



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Mikroregion Sokolov – východ

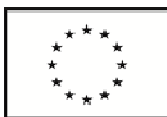
Lázeňská 114, Královské Poříčí 356 01

Analýza implementace GDPR v obcích Mikroregionu Sokolov – východ

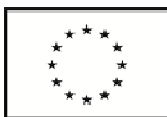


Obsah

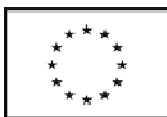
Úvod	1
Seznam zkratk	3
Seznam právních předpisů	3
1. Základy prameny právní úpravy a základní pojmy	4
1.1 Obecné nařízení (GDPR).....	5
1.1.1 Struktura obecného nařízení GDPR	6
1.1.2 Působnost obecného nařízení GDPR	6
1.1.2.1 Působnost místní a časová	6
1.1.2.2 Působnost osobní	7
1.1.2.3 Působnost věcná.....	7
2. Zákon o ochraně osobních údajů.....	8
2.1.1 Historie úpravy v ČR.....	8
2.1.2 Význam zákona o ochraně osobních údajů	8
2.2 Zákon o zpracování osobních údajů.....	9
2.3 Základní pojmy používané v ochraně osobních dat.....	9
2.3.1 Osobní údaj	10
2.3.2 Správce	11
2.3.3 Zpracovatel	11
2.3.4 Zpracování	12
2.3.5 Subjekt údajů	12
2.3.6 Práva subjektu údajů	12
2.3.7 Příjemce.....	14
2.3.8 Pověřenec pro ochranu osobních údajů.....	14
2.3.8.1 Úkoly pověřence pro ochranu osobních údajů	15



2.3.8.2	Pověřenec pro ochranu osobních údajů na konkrétních obcích.....	16
2.4	Dozorový úřad	16
2.4.1	Úkoly dozorového úřadu	16
2.4.2	Pravomoci dozorového úřadu	18
2.4.3	Vedoucí dozorový úřad	21
3.	Zpracování osobních údajů a jeho zásady	21
3.1	Zásada zákonnosti	22
3.2	Zásada korektnosti a zásada transparentnosti	22
3.3	Zásada omezení účelu	23
3.4	Zásada minimalizace údajů.....	23
3.5	Zásada přesnosti.....	23
3.6	Zásada omezení uložení	24
3.7	Zásada integrity a důvěrnosti.....	24
4.	Právní důvody zpracování.....	24
4.1	Souhlas subjektu údajů	25
4.2	Plnění smlouvy.....	26
4.3	Plnění zákonem stanovené povinnosti	26
4.4	Ochrana životně důležitých zájmů subjektu údajů	26
4.5	Plnění úkolů ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.....	27
4.6	Oprávněný zájem správce.....	27
5.	Zabezpečení osobních údajů	27
5.1	Ohlašování případů porušení zabezpečení	29
6.	Posouzení vlivu na ochranu osobních údajů	30
6.1	Posouzení vlivu na ochranu osobních údajů.....	30
6.2	Předchozí konzultace s dozorovým úřadem	32



7.	Práva subjektu údajů	32
7.1	Právo na informace	33
7.2	Právo na přístup k osobním údajům	35
7.3	Právo na opravu a doplnění	36
7.4	Právo na výmaz	36
7.5	Právo na omezení zpracování	38
7.6	Oznamovací povinnost	39
7.7	Právo na přenositelnost údajů	39
7.8	Právo vznést námitku	40
7.9	Právo nebýt předmětem automatizovaného rozhodování	41
7.10	Limity práv a zásad zpracování	41
8.	Předávání osobních údajů do zahraničí	42
9.	Zajištění a dokládání souladu zpracování	43
9.1	Revize zpracování	43
9.2	Záznamy o činnosti zpracování	44
9.3	Kodexy chování	45
9.4	Osvědčení	46
9.5	Vnitřní koncepce ochrany osobních údajů (směrnice)	47
10.	Sankce a pokuty	48
10.1	Sankce a pokuty pro obce	50
11.	Právní ochrana a odpovědnost, včetně odpovědnosti trestní	51
11.1	Právo subjektu údajů podat stížnost u dozorového úřadu	52
11.2	Právo na účinnou soudní ochranu vůči dozorovému úřadu	52
11.3	Právo na účinnou soudní ochranu vůči správci nebo zpracovateli	53
11.4	Zastupování subjektů údajů	53



11.5	Právo na náhradu újmy a odpovědnost	54
11.6	Trestní odpovědnost správce a zpracovatele jako právnické osoby	55
11.6.1	Neoprávněné nakládání s osobními údaji	56
11.6.2	Kontrola zaměstnanců za účelem předcházení přičitatelnosti jejich trestního jednání	58
12.	Praktická část – analýzy rizik obcí	58
12.1	Analýza rizik obce Vintřov	60
12.2	Analýza rizik obce Hory	87
12.3	Analýza rizik obce Jenišov	111
12.4	Analýza rizik obce Lomnice	130
12.5	Analýza rizik obce Staré Sedlo	157
12.6	Analýza rizik obce Šabina	180
13.	Praktická část – pověřenec pro ochranu osobních údajů	202
13.1	Činnost pověřence	203
13.2	Doporučení k činnosti pověřence	203
14.	Praktická část – návrhy a doporučení	204
14.1	Přijetí a aktualizace Analýzy rizik	204
14.2	Přijetí a aktualizace Záznamů o činnosti zpracování	205
14.3	Fyzická bezpečnost	206
14.4	IT bezpečnost	207
14.5	Interní předpisy a směrnice	207
14.6	Kamerový systém	208
14.7	Proškolení zaměstnanců	210
14.8	Příklady dobré praxe / konkrétní postupy	211
14.8.1	Výkon spisové služby, ukládání a skartace dokumentů	211
14.8.2	Kontrolní činnost	215



14.8.3	Správní řízení.....	219
14.8.4	Činnost obecních knihoven	223
14.8.5	Pořádání kulturních akcí.....	227
14.8.6	Uveřejňování dokumentů na webu obce	235
14.8.7	Uveřejňování materiálů ze zastupitelstva.....	241
14.8.8	Zveřejňování na úředních deskách.....	245
14.8.9	Kyberbezpečnost.....	249
14.8.10	Personální praxe a výběrová řízení.....	252
15.	Závěr	259



Tento dokument byl zpracován v rámci projektu

Efektivní veřejná správa v Mikroregionu Sokolov- východ II

Registrační číslo projektu CZ.03.4.74/0.0/0.0/17_080/0009899

Úvod

Tento dokument zpracovává teoretické a praktické poznatky z implementace 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); (dále také „GDPR“) ve vybraných obcích Mikroregionu Sokolov – východ. Při zpracování bylo pracováno rovněž se zněním zákona č. 101/2000 Sb., zákon o ochraně osobních údajů a předpisem, který ho nahradil, tedy zákonem č. 110/2019 Sb., o zpracování osobních údajů, který si klade za úkol být prováděcím a upřesňujícím právním předpisem pro GDPR.

Na tomto místě je vhodné uvést, že přijetím GDPR se výrazně zvýšila, pro některé subjekty, zodpovědnost za kontrolu nad procesy, při kterých dochází k ochraně osobních údajů. Obce však dle názoru zpracovatele tohoto dokumentu měly připravenou půdu pro implementaci tím, že dlouhodobě a správně dodržovaly ustanovení zákona o ochraně osobních údajů.

Při zpracovávání tohoto dokumentu je patrné více než kdykoliv, že moderní doba na jedné straně umožňuje rozvoj informačních technologií a technický pokrok s rychlou komunikací, na straně druhé však dochází k pořizování a volnému přenášení velkého množství údajů o fyzických osobách, a to jak při výkonu soukromé správy (samosprávy) tak veřejné správy (státní správy), která obcím náleží. Tato situace vede k zahlcení databází počítačů, které obsahují desítky citlivých dat, které mohou být zneužity. Z tohoto důvodu vznikla potřeba obcí nejen správně implementovat GDPR, ale také nasměrovat k dalšímu vývoji, získat správné návyky při správě dat, prověřit zabezpečení dat a vhodně posuzovat, která data obec je oprávněna nebo povinna ukládat a nakládat s nimi.



Cílem tohoto dokumentu je také analýza a identifikace procesů, ke kterým v rámci výkonu působnosti obce (samosprávy i státní správy) dochází. Praktické informace budou porovnány s požadavky Nařízení GDPR a v případě nesouladů budou navržena konkrétní opatření k jejich odstranění.

Z důvodu komplexnosti je nutné rozdělit dokument na dvě části. První všeobecná část definuje (a musí definovat) základní pojmy a instituty v souvislosti s ochranou osobních údajů. Bez těchto údajů a informací by nebyl dokument komplexní a nebylo by možné do problematiky řádně vstoupit. Jsou zde také popsány základní kroky, které definují implementaci GDPR do organizací. Druhá, praktická část a rozsáhlejší část, je pak věnována konkrétní problematice ve vybraných obcích, konkrétním problémům implementace vč. vypracování návrhů řešení na konkrétních případech a obcích. Závěrečná část se věnuje Analýzám rizik GDPR na jednotlivých obcích a porovnává je se zásadami uvedenými v GDPR a s novou tuzemskou právní úpravou problematiky ochrany osobních údajů. V neposlední řadě je také vyhodnoceno fungování pověřence pro ochranu osobních údajů a jeho potřebnost. Samostatnou kapitolu pak tvoří příklady dobré praxe, návrhy a doporučení pro vybrané obce.

Před závěrem tohoto dokumentu byly vypracovány kompletní Analýzy rizik GDPR pro všechny dotčené obce, které byly rovněž předány jako samostatný dokument. Tyto dokumenty jsou vysoce praktické a pomáhají splnit obcím povinnosti dle nařízení GDPR. Zároveň proklamují dodržování nařízení GDPR a jeho implementaci. Tyto dokumenty budou zástupci obcí vhodně doplněny v rámci praktické implementace GDPR za spolupráce s Pověřencem pro ochranu osobních údajů.

Dále jsou v textu tohoto dokumentu řešeny naprosto elementární otázky, které vznikají při každodenní činnosti pracovníků obcí, jak bylo vyzorováno z osobních návštěv a konzultací autora. Na tyto otázky jsou pak uvedeny srozumitelné a praktické odpovědi.

Závěr tohoto dokumentu je věnován změnám v jednotlivých procesech probíhajících v rámci obcí a implementaci technických a organizačních opatření k zajištění ochrany osobních údajů ve zvolených obcích, jak v každodenní praxi, tak v dlouhodobém výhledu.



Seznam zkratek

GDPR – General Data Protection Regulation – obecné nařízení o ochraně osobních údajů

EDPS – European Data Protection Supervisor – Evropský sbor pro ochranu osobních údajů

DPA – Data Protection Authority – dozorový úřad

DPO – Data Protection Officer – pověřenec pro ochranu osobních údajů

ICT – Information and Communication Technologies – informační a komunikační technologie

CCTV – Closed Circuit Television – uzavřený televizní okruh, resp. kamerový systém

Seznam právních předpisů

Zákon č. 89/2012 Sb., občanský zákoník, v platném znění.

Zákon č. 128/2000 Sb., zákon o obcích, v platném znění.

Zákon č. 500/2004 Sb., správní řád, v platném znění.

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Zákon č. 110/2019 Sb., o zpracování osobních údajů, v platném znění.



1. Základy prameny právní úpravy a základní pojmy

Tato kapitola uvádí do problematiky základních pramenů a úpravy ochrany osobních údajů a základních pojmů, se kterými je dále pracováno. Dnes již nelze zpochybňovat skutečnost, že o každém z nás, se shromažďuje celá řada osobních údajů různé povahy. Za svůj život tak různým institucím a organizacím poskytujeme informace, které umožňují jednoznačnou identifikaci např.: jméno, příjmení, adresu bydliště, místo a datum narození, rodné číslo nebo číslo občanského průkazu. Moderní právní systém tak musí stanovit ochranu těchto údajů vč. stanovení sankcí za jejich zneužití.

Zcela mimořádný význam ochrany osobnosti člověka a ochrany informací o člověku samotném je znám již od dávných dob lidské historie. Bohužel je smutným faktem, že opravdový důsledek masového zneužití osobních údajů nám ukázalo období druhé světové války a nacismus, který zneužitím osobních údajů umožnil genocidu nevinných. Tyto bezprecedentní tragické události položily základy k ochraně soukromí dat a osob.

Snahy o ochranu soukromí vyvrcholily již v roce 1948 schválením Všeobecné deklarace lidských práv¹, která ve svých člancích zaručovala ochranu soukromí, jehož přirozenou součástí byla i ochrana osobních údajů. Technický pokrok si pak vyžádal přijetí dalšího dokumentu: Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. Tyto dokumenty tak položily základní kameny, na kterých poté vycházely i další evropské dokumenty řešící otázky ochrany dat (např. Listina základních práv EU nebo Smlouva o fungování Evropské unie). Není třeba připomínat, že tyto dokumenty již musely reagovat na masivní využívání informační a komunikační technologie (dále jen „ICT“).

Další nárůst potřeby ochrany osobních údajů tak byl vyvolán právě vznikem Evropské unie, která umožnila volný pohyb osob, zboží a služeb, což neslo rovněž i volný pohyb osobních údajů. Státy Evropské unie tak považovaly za vhodné přijmout jednotnou regulaci pro celý evropský prostor. Odpovědí na tento požadavek měla být Směrnice

¹ Schváleno Valným shromážděním Organizace spojených národů.



Evropského parlamentu a Rady 95/46/ES (tzv. obecné nařízení o ochraně osobních údajů), která měla za úkol zakotvit jednotnou úpravu ochrany osobních údajů na území států Evropského společenství. Toto obecné nařízení však stanovovalo pouze právní rámec, takže se právní úprava na území jednotlivých států poměrně lišila, se vzrůstající globalizací se ukázalo, že není možné pokračovat bez stanovení práv a povinností v jednotlivých zemích. Vyústěním snahy o úpravu této problematiky v rámci EU pak bylo tedy přijetí nařízení GDPR, které zrušilo obecné nařízení o ochraně osobních údajů a kterému bude věnována následující kapitola.

1.1 Obecné nařízení (GDPR)

Obecné nařízení EU o ochraně osobních údajů neboli GDPR, z anglického „General Data Protection Regulation“ vstoupilo v platnost dne 25. 05. 2018 a týká se všech subjektů, kteří zpracovávají data fyzických osob. Jak bylo naznačeno výše, GDPR má za cíl hlavně sjednocení práv a ochrany osobních údajů všech zemí EU. Jedná se, oproti směrnici 95/94/ES, o daleko důmyslnější a propracovanější systém ochrany osobních údajů, nejen při jejich zpracování. Zcela nově je tak pojata odpovědnost správce za zajištění a dokládání souladu zpracování s GDPR, v rámci čehož GDPR přináší zcela nové nástroje (které neznal ani tuzemský zákon o ochraně osobních údajů), můžeme zde např. jmenovat karty procesu, záznamy o činnostech zpracování nebo institut pověření pro ochranu osobních údajů.

Zcela nové je také pojetí rizika jako základního ukazatele, podle kterého se pak u jednotlivého správce stanoví adekvátní povinnosti. Z tohoto je tedy jasné, že každého správce osobních údajů se GDPR dotkne jinak, právě v závislosti na operacích, které provádí (a na míře jejich rizika). Nejvíce povinností je tak uloženo správcům, kteří zpracovávají velké množství osobních údajů nebo kteří zpracovávají citlivé osobní údaje, s čímž souvisí i posílení práva subjektu údajů a jejich propracovanější pojetí.

Pro komplexní výklad lze také zmínit, že došlo k daleko přesnější úpravě pro předávání osobních údajů do třetích zemí (země mimo EU) nebo pro přeshraniční předávání osobních údajů, tyto skutečnosti se ale sledovaných obcí netýkají.



1.1.1 Struktura obecného nařízení GDPR

Oproti běžným zákonům, se kterými se pracovníci obecních úřadů setkávají běžně, má obecné nařízení odlišnou strukturu. Skládá se totiž ze dvou částí, tj. z Preambule a z vlastního textu nařízení (tento text je již obdobný jako text zákona – stanoví jednotlivá práva a povinnosti). Preambuli tvoří recitály, které můžeme připodobnit důvodové zprávě zákona – obsahují odůvodnění přijetí nařízení, výklady a doporučení pro práci s novými instituty. Samotný text nařízení je pak členěn do článků (nikoliv do paragrafů), které již obsahují samotná pravidla pro zpracování osobních údajů. Pro komplexní pochopení celého nařízení je tedy potřeba pracovat s oběma částmi, jelikož jednotlivé recitály často poskytují výklad článkům nařízení.

1.1.2 Působnost obecného nařízení GDPR

Dle obecné teorie práva má každý právní předpis svou působnost, nařízení GDPR tak není výjimkou. Pro účely tohoto dokumentu můžeme rozdělit působnost na místní a časovou, osobní a věcnou.

1.1.2.1 Působnost místní a časová

Působnost GDPR z místního hlediska postihuje všechny členské státy Evropské unie (a navíc Velkou Británii, která přijala nařízení do svého právního řádu dobrovolně). Důležité je si ovšem uvědomit, že ochrana osobních údajů cestuje s osobními údaji² – což znamená, že se nelze vyhnout dopadům GDPR tím, že by zpracovatel prováděl zpracování osobních údajů mimo území Evropské unie. Výklad pojmu provozovna není pro naše účely důležitý, jelikož pro námi zkoumané správce se jedná o sídlo obecního úřadu.

Pro úplnost lze dodat, že nařízení se vztahuje i na zpracovatele mimo území EU v případě, že zpracovávají údaje osob, které se nacházejí v Evropské unii. Toto se uplatní zejména v obchodním styku, pro účely monitorování nákupního chování, pro účely nabídky zboží apod. Vymahatelnost této působnosti je však sporná, z důvodu nemožnosti účinného vymáhání dodržování povinností stanovených GDPR, přesto je

² Obecné nařízení se vztahuje na zpracování osobních údajů, k němuž dochází v souvislosti s činností správce nebo zpracovatele v EU – nezáleží tedy na tom, kde fakticky zpracování probíhá.



důležitá. Je totiž možné otevřeně říci, že toto ustanovení cílí zejména na velké zpracovatele (např. Facebook), kteří mají svou provozovnu (sídlo) mimo území EU.

