvisejících auditů, byli proškolováni v oblasti ochrany osobních údajů.

Mezi další úkol pověřence, který je zakotven v čl. 39 odst. 1 písm. c) GDPR, patří poskytování poradenství a vypracovávání odborných stanovisek pro správce v souvislosti s posouzením vlivu na ochranu osobních údajů dle čl. 35 GDPR. Pověřenec by měl dle výkladového stanoviska WP29 zejména stanovit, zda je nutné provést posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR, jaká metodika při vypracování posouzení vlivu na ochranu osobních údajů by měla být správcem použita či zda bude třeba zpracování posouzení vlivu na ochranu osobních údajů zadat externímu subjektu. Pověřenec by měl dále doporučit, jaká jsou vhodná technická a organizační opatření pro zmírnění rizik pro zájmy a práva subjektů údajů. Součástí působnosti pověřence by mělo být též posouzení, zda bylo posouzení vlivu dle čl. 35 GDPR správce zpracováno dle GDPR formálně správně.

Důležitá je rovněž spolupráce pověřence s dozorovým úřadem. S tím se pojí také působnost pověřence coby kontaktního místa pro dozorový úřad. V případě potřeby by měl pověřenec poskytnout dozorovému úřadu veškerou potřebnou součinnost jménem správce nebo zpracovatele. Správce nebo zpracovatel nesmí pověřenci dávat pokyny, jak jednat v dané oblasti, například jakého výsledku se má dosáhnout, jak prošetřovat stížnost nebo zda a kdy kontaktovat dozorový úřad.

Pověřenec je rovněž dle čl. 38 odst. 4 GDPR kontaktním místem pro subjekty údajů, a to jak vně správce nebo zpracovatele, tak uvnitř správce (vůči zaměstnancům), a to za účelem poskytování informací a poradenství subjektům údajů.

Jednou z nutných podmínek řádného výkonu povinností pověřence je rovněž jakási systematická kontrolní činnost. Z toho vyplývá, že správce, případně zpracovatel musí pověřenci umožnit přístup k veškeré dokumentaci a záznamům navázaným na zpracování osobních údajů (právo na přístup

[58] Čl. 39 odst. 1 písm. a) a b) GDPR a bod 4.1. výkladového stanoviska WP29.

k záznamům a informacím, vč. auditních zpráv, nálezů regulačních orgánů apod.) a podle ustanovení čl. 38 odst. 2 GDPR by mu k tomu měl umožnit i vybudování přiměřeného administrativního aparátu.

Výčet úkolů a povinností pověřence stanovených v GDPR není dle čl. 38 odst. 6 GDPR taxativní. Je tedy možné, aby pověřenec plnil i jiné úkoly a povinnosti, než které nejsou výslovně v GDPR stanoveny, vždy ale musí být zohledněn princip zákazu střetu zájmů (viz výše).

Při poskytování informací a poradenství a v souvislosti s řešením dalších svých úkolů má pověřenec povinnost postupovat čestně a poctivě, ale zároveň zohledňovat také oprávněné zájmy správce nebo zpracovatele.

4.4 Plán

Zhotovitel zpracoval plán zavedení navržených opatření do praxe obce. Jedná se o komplexní plán, jehož činnosti není nutné realizovat v přesně předepsaném pořadí. Vybrané činnosti (např. ustanovení pověřence) může obec s rozšířenou působností provést i bez dokončených činností v přípravné fázi.

Elektronická verze plánu je obsažena v Příloze č.7.

Tabulka 23 Plán s rozšířenou působností

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis II	Výstup činnosti
1	Přípravná fáze	Sestavení projektového týmu		Čl. 24	Správce ustanoví projektový tým zahrnující nejméně tajemníka úřadu, vedoucí klíčových odborů z oblasti výkonu samostatné a přenesené působnosti, archiváře, zástupce IT a osoby zodpovědné za objektovou bezpečnost.	Výstupem je zápis o sestavení týmu, určení odpovědností a stanovení kompetencí jednotlivých členů týmu.
2		Zpracování úvodní analýzy včetně mapování aktuálního zpracování osobních údajů		Čl. 5	Správce zajistí zpracování mapování osobních údajů alespoň v rozsahu definovaném touto systémovou analýzou včetně zohlednění situací výkonu přenesené působnosti a určení vztahů se zpracovateli.	Výstupem je zpracovaná analýza popisující věrně aktuální stav.
3		Zpracování záznamů o činnostech zpracování		Čl. 6, čl. 30	Správce vytvoří kvalifikované záznamy o činnostech zpracování na základě provedeného mapování.	Výstupem jsou záznamy o činnostech zpracování.
4		Nastavení interních procesů řízení rizik		Čl. 24	Správce ustanoví interní proces řízení rizik.	Výstupem je směrnice o řízení rizik.
5		Vymezení aktiv	Vymezení listinných úložišť	Čl. 5 a čl. 6	Správce detailně vymezí listinná úložiště v návaznosti na záznamy o činnostech zpracování. Součástí je revize práv přístupů k těmto úložištím a zhodnocení jejich stavu z pohledu fyzické a objektové bezpečnosti.	Výstupem je seznam listinných úložišť a zhodnocení jejich stavu.
6			Vymezení nástrojů užívaných		Správce detailně zhodnotí rozsah užívaných aplikací a IS, v rámci	Výstupem je seznam aplikací a IS zpracovávající OÚ a zhodnocení

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis II	Výstup činnosti
			pro zpracování osobních údajů ve strukturované (databáze) a nestrukturované formě (e-mail, sdílené disky apod.)		kterých zpracovává osobní údaje. Provede zhodnocení úrovně a kvality poskytované legislativní podpory ze strany dodavatele ve vztahu ke GDPR a provede revizi práv a oprávnění k aplikacím a IS. Správce provede revizi e-mailu a sdílených disků a odstraní neoprávněně zpracovávaná data s osobními údaji.	jejich stavu.
7		Provedení analýzy rizik		Čl. 24	Správce provede analýzu rizik na základě nastavených interních procesů řízení rizik. Výstupem analýzy rizik je prioritizace oblastí, které následně správce řeší organizačními a technickými opatřeními.	Výstupem je analýza rizik. Správce zajistí, aby tato analýza rizik byla známa vedení obce a vedení obce je povinno se závěry analýzy rizik řídit.
8		Zpracování rozdílové analýzy		Čl.5	Správce zpracuje rozdílovou analýzu s ohledem na závěry mapování a provedené analýzy rizik a to tak, aby v rozdílové analýze byly detailně popsány nedostatky současného stavu oproti cílovému stavu naplnění povinností správce dle GDPR. Správce si v rozdílové analýze určí ideální cílový stav souladu s GDPR.	Výstupem je rozdílová analýza. Správce zajistí, aby tato rozdílová analýza byla známa vedení obce.
9		Vyhodnocení přípravné fáze a určení interních projektů pro implementaci organizačních a technických opatření		Čl. 24 a čl. 25	Správce provede vyhodnocení přípravné fáze a připraví projekty implementace organizačních a	Výstupem je přehled projektů, jejich věcných garantů, detailní popis projektů včetně jejich rozpočtu.

P.č.	Fáze	Činnosti	Relevantní článek GDPR	Popis II	Výstup činnosti
				technických opatření a zahájí jejich realizaci.	
10	Implementační fáze	Ustanovit pověřence	Čl. 37	Správce ustanoví pověřence a informuje o tomto kroku obec.	Výstupem je ustanovení pověřence včetně uzavření pracovně právního vztahu s pověřencem nebo jiného vztahu, na základě kterého bude pověřenec vykonávat svoji činnost.
11		Přijmout směrnici o ochraně osobních údajů nebo kodexu	Čl. 24	Správce přijme směrnici o ochraně osobních údajů nebo kodex a zajití jeho implementaci do organizace.	Směrnice o ochraně osobních údajů nebo kodex.
12		Proškolit zaměstnance	Čl. 24	Správce proškolí zaměstnance či jiné spolupracující osoby v oblasti ochrany a zpracování osobních údajů a interních pravidel a postupů pro dotčenou problematiku GDPR.	Výstupem je školení a záznam o proškolení zaměstnanců.
13		Implementace organizačních opatření	Čl. 25	Správce určí organizační opatření a provede jejich implementaci v souladu s definicí projektů v přípravné fázi. Správce provede ověření organizačních opatření např. formou penetračních testů či jiným testováním přijatých opatření s cílem vyhodnotit kvalitu přijatých opatření.	Výstupem je zpráva o implementaci organizačních opatření.
14		Implementace technických opatření	Čl. 25	Správce určí technická opatření a provede jejich implementaci v souladu s definicí projektů v přípravné fázi. Správce provede	Výstupem je zpráva o implementaci technických opatření.