Časová působnost nám říká, kdy je nařízení součástí právního řádu. Platnosti nabylo GDPR dne 24. května 2016³, což znamená, že v tento den prošlo legislativním procesem a bylo vyhlášeno (uveřejněno v Úředním věstníku Evropské unie) čímž se stalo součástí právního řádu. Účinnost, která je pro nás důležitější, byla stanovena na den 25. května 2018 – od tohoto data je nařízení přímo použitelné, aplikovatelné, závazné a vynutitelné.

1.1.2.2 Působnost osobní

Osobní působnost stanovuje okruh subjektů (adresátů), na které se nařízení vztahuje. Za hlavní adresáty můžeme považovat správce, zpracovatele a subjekty údajů. Všechny tyto pojmy budou rozebrány v příslušných kapitolách tohoto dokumentu.

1.1.2.3 Působnost věcná

Věcná působnost stanovuje okruh vztahů, na které se nařízení vztahuje. Teorie práva pak rozlišuje vymezení pozitivní – to na co se vztahuje a negativní – to na co se nevztahuje. Nařízení používá kombinaci těchto vymezení. Přímě se tak nařízení vztahuje na automatizované zpracování osobních údajů a neautomatizované zpracování osobních údajů, které jsou zařazovány (nebo již jsou zařazeny) v nějaké evidenci (pozitivní vymezení).

Pokud bychom se chtěli podívat na negativní vymezení, pak nám nařízení říká, že se nepoužije např. na vedení osobních záznamů (např. osobní korespondence), osobní podnikatelské využívání sociálních sítí, zpracování pro odhalování trestných činů a nakládání s údaji zesnulých osob.

³ Přesněji vstoupilo v platnost.



2. Zákon o ochraně osobních údajů

2.1.1 Historie úpravy v ČR

Tuzemská právní úprava ochrany osobních údajů má počátek v zákoně č. 87/1862 Sb., o ochraně svobody osobní a v zákoně č. 88/1862 Sb., na ochranu svobody domovní. V období První republiky byla tato otázka řešena zákonem Ústavním – tedy konkrétně zákonem č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního. Samostatného řešení ochrany osobních údajů však bylo dosaženo až přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Zde je ovšem nutné podotknout, že tento zákon upravoval ochranu osobních údajů opravdu pouze v informačních systémech, nemohl být tedy považován za komplexní řešení. Podpůrně pak tedy působila Listina základních práv a svobod, která ochranu osobních údajů zaručovala (ale opět neřešila komplexně), Zákon o ochraně osobních údajů v informačních systémech již nahradil samotný zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

2.1.2 Význam zákona o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů byl první plnohodnotným zákonem na území ČR, který komplexně upravoval ochranu osobních údajů. Účinnosti zákon nabyl 1. června 2000. Je nutné podotknout, že tento zákon rovněž zřídil Úřad pro ochranu osobních údajů, jako dozorový úřad pověřený kontrolou nad dodržováním povinností stanovených při zpracování osobních údajů.

Význam zákona o ochraně osobních údajů spočívá zejména v tom, že připravil vhodnou půdu pro implementaci GDPR, jelikož vycházel z moderních přístupů k ochraně osobních údajů a naučil obce s osobními údaji vhodně pracovat. Průzkumem situace na vybraných obcích bylo zjištěno, že zákon o ochraně osobních údajů byl ve velké míře přesně dodržován, takže přechod na dodržování GDPR byl značně usnadněn. Navíc se tento zákon dočkal v roce 2004 významné novely kvůli transponování Směrnice 95/46/ES, což dále usnadnilo přechod k GDPR.

Významné bylo také zakotvení a zřízení Úřadu pro ochranu osobních údajů, který (jak už dnes víme) převzal funkci dozorového úřadu nad dodržováním GDPR.



Závěrem je tedy možné shrnout, že přijetí komplexního zákona upravujícího ochranu osobních údajů na území ČR vč. úpravy a zřízení orgánu pro kontrolu nad dodržováním tohoto zákona, bylo pro ČR významným krokem, který velkou měrou usnadnil implementaci GDPR. Ke dni zpracování tohoto dokumentu byl již zákon o ochraně osobních údajů zrušen a nahrazen zákonem o zpracování osobních údajů.

2.2 Zákon o zpracování osobních údajů

Zákon o zpracování osobních údajů č. 110/2019 Sb., (dále také ZZOU) nahradil právní úpravu obsaženou v zákoně o ochraně osobních údajů (č. 101/2000 Sb.) jako adaptační zákon nařízení GDPR. Tato skutečnost je dána tím, že vedle GDPR má každá země právo přijmout a používat tzv. adaptační zákon, který může ve vymezeném rámci upravovat doplňovat některé oblasti ochrany osobních údajů dle GDPR. Tento zákon je vybaven pouhými 68 § a nelze jej tak považovat za komplexní zákon upravující ochranu osobních údajů, přesto však upravuje důležité instituty. Zcela zásadní je v našem případě snížení pokut a vynětí odpovědnosti za přestupky na poli ochrany osobních údajů pro orgány veřejné moci. Nutno podotknout, že bez přijetí adaptačního zákona by mohla pokuta pro orgány veřejné moci činit až 20.000.000, - Eur.

Tato skutečnost přesto neznamena, že by byly obce zbaveny povinnosti, při výkonu své moci, postupovat při zpracování osobních údajů řádně a v souladu s nařízením GDPR. Dohled nad touto skutečností byl stanoven Úřadu pro ochranu osobních údajů.

2.3 Základní pojmy používané v ochraně osobních dat

Znalost základních pojmů a orientace v nich je základním pilířem k pochopení a správné aplikaci GDPR. GDPR v článku 4 obsahuje výčet definic, jenž ovlivňují samotnou aplikaci GDPR a také aplikaci některých povinností.

Alespoň elementární znalost základních pojmů je tak nezbytná pro správnou práci s nařízením i pro porozumění tomuto dokumentu. Pokud bychom to měli demonstrovat na příkladu, tak již první pojem „osobní údaj“ a jeho správné zařazení rozhoduje, zda je zpracovávaný údaj skutečně údajem osobním a patří tak do oblasti ochrany osobních údajů a nařízení se na ně vztahuje.



2.3.1 Osobní údaj

Osobní údaj je nejzásadnějším a nejpoužívanějším termínem v GDPR – jedná se o jakoukoliv informaci, týkající se identifikované nebo identifikovatelné fyzické osoby.⁴ Za identifikovatelnou fyzickou osobu lze označit každou fyzickou osobu, kterou je možné přímo, tedy přímým vztahem mezi údajem a osobou nebo nepřímo, přes spojení s disponujícím daty, identifikovat zejména odkazem na určitý identifikátor. Tímto identifikačním prvkem může být např. jméno a příjmení, rodné číslo, datum narození, povolání, kód, sociální nebo kulturní identita apod. Fyzická osoba, které se osobní údaje týkají, je subjektem údajů. Pro naše účely je vhodné uvést i další rozdělení údajů podle vazby k fyzické osobě, jedná se o:

- identifikační údaje osobní (jméno, příjmení atd.)
- číselné osobní údaje (např. datum narození)
- citlivé údaje (např. zdravotní stav)
- audiovizuální osobní údaje (např. fotografie)
- biometrické osobní údaje (např. otisky prstů)
- anonymní údaje – údaje které nemají přímou vazbu ke konkrétní fyz. osobě
- pseudoanonymizované údaje – údaje, které lze přiřadit ke konkrétní osobě jen za použití dalších údajů/dat
- zveřejněný osobní údaj – osobní údaje, které jsou součástí veřejných seznamů nebo jsou zpřístupněny sdělovacími prostředky

Pro příklad se uvádí tabulka znázorňující rozdíly mezi výše uvedeným:

Tabulka 1: Rozdělení osobních údajů

Údaje:	Jméno	Adresa	Věk	Stav	Hrubá mzda
Osobní údaje	Karel Novák	Náves 8, Radvanov 35601	33	Svobodný	18500
Anonymní údaje			33	Svobodný	18500

⁴ GDPR se tedy netýká právnických osob.



Pseudoanonymní údaje	001		33	Svobodný	18500
----------------------	-----	--	----	----------	-------

U pseudoanonymních údajů by pak byl údaj, že pod číslem 001 se skrývá jméno Karel Novák s bydlištěm Náves 8, Radvanov 356 01, uchovávan odděleně. Spojením těchto informací by pak byly údaje odtajněny.

2.3.2 Správce

Správce je fyzická nebo právnická osoba, pokud zpracovává osobní údaje. V našem případě tedy bude správcem obec, vykonávající jak samostatnou, tak přenesenou působnost. Obce mají v postavení správce povinnost zavést vhodná technická a organizační opatření, aby byly schopny doložit, že osobní údaje zpracovávají řádně a v souladu s nařízením GDPR. Tato opatření musí být samozřejmě řádně zdokumentována, sledována a průběžně aktualizována.

Správce je hlavním adresátem povinností, které stanoví nařízení GDPR.

2.3.3 Zpracovatel

Zpracovatelem je fyzická nebo právnická osoba, která osobní údaje zpracovává (pouze zpracovává) a to tak jak určí zpracovatel. Data předává správce zpracovateli na základě smluvního vztahu, zákonného zmocnění nebo na základě zákona. Je nutné podotknout, že předáním dat ke zpracování se správce nezbavuje své odpovědnosti. Proto musí smluvní vztah obsahovat ustanovení která zaručí, že zpracovatel bude dodržovat podmínky a požadavky GDPR. U obcí se nejčastěji setkáváme s tím, že v postavení zpracovatele je subjekt, který pro obec zpracovává účetnictví, mzdy apod. Pokud je mezi správcem a zpracovatelem uzavřena smlouva, musí tato obsahovat povinné náležitosti, smlouva tedy musí zpracovatele zavazovat k tomu, že:

- bude zpracovávat osobní údaje na základě pokynů správce
- zabezpečí mlčenlivost osob, které se zúčastní zpracování
- poskytne bezpečnostní opatření dle č. 32 GDPR
- dodrží podmínky pro řetězení zpracovatelů a bude se řídit pokyny správce



- smaže údaje po ukončení zpracování, dle pokynů správce.

2.3.4 Zpracování

Podle nařízení GDPR je zpracováním jakákoliv operace, která je prováděna s osobními údaji nebo se souborem osobních údajů s pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, šíření, omezení, výmaz, zničení apod. Důležitost pojmu zpracování spočívá ve skutečnosti, že pokud GDPR nevyhodnotí nějakou činnost jako zpracování osobních údajů, nespadá tato činnost do působnosti GDPR. Hlavními znaky zpracování je tak automatizované nebo částečně automatizované zpracování, případně neautomatizované zpracování těch údajů, které jsou obsaženy nebo budou zařazeny do evidence. Toto zpracování se pak musí týkat subjektů údajů, které GDPR definuje. Jako příklad zpracování, na které se GDPR nevztahuje, jsou např. fotografie z vánočního večírku zaměstnanců úřadu, které budou pořízeny pro rozeslání účastníkům. Naopak fotografie zaměstnanců do personální evidence již GDPR podléhat budou. Za typické zpracování tak můžeme považovat: personální agendu, evidenci obyvatel, adpod.

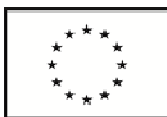
Je zde si třeba uvědomit, že i u osobních dat, na která se podle GDPR nevztahuje zpracování, je možné se domáhat ochrany, a to dle zákona č. 89/2012 Sb., občanský zákoník tedy v rámci institutu ochrany osobnosti.

2.3.5 Subjekt údajů

Subjekt údajů je dle GDPR fyzickou osobou, ke které se osobní údaje vztahují. GDPR se tak dotýká výhradně žijících fyzických osob. Zcela vyjmuta je tedy problematika právnických osob a zemřelých fyzických osob, která má být upravena na vnitrostátní úrovni. V případě fyzické osoby podnikající musíme rozlišovat údaje, které jsou spjaty s výkonem podnikatelské činnosti. Tyto údaje totiž pod ochranu GDPR nespadají.

2.3.6 Práva subjektu údajů

GDPR výrazně posiluje práva subjektu a údajů a rozšiřuje jejich okruh (oproti zákonu o ochraně osobních údajů nebo oproti Směrnici 95/46/ES). V první řadě by měla být vždy zaručena transparentnost zpracování a zachováno právo subjektu údajů na informace,



aniž by o výkon tohoto práva nebo o tyto informace musel správce žádat. Vysoká míra transparentnosti je spojena zejména s právem subjektu údajů na přístup k osobním údajům, které správce zpracovává. Základní informací pro každý subjekt údajů je také totožnost osoby správce (nebo jeho zástupce příp. pověřence).

Pokud je zpracování prováděno na základě právního důvodu, měl by subjekt údajů znát oprávněný zájem správce nebo třetí strany, který údaje zpracovává. Stejně tak by měl být subjekt údajů seznámen s tím, že správce hodlá předat zpracovávané údaje do třetích zemí. V neposlední řadě má každý subjekt údajů právo vědět, jaká je kategorie dotčených zpracovávaných údajů.

Správce samozřejmě může nad tento základní rámec poskytovat i další informace (což lze doporučit). Vhodné je například informovat o době, po kterou budou informace používány a o titulu na základě kterého jsou zpracovávány (důvod zpracování). Subjekt údajů má samozřejmě také právo vědět, z jakého zdroje byly informace získány, také by měl být informován o možnosti kontroly, opravy, doplnění nebo výmazu těchto dat, k tomuto se také váže právo podat námitku.

Subjekt údajů má samozřejmě také právo požádat o výmaz dat v případě, že již pominul důvod zpracování a shromažďování (nelze se tak domáhat výmazu údajů, které jsou zpracovávány na základě zákona a důvod tohoto zpracování trvá). Důvodem takového výmazu by mohlo být například odvolání souhlasu, pokud byly údaje na základě tohoto souhlasu získány. Mírnější formou výkonu práva než je výmaz, je možnost požádat o omezení zpracování – tedy užití získaných dat může být do budoucna, na žádost subjektu údajů, omezeno.

Předposledním právem subjektu údajů je nový institut práva na přenositelnost údajů. Toto právo obnáší možnost získat osobní údaje poskytnuté správci ve strukturovaném, běžně používaném a strojově čitelném formátu a zároveň tyto údaje předat jinému správci, a to i prostřednictvím správce stávajícího. Toto právo je možné prakticky využít například při změně telefonního operátora apod.

Posledním právem je pak právo na to nebýt předmětem automatizovaného zpracování, což znamená, že rozhodování s právními účinky vůči člověku není možné provádět plně automaticky. Např. nemůže být plně automaticky vyměřena pokuta na základě pozdně zaslání daňového přiznání do datové schránky finančního úřadu, ačkoliv dnes by to



již bylo prakticky možné (systém by identifikoval pozdní podání, subjekt a adresu a automaticky by vygeneroval správní rozhodnutí, které by vypravila automatická tiskárna a třídička). Samozřejmě výjimky z tohoto práva lze upravit např. pro kontraktační proces mezi subjektem a správcem údajů (např. automatické posouzení bonity při žádosti o půjčku).

2.3.7 Příjemce

Příjemce je zvláštní kategorií subjektu, protože osobní údaje sám nezpracovává, ale jsou mu při jejich zpracování zpřístupněny. Mezi příjemce můžeme řadit zejména dozorové a jiné orgány státní správy, poskytovatele informačních systémů, dodavatele služeb apod. Činnost příjemce při nakládání s osobními údaji samozřejmě spadá pod nařízení GDPR.

2.3.8 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů je nový pojem, který zákon o ochraně osobních údajů neznal. Hlavním úkolem pověřence by mělo být poskytování odborné pomoci v oblasti plnění povinnosti dle GDPR. Tento institut se dostal do nařízení GDPR na základě dobré praxe v institucích Evropské unie. Povinnost jmenovat pověřence je stanovena pouze pro některé správce, a to v souladu s přístupem založeným na riziku. Pověřenec pak může působit jako kontaktní místo pro dozorový orgán a pro subjekty údajů.

Vzhledem ke skutečnosti, že obce, se kterými bylo pracováno, jsou orgány veřejné moci, musí dle čl. 37 odst. 1 jmenovat pověřence pro ochranu osobních údajů, ačkoliv je sporné, zda pro jmenování nemusí být naplněny všechny podmínky pro povinné jmenování pověřence dle písm. a), b) a c). V této otázce nám pak dává vodítko Ministerstvo vnitra ČR, které ve svých metodických pokynech jednoznačně říká, že jsou obce povinny jmenovat pověřence pro ochranu osobních údajů (tato informace je aktuální k 25. 03. 2021). Obce tedy jmenují svého pověřence dle čl. 37 odst. 1 písm. a) a další je nemusí zajímat.



2.3.8.1 Úkoly pověřence pro ochranu osobních údajů

Úkoly pověřence jsou dány samotným nařízením GDPR. Obce, které jsou povinny pověřence jmenovat, tímto jmenováním částečně prokazují soulad zpracování s GDPR – tento pověřenec by pak měl pomáhat k dosažení a udržení souladu zpracování s GDPR. Toho má být dosaženo monitorováním souladu zpracování, zvyšování podvědomí o problematice ochrany osobních údajů, sledování aktuálních výkladů GDPR, příprava dokumentů, aktualizace analýzy rizik, karet zpracování, poskytování informací a poradenství. Dále má pověřenec poskytovat poradenství ve věci posouzení vlivu zpracování na ochranu osobních údajů. Jak již bylo uvedeno výše, pověřenec také funguje jako kontaktní místo pro subjekty zpracování a dozorový orgán.

V neposlední řadě má pověřenec za úkol prošetřovat stížnosti, které byly obdrženy od subjektů údajů. Další úkoly pověřence jsou pak na dohodě obou stran, která může mít různou podobou. Vždy je však třeba mít na paměti, že pověřenec nesmí být při výkonu své funkce ve střetu zájmů.

2.3.8.1.1 Odpovědnost pověřence

Ačkoliv je úkolem pověřence monitorování zpracování, není pověřenec za soulad zpracování osobně odpovědný. Odpovědnost leží vždy na správci (stejně jako např. za správnost účetnictví odpovídá podnikatel). Tím by měla být zajištěna zejména ochrana před formálním zaměstnáním pověřence, jen k naplnění požadavků GDPR.

Výše uvedeným není vyloučena odpovědnost za spáchané úmyslné poškození správce v souvislosti se souladem zpracování.

2.3.8.1.2 Požadavky na pověřence

Pověřenec pro ochranu osobních údajů může být fyzická nebo právnická osoba, jmenovaná na základě svých odborných a profesních kvality. Konkrétní požadavky však nejsou stanoveny GDPR ani zákonem o zpracování osobních údajů. Bude tak na správci, aby si volbu svého pověřence obhájil. Dále není nutné, aby pověřenec byl vybaven nějakým certifikátem, ačkoliv se před nabytím účinnosti GDPR našlo mnoho firem, které takovouto certifikaci nabízely. Takovýto certifikát je pak pouze potvrzením absolvování určitého kurzu a jeho váha bude značně ovlivněna kvalitou kurzu samotného.



2.3.8.2 Pověřenec pro ochranu osobních údajů na konkrétních obcích

Všechny obce, které jsou popisovány v tomto dokumentu, využívají jednotného pověřence: společnost ABRI, s. r. o., se sídlem: Ondříčkova 537, Sokolov 356 01. Podle internetových stránek se jedná o rozvojovou a dotační agenturu, která zároveň poskytuje služby pověřence pro ochranu osobních údajů. Šetřením na konkrétních obcích bylo zjištěno, že obce využívají služeb pověřence k příležitostným konzultacím konkrétní problematiky (např. zda je vhodné uveřejnit fotografie na webových stránkách, zda je možné uvádět konkrétní údaje v gratulacích v místním tisku apod.). Služby pověřence jsou tedy na obcích zajišťovány externě a jsou hrazeny paušálně, pravidelnou měsíční platbou.

Všechny obce mají pověřence stanoveného od doby nabytí účinnosti nařízení GDPR.

2.4 Dozorový úřad

Dozorový úřad je nezbytnou součástí ochrany osobních údajů při zpracování osobních údajů, a to z toho důvodu, že jsou mu svěřeny pravomoci k výkonu kontroly a další působnost. Podle nařízení GDPR je dozorový úřad nezávislým orgánem veřejné správy, který je zřízen členským státem. Základním úkolem každého dozorového úřadu je monitorování souladu s nařízením GDPR, uplatňování nařízení a ochrana práv a svobod subjektů údajů v souvislosti se zpracováním jejich osobních údajů.

Dozorový úřad však v ČR nemá neomezenou pravomoc, omezená pravomoc dozorového úřadu se projevuje zejména ve vztahu k soudnictví, kdy dozorový úřad nemá pravomoc dozoru nad zpracováním, které provádějí soudy jednající v rámci svých soudních pravomocí.

2.4.1 Úkoly dozorového úřadu

Úkoly dozorového úřadu jsou stanoveny přímo textem nařízení takto:

monitoruje a vymáhá uplatňování tohoto nařízení;

- zvyšuje povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním a podporuje porozumění těmto otázkám. Zvláštní pozornost se přitom věnuje akcím, které jsou určeny speciálně pro děti;



- v souladu s právem členského státu poskytuje poradenství vnitrostátnímu parlamentu, vládě a dalším orgánům a institucím ohledně legislativních a správních opatření týkajících se ochrany práv a svobod fyzických osob v souvislosti se zpracováním;
- podporuje povědomí správců a zpracovatelů o jejich povinnostech podle tohoto nařízení;
- na požádání poskytuje všem subjektům údajů informace ohledně výkonu jejich práv podle tohoto nařízení a, je-li to vhodné, spolupracuje za tímto účelem s dozorovými úřady v jiných členských státech;
- zabývá se stížnostmi, které mu podá subjekt údajů nebo subjekt, organizace či sdružení v souladu s článkem 80, a ve vhodné míře prošetřuje předmět stížnosti a v přiměřené lhůtě informuje stěžovatele o vývoji a výsledku šetření, zejména v případech, kdy je zapotřebí další šetření nebo koordinace s jiným dozorovým úřadem;
- s cílem zajistit jednotné uplatňování a prosazování tohoto nařízení spolupracuje s dalšími dozorovými úřady, mimo jiné formou sdílení informací, a s těmito úřady si vzájemně poskytuje pomoc;
- provádí šetření o uplatňování tohoto nařízení, mimo jiné na základě informací obdržených od jiného dozorového úřadu či jiného orgánu veřejné moci;
- monitoruje vývoj v relevantních oblastech, pokud má vliv na ochranu osobních údajů, zejména vývoj informačních a komunikačních technologií a obchodních praktik;
- přijímá standardní smluvní doložky uvedené v čl. 28 odst. 8 a čl. 46 odst. 2 písm. d);
- připravuje a udržuje seznam v souvislosti s požadavkem provádět posouzení vlivu na ochranu osobních údajů podle čl. 35 odst. 4;
- poskytuje poradenství o operacích zpracování uvedených v čl. 36 odst. 2;



- podporuje vypracování kodexů chování podle čl. 40 odst. 1, vydává stanoviska a schvaluje takové kodexy chování, které poskytují dostatečné záruky podle čl. 40 odst. 5;
- vybízí k zavedení mechanismů pro vydávání osvědčení o ochraně údajů a pečeti a známek dokládajících ochranu údajů podle čl. 42 odst. 1 a schvaluje kritéria pro vydávání osvědčení podle čl. 42 odst. 5;
- případně provádí pravidelný přezkum osvědčení vydaných v souladu s čl. 42 odst. 7;
- navrhuje a zveřejňuje kritéria pro schvalování subjektu pro monitorování kodexů chování podle článku 41 a subjektu pro vydávání osvědčení podle článku 43;
- provádí schvalování subjektu pro monitorování kodexů chování podle článku 41 a subjektu pro vydávání osvědčení podle článku 43;
- schvaluje smluvní doložky a ustanovení uvedené v čl. 46 odst. 3;
- schvaluje závazná podniková pravidla podle článku 47;
- přispívá k činnostem sboru;
- vede interní záznamy o porušeních tohoto nařízení a o opatřeních přijatých podle čl. 58 odst. 2; a
- plní veškeré další úkoly související s ochranou osobních údajů,

a je dobré zdůraznit, že tyto úkoly jsou pro subjekty údajů a pověřence pro ochranu osobních údajů bezplatné. Nicméně zjevně nedůvodné nebo nepřiměřené požadavky může úřad odmítnout nebo za ně uložit přiměřený poplatek.

2.4.2 Pravomoci dozorového úřadu

Pravomoci Úřadu pro ochranu osobních údajů dělíme dle nařízení GDPR následovně:

Pravomoci vyšetřovací:

- nařídit správci a zpracovateli, případně zástupci správce nebo zpracovatele, aby mu poskytli veškeré informace, které potřebuje k plnění svých úkolů;
- provádět vyšetřování formou auditů ochrany údajů;



- provádět přezkum osvědčení vydaných v souladu s čl. 42 odst. 7;
- ohlásit správci nebo zpracovateli údajné porušení tohoto nařízení;
- získat od správce a zpracovatele přístup ke všem osobním údajům a ke všem informacím, které potřebuje k výkonu svých úkolů;
- získat přístup do všech prostor, v nichž správce a zpracovatel působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů, v souladu s procesním právem Unie nebo členského státu.

K naplnění této pravomoci bude Úřadu sloužit zejména kontrolní řád (zákon č. 255/2012 Sb.) a správní řád (zákon č. 500/2004 Sb.). Základním nástrojem je pak provádění auditů (kontrol).

Pravomoci nápravné:

- upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení;
- udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily toto nařízení;
- nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení;
- nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;
- nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů;
- uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu;
- nařídit opravu či výmaz osobních údajů nebo omezení zpracování podle článků 16, 17 a 18 a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny podle čl. 17 odst. 2 a článku 19;
- odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení vydané podle článků 42 a 43, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny;



- uložit správní pokutu podle článku 83 vedle či namísto opatření uvedených v tomto odstavci, podle okolností každého jednotlivého případu;
- nařídit přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.

Pravomoci povolovací a poradní:

- poskytovat poradenství správci v souladu s postupem předchozí konzultace podle článku 36;
- z vlastního podnětu nebo na požádání vydávat stanoviska určená vnitrostátnímu parlamentu, vládě členského státu nebo v souladu s právem členského státu dalším institucím a subjektům, jakož i veřejnosti, ohledně veškerých otázek souvisejících s ochranou osobních údajů;
- povolovat zpracování uvedené v čl. 36 odst. 5, pokud právo členského státu takové předchozí povolení vyžaduje;
- vydávat stanoviska a schvalovat návrhy kodexů chování podle čl. 40 odst. 5;
- akreditovat subjekty pro vydávání osvědčení podle článku 43;
- vydávat osvědčení a schvalovat kritéria pro vydávání osvědčení podle čl. 42 odst. 5;
- přijímat standardní doložky o ochraně údajů podle čl. 28 odst. 8 a čl. 46 odst. 2 písm. d);
- povolovat smluvní doložky podle čl. 46 odst. 3 písm. a);
- povolovat správní ujednání podle čl. 46 odst. 3 písm. b);
- schvalovat závazná podniková pravidla podle článku 47.

Dozorové úřady mají také stanovenou povinnost spolupracovat při uplatňování nařízení GDPR a poskytovat si informace, nesmíme totiž zapomínat, že nařízení platí pro všechny členské státy EU. Pokud tuzemský dozorový úřad zašle žádost úřadu v jiném členském státu, musí tento žádosti vyhovět do jednoho měsíce (pokud nebude mít důvody pro odložení nebo nevyhovění žádosti).



2.4.3 Vedoucí dozorový úřad

Jak bylo nastíněno výše, každá členská země EU má svůj dozorový úřad, který vykonává dohled nad dodržováním nařízení GDPR. Správce osobních údajů však může provádět zpracování, které se dotýká subjektů údajů z více členských států nebo dokonce může působit ve více členských státech. Z tohoto důvodu byl ustanoven ještě vedoucí dozorový úřad. Kromě samotné úpravy působnosti pak nařízení GDPR stanoví podmínky a povinnosti vzájemné součinnosti vedoucího dozorového úřadu a dozorových úřadů v jednotlivých členských státech.

Smyslem vedoucího dozorového úřadu je, aby i v případech přeshraničního zpracování byly vůči správci a zpracovateli efektivně využity pravomoci jedním dozorovým úřadem a daný subjekt tak byl efektivně postihnut za přeshraniční zpracování jedním dozorovým úřadem, než kdyby mělo jeho jednání dozorovat např. pět dozorových úřadů jednotlivě.

Další otázky ohledně přeshraničního zpracování již nebudou tímto textem řešeny, protože nedopadají na obce, které jsou v postavení správce a pro které je tento dokument zpracováván.

3. Zpracování osobních údajů a jeho zásady

Pojem zpracování osobních údajů je dalším základním pojmem, bez jehož vysvětlení není možné pokračovat ve smysluplné a soustavné práci na implementaci GDPR. Jak již bylo uvedeno výše v této analýze zpracování osobních údajů je tedy činnost, při které dochází k aplikaci pravidel GDPR – jakékoliv nakládání s osobními údaji tak nelze automaticky považovat za zpracování. Zpracování osobních údajů je definováno jako činnost soustavná a systematická, za využití automatizace, či jiných prostředků.

Obecné nařízení pak definuje zpracování jako operaci nebo soubor operací s osobními údaji, která je prováděna s osobními údaji nebo soubory osobních údajů (s pomocí nebo bez pomoci automatizace), jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použití,



zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

V tomto kontextu je nutné zmínit, že dotečené obce nevyužívají automatizaci, ale neautomatizované zpracování osobních údajů, které jsou obsaženy v evidenci nebo do ní budou zařazeny.

Při všech činnostech zpracování musí být dodrženy základní zásady pro zpracování osobních údajů, těmito zásadami jsou: zákonnost, korektnost, transparentnost, omezení účelu, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost. Všechny zásady budou podrobně popsány níže.

3.1 Zásada zákonnosti

Jedná se o nejdůležitější zásadu při zpracování osobních údajů a to proto, že nám říká, že správce osobních údajů musí mít pro zpracování alespoň jeden zákonný/právní důvod. Za tento důvod se pak považuje oprávnění, předpokládané právním řádem, v našem případě tedy nejen nařízením GDPR ale i tuzemskými právními předpisy, které dávají správci oprávnění zpracovávat osobní údaje za určitým legitimním účelem.

Pokud u správce absentuje právní důvod zpracování, je takovýto správce povinen osobní údaje, které zpracovává, odstranit. Uplatní-li se absence právního důvodu jen na část zpracovávaných osobních údajů, je pak správce povinen odstranit tuto dotčenou část.

Pokud chybí právní důvod zpracování od začátku, jedná se o nelegální zpracování. Přítomnost právního důvodu zpracování je tedy základním předpokladem proto, abychom mohli mluvit o legálním zpracování osobních údajů. Právní důvody zpracování jsou pak uvedeny v čl. 6 odst. 1 GDPR, případně v čl. 9 odst. 2 GDPR pro zvláštní kategorie osobních údajů.

3.2 Zásada korektnosti a zásada transparentnosti

Zásada korektnosti znamená, že správce vždy musí subjektu údajů sdělit účel zpracování a poskytnout další nezbytné informace, tedy kdo a jak údaje zpracovává, popřípadě komu budou předány.



Jako důležitější se zde jeví související zásada transparentnosti, která říká, že informace, které subjekt údajů obdrží, musí být dostatečně přesné, srozumitelné a přístupné. Tato zásada je pak promítnuta do práva subjektu údajů na přístup k osobním údajům a v ustanoveních o poskytování informací správcem subjektu údajů.

3.3 Zásada omezení účelu

Tato zásada nám říká, že osobní údaje musí být zpracovávány a shromažďovány vždy po určitý legitimní účel, který je výslovně vyjádřený. Od účelu zpracování se pak odvíjí právní důvod zpracování (který je, jak bylo uvedeno výše, zcela zásadní). Zpracovává-li tedy správce osobní údaje za konkrétním účelem který pomine, je povinen tyto osobní údaje zlikvidovat, není-li dán jiný účel zpracování (např. povinnost archivace). Obecné nařízení dokonce stanoví, že správce musí přijmout vhodná technická a organizační opatření tak, aby byly zpracovány pouze osobní údaje, které jsou pro každý konkrétní účel daného zpracování nezbytné.

3.4 Zásada minimalizace údajů

Zásada minimalizace údajů nám říká, že osobní údaje mají být zpracovávány pouze v přiměřené míře, relevantně a nezbytně ve vztahu k účelu zpracování. Správce tak v souvislosti se zpracováním nemůže požadovat po subjektu údajů více údajů, než je nezbytně nutné. Zásada minimalizace údajů může do jisté míry správci pomoci, protože méně shromážděných údajů pomáhá k zvýšení bezpečnosti a k lepšímu přehledu o osobních údajích, které jsou zpracovávány.

3.5 Zásada přesnosti

Osobní údaje musí být zpracovány přesně a měly by být průběžně aktualizovány. Tato zásada nám říká, že pokud správce narazí na zjevně nepřesné nebo neaktualizované údaje měl by poskytnout kroky k nápravě. Možností nápravy je pak oprava zpracovávaného údaje nebo jeho výmaz. Provádění této zásady má nám zaručuje právo na opravu a doplnění osobních údajů dle čl. 16 GDPR a právo na omezení zpracování dle článku 18 GDPR. V běžném životě lze na tuto aplikovanou zásadu narazit např. při vytváření nového hesla – systém většinou vyžaduje dvojí zadání hesla, aby bylo



odstraněno riziko překlepů či nepřesností. Stejně tak často např. internetové stránky vyžadují zadání e-mailu. Na tento e-mail je pak zaslán potvrzující odkaz. Tento postup má zabránit nesprávnému uvedení údajů – v tomto případě emailu, který je např. pro poskytovatele služeb důležitou informací.

3.6 Zásada omezení uložení

Tato zásada je opět svázána s účelem zpracování, kdy by osobní údaje neměly být uloženy déle než to účel zpracování vyžaduje. Zde si musíme uvědomit, že to že „cizí“ subjekt má k dispozici osobní údaje o nějaké osobě, představuje (někdy ne nevýznamné) bezpečnostní riziko. Proto je správce údajů povinen všechny osobní údaje zlikvidovat, pokud pomine účel zpracování. Tato skutečnost je i výslovně zakotveným právem subjektu údajů (právo na výmaz).

3.7 Zásada integrity a důvěrnosti

Zpracovávané osobní údaje by měly být zpracovávány celistvě, důvěryhodným, ověřitelným způsobem. Tento požadavek klade nároky zejména na systémy provádějící automatizované zpracování. Ochrana spočívá zejména v zabránění ztrátě, zcizení nebo poškození. Zabezpečení osobních údajů musí vždy odpovídat povaze, rozsahu, kontextu a účelům zpracování.

4. Právní důvody zpracování

Právní důvod zpracování je základním předpokladem pro legální zpracování osobních údajů. Každé zpracování tak musí probíhat na základě prvního důvodu, jehož absenci nelze zhojit. Proto je právním důvodům zpracování vyhrazen prostor i v tomto dokumentu.

Důležité pro správce osobních údajů je si uvědomit, že zpracování osobních údajů se děje za určitým účelem a právní důvod zpracování musí tento účel pokrývat. Určité údaje mohou být zpracovávány pro více účelů, a tedy může jim svědčit i více právních důvodů zpracování. Vždy je však nutné, aby tu byl alespoň jeden právní důvod



zpracování. Pokud tento právní důvod zpracování zanikne v průběhu zpracování (např. odvolání souhlasu subjektu údajů) je správce povinen zpracovávané osobní údaje zlikvidovat.