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis II	Výstup činnosti
					ověření technických opatření např. formou penetračních testů či jiným testováním přijatých opatření s cílem vyhodnotit kvalitu přijatých opatření	
15		Implementace procesů k realizaci práv subjektů údajů	Nastavení postupů zpracování žádostí subjektů údajů	Čl. 15 až čl. 22	Správce provede nastavení postupů pro zpracování žádostí subjektů údajů např. o rozsahu zpracování, uplatnění "práva být zapomenut" a přenositelnosti. Správce připraví technické a organizační zázemí pro zpracování žádostí subjektů údajů včetně přidělení odpovídajících materiálních a lidských zdrojů. Správce je povinen identifikovat úložiště informací obsahující osobní údaje a to jak ve strukturované, tak i nestrukturované formě a v elektronické a listinné podobě a zajistí výkon zpracování žádostí subjektů údajů nad těmito úložišti. Úložiště měl správce určit v provedeném mapování a při zpracování záznamů o činnostech. Správce nesmí opomenout žádné úložiště osobních údajů (listinné archivy, kartotéky, aplikace, IS apod.).	Zpráva o testu zpracování žádostí subjektů údajů. Zdokumentované a zavedené nové procesy pro zpracování žádostí subjektů údajů.
16			Publikace postupů a	Kap. 3	Správce publikuje na veřejně	Publikované pokyny např. formou

P.č.	Fáze	Činnosti		Relevantní článek GDPR	Popis II	Výstup činnosti
			případných podmínek k uplatnění práv subjektů údajů na veřejně dostupných zdrojích		dostupných zdrojích pokyny k uplatnění práv subjektů údajů.	životních situací na webových stránkách obce.
17		Revize zpracovatelských smluv, pokud existují		Čl. 28	Správce s ohledem na provedené mapování a záznamy o činnostech zpracování provede revizi smluv se zpracovateli a zajistí odpovídající kvalitu zpracování osobních údajů včetně sankcí a dalších vhodných mechanismů (např. informační povinnost při kompromitaci zpracovávaných osobních údajů a způsobů řešení či eskalace těchto situací).	Zpráva o revizi zpracovatelských smluv.
18		Revize souhlasů subjektů údajů		Čl. 7	Správce provede revizi souhlasů subjektů údajů na základě provedeného mapování a záznamů o činnostech. Pokud je to nezbytně nutné, vyžádá si informovaný souhlas subjektu údajů ke zpracovávaným osobním údajům v již používaných evidencích a agendách.	Revidované informované souhlasy subjektů údajů.
19		Vyhodnocení implementace organizačních a technických opatření		Čl. 24	Správce provede vyhodnocení implementace organizačních a	Zpráva o stavu implementace organizačních a technických