4.1 Souhlas subjektu údajů

Souhlas subjektu údajů je prvním právním důvodem zpracování, se kterým se každý setkává v běžném životě. V roce 2018, kdy nařízení GDPR vstoupilo v účinnost začali správci osobních údajů doslova chrlit souhlasy a požadovali po každém subjektu údajů jeho souhlas. Tímto krokem se správci chtěli vyhnout drakonickým pokutám a většinou ani nevěděli, že pro zpracování osobních údajů jim svědčí jiný právní důvod (např. plnění smlouvy). Začalo tak podepisování a udělování souhlasů „pro jistotu“, což brzy zastavil Úřad pro ochranu osobních údajů, který ve svých doporučeních důrazně varoval před nadbytečným vyžadováním souhlasů a zejména poukazoval na jejich nadbytečnost a případnou odvolatelnost.

Samotný souhlas je definován jako svobodný, konkrétní, informovaný a jednoznačný projev vůle, který je dáván prohlášením nebo zjevným potvrzením. Jak bylo uvedeno výše, souhlas by měl být použit pouze v tom případě, že správci nesvědčí jiný právní důvod zpracování. Nejčastěji se tak se souhlasem můžeme setkat spíše jako s doplňkovým institutem, který slouží např. správci, který může zpracovávat část osobních údajů subjektu údajů na základě smlouvy. Pokud by v našem případě obec vyžadovala udělení souhlasu, je nutné, aby tento souhlas byl přezkoumatelný. Není tedy vhodné vyjádření souhlasu např. konkludentně. Navíc nařízení říká, že souhlas má splňovat určitá kritéria, kterými jsou: uvedení totožnosti správce, účelu zpracování, rozsahu zpracovávaných osobních údajů a informace o právu subjektu údajů souhlas odvolat.

Tím se dostáváme ke skutečnosti, že souhlas je odvolatelný. To je také důvod, proč vyžadování souhlasu není, v případě obcí jako správců, příliš vhodné. Pokud subjekt osobních údajů svůj souhlas odvolá, je správce povinen zpracovávané osobní údaje odstranit (nesvědčí-li mu pro zpracování jiný právní důvod zpracování).



4.2 Plnění smlouvy

Zpracování osobních údajů na základě plnění smlouvy je častým právním důvodem, se kterým se obce setkávají. Na základě tohoto lze tedy zpracovávat takové osobní údaje, které jsou nezbytné pro plnění smlouvy. Nezřídka jsou takovéto údaje dále uveřejňovány obcí např. v registru smluv nebo na profilu zadavatele. Plnění smlouvy je tedy jasně ohraničeným účelem zpracování, který může být doplněn o účel zpracování před uzavřením smlouvy při plnění souvisejících opatření. Před uzavřením smlouvy totiž často probíhají jednání o uzavření smlouvy, jsou vznášeny dotazy na správce nebo jsou předkládány nabídky. Všechny tyto údaje jsou pak zpracovávány za konkrétním účelem (smlouvy) a na základě jasného právního důvodu (plnění smlouvy). V souvislosti s plněním smlouvy je vhodné brát ohled na zásadu minimalizace údajů.

4.3 Plnění zákonem stanovené povinnosti

Obce jako správce osobních údajů plní v samostatné působnosti celou řadu zákonných povinností a v této souvislosti zpracovávají osobní údaje subjektů údajů na základě zákonem stanovené povinnosti. Tato povinnost tedy vyplývá především z tuzemské právní úpravy případně z práva Evropské unie. Zákonem je správci stanoven účel zpracování a případně rovněž rozsah a kategorie zpracovávaných osobních údajů, které je správce povinen pro tento účel zpracovávat.

Pokud je správci stanovenou pouze splnění určité povinnosti, která v sobě zahrnuje rovněž zpracování osobních údajů, použije správce zásadu omezení účelu zpracování a zásadu minimalizace údajů.

4.4 Ochrana životně důležitých zájmů subjektu údajů

Tento právní důvod zpracování není v době zpracování tohoto dokumentu využíván (ani nebyl využit) žádnou obcí. Zpracování osobních údajů na základě životně důležitého zájmu jiné fyzické osob, aby mělo v zásadě proběhnout pouze, tehdy pokud zjevně nemůže být založeno na jiném právním základě. Některé důhly zpracování mohou sloužit jak důležitým důvodům veřejného zájmu, tak životně důležitým zájmům subjektu údajů, např. je-li zpracování nezbytné pro humanitární účely, včetně monitorování epidemií a jejich šíření nebo v naléhavých humanitárních situacích,



zejména v případech přírodních a člověkem způsobených katastrof. Ač je tato možnost obcím dána, nebyla využita ani v rámci koronavirové krize, která začala v březnu roku 2020.

4.5 Plnění úkolů ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen

Zásadním právním důvodem zpracování pro obce je plnění úkolů, které jsou jim svěřeny v rámci přenesené působnosti. Je to tedy výkon veřejné správy nebo výkon veřejné moci, který ospravedlňuje správce ke zpracování osobních údajů subjektů zpracování. Při uplatňování tohoto právního důvodu zpracování dochází velmi často k souběhu s důvodem „plnění zákonem stanovené povinnosti“. Plnění úkolů při výkonu veřejné moci je ovšem právním důvodem, který může zahrnovat širší okruh záležitostí.

4.6 Oprávněný zájem správce

Oprávněný zájem správce je právní důvod zpracování, který v sobě zahrnuje více důvodů, které nemohou být podřazeny pod výše uvedené. Právě vzhledem k jeho rozmanitosti, je poměrně složité jednoznačné určení, co je „oprávněným zájmem“ správce a co již nikoliv. Správce tak při užití tohoto důvodu musí vždy pečlivě zvážit, zda jsou jeho oprávněné zájmy větší než základní práva a svobody subjektu údajů. Jedná se o tzv. test proporcionality, ten znamená, že by subjekt údajů měl důvodně očekávat, že správce bude jeho osobní údaje zpracovávat a v jaké míře je bude zpracovávat. Nařízení nám příkladem říká, že k takovému zpracování může dojít např. pokud chce správce zabránit podvodům, či uplatňuje své marketingové zájmy. Obce se s tímto právním důvodem setkávají zejména v případě provozu kamerového systému, což je oprávněný zájem správce racionální a obhajitelný (ochrana majetku, péče řádného hospodáře) Za neobhajitelný oprávněný zájem správce pak lze považovat např. zveřejnění seznamu dlužníků v obecních bytech.

5. Zabezpečení osobních údajů

Řádné zabezpečení osobních údajů by mělo být na straně správce/obcí samozřejmostí. Obecně lze říci, že obce musí při zabezpečení osobních údajů uplatňovat přístup



založený na riziku a přijmout bezpečnostní opatření odpovídající danému riziku, zejména tak na obce může být kladen požadavek:

- šifrování a pseudonymizace osobních údajů
- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
- schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů
- procesu pravidelného testování posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Na všech obcích jsou pak osobní údaje zpracovávány pomocí počítačů. Prvním úkolem na obcích tak bylo revidovat zabezpečení spojené právě s těmito elektronickými zařízeními. V rámci veřejné správy pak každá obec zveřejňuje na internetu celou řadu dokumentů. Problematické je v tomto případě třeba zjistit, zda došlo k odcizení některých dokumentů (nechybí „fyzická“ kopie). Proto je důležité a bylo to prosazováno, aby každá obec řádně zabezpečila všechny počítače, na kterých pracují zaměstnanci obce a aby proběhlo školení o bezpečném používání internetu. Není totiž tajemstvím, že většinu bezpečnostních incidentů při tomto zpracování zaviní právě lidský faktor, ať již úmyslně nebo z nedbalosti.

Dále obce zpracovávají celou řadu údajů manuálně prostřednictvím evidencí v listinné podobě. Zde lze rovněž doporučit vhodně zabezpečit materiály a dokumenty, které obsahují osobní údaje. Častým nešvarem na obcích bylo např. nechávání dokumentů na stole, takže každý, kdo přišel na úřad, se mohl při vstupu do kanceláře seznámit se všemi položenými dokumenty. Tato praxe se naštěstí rychle ukázala jako nevhodná a je od ní v současné době upouštěno. Dále proběhla na obcích revize uzamykatelných skříní (pro zvláště citlivé dokumenty) a vyhodnocení dalších technických prostředků (zámky, bezpečnostní zařízení).

V neposlední řadě bylo na obcích doporučeno zpracování bezpečnostní směrnice a seznamu osob, které mají přístup k heslům pro počítače nebo ke klíčům od archivů apod.



5.1 Ohlašování případů porušení zabezpečení

Nařízení GDPR klade správci povinnost nahlášení případu porušení zabezpečení osobních v případě, že vznikne riziko pro práva a svobody fyzických osob. V případě, že toto riziko vyhodnotí správce jako mimořádné, je dokonce povinen toto porušení nahlásit do 72 hod od vzniku porušení, resp. od chvíle, kdy se o porušení dozvěděl. Situace se bude nahlašovat Úřadu pro ochranu osobních údajů.

Účelem této povinnosti je ochrana práv a svobod fyzických osob, která má být zajištěna v součinnosti s dozorovým úřadem, který poskytne správci zpětnou vazbu a reakci na situaci. Výše uvedená povinnost tak má preventivní charakter, protože pomůže správci minimalizovat dopady porušení zabezpečení.

Nařízení pak uvádí obligatorní náležitosti takového nahlášení:

- popis povahy daného případu, včetně kategorií a přibližného počtu dotčených subjektů údajů a množství dotčených záznamů (vše přibližně)
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů, pokud byl ustaven,
- popis pravděpodobných důsledků
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit porušení, včetně opatření zmiňujících dopad porušení.

Vše by samozřejmě mělo být řádně zdokumentováno, pro případ dalšího šetření.

Vyjma povinnosti oznámení dozorovému úřadu, má obec ještě povinnost oznámit porušení zabezpečení osobních údajů také subjektu údajů, kterého se porušení týká (nebo může týkat). Jedná se ale pouze o situaci kdy můžeme předpokládat následek, který bude obsahovat vysoké riziko pro práva a svobody fyzických osob. V případě takového porušení musí být porušení oznámeno subjektu údajů bez zbytečného odkladu (již zde není stanovených 72 hodin). Takovéto oznámení by mělo být jasné a srozumitelné a učiněno tak, aby sám subjekt údajů měl možnost přijmout adekvátní opatření.



6. Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů a povinná konzultace s dozorovým úřadem jsou nové instituty zavedené GDPR, se kterými se může obec v postavení správce setkat. Oba tyto instituty v sobě zahrnují přístup založený na riziku, a to z toho důvodu, že se uplatňují pouze v případě, že uvažované zpracování představuje vysoké riziko pro práva a svobody fyzických osob. Z výše uvedeného je patrné, že obce se v postavení správce s těmito instituty s větší pravděpodobností nesetkají. Obdobnou povinnost měli totiž tuzemští správci stanovenou v § 16 odst. 1 zákona o ochraně osobních údajů, kdy bylo nutné předem hlásit riziková zpracování tak, aby Úřad pro ochranu osobních údajů včas zaznamenal riziková zpracování a mohl jim věnovat náležitou pozornost.

6.1 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů je tedy prvním institutem, který musí správce provést, provádí-li vysoce rizikové zpracování. Dá se tedy přepokládat, že by se jednalo např. o zpracování s využitím nových automatických technologií apod. V tomto případě by tedy výše uvedené posouzení muselo být provedeno, a to ještě před samotnou operací zpracování osobních údajů.

Účelem posouzení je tak zejména eliminace rizik, které vysoce rizikové zpracování osobních údajů pro práva a svobody subjektů údajů představují.

Dozorové úřady jsou povinny sestavit seznam rizikových zpracování, aby usnadnili správčům rozhodování, při jakém zpracování musí posoudit vliv na ochranu osobních údajů. Vycházíme-li z dokumentů, které uveřejnil Úřad pro ochranu osobních údajů, zjistíme, že vysoce rizikové zpracování je to, které splňuje některý z níže uvedených bodů:

- provádí se ohodnocení nebo hodnocení bonity fyzických osob, včetně profilování a předpovědi,
- provádí se automatické rozhodování s právním nebo obdobným významným účinkem,



- provádí se systematické monitorování, včetně monitorování veřejně přístupných prostor,
- provádí se zpracování citlivých údajů,
- provádí se zpracování velkého rozsahu,
- provádí se kombinace nebo propojování dat různých zpracování,
- provádí se zpracování údajů týkající se zranitelných subjektů údajů,
- dochází k inovativnímu využití nebo aplikaci technologických nebo organizačních řešení
- provádí se zpracování s obtížně uplatnitelnými právy subjektů údajů - pro procesy prováděné ve veřejné oblasti, jimž se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnout přístup subjektů údajů k službě nebo uzavření smlouvy.

Dále lze dovodit dle č. 35 odst. 3 nařízení, že posouzení vlivu je nutno provádět u zpracování, které obsahuje:

- systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založena na automatizovaném zpracování, včetně profilování, na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,
- rozsáhlé zpracování zvláštních kategorií osobních údajů uvedených v čl. 9 odst. 1 GDPR nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10 GDPR
- rozsáhle systematické zpracování a monitorování veřejně přístupných prostorů.
- Samotné posouzení vlivu pak obsahuje minimálně tyto náležitosti:
- systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce,
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,



- posouzení rizik pro práva a svobody subjektů údajů,
- plánovaná opatření k řešení rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a doložení souladu s Obecným nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Nařízení GDPR pak stanoví, že by správce měl v takovémto případě získat k předběžnému posouzení stanovisko dotčených subjektů osobních údajů nebo jejich zástupců.

V době zpracování tohoto dokumentu žádná z dotčených obcí neprováděla vysoce rizikové zpracování podléhající povinnosti vypracování předběžného posouzení ani se nedá předpokládat, že by v dohledné době toto vysoce rizikové zpracování prováděla.

6.2 Předchozí konzultace s dozorovým úřadem

Povinná předchozí konzultace s dozorovým úřadem se uplatní pouze tehdy, pokud z posouzení vlivu na ochranu osobních údajů správce zjistí, že zamýšlené zpracování má za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika. Jde tedy o povinnost navazující na posouzení vlivu na ochranu osobních údajů v případě, že ani správcem přijatá opatření nejsou dostatečná ke snížení rizika při vysoce rizikovém zpracování osobních údajů.

Žádost o konzultaci se podává, společně s vyjádřením pověřence, k dozorovému úřadu, který k věci vydá vyjádření.

7. Práva subjektu údajů

Subjekt osobních údajů je ve vztahu se správcem často slabší stranou, jelikož je to právě on, kdo často musí zpracování osobních údajů strpět. K rovnosti tohoto vztahu pak přispívají nařízením stanovená práva subjektu osobních údajů. Nařízení GDPR pak



zpracovává práva subjektu údajů velmi podrobně tak, aby správce zajistil řádný soulad zpracování.

V obecné rovině nám nařízení GDPR říká, že správce musí informovat či provádět výkon práv subjektu údajů stručně, transparentně, srozumitelně a snadno přístupným způsobem, za použití jednoduchých jazykových prostředků. Přičemž není vyloučena žádná forma, tedy písemná, elektronická ani ústní. Dále je obecně stanoveno, že správce musí poskytnout subjektu údajů informace o přijatých opatřeních do 1 měsíce od obdržení žádosti, případně bezodkladně, je-li to v daném případě možné. Tuto lhůtu lze prodloužit maximálně na dva měsíce, s ohledem na složitost a četnost žádostí.

V případě že správce nevyhoví subjektu údajů, musí to tomuto subjektu sdělit a informovat jej o možnosti podat stížnost u dozorového úřadu. Subjekt údajů se v tomto případě také může domáhat soudní ochrany.

Aby správci osobních údajů nebyli zbytečně zahlceni žádostmi, dává GDPR možnost obrany a to dvojí: zaprvé stanovit přiměřený poplatek za zpracování žádostí, za druhé odmítnout žádosti vyhovět v případě, že je nedůvodná nebo nepřiměřená. Obce, na kterých byla analýza GDPR prováděna jsou si této skutečnosti vědomi, protože možnost obdobného postupu jim dává zákon č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění.

7.1 Právo na informace

Právo na informace je právem základním, které musí být dodrženo za každých okolností k naplnění zásady transparentnosti. Každý subjekt údajů má totiž právo být řádně informován o zpracování jeho osobních údajů. Právo na informace tedy představuje pro správce aktivní povinnost, kterou musí splnit automaticky (nikoliv například až po dotazu subjektu údajů). Nařízení GDPR pak v této souvislosti rozlišuje informace podle toho, zda je správce získal přímo od subjektu osobních údajů či nikoliv. Správce je tedy vždy povinen poskytnout subjektu údajů tyto informace:

- totožnost a kontaktní údaje správce a jeho případného zástupce,
- kontaktní údaje na pověřence, byl-li ustaven,
- účely zpracování a právní důvody zpracování,



- oprávněné zájmy správce nebo třetí strany, pokud je zpracování prováděno na základě tohoto právního důvodu,
- případní příjemce nebo kategorie příjemců osobních údajů,
- případný úmysl správce předat osobní údaje do třetí země a právní podklad, na základě kterého dojde k předání,
- kategorie dotčených osobních údajů.

Ve výše uvedeném pak lze najít drobné odchylky, a to například ty, že v případě, kdy správce získá údaje přímo od subjektu osobních údajů, nemusí mu sdělovat kategorie dotčených osobních údajů. Přesto však lze správcům (zejména obcím) doporučit, aby informoval o všech výše uvedených bodech, je-li to relevantní ve vztahu k subjektu údajů a má-li tyto informace k dispozici.

Nad rámec výše uvedených musí v odůvodněných případech (je-li to nezbytné pro zajištění spravedlivého a transparentního zpracování) poskytnout tyto další informace:

- doba po kterou budou údaje uloženy, nebo stanovení výpočtu této doby,
- oprávněné zájmy správce nebo třetí strany (pokud je zpracováváno na základě oprávněného zájmu),
- existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu, výmaz nebo práva vznést námitku a práva na přenositelnost,
- možnost odvolat souhlas subjektu údajů,
- existence práva podat stížnost u dozorového úřadu,
- zdroj, ze kterého osobní údaje pocházejí, případně informace, zda pocházejí z veřejných zdrojů,
- skutečnost, zda poskytnutí osobních údajů je zákonným či smluvním požadavkem a důsledky neposkytnutí osobních údajů,
- skutečnost, zda dochází k automatizovanému rozhodování

Samozřejmostí pak je, že výše uvedené body nemusí být využity vždy v plném rozsahu, vždy záleží na rozsahu zpracování, jeho charakteru a kontextu. Informace se vždy



poskytují v tom rozsahu, v jakém s nimi subjekt údajů nedisponuje. Nařízení GDPR u některých informací stanoví i lhůtu pro jejich poskytnutí (pokud má tyto informace správce bez vědomí subjektu podle čl. 14 odst. 3), lhůty jsou pak nastaveny takto:

- v přiměřené lhůtě, nejpozději však do měsíce
- nejpozději k okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity v této komunikaci
- nejpozději při prvním zpřístupnění osobních údajů, pokud je má správce v úmyslu zpřístupnit příjemci.

Poskytování informací by mělo být vždy jednoduché a srozumitelné v přiměřeném rozsahu, tak, aby subjekt údajů nebyl zahlcen několika stranami textu, ve kterém se snadno může přestat orientovat, či mu mohou unikat souvislosti.

7.2 Právo na přístup k osobním údajům

Právo na přístup k osobním údajům úzce souvisí se zásadou transparentnosti, jedná se o aktivní právo subjektů osobních údajů – subjekt jej využívá svým aktivním přístupem dle vlastního uvážení. Oproti práva na informace tedy vzniká povinnost správce až aktivním jednáním subjektu údajů. Cílem práva na přístup k osobním údajům je získání potvrzení pro subjekt osobních údajů o skutečnosti, zda a jakým způsobem jsou zpracovávány jeho osobní údaje. Subjekt údajů musí mít zajištěn přístup k těmto údajům:

- účely zpracování,
- kategorie dotčených osobních údajů,
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- doba, pro kterou budou osobní údaje uloženy, nebo kritérium stanovení této doby,
- právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji osobních údajů, pokud nebyly získány od subjektu údajů,



- skutečnost, zda dochází k automatizovanému rozhodování, včetně profilování a související smysluplné informace týkající se použitého postupu.

V první řadě tak subjekt údajů získá potvrzení o tom, zda jsou jeho osobní údaje skutečně zpracovávány. Povinností správce je i sdělení toho, že žádné osobní údaje subjektu údajů nezpracovává. V případě, že zpracovávány jsou, poskytne správce všechny informace dle výše uvedených bodů. Stejně tak má správce povinnost poskytnout subjektu údajů kopii zpracovávaných údajů a další informace. Tyto služby jsou pro subjekt údajů poskytovány bezplatně (musí být – v případě velkého rozsahu lze účtovat pouze poplatek nepřevyšující administrativní náklady).

7.3 Právo na opravu a doplnění

Právo na opravu a doplnění je specifickým právem, které souvisí s tím, že zpracovávané informace (údaje) mají být přesné, úplné, správné a aktualizované. Je to tedy právo subjektu údajů požadovat, aby správce opravil nepřesné osobní údaje nebo doplnil osobní údaje chybějící. Pokud tedy správce žádost o opravu nebo doplnění osobních údajů obdrží, musí vyvinout adekvátní úsilí na odstranění závadného nebo nevyhovujícího stavu. Toto právo je stanovena zejména kvůli tomu, že správce nemá povinnost aktivně vyhledávat nepřesné osobní údaje nebo přezkoumávat, zda jsou neaktuální apod. (ani to nebude v jeho silách).

7.4 Právo na výmaz

Právo na výmaz neboli „právo být zapomenut“ je zajímavým institutem, se kterým se setkáme v čl. 17 GDPR. Jak je z názvu patrné jedná se o právo dožadovat se toho, aby správce bez zbytečného odkladu vymazal osobní údaje, které se týkají subjektu údajů a které nejsou zpracovávány na základě oprávněného důvodu zpracování. Zároveň je však povinností správce vymazat osobní údaje o subjektu údajů v případě, že:

- osobní údaje nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas, na základě kterého byly osobní údaje zpracovávány, a současně neexistuje žádný další právní důvod pro zpracování,



- subjekt údajů vznesl námitky proti zpracování a neexistují převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovávány (nebo získány) protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti vztahující se na správce,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 Obecného nařízení.

Je důležité upozornit, že při naplnění výše uvedeného je povinností správce osobní údaje zklidit. Nelze tedy brát v potaz pouze případy, kdy bude založeno právo na výmaz aktivním jednáním subjektu údajů. V některých případech má totiž sám správce povinnost osobní údaje, které mají být vymazány, nalézt a vymazat. Nejčastějším důvodem, který založí právo na výmaz osobních údajů, bude naplnění účelu pro který byly osobní údaje zpracovávány, dále odvolání souhlasu, či vznesení námitky proti zpracování, vždy však pouze za předpokladu, že nebudou existovat jiné právní důvody pro zpracování.

Důvody pro naplnění práva být zapomenut se nepoužijí v případě, že:

- jsou tyto údaje nutné pro výkon práva na svobodu projevu a informace,
- jsou nutné pro splnění právní povinnosti, která se na správce vztahuje nebo pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci,
- je dán veřejný zájem v oblasti ochrany veřejného zdraví,
- je dán veřejný zájem na archivaci, vědeckém nebo historickém výzkumu, či statistických údajích,
- je dán zájem na určení, výkon nebo obhajobu právních nároků.

Správce je odpovědný i za likvidaci osobních údajů, a proto lze doporučit, aby tuto činnost prováděl svědomitě a správně. Nelze tak např. listinné dokumenty vyhodit pouze do nádoby na tříděný odpad. Na likvidaci by měl vždy dohlížet pověřený pracovník správce osobních údajů, aby bylo vše provedeno řádně.

Samostatně pak nařízení GDPR řeší situaci, pokud jsou osobní údaje uveřejňovány na internetu tím, že stanoví pro správce povinnost vynaložit přiměřené náklady s ohledem



na dostupnou technologii tak, aby k výmazu došlo. Také musí informovat všechny ostatní správce, kteří tyto osobní údaje zpracovávají. Právo být zapomenut tedy platí i v internetovém prostředí, i když jeho uplatnění je ztíženo.

7.5 Právo na omezení zpracování

Subjekt údajů má právo, aby správce omezil zpracování osobních údajů v případě, že:

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

Definice omezení zpracování nám říká, že údaje by měly být označeny jako dočasně omezeny na zpracování. Ona dočasnost je pak zásadní odlišností od smazání osobních údajů, které je trvalé. Pokud jsou tedy některé osobní údaje omezeny na zpracování, lze je dále zpracovávat pouze se souhlasem subjektu osobních údajů (nejedná-li se o případ uplatňování právních nároků).

Nařízení GDPR pak naznačuje praktickou aplikaci omezení zpracování, když říká, že tyto údaje by měly být dočasně zneprístupněny třetím osobám, tedy např. dočasně odstraněny z webových stránek. Samozřejmostí je pak jasné označení těchto osobních údajů tak, aby správce nezapomněl, že je jejich zpracování omezeno.

Obcím, pro které je tento dokument zpracováván, tak lze vždy doporučit, aby v případě pochybností využili a připustili využití práva na omezení zpracování. Tento krok může získat správci osobních údajů čas na prověření celé situace, informování pověřence pro ochranu osobních údajů atd.



7.6 Oznamovací povinnost

Správce osobních údajů má podle čl. 19 Obecného nařízení povinnost oznamovat jednotlivým příjemcům, které mají k osobní údajům přístup, veškeré opravy nebo výmazy osobních údajů, popřípadě právě výše uvedené omezení zpracování. Toto samozřejmě není vyžadováno za situace, kdy se oznamovací povinnost stane nemožnou nebo její splnění vyžaduje nepřiměřené úsilí. Pokud si to subjekt údajů vyžádá, předá mu správce také informaci o tom, které subjekty byly takto informovány. Pokud jsou osobní údaje vedeny v nějaké evidenci a toto je zpřístupňována jednotlivým příjemcům, lze tyto příjemce informovat pouhou změnou v takto předložené evidenci, pokud je pravidelně zpřístupňován její platný obsah.

7.7 Právo na přenositelnost údajů

Právo na přenositelnost osobních údajů je zcela novým institutem, který dosavadní právní úprava neznala. Toto právo znamená právo subjektu údajů získat osobní údaje, které správci poskytl, ve strukturovaném, strojově čitelném a běžně čitelném (za pomoci elektronických prostředků) formátu a zároveň je to právo požadovat předání těchto údajů jinému správci za předpokladu, že jsou údaje zpracovávány na základě souhlasu, na základě smlouvy nebo se provádí automatizovaně. Vše výše uvedené je podstatou práva na přenositelnost, které nemůže původní správce bránit.

Základní myšlenkou tohoto práva je umožnit subjektům údajů hladký přechod od jednoho správce k druhému, tedy zejména se setkáme s přechodem od jednoho poskytovatele služeb (např. T-mobile) k jinému (např. O2). Takto nastavené právo by tak mělo zvýšit konkurenceschopnost.

Při uplatnění tohoto práva musí být kumulativně splněny podmínky pro výkon tohoto práva. První podmínkou je, aby se zpracování provádělo na základě souhlasu nebo smlouvy. Rovněž se musí jednat o zpracování automatizované.

Další podmínkou je, že se jedná o osobní údaje (neanonymní), které se týkají subjektu údajů a byly tímto subjektem údajů správci poskytnuty (tz., že se bude jednat o aktivně a vědomě poskytnuté osobní údaje).



Tyto údaje jsou pak subjektu údajů poskytnuty v běžně používaném a strojově čitelném formátu – přesnou definici výše uvedeného však v nařízení GDPR nenajdeme. Předpokládá se však součinnost více správců a ustálení na běžně přístupném softwarovém vybavení. Výklad k tomuto právu říká, že by mělo být používáno takových forem, které zachovávají a umožňují číst strukturu dokumentů, jsou tzv. ve strukturovaném formátu. V českém právním řádu je odkázáno na strojově čitelný formát, což lze považovat za nejvhodnější řešení. Do budoucna lze jen předpokládat, že se společnou kooperací v různých sektorech (bankovníctví, telekomunikace) podaří zajistit shodu na používání existujících nebo nových společných formátů.

Výše uvedené právo na přenositelnost nelze v tedy chápat pouze jako rigidní právní normu ale také jako ideu, jak by měly být údaje dále předávány a poskytovány, bez zátěže pro subjekt údajů. Nelze tedy rozumně vyžadovat, že právo na přenositelnost údajů půjde uplatnit u všech správců osobních údajů, zde opět nastupuje již zmíněná zásada přiměřenosti, které provází celé nařízení GDPR.

7.8 Právo vznést námitku

Právo vznést námitku je možné uplatnit kdykoliv při zpracování osobních údajů subjektu údajů správcem, pokud se tato námitka týká zpracování na základě právního důvodu podle č. 6 odstavce 1 písmene e) nebo f). Tato námitka se podává právě proti zpracování osobních údajů, jako specifické činnosti. V případě, že je námitka podána, nesmí správce dále provádět zpracování osobních údajů pokud neprokáže, že má ke zpracování závažné oprávněné důvody pro zpracování, které převažují nad zájmy a právy svobodami subjektu údajů (případně pro určení nebo obhajobu právních nároků).

Subjekt údajů má právo vznést námitku proti zpracování vždy, týká-li se toto zpracování přímého marketingu (námitky jsou bezplatné). V případě, že subjekt údajů takovouto námitku vznesl, nesmí správce osobních údajů jeho osobní údaje dále zpracovávat (pro účely přímého marketingu). Zároveň by měl správce tyto osobní údaje označit tak, aby už k přímému marketingu u subjektu údajů nedocházelo.

Na možnost uplatnění práva vznést námitku by měl být subjekt údajů výslovně upozorněn, včetně vhodného odlišení tohoto práva od jiných informací.



7.9 Právo nebýt předmětem automatizovaného rozhodování

Právo nebýt předmětem automatizovaného rozhodování je jedním ze zásadních práv, kdy je jasné stanoveno, že rozhodování mající účinky vůči člověku ať už právní nebo obdobné nesmí být prováděno výhradně automatizovaně. Není např. možné zaslat rozhodnutí o přestupku pouze na základě automaticky vyhodnoceného záběru z rychlostní kamery. Samozřejmě nelze pochybovat o tom, že by toto zpracování velmi zrychlilo některé činnosti např. právě v oblasti přestupků.

Nařízení GDPR zná ale výjimky, kdy automatické zpracování použít lze – např. u automatického vyhodnocení bonity žadatele o úvěr. Samozřejmě lze také automatizované zpracování využívat v případě, že s tím subjekt údajů souhlasí.

7.10 Limity práv a zásad zpracování

Ačkoliv práva a zásady zpracování jsou stěžejní částí nařízení GDPR, jsou jasné definovány případy, kdy mohou být částečně odloženy nebo omezeny, je-li to nezbytné, a to v případě předcházení vážného ohrožení v oblasti:

- obrany nebo bezpečnosti České republiky,
- veřejného pořádku a vnitřní bezpečnosti,
- předcházení, vyšetřování, odhalování či stíhání trestních činů nebo výkonu trestů,
- jiného důležitého obecného veřejného zájmu Evropské unie nebo členského státu,
- ochrany nezávislosti soudnictví a soudních řízení.

V každém výše uvedeném případě ale musí správce osobních údajů o svém postupu informovat Úřad pro ochranu osobních údajů.



8. Předávání osobních údajů do zahraničí

Vzhledem ke skutečnosti, že předáváním údajů do zahraničí není jen předání od jednoho subjektu (tuzemského) jinému subjektu (zahraničnímu), ale i jejich zpřístupnění subjektu třetí země, tj. zpřístupnění na internetu, bude i v tomto dokumentu o předávání osobních údajů do zahraničí krátce pojednáno.

Předávání osobních údajů do zahraničí je tedy zpracovatelskou operací, která vyžaduje zvýšenou míru ochrany vzhledem k různosti právní úpravy ochrany osobních údajů v různých zemích. Cílem nařízení GDPR je to, aby subjekt osobních údajů požíval stejné ochrany osobních údajů v třetích zemích, stejně tak jako ji požívá v zemích Evropské unie.

Předání osobních údajů do zahraničí lze učinit pouze na základě konkrétního právního důvodu (čl. 6 odst. 1 resp. čl. 9 GDPR). V rámci EU pak lze na základě tohoto právního důvodu poskytovat údaje volně, jelikož právní úprava ochrany osobních údajů je sjednocena. V případě předávání osobních údajů mimo státy EU, bude složitost takového předání ovlivňovat zejména to, o jaký stát se jedná. Směrodatným ukazatelem je pak rozhodnutí Evropské komise, která určila, které země případně které organizace a ve kterém odvětví poskytují dostatečný standard ochrany osobních údajů. Do těchto zemí a těmito organizacím pak lze předávat ve stejném režimu jako při předávání do zemí EU.

Do ostatních zemí pak lze předávat pouze v případě, že příjemce poskytl dostatečné záruky toho, že bude zpracovávat osobní údaje v režimu obdobném GDPR. Zároveň musí být zaručena dostatečná vymahatelnost práv subjektů údajů. K tomuto lze použít celou řadu instrumentů: smluvní doložky, smluvní záruky, kodex chování, vnitropodniková pravidla a další.

Na závěr tohoto pojednání lze dodat, že existuje několik výjimek, kdy lze předat osobní údaje do zahraničí z nichž nejběžnější bude zřejmě výslovný souhlas subjektu údajů.



9. Zajištění a dokládání souladu zpracování

Dle nařízení GDPR je správce povinen zavést vhodná technická a organizační opatření tak, aby docházelo k řádnému zpracování a toto řádné zpracování je povinen v případě potřeby doložit, resp. musí být schopen doložit soulad zpracování. Tento soulad zpracování musí mít trvalý a dlouhodobý charakter a musí provázet celé zpracovávání osobních údajů. Nelze se tedy dovolávat toho, že soulad byl prokázán a řádně plněn v minulosti.

Prakticky je soulad zpracování souborem činností, tedy přijetí organizačních a technických opatření, jmenování pověřence, realizace kontrolních činností apod. Samotné prokazování pak může probíhat pomocí záznamů o činnostech zpracování, kodexů chování, osvědčení apod. Všechny tyto nástroje, vyjma záznamu o činnostech zpracování, jsou pro správce nepovinné, ale jejich využívání lze doporučit.

9.1 Revize zpracování

Před přijetím jednotlivých opatření musí mít správce přehled o tom, jaké zpracování a s jakými údaji provádí. Činnosti zjišťování uvedeného můžeme nazvat jako revizi zpracování. Tato revize by měla říci správci, jakým způsobem osobní údaje získává, v jakém rozsahu, formátu, jaké kategorie, na základě, jakého právního důvodu je zpracovává, jaké s nimi provádí operace, za jakým účelem jsou získávány, zda je využíván zpracovatel, v jakém je zpracování prováděno systémem apod.

Tato revize pak pomůže správci určit jaké povinnosti se na něj z titulu jím prováděného zpracování vztahují, a tím pádem i jaké konkrétní opatření má přijmout, aby odstranil zjištěné nedostatky a uvedl zpracování do souladu s GDPR.

Bez této revize pak není možné dobře posoudit výše uvedené což sebou může přinést zpracování v nesouladu s GDPR. V neposlední řadě revize pomůže správci vyhodnotit rizika a jak bylo uvedeno výše, přístup GDPR je založen zejména na riziku.

Revizi může provést sám správce nebo pověřenec případně jiná osoba, kterou správce pověří.



9.2 Záznamy o činnosti zpracování

Záznamy o činnosti zpracování lze označit za výstup mapování zpracování, které lze považovat za povinné (bez mapování nemůže správce přijmout adekvátní opatření). V první řadě je tedy třeba provést mapování a jeho výstupem budou právě záznamy o činnosti zpracování. Toto záznamy pak prakticky doporučujeme vést pro každou zpracovávanou agendu zvlášť, pro zvýšení přehlednosti a orientace ve zpracování.