P.č.	Fáze	Činnosti	Relevantní článek GDPR	Popis II	Výstup činnosti
		ve vztahu k rozdílové analýze		technických opatření na základě výstupů přípravné fáze. Vedení obce vyhodnocení vezme na vědomí.	opatření.
20	Provozní fáze (od 25.5.2018)	Úvodní posouzení stavu zpracování osobních údajů ze strany pověřence a průběžné monitorování stavu zpracování osobních údajů	Čl. 39	Pověřenec provede úvodní posouzení stavu každé situace či činnosti, kdy dochází k nakládání s osobními údaji a to na základě záznamů o činnostech zpracování.	Zpráva o posouzení stavu obsahující případné nálezy a postup jejich nápravy.
21		Pravidelné sebehodnocení Správce formou aktualizace analýzy rizik	Čl. 5	Správce s ohledem na přijaté procesy řízení rizik provede aktualizaci analýzy rizik.	Výstupem je aktualizace analýzy rizik.
22		Pravidelná aktualizace rozdílové analýzy (např. v ročním cyklu)	Čl.5	Správce zajistí provádění pravidelné aktualizace rozdílové analýzy na základě postupu implementace organizačních a technických opatření zpravidla v ročním cyklu. Aktualizace rozdílové analýzy by měly správci ukázat vývoj a postup v implementaci opatření a vývoj jeho vyspělosti v oblasti zpracování osobních údajů dle požadavků GDPR.	Výstupem je aktualizovaná rozdílová analýza na základě dosavadního postupu implementace organizačních a technických opatření.
23		Aktualizace záznamů o činnostech při změnách nebo implementaci nových agend či povinností obce v porovnání se zpracovaným mapováním a zpracovaných záznamů o činnostech	Čl. 30	V případě, že dojde k úpravě určujícího právního předpisu, účelu nebo ke změně oprávněného zájmu při zpracování osobních údajů, provede správce neprodleně odpovídající aktualizaci záznamů	Výstupem jsou aktualizované záznamy o činnostech zpracování.

P.č.	Fáze	Činnosti	Relevantní článek GDPR	Popis II	Výstup činnosti
				o činnostech zpracování.	
24		Uplatňování práv subjektů údajů	Kap. 3	Na webových stránkách obce jsou publikovány pokyny a vzory žádostí k uplatnění práv subjektu údajů.	Výstupem jsou žádosti subjektů údajů a jejich zpracování v řádných termínech a deklarované kvalitě.
25		Vyhodnocení dosavadního průběhu interních projektů z přípravné fáze a jejich případná aktualizace a optimalizace	Čl. 24 a čl. 25	Správce provede vyhodnocení realizace projektů definovaných v přípravné fázi zaměřených na implementaci organizačních a technických projektů. Následně navrhne jejich ukončení, aktualizaci nebo optimalizaci. Toto vyhodnocení je vhodné provádět pravidelně a to alespoň jednou ročně.	Výstupem je zpráva o aktuálním stavu. Tato zpráva by měla být aktualizována nejméně jednou ročně či v závislosti na implementaci organizačních a technických opatření. Zpráva by měla též zhodnotit úroveň vyspělosti obce a měla by být vodítkem pro posuzování přiměřenosti implementovaných opatření.
26		Pravidelné každoroční školení zaměstnanců	Čl. 24	Správce zajistí pravidelné školení zaměstnanců v oblasti zpracování osobních údajů a jejich ochrany a to s cílem průběžného zvyšování povědomí o předmětné problematice.	Výstupem je záznam o proškolení zaměstnanců.

5 Přílohy

Přílohy jsou uloženy v elektronické podobě na přiloženém CD.

5.1 Příloha č. 1 – Výsledky místního šetření včetně zaslaných dokumentů od obcí se základním rozsahem

5.2 Příloha č. 2 – Výsledky místního šetření včetně zaslaných dokumentů od obcí s rozšířenou působností

5.3 Příloha č. 3 – Přehled agend zpracovávajících osobní údaje v obcích I. stupně

5.4 Příloha č. 4 – Přehled agend zpracovávajících osobní údaje v obcích II. stupně

5.5 Příloha č. 5 – Přehled agend zpracovávajících osobní údaje v obcích III. stupně

5.6 Příloha č. 6 - Přehled agend zpracovávajících osobní údaje ve vybraných podřízených organizacích obce

5.7 Příloha č. 7 – Plány zavedení navržených opatření do praxe

5.8 Příloha č. 8 - Metodika mapování obcí