Znalost prováděného zpracování, rozsahu zpracování, účelů zpracování, právního základu a dalších skutečností je základním předpokladem pro to, aby zpracování probíhalo v souladu s nařízením GDPR a aby byl správce tento soulad schopen prokázat (doložit).

Záznamy zpracování u správce obsahují:

- jméno a kontaktní údaje správce, včetně společného správce, a pověřence, byl-li jmenován (v naše případě jmenován na všech obcích),
- účely zpracování,
- popis kategorií subjektů údajů a kategorií osobních údajů,
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny,
- informace o případném předání osobních údajů do třetí země,
- plánovanou lhůtu pro výmaz jednotlivých údajů, je-li to možné,
- obecný popis technických a organizačních bezpečnostních opatření, je-li to možné.

Pokud zpracování osobních údajů provádí zpracovatel, pak musí vést také záznamy o činnostech zpracování, které budou obsahovat:

- jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a pověřence,
- kategorie zpracování prováděného pro každého ze správců,
- informace o případném předání osobních údajů do třetí země,



- obecný popis technických a organizačních bezpečnostních opatření, je-li to možné,
- informace o případném předání osobních údajů do třetí země,
- obecný popis technických a organizačních bezpečnostních opatření, je-li to možné.

Obecné nařízení tedy stanovuje správcům minimální požadavky, které má záznam o činnosti zpracování obsahovat. Pro naše účely mají záznamy o činnostech zpracování (jak byly navrženy) pro jednotlivé obce jednoduchou strukturu, tak aby byly přehledné a jejich vyplnění nebylo přílišnou administrativní zátěží pro mnohdy již vytížené pracovníky. Záznamy se mohou vyhotovovat písemně, vč. elektronické formy, Ústní forma se samozřejmě nepředpokládá.

Záznamy o činnostech zpracování může vypracovat i Pověřenec pro ochranu osobních údajů a lze toto delegování jen doporučit. Nevýhodou záznamů je nutnost jejich pravidelné aktualizace s tím, jak se mění jednotlivé agendy (a zpracovávané údaje).

Vypracované záznamy o činnostech zpracování jsou vhodným podkladem pro výkon práv subjektů údajů – především pro výkon práva na informace.

9.3 Kodexy chování

Kodexy chování jsou souborné dokumenty, které upřesňují uplatňování ustanovení Obecného nařízení v daném sektoru nebo odvětví, mimo jiné pokud jde o:

- spravedlivé a transparentní zpracování,
- upřesnění oprávněných zájmů správců,
- shromažďování osobních údajů,
- pseudonymizaci osobních údajů,
- informace poskytované subjektům údajů a veřejnosti,
- výkon práv subjektů údajů,
- informace poskytované dětem a jejich ochranu a způsob získávání souhlasu nositele rodičovské odpovědnosti,



- opatření a postupy podle č. 24 a čl. 25 GDPR a opatření k zajištění zabezpečení osobních údajů podle čl. 34 GDPR,
- ohlašování, resp. oznamování porušení zabezpečení osobních údajů dozorovému úřadu, resp. subjektům údajů,
- předávání osobních údajů do třetích zemí,
- mimosoudní vyrovnání a další postupy řešení sporů mezi správcem a subjektem údajů.

Samozřejmě kodex chování může obsahovat i jiné údaje a pokyny, specifické pro dané odvětví. Nespornou výhodou kodexů chování je to, že pomocí nich správce může doložit soulad zpracování dle nařízení GDPR. V neposlední řadě je také důležité říci, že při případném řízení o uložení pokuty se při stanovení její výše přihlédně k tomu, zda byl přijat a dodržován kodex chování.

S kodexy chování se setkáme například v bankovním sektoru, v sektoru poskytovatelů telekomunikací, pojišťovacích služeb apod. Ve všech těchto sektorech je zpracování osobních údajů poměrně specifické se stejnými otázkami a problémy. Kodexy mají za úkol právě reagovat na specifika jednotlivých odvětví – představují tak návod dobré praxe zohledňující daný sektor.

Navrhovaný kodex chování se předkládá místně příslušnému dozorovému úřadu, který jej schválí a zveřejní (nemá-li připomínky).

Závěrem ke kodexu chování lze říci, že přes nesporné výhody zatím k jejich masovému rozšíření nedošlo. Překážkou pro přijetí je zejména schvalovací proces a zvýšené nároky na dohled nad dodržováním přijatého kodexu.

Dozor nad dodržováním kodexu chování provádí příslušný dozorový úřad (Úřad pro ochranu osobních údajů).

9.4 Osvědčení

Osvědčení jsou obdobou kodexů chování – mají za úkol dokládat ochranu osobních údajů. Osvědčení by se mělo týkat pouze operací zpracování. Pro správce tak může být osvědčení konkurenční výhodou, protože dává subjektům údajů najevo, že řádně zpracovává osobní údaje, což u subjektů údajů může podpořit dobrý obraz správce.



Akreditovat může jednotlivé správce dozorový úřad nebo pověřená instituce (v ČR Český institut pro akreditaci, o. p. s.) – tato instituce bude tedy akreditovat subjekty, které budou moci vydávat osvědčení pro správce a zpracovatele, že dané zpracování je v souladu s nařízením GDPR. Další úprava je pak obsažena v textu zákona č. 90/2016 Sb., o posuzování stanovených výrobků při jejich dodávání na trh.

Osvědčení lze vydat na dobu max. 3 let a lze jej obnovit. K tomuto musí správce akreditačnímu orgánu poskytnout dostatečnou součinnost.

Nařízení GDPR počítá i s možným odejmutím osvědčení v případě, že bude prokázáno, že zpracování neprobíhá v souladu s nařízením GDPR. Možnost odejmout osvědčení má pak subjekt který jej vydal nebo dozorový úřad.

Orgány, které mohou osvědčení vydávat, musí splňovat tyto podmínky:

- prokázat dozorovému úřadu svou nezávislost a odborné znalosti ohledně předmětu osvědčení,
- zavázat se dodržovat kritéria uvedená v čl. 42 odst. 5 GDPR schválená dozorovým úřadem,
- stanovit postupy pro vydávání, pravidelný přezkum a odebírání osvědčení, pečeti a známek dokládající ochranu osobních údajů,
- doložit dozorovému úřadu, že jeho úkoly a povinnosti nevedou ke střetu zájmů.

9.5 Vnitřní koncepce ochrany osobních údajů (směrnice)

Podle nařízení GDPR musí být tam, kde je to vhodné, součástí přijatých technických a organizačních opatření Vnitřní koncepce ochrany osobních údajů – v našem případě, by tato koncepce měla podobu vnitřní směrnice pro pracovníky obecního /městského úřadu. Vnitřní koncepce ochrany osobních údajů je tak povinná pouze pro správce, kteří provádějí rizikové operace nebo provádějí zpracování velkého rozsahu.

Vypracováním takovéto koncepce může být pověřen pověřenec pro ochranu osobních údajů. V době získávání údajů pro tento dokument neměla žádná z dotčených obcí vnitřní koncepci (směrnici) ani o ní neuvažovala.



Nařízení GDPR nestanoví žádné nároky na obsah takovéto směrnice a je tak zcela na vůli správce v jakém rozsahu (a zda vůbec) směrnici přijme. Pokud však již byla přijata je nutné ji pravidelně revidovat a umožnit všem zaměstnancům seznámení s ní.

10. Sankce a pokuty

Součástí každé právní normy zpravidla bývá hypotéza, dispozice a sankce. Nejinak je tomu u nařízení GDPR. Sankce mají donucovací účinek pro adresáty právní normy, tedy pod hrozbou sankce nutí adresáty k určitému konání, či naopak ke zdržení se nějakého konání. Obecné nařízení se blíže věnuje sankcím v čl. 83, kde stanovuje podmínky pro ukládání sankcí vč. jejich výše.

V době přijetí nařízení GDPR způsobila mnoha zpracovatelům doslova šok výše pokut, kterou nařízení GDPR stanovovalo – maximální výše pokuty 20 000 000 EUR, resp. jedná-li se o podnik až do výše 4 % celkového obrátu celosvětově, podle vyšší hodnoty. Kdy podnikem se rozumí jakákoliv fyzická nebo právnická osoba vykonávající hospodářskou činnost, bez ohledu na právní formu. Na základě těchto drakonických pokut a vyvolaných obav se okamžitě začaly objevovat „odborné“ společnosti zabývající se implementací GDPR. Tyto společnosti všem zpracovatelům právě „vyhrožovaly“ značným rizikem likvidačních pokut a za své služby si inkasovaly nemalé částky. Uklidnění přinesl až zásah Úřad pro ochranu osobních údajů, který ve svých stanoviscích poukazoval zejména na nutnost proporcionality udělovaných pokut, dosavadní praxi a zákaz uložení likvidačních pokut (znám z českého právního řádu). Dále úřad upozorňoval také na to, že i zákon o ochraně osobních údajů zná pokuty až do výše 10 000 000,- Kč, a že tato nebyla nikdy udělena.

Úřad pak dále správně poukazoval na to, že nařízení GDPR je celoevropským předpisem, který dopadá na správce nejen v ČR, ale i v dalších členských zemích, kde mají sídlo největší světové společnosti v pozici správců. Dále je potřeba poukázat na to, že nařízení GDPR se vztahuje i na některé subjekty mimo EU – např. společnost Google, Facebook apod. Zde musí mít výše pokuty motivační účinek, který se nedá zajistit pokutou do 1.000.000,- Kč. Možnost udělení velmi vysoké pokuty tedy může být v některých případech zcela na místě.



Ke zmírnění obav pak přispívá zejména to, že samotné nařízení reguluje ukládání pokut a jejich výši v čl. 83 odst. 1, když říká, že konkrétní dozorový úřad má na území členského státu zajistit, aby ukládání pokut bylo účinné, přiměřené a odrazující, dále nařízení umožňuje pokutu vůbec neukládat, nebo ji uložit společně s nápravným opatřením, či uložit pouze nápravné opatření. Při rozhodování o skutečnosti zda uložit pokutu, a při rozhodování o její výši v jednotlivých případech musí dozorový úřad zohlednit následující okolnosti:

- povahu, závažnost a délku trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena,
- zda k porušení došlo úmyslně nebo z nedbalosti,
- kroky podniknuté ke zmírnění škod způsobených subjektům údajů,
- míru odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedených podle čl. 25 a čl. 32 GDPR,
- veškerá relevantní předchozí porušení správcem či zpracovatelem,
- míru spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho nežádoucích účinků,
- kategorie osobních údajů dotčené daným porušením,
- způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře,
- v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s tímž předmětem dříve nařízena opatření uvedená v čl. 58 odst. 2 GDPR, splnění těchto opatření,
- dodržování schválených kodexů chování nebo schváleného mechanismu pro vydávání osvědčení,
- jakoukoliv jinou přitěžující nebo polehčující okolnost, jako je finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

Z výše uvedeného je jasné, že výše pokuty bude vždy na uvážení příslušného orgánu vykonávající na území dohled. Za každé porušení nařízení GDPR tak ani nemusí být



udělena pokuta – postačí udělení nápravného opatření, tyto lze udělit také současně s pokutou nebo zcela samostatně. Mezi nápravná opatření patří:

- upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují nařízení GDPR,
- upozornit správce či zpracovatele formou napomenutí, že operace zpracování porušily nařízení GDPR,
- nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle nařízení GDPR,
- nařídit správci nebo zpracovateli, aby uvedl operace zpracování do souladu s nařízením GDPR a to případně předepsaným způsobem ve stanovené době,
- nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů,
- uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu,
- nařídit opravu, výmaz nebo omezení zpracování a ohlašování takových opatření příjemcům,
- odebrat osvědčení nebo nařídit, aby jej subjekt oprávněný k vydávání osvědčení odebral nebo nevydal,
- uložit správní pokutu podle čl. 83 nařízení GDPR vedle či namísto dalších nápravných opatření, podle okolností každého jednotlivého případu,
- nařídit přerušování toků údajů příjemci ve třetí zemi nebo mezinárodní organizaci.

V případě, že půjde o bagatelní případ, s minimální společenskou škodlivostí, nebude pokuta muset být vůbec udělena. Je možné, že bude postačovat některé z výše uvedených nápravných opatření nebo pouze informování správce.

10.1 Sankce a pokuty pro obce

Vzhledem k přijetí zákona o ochraně osobních údajů, nemá příliš smysl zabývat se výší pokuty pro obce, jelikož tento zákon pokuty **pro obce a kraje zrušil**. Tato výjimka byla schválena na žádost senátu, který za zrušení pokut dlouho bojoval. Hlavním argumentem pro zrušení bylo to, že by se jednalo pouze o přelévání finančních



prostředků v rámci veřejné správy. Toto ovšem neznamená, že by obce a kraje nemusely nařízení GDPR dodržovat. Z vlastní praxe pak autor tohoto dokumentu může potvrdit, že i přes neexistenci pokut, obce nařízení GDPR dodržují, dbají na něj a mají trvalou snahu zpracování osobních údajů provádět v souladu s nařízením GDPR.

Sankcím a pokutám vzhledem k výše uvedenému nebude tedy již v tomto dokumentu věnována další pozornost.

11. Právní ochrana a odpovědnost, včetně odpovědnosti trestní

Nařízení GDPR je komplexním právním předpisem upravujícím celou řadu práv a povinností, při zpracování osobních údajů. Stejně tak nařízení GDPR upravuje i navazující otázky, které mohou při zpracování osobních údajů vyvstat, resp. které dovršují komplexní ochranu subjektu údajů, resp. dalších zainteresovaných či dotčených osob.

Pro subjekt údajů bude hlavním právem, právo podání stížnosti dozorového úřadu a také právo na soudní ochranu v případě nečinnosti dozorového úřadu, dále také právo na soudní ochranu vůči správci nebo zpracovateli (zejména náhrada újmy způsobené v důsledku porušení nařízení GDPR). Zde je důležité poznamenat, že náhradu způsobené újmy může požadovat i jiná osoba, než je subjekt údajů (je tu dokonce možnost být zastupován neziskovým subjektem).

Dále obecné nařízení přiznává právo na soudní ochranu jakékoliv fyzické nebo právnické osobě proti právně závaznému rozhodnutí dozorového úřadu, které se jí týká. Takováto soudní ochrana bude poskytována na základě správního soudnictví (pro náhradu újmy se použije občanský zákoník).



11.1 Právo subjektu údajů podat stížnost u dozorového úřadu

Stížnost u dozorového úřadu je základním právem subjektu údajů, pokud se domnívá, že zpracováním jeho osobních údajů je porušeno nařízení GDPR. Stížnost se podává k místně příslušnému dozorovému úřadu, dle místa bydliště subjektu údajů (případně dle místa výkonu zaměstnání, nebo místa kde došlo k porušení). Dozorový úřad má povinnost subjekt údajů informovat o průběhu vyřizování podané stížnosti, jakož i použít subjekt údajů o jeho právu podat žalobu při nečinnosti dozorového úřadu.

Tyto podmínky mohou podávat mimo subjektu údajů i třetí osoby (fyzické i právnické osoby), které se domnívají, že dochází k porušování nařízení GDPR.

Forma podání stížnosti není dána, lze ji tedy podat písemně, elektronicky i ústně.

Informace o stížnostní agendě Úřadu pro ochranu osobních údajů lze získat v každoročně zveřejňovaných výročních zprávách, které jsou zveřejněny na stránkách www.uoou.cz vždy na konci jara.

11.2 Právo na účinnou soudní ochranu vůči dozorovému úřadu

Stejně jako je tomu u jiných úřadů (např. u Úřadu pro ochranu hospodářské soutěže), má i nad Úřadem pro ochranu osobních údajů jakýsi „dozor“ soud. Tato skutečnost je dána tím, že i Úřad může při svém jednání pochybit. Právo na soudní ochranu tak zůstává zachováno i nařízením GDPR. Proti rozhodnutí Úřadu (vůči různým subjektům) se tedy lze bránit před správním soudem. Nejčastěji se bude pravděpodobně jednat o soudní ochranu před rozhodnutím Úřadu pro ochranu osobních údajů o uložení pokuty, vyloučena není ani ochrana před uloženým nápravným opatřením nebo při využití některých povolovacích oprávnění. Právo na účinnou soudní ochranu se nevztahuje na opatření dozorového úřadu, která nejsou právně závazná, jako jsou stanoviska, metodiky a poradenství.

Pokud se dozorový úřad nezabývá stížnostmi subjektu údajů, či neinformuje subjekt údajů o svém postupu do tří měsíců, je tím založeno právo na soudní ochranu. Řízení se proti dozorovému úřadu se zahajuje u soudu místně příslušného (v ČR správní soudnictví).



11.3 Právo na účinnou soudní ochranu vůči správci nebo zpracovateli

Nařízení GDPR přiznává subjektu údajů právo na soudní ochranu v případě, že se tento domnívá, že jeho práva byla poškozena v důsledku zpracování osobních údajů v rozporu s nařízením GDPR. Tímto je zejména zajištěno právo na náhradu újmy, která vznikla subjektu údajů v důsledku porušení nařízení GDPR správcem nebo zpracovatelem.

Řízení se bude zahajovat u soudu členského státu, v němž má správce nebo zpracovatel provozovnu, případně v místě, ve kterém má subjekt údajů své bydliště, s výjimkou případů, kdy je správce nebo zpracovatel orgánem veřejné moci, která jedná v rámci výkonu veřejné moci.

Vzhledem ke skutečnosti, že se pro naše účely budeme pohybovat vždy na území ČR, bude používán výhradně občanský soudní řád, pokud se řízení povede v ČR (zákon o zvláštních řízeních soudních se neuplatní).

11.4 Zastupování subjektů údajů

Možnost zvolit si zástupce je upravena v čl. 80 odst. 1 nařízení GDPR, kdy tento článek stanoví, že subjekt údajů má právo zvolit si jako svého zástupce neziskovou organizaci (subjekt), organizaci nebo sdružení, jejichž cílem je ve veřejném zájmu vyvíjet činnost v oblasti ochrany práv a svobod subjektů údajů ohledně ochrany jejich osobních údajů.

Pověřit tento subjekt lze k tomu, aby za subjekt údajů podal stížnost a dále uplatnil právo na soudní ochranu proti dozorovému úřadu či správci nebo zpracovateli.

Zároveň nařízení GDPR připouští, aby prostřednictvím výše uvedených subjektů bylo možné rovněž žádat náhradu újmy (podle čl. 82 nařízení GDPR). Tato skutečnost ovšem musí být upravena tuzemskou právní úpravou (resp. právní úpravou každého členského státu). Zákon o zpracování osobních údajů tuto možnost neupravuje.

Dále nařízení GDPR dává členským státům možnost přijmout do vnitrostátní právní úpravy ustanovení, které dává výše uvedeným subjektům právo podat stížnost či upravit právo, a to i bez toho, aby tyto subjekty byly pověřeny subjektem údajů. Tyto žaloby ve veřejném zájmu by mohl podat tedy kdokoli. Nový zákon o ochraně osobních údajů



ovšem s touto variantou nepočítá. Můžeme se pouze domnívat, že je tomu tak proto, že zákonodárce nechtěl dále zatěžovat již tak přetížený soudní systém.

V neposlední řadě je nutné dodat, že možnost zvolit si zástupce z řad fyzických nebo právnických osob, subjektem údajů, není dotčena.

11.5 Právo na náhradu újmy a odpovědnost

Kdokoliv, kdo v důsledku porušení nařízení GDPR utrpí škodu či újmu, je oprávněn obdržet od správce nebo zpracovatele přiměřené odškodnění (přiměřenou náhradu). Nařízení GDPR výslovně stanoví „kdokoliv“ což je významné rozšíření oproti bývalé tuzemské právní úpravě, která přiznávala právo na náhradu pouze subjektu údajů, a navíc byla přiznána pouze náhrada za nemajetkovou újmu.

Lze tak očekávat, že se budeme setkávat nejvíce s náhradou nemajetkové újmy, která vznikla v souvislosti se zpracováním osobních údajů, tím, že bylo zasaženo do práva na ochranu soukromí (které je chráněno občanským zákoníkem). Dnes kdy má snad každý přístup k internetovému připojení si lze snadno představit situaci, kdy zásah do soukromí, utrhání na cti nebo zneužití jména vyvolá tak závažné důsledky, že bude na místě soudní ochrana a možnost získání náhrady utrpěné újmy.

Náhradu škody pak může žádat také správce vůči zpracovateli, kterému v důsledku porušení povinností ze strany zpracovatele vznikla újma. Správce odpovídá za újmu, kterou způsobil zpracováním, jež porušuje nařízení GDPR, přičemž zpracovatel je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené nařízením GDPR pro zpracovatele nebo v případě, že jednal nad rámec pokynů správce nebo v dokonce v rozporu s nimi.

Zde je nutné poukázat na to, že pokud má být správce nebo zpracovatel potrestán, je nutné prokázat příčinou souvislost mezi jejich konáním (příp. opomenutím) a újmu, která vznikla. Správce ani zpracovatel totiž nenesou zodpovědnost za událost, která ke vzniku újmy vedla, pokud za ni žádným způsobem nemohou.

V případě, že za vznik újmy odpovídá více správců (případně více zpracovatelů) nesou tito odpovědnost solidárně, pro zajištění náhrady újmy subjektu údajů jako slabší strany (zde najdeme podobnost s postavením spotřebitele). Pokud některý ze správců nahradí



újmu v plné výši, má právo vyžadovat od ostatních správců, kteří jsou solidárně zavázání, žádat od každého z nich vrácení části vynaložené náhrady.

Soudní řízení v souvislosti s výkonem práva na náhradu újmy se zahajuje u soudu členského státu, v němž má správce nebo zpracovatel provozovnu, případně u soudu členského státu, ve kterém má poškozená osoba bydliště či sídlo, s výjimkou případů, kdy je správce nebo zpracovatel orgánem veřejné moci, který jedná v rámci výkonu veřejné moci, kdy se zahajuje soudní řízení u toho členského státu, v němž orgán veřejné moci působí.

11.6 Trestní odpovědnost správce a zpracovatele jako právnické osoby

Valná část odpovědnosti správce a zpracovatele se bude pohybovat v rovině správního práva – vč. správního trestání pokutami, resp. také v rovině práva občanského při náhradě újmy. Ve výjimečně závažných případech se ovšem můžeme přesunout až k trestněprávní odpovědnosti. Zvláště pak v případě, že na straně správce či zpracovatele stojí právnické osoby.

Trestní odpovědnost právnických osob je založena zákonem č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim. Tento zákon vyjmenovává trestné činy, kterých se právnická osoba nemůže dopustit, přičemž platí, že všechny ostatní trestné činy uvedené v zákoně č. 40/2009 Sb., trestní zákoník, spáchat může.

Právnická osoba je odpovědná za trestné činy spáchané v jejím zájmu nebo v rámci její činnosti, jednal-li tak:

- statutární orgán nebo člen statutárního orgánu nebo jiná osoba ve vedoucím postavení v rámci právnické osoby která je oprávněna jménem nebo za právnickou osobu jednat,
- osoba ve vedoucím postavení v rámci právnické osoby, která u této právnické osoby vykonává řídicí nebo kontrolní činnost, i když není osobou uvedenou v předchozím bodě,



- ten, kdo vykovává rozhodující vliv na řízení této právnické osoby, jestliže jeho jednání bylo alespoň jednou z podmínek vzniku následku zakládajícího trestní odpovědnost právnické osoby, nebo
- zaměstnanec nebo osoba v obdobném postavení při plnění pracovních úkolů, i když není osobou uvedeno v předchozích bodech.

Dále lze právnické osobě přičítat spáchání trestního činu v případě, že byl spáchán:

- jedním z orgánů právnické osoby nebo osob shora uvedených,
- shora uvedeným zaměstnancem na podkladě rozhodnutí, schválení nebo pokynu orgánu právnické osoby nebo osob shora uvedených anebo proto, že orgány právnické osoby shora uvedené neprovedly taková opatření, která měly provést podle jiného právního předpisu nebo která po nich lze spravedlivě požadovat, zejména neprovedly povinnou nebo potřebnou kontrolu činností zaměstnanců nebo jiných osob, jímž jsou nadřízeny, nebo neučinily nezbytná opatření k zamezení nebo odvrácení následků spáchaného trestného činu.

Liberační ustanovení zákona pak říká, že trestní odpovědnosti se zbaví ta právnická osoba, která prokazatelně vynaložila veškeré úsilí, které na ni bylo možné vyžadovat, k tomu, aby ke spáchání protiprávního činu výše uvedenými osobami nedošlo nebo aby jim bylo zabráněno.

Právnická osoba se tak může dopustit trestního činu neoprávněného nakládání s osobními údaji. Lze tedy každé právnické osobě jen doporučit, aby prováděla pečlivou kontrolu svých zaměstnanců k přecházení trestné činnosti, která by mohla být poté přičítána právě právnické osobě (z důvodu neprovedené kontroly).

11.6.1 Neoprávněné nakládání s osobními údaji

Primární trestný čin, který souvisí se zpracováním osobních údajů, je neoprávněné nakládání s osobními údaji. Tohoto trestného činu se mohla před rokem 2016 dopustit pouze osoba fyzická, po 1. prosinci 2016 se ho může dopustit i osoba právnická, přičemž skutková podstata zní:



„(1) Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem.

(2) Stejně bude potrestán, kdo osobní údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, byť i z nedbalosti, sdělí nebo zpřístupní, a tím poruší právním předpisem stanovenou povinnost mlčenlivosti.

(3) Odnětím svobody na jeden rok až pět let nebo zákazem činnosti nebo peněžitým trestem bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se údaj týká,

b) spáchá-li čin uvedený v odstavci 1 nebo 2 tiskem, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem, nebo

c) spáchá-li čin uvedený v odstavci 1 nebo 2 porušením povinností vyplývajících z jeho povolání, zaměstnání nebo funkce.“

V následujícím paragrafu 180 pak nalezneme tzv. kvalifikované skutkové podstaty, výčet okolností, za kterých hrozí přísnější tresty, např. za spáchání výše uvedeného v organizované skupině, prostřednictvím počítačové sítě nebo vznikne-li škoda velkého rozsahu.

Základním kamenem trestněprávní odpovědnosti je způsobení závažné újmy, nelze tedy uvažovat o trestu za bagatelní újmu. Důležité je, že výše uvedený trestný čin lze spáchat jak úmyslně, tak z nedbalosti. Aby nastala možná trestnost právnické osoby muselo by se jednat o velmi závažný excés, který by způsobil vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, navíc jak bylo výše uvedeno, musel by takový trestný čin být právnické osobě přičitatelný. Nicméně nelze říci, že by k takovýmto jednáním nedocházelo. Například v roce 2016 bylo za tento trestný čin odsouzeno 34 osob. V roce 2015 34 osob. Nutno ovšem říci, že v žádném z uvedených případů nebyla odsouzena právnická osoba, nýbrž fyzická osoba, která nakládala s osobními údaji v rámci výkonu svého povolání/zaměstnání.



11.6.2 Kontrola zaměstnanců za účelem předcházení přičitatelnosti jejich trestního jednání

Právnícké osoby mohou být odpovědné i za jiné trestné činy, než je výše uvedený trestný čin neoprávněného nakládání s osobními údaji. Proto je vhodné vykonávat kontrolu nad činností svých zaměstnanců. Právnícké osoby mohou být totiž trestně odpovědné zejména v případě, že neprovedly povinnou nebo potřebnou kontrolu nad činností zaměstnanců nebo jiných osob, jimž jsou nadřizeny, anebo neučinily nezbytná opatření k zamezení nebo odvrácení následků spáchaného trestného činu. Kontrola zaměstnanců tedy hraje důležitou roli při předcházení trestní odpovědnosti právnické osoby. Zavádění kontrolních mechanismů tak lze všem právnickým osobám doporučit, společně s jejich řádným dodržováním a pravidelnou aktualizací. Na tomto místě je vhodné uvést, že povinná kontrola nesmí přesahovat hranici a dojít ke „sledování“ zaměstnanců, která je zakázáno zákoníkem práce v § 316 a násl. Kontrola musí být přiměřená danému kontextu a činností zaměstnavatele a stejně tak rizikům, která činnost zaměstnavatele přináší. Všem právnickým osobám, tedy i obcím lze doporučit tzv. compliance program, tedy soubor nejen kontrolních opatření ale také vzdělávání a formování zaměstnanců, který napomůže snížení rizika a zároveň bude dostačující k vyvinění z případné trestní odpovědnosti.

12. Praktická část – analýzy rizik obcí

V rámci zpracování tohoto dokumentu byla pro šest obcí zpracována kompletní a aktualizovaná Analýza rizik. Každá tato analýza bude samostatnou kapitolou této práce, pro lepší orientaci v textu. Tato část dokumentu není teoretickou rozpravou, ale prakticky připraveným dokumentem, který po doplnění konkrétních údajů může být obratem implementován.

Zpracované kompletní aktualizované Analýzy rizik, reflektují všechny oblasti, které jsou uvedeny výše v tomto dokumentu a mají za cíl, jednoznačně prokázat, že obce, pro které je tento dokument zpracováván, zpracovávají osobní údaje v souladu s nařízením GDPR a mají být také dokladem, že zpracování probíhá v souladu s nařízením GDPR.



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Pro tuto skutečnost, je nutné s analýzami dále pracovat, doplňovat je a seznámit s jejich obsahem dotčené zaměstnance úřadů.

Vypracované kompletní aktualizované Analýzy rizik, budou poskytnuty všem obcím také jako samostatný dokument, pro další zpracování.



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

12.1 Analýza rizik obce Vintířov



Obec Vintířov, Vintířov 62, 357 44 Vintířov

Analýza rizik

zpracovaná v souladu s Nařízením 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 (dále jen „GDPR“), zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“) a dle zákona o zpracování osobních údajů č. 110/2019 Sb.,

Správce:

Obec Vintířov

Vintířov 62

357 44 Vintířov

IČ: 00259641



1. Úvodní ustanovení

1.1. 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 povinná 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 správce v postavení obce

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 vyplývajících, 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 pojmu 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.

1.4. Definice pojmu 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.

1.5. Definice pojmu 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.

1.6. 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.

1.7. Definice pojmu rizikové zpracování

Posouzení vlivu na ochranu osobních údajů musí provést správce, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, bude představovat vysoké riziko pro práva a svobody fyzických osob. Posouzení se musí provést před započítím předmětného zpracování. Pokud byl ustanoven pověřenec pro ochranu osobních údajů, vyžádá si správce jeho posudek. Posouzení vlivu na ochranu osobních údajů se vyžaduje především:

- u systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování,



včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky

- u rozsáhlého zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech
- u rozsáhlého systematického monitorování veřejně přístupných prostorů

Správci osobních údajů budou povinni sami vést záznamy o činnostech zpracování (čl. 30), v případě vysoce rizikových zpracování provést posouzení vlivu na ochranu osobních údajů (čl. 35), a teprve v případě, že vysoká rizika nelze eliminovat, obrátit se na Úřad s žádostí o konzultaci (čl. 36).

2. Obecné informace

2.1. Metoda zpracování analýzy

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, a to s ohledem na posuzování hodnoty aktiv, hrozeb a stanovení dalších parametrů analýzy rizik z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

Zpracovatel ve spolupráci se správcem osobních údajů zvolil metodu zhodnocení každé zpracovávané agendy, která osahuje osobní údaje. V rámci tohoto zhodnocení došlo k ohodnocení primárních aktiv dle jejich kritičnosti, a to v souladu s nařízením GDPR. Vzhledem ke skutečnosti, že GDPR nepředepisuje povinný formát analýzy rizik a taktéž nikterak neuvažuje hodnotu rizika, hodnotil správce riziko z pohledu ohrožení práv subjektů údajů.

Samotná definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u každé agendy je popsána v příslušném agendovém listu (dokument, který byl vypracován ke každé agendě zvlášť). Tyto údaje budou rovněž uvedeny v tomto dokumentu, v oddílu s názvem: „Řešení zabezpečení jednotlivých agend“.

Zpracovatel analýzy rizik předkládá agendový list jako přílohu této analýzy (**příloha č. 1**)

2.2. Metoda určení a hodnocení aktiv

Zhotovitel určí primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení. Aktivum je chápáno jako objekt (dokument, informační systém, kartotéka, spisovna, portál, evidence či jiné listinné nebo elektronické úložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR. Každá agenda pak obsahuje více těchto aktiv.

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.



2.3. Účel zpracování dokumentu

Tento dokument s názvem „Analýza rizik“ je zpracován v souladu s Nařízením 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 (dále jen „GDPR“), zejména dle článku 24 a článku 25.

Dokument představuje ucelený souhrn informací týkající se implementace GDPR do vnitřních i vnějších procesů obce. Osoby, které vystupují v obci v postavení správce, jsou s tímto dokumentem plně seznámeny.

Dokument popisuje vyhodnocení rizik, která vznikají správci v souvislosti se zpracováním údajů o subjektech údajů. Na základě vyhodnocených rizik přijal správce vhodná opatření, které jsou v tomto dokumentu rovněž popsána.

Opatření přijatá správcem

Správce osobních údajů přijal všechna opatření vhodná ke snížení/vyloučení rizik, která vyhodnotil jako přiměřená a v souladu s GDPR. Přijatá opatření budou podrobně popsána v tomto dokumentu.

3. Charakteristika posuzovaného subjektu – správce osobních údajů

3.1. Identifikační údaje správce

Název: Obec Vintířov

Sídlo: Vintířov 62, 357 44 Vintířov

IČ: 00259641

Telefon: +420 352 665 416

e-mail: podatelna@vintirov.cz

Profil zadavatele: https://ezak.olivius.cz/profile_display_98.html

Webové stránky: <http://www.vintirov.cz/cs/>

Počet členů zastupitelstva: 11 členů

Počet obyvatel: 1182⁵

3.2. Struktura obecního úřadu

Obecní úřad tvoří starosta, místostarosta a zaměstnanci obce zařazení do obecního úřadu.

Úřední hodiny obecního úřadu jsou:

Po 7.30 – 12.00 hod. a 13.00 – 17.00 hod.

St 7.30 – 12.00 hod. a 13.00 – 17.00 hod.

3.3. Zveřejňování informací

Obec zveřejňuje informace na webových stránkách obce, a to včetně informací povinně zveřejňovaných dle jiného právního předpisu. Obec dále zveřejňuje

⁵ Tento údaj je pouze orientační.



informace na úřední desce obce, a to jak na úřední desce elektronické, tak fyzické. Při zveřejňování informací obec dlouhodobě dodržuje ustanovení zákona o ochraně osobních údajů (zákon č. 101/2000 Sb.). Obec při zveřejňování všech informací dbá na dodržení nařízení GDPR. Informace, o kterých není známo, zda podléhají ochraně dle GDPR, jsou konzultovány před zveřejněním s pověřencem pro ochranu osobních údajů. Správce osobních údajů rovněž poskytuje informace písemně a ústně, vše při dodržování nařízení GDPR.

4. Obecná struktura uchovávání osobních údajů v obci

4.1. Evidence údajů nahlášená Úřadu pro ochranu osobních údajů

V současné době nevede správce žádnou evidenci, která by podléhala nahlášení Úřadu pro ochranu osobních údajů.

4.2. Technické a organizační opatření

Správce osobních údajů přijal organizační a technická opatření v souladu s GDPR. Správce osobních údajů soustavně pracuje na modernizaci organizačních i technických opatření tak, aby bylo zajištěno maximální zabezpečení všech zpracovávaných údajů.

4.3. Předpisy obce

Technicko-organizační opatření ve formě předpisu k ochraně osobních údajů: ne
Obec v postavení správce osobních údajů se řídí těmito vnitřními předpisy:

- organizační řád
- spisový a skartační řád schválený věcně a místně příslušným archivem
- vnitřní organizační směrnice pro používání IT
- směrnice...
- vnitřní předpis...

4.4. Elektronické zdroje/evidence

4.5. Za zajištění jednotlivých informačních systémů odpovídá správce informačního systému.

4.6. Poskytovatelem internetového připojení je společnost: (doplňt název)

4.7. Elektronické zdroje popisují programové vybavení (software) využívané správcem při zpracování a evidenci údajů dle GDPR.

4.8. Veškeré programové vybavení (software) bylo pořízeno legálně a je pravidelně aktualizováno. Správce dbá na to, aby poskytovatel software zpracovával osobní údaje v souladu s GDPR.

4.9. Správce používá při své činnosti tyto elektronické zdroje/evidence:



- **Účetní program** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program evidence obyvatel** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program pokladny** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program evidence majetku** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Kancelářské programy Office** – jedná se o běžné kancelářské programy „Office“ od společnosti Microsoft.

4.10. Zaměstnanci obce mohou zpracovávat elektronické evidence s povahou zpracování pro osobní potřebu (např. adresáře). Tyto evidence nespadají pod působnost GDPR.

4.11. Listinné zdroje/evidence

Veškeré listinné zdroje/evidence jsou řádně uloženy v příslušných označených šanonech. Každá listinná evidence je vedena v rámci příslušné agendy. Ke každé agendě byl vypracován řádný agendový list. Pro přehled agend byl vypracován dokument s povahou soupisu agend, který obsahuje přehledné informace o vedených agendách (listinných i elektronických).

Veškeré listinné zdroje/evidence jsou uloženy v zamčených skříních/uzavřených skříních/policích vždy tak, aby k nim neměla přístup žádná třetí osoba. V případě, že je dokument uložen v kanceláři volně, dbá příslušný zaměstnanec na to, aby k němu neměla přístup žádná třetí osoba. Každá kancelář je mimo pracovní dobu uzamčena. Budova úřadu je mimo pracovní dobu vždy uzamčena a zabezpečena.

5. Popis implementace GDPR

5.1. Správce v souladu s GDPR vytvořil ke všem vedeným agendám podrobný agendový list. Tento agendový list obsahuje vždy následující údaje:

- **Název a popis agendy**
- **Účel zpracování**
- **Forma zpracování (listinná/elektronická)**
- **Forma zpracování (strukturovaná/nestrukturovaná)**
- **Podobný popis způsobu zpracování**
- **Kategorie subjektu údajů**
- **Kategorie příjemců**
- **Informaci o tom, zda jsou údaje předávány do třetích zemí**



- **Označení správce a zpracovatele**
- **Označení pověřence pro ochranu osobních údajů**
- **Označení dokladu (nosiče údajů)**
- **Určení doby zpracování**
- **Informaci o tom, zda je zpracování rizikové**
- **Informaci o tom, zda je informace zpracovávána na základě zákona**
- **Popis technických a organizačních opatření**
- **Komentář**

5.2. Vypracovaný dokument slouží správci rovněž pro posouzení, zda je zpracování v souladu s GDPR. V případě, že byl správcem vyhodnocen nesoulad, bylo přijato opatření k nápravě. Na základě vypracovaných agendových listů byl vytvořen seznam agend. Seznam agend poskytuje ucelený přehled o všech agendách, které správce zpracovává.

5.3. Při zpracování agendových listů nebyl správcem vyhodnocen nesoulad s nařízením GDPR.

5.4. Při zpracování agendových listů nevyhodnotil správce žádnou agendu jako rizikovou (obsahující citlivé osobní údaje o náboženském vyznání, sexuální orientaci, politickém přesvědčení apod.)

5.5. Postup správce osobních údajů při zpracování agendových listů byl vyhodnocen jako zcela legitimní, v souladu s požadavky GDPR.

5.6. Záznamy o zpracování osobních údajů

Správce vede záznamy o zpracování osobních údajů. Tyto záznamy popisují důležité skutečnosti, které se ke zpracování osobních údajů vztahují. Tuto činnost vykonává správce na základě čl. 30 nařízení GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě zvlášť a obsahují všechny informace obsažené v čl. 30 nařízení GDPR (např. údaje o správci, účel zpracování, popis kategorií subjektů údajů apod.). Všechny tyto záznamy budou pravidelně aktualizovány.

5.7. Návrh na doplnění vnitřních předpisů

Správci osobních údajů lze doporučit přijetí směrnice, která by upravovala zpracování osobních údajů dle nařízení GDPR (směrnice na ochranu osobních údajů). Vzhledem ke skutečnosti, že přijetí směrnice není povinností obce, nelze přijetí takovéto směrnice autoritativně nařídit.

Další doporučení nejsou navrhována. Správce zpracovává osobní údaje zcela v souladu s nařízením GDPR.

6. Riziková zpracování

6.1. Obec zpracovává většinu osobních údajů na základě čl. 6 odst. 1 písm. c), tedy za plnění zákonné povinnosti obce, případně písm. e), kdy dochází ke zpracování



veřejného zájmu nebo písm. b) na základě plnění smlouvy. V minimální míře pak obec zpracovává osobní údaje na základě souhlasu a oprávněného zájmu správce.

6.2. Na základě pečlivého studia dokumentů v rámci ochrany osobních údajů **nebyly zjištěny agendy, které vykazují vyšší míru rizika incidentních hrozeb.**

6.3. Obec v minulosti nezaznamenala ztrátu nebo odcizení osobních údajů.

6.4. Obec v minulosti nebyla sankcionována Úřadem pro ochranu osobních údajů, pro porušení povinností souvisejících s ochranou osobních údajů.

6.5. **Žádné ze zpracovávaných osobních údajů nespadají do zvláštní kategorie osobních údajů ve smyslu čl. 9 nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (dále jen GDPR). Výjimku představují nanejvýš osobní údaje zaměstnanců vyžadované právními předpisy za účelem plnění zákonných povinností zaměstnavatele (např. údaje o zdravotním stavu zaměstnanců).**

7. Obecný popis technických a organizačních opatření

7.1. Technická opatření obce

Technická opatření obce jsou navržena tak, aby splňovala veškeré nároky nařízení GDPR. V první řadě jsou všechny počítače v budově úřadu zabezpečeny proti neoprávněnému přístupu heslem. Použité heslo je kombinací znaků a čísel a je pravidelně aktualizováno. Použité heslo k samotnému přístupu do PC (po zapnutí) zná vždy jen konkrétní zaměstnanec, který s PC pracuje. Zároveň obec dbá na to, aby k žádnému počítači neměla přístup třetí osoba. Z obecného hlediska lze říci, že veškerý používaný software je pravidelně aktualizován. Veškerý software byl také legálně zakoupen a je užíván dle příslušných uživatelských příruček a dokumentů obdobných. Správce dbá na to, aby případný zpracovatel (který je zároveň poskytovatelem software) dbal na ochranu osobních údajů v souladu s nařízením GDPR.

Správce dlouhodobě využívá příslušný antivirový program. Každý počítač je také chráněn branou firewall. Každý zaměstnanec při práci využívá pouze ověřené a důvěryhodné zdroje.

Správce má s tímto zabezpečením dlouhodobě dobré zkušenosti. V minulosti nikdy nedošlo k úniku dat z důvodu nedostatečného technického zabezpečení na straně správce (či zpracovatele). Riziko bylo vyhodnoceno jako minimální/žádné.

7.1.1. Dodavatelé IT software a programů

Pro elektronické zdroje je zajištěna dokumentace všech IT programů, které obecní úřad používá a postupnými kroky se zároveň bude chystat systémová příručka. V systémové příručce obce budou následující body:

1. Popis implementovaného systému nebo programu (nutné podmínky pro instalaci a následný provoz)
2. Licenční podmínky
3. Popis podpory uživatele (hot-line, helpdesk)



4. Bezpečnostní podmínky (jak je systém zabezpečen – přístupy, šifrování, zálohování a bezpečnostní kopie).

5. Popisy systémem vytvářených logů – systémových a transakčních

6. Zprávy a výsledky testů a certifikací, které informační systém nebo program získal

7. Případně cloudové služby

V současné době obec nevyužívá cloudové služby a nemá to ani v plánu. Pokud ale po změně vedení, případně jiného vedení, obec tyto služby začne používat, obec si vyžádá informace o tom, kde se úložiště nachází a že úložiště je zabezpečeno podle GDPR.

7.1.2. Smluvní vztahy s dodavateli software

Správce se v rámci svých elektronických zdrojů a informačních systémů písemně dotázal dodavatelů IS programů, zda jeho systém je na GDPR připraven. Smluvní strany jsou připraveny spolupracovat s pověřencem pro ochranu osobních údajů, včetně kooperace s případnými kontrolami. Správce uzavřel / uzavře s poskytovateli IS dodatek ke smlouvě, který bude zaručovat odpovědnost zpracovatele za nakládání s os. údaji.

Správce po dodavateli IT softwaru požaduje závazek:

- spolupracovat s pověřencem pro ochranu os. údajů
- subjekt údajů bude mít dobrou dostupnost k informacím o zpracování svých údajů
- možnost realizovat právo subjektu na opravu nebo výmaz údajů s tím, že se uvede, v jaké formě (nejlépe v písemné formě),
- možnost realizovat právo na omezení zpracování,
- možnost subjektu poskytnout kopii zpracovávaných osobních údajů,
- možnost výkonu práva na přenositelnost údajů,
- zajištění podpory logování v čitelné formě s vazbou na uživatele a jeho činnosti,
- zajištění ochrany dat po ukončení smlouvy.

Dále správce zreviduje/zrevidoval smlouvy, které obsahují osobní údaje následujícím způsobem:

- Zajištění mlčenlivosti osob, které přijdou do styku s osobními údaji (u externích dodavatelů, případně tam, kde není zákonná povinnost)
- Zajištění a nastavení podmínek pro zapojení dalšího zpracovatele dle nařízení GDPR
- Zajistit práva subjektu údajů (informace o vedených údajích apod., dle GDPR)
- Zajistit podporu pověřence pro ochranu osobních údajů
- Zajistit ujednání o náhradě škody, včetně regresních nároků (s pozorností na smluvní pokuty, aby nevylučovaly náhradu škody).
- Zajistit po ukončení smlouvy odstranění kopií, zničení kopií, případně předání osobních údajů.

7.1.3. Obecný návrh opatření



Považuje se za vhodné zajistit pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Tento proces by měl být náležitě popsán (případně zaznamenán do systémové příručky/analýzy rizik), tak aby kontrola a realizace procesu byla součástí provozního testování, posuzování a hodnocení účinnosti zavedených opatření.

Správce bude nadále pokračovat v zajišťování souladu s GDPR. Správce bude postupně implementovat do všech dokumentací, vnitřních předpisů a nařízení ustanovení, která budou sloužit k:

- pseudoanonymizaci a šifrování osobních údajů k zajištění, aby tyto postupy byly běžnou součástí každodenního výkonu činností správce,
- zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování,
- schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů.

7.2. Organizační opatření obce

Organizační opatření správce spočívají v zajištění ochrany osobních údajů, které správce uchovává v listinné podobě (případně na fyzických datových nosičích). Toto zajištění spočívá zejména ve znemožnění třetím osobám k volnému přístupu k dokumentům, které obsahují osobní údaje. Správce provádí toto opatření zejména tak, že uzamyká budovu úřadu mimo úřední hodiny. Stejně jako budova obecního úřadu jsou uzamčeny i všechny kanceláře. V pracovní době jsou všechny výše uvedené nosiče dat pod dozorem příslušného pracovníka úřadu. Některé významné dokumenty jsou uchovány v trezoru úřadu. Zaměstnanci obce mají rovněž možnost dokumenty ukládat do uzamykatelných skříní.

Správce v minulosti nezaznamenal žádné porušení bezpečnosti, které by vedlo ke ztrátě či zneužití spravovaných údajů. Všichni zaměstnanci obce jsou řádně proškoleni.

Správce má s výše uvedeným zabezpečením dlouhodobě dobré zkušenosti. Riziko bylo vyhodnoceno jako minimální/žádné.

7.3. Personální opatření obce

Personální opatření obce, v postavení správce, spočívá v proškolení všech stávajících zaměstnanců a osob, které přichází do kontaktu s osobními údaji. Všichni zaměstnanci správce jsou řádně proškoleni na prezenčních školeních. V případě neznalosti některé problematiky se mohou obrátit na pověřence pro ochranu osobních údajů. Zároveň správce do budoucna plánuje další školení, která budou utvrzovat vzdělání všech dotčených osob v daném směru.

Správce považuje přijatá opatření za naprosto dostatečná. Riziko úniku osobních údajů subjektů údajů v důsledku neznalosti dotčených osob bylo vyhodnoceno jako minimální/žádné.



8. Řešení zabezpečení jednotlivých agend

8.1. Czech Point

Stávající stav: Žádosti, které stanoví zákon, se ukládají a evidují v šanonech v kanceláři č. 4, odbor správy majetku. V digitální podobě je Czech Point prováděn na počítačích v kancelářích č. 4 a č. 7 (odbor správy majetku a odbor místního hospodářství).

Agenda je vedena na základě zákona č.:

- 128/2000 Sb., - Zákon o obcích,
- 361/2000 Sb., - Zákon o provozu pozemních komunikací a o změnách některých zákonů,
- 247/2000 Sb., - Zákon o získávání a zdokonalování odborné způsobilosti k řízení motorových vozidel a o změnách některých zákonů,
- 500/2004 Sb., - správní řád,
- 269/1994 Sb., - Zákon o Rejstříku trestů,
- 256/2013 Sb., - Zákon o katastru nemovitostí (katastrální zákon),
- 133/2000 Sb., - Zákon o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel),
- 300/2008 Sb. - Zákon o elektronických úkonech a autorizované konverzi dokumentů,
- 365/2000 Sb. - Zákon o informačních systémech veřejné správy,
- 364/2009 Sb. - Vyhláška o kontaktních místech veřejné správy,
- 193/2009 Sb. - Vyhláška o stanovení podrobností provádění autorizované konverze dokumentů

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.2. Evidence nálezů a majitelů nalezených věcí

Stávající stav: Evidence nálezů a majitelů nalezených věcí se vede v počítači č. 6 v MS Office -Word. Agenda je vedena na základě zákona:

- 89/2012 Sb., - Občanský zákoník,
- 128/2000 Sb., Zákon o obcích,

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne



Zpracování citlivých osobních údajů: ne

8.3. Evidence obyvatel

Stávající stav: Evidence obyvatel se provádí v digitální a papírové podobě. Papírová podoba je pomocí karet registru obyvatel, ten je veden v uzamčené kartotéce v kanceláři č. 4 (odboru správy majetku obce). Digitální data jsou umístěna na serveru a zobrazována v počítačích v kancelářích č. 4 a 5. Agenda je vedena na základě zákona:

- 111/2009 Sb., - Zákon o základních registrech,
- 133/2000 Sb., - Zákon o evidenci obyvatel,
- 296/2004 Sb., - Vyhláška, kterou se provádí zákon o evidenci obyvatel,
- 500/2004 Sb., - Správní řád,
- 634/2004 Sb., - Zákon o správních poplatcích,
- 561/2004 Sb., - Školský zákon.

Oprávněná osoba: úředník odboru financí a odboru správy majetku obce.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.4. Hospodářské smlouvy

Stávající stav: Smlouvy jsou evidovány na základě obchodního a občanského zákoníku a na základě zákona o účetnictví, všechny smlouvy jsou uloženy v příslušném šanonu, který je označen "Hospodářské smlouvy", seznamy smluv jsou ukládány též v digitální podobě v počítači tajemníka a k dokumentu má přístup pouze tajemník a správce sítě po odsouhlasení přístupu. Oprávněná osoba: tajemník, starosta.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.5. Poskytování informací dle zákona č. 106/1999 Sb.

Stávající stav: Poskytování informací dle zákona č. 106/1999 Sb., je zpracováváno elektronicky v počítačích úředníků, vedoucího odboru, starosty, místostarosty a tajemníka, dle okruhu požadovaných informací. Následné vyvěšení na úřední desku a el. úřední desku (stránky obce) provádí tajemník.

Spis v písemné formě je uchováván v kanceláři č. 6 v šanonu "Poskytování informací dle zákona č. 106/1999 Sb. ". Zpracovávají se v MS Office Word, ev. excel. Oprávněná



osoba starosta, místostarosta, tajemník, úředníci, vedoucí odboru místního hospodářství.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.6. Kácení stromů

Stávající stav: Kácení dřevin je zpracováváno na základě zákona: 114/1992 Sb., - Zákon o ochraně přírody a krajiny, vyhlášky č. 175/2006, kterou se provádějí některá ustanovení zákona o ochraně přírody a krajiny.

Spis k povolení kácení dřevin je uložen v kanceláři č. 7 a rozhodnutí je uloženo v počítači v kanceláři č. 7, zpracovává se v MS Office Word. Oprávněná osoba starosta.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.7. Katastr nemovitostí

Stávající stav: Žádosti, které stanoví zákon se ukládají a evidují v šanonech v kanceláři č. 4, odbor správy majetku. V digitální podobě je Czech Point prováděn na počítačích v kancelářích č. 4 a č. 7 (odbor správy majetku a odbor místního hospodářství).

Agenda je vedena na základě zákona:

- 256/2013 Sb., - Zákon o katastru nemovitostí (katastrální zákon),
- Vyhláška č. 357/2013 Sb., o katastru nemovitostí (katastrální vyhláška),
- 21/2006 Sb., - Zákon o ověřování,
- 36/2006 Sb., - Vyhláška o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu,
- 634/2004 Sb., - Zákon o správních poplatcích.

Oprávněná osoba: úředník správy majetku obce, vedoucí odboru místního hospodářství.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne



Zpracování citlivých osobních údajů: ne

8.8. Knihovna

Stávající stav: Evidence čtenářů se provádí na základě přihlášky, která je vedena v papírové podobě a následně zapisována data z přihlášky do programu Clavius. Data k vystavování upomínek. Seznam knihovního fondu autor, název knihy se vede v počítači programu Clavius. Agenda je vedena na základě zákona:

- 257/2001 Sb., - Zákon o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon),
- 128/2000 Sb., - Zákon o obcích.

Oprávněná osoba: knihovnice.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.9. Místní poplatky

Stávající stav: Místní poplatky jsou zpracovávány na základě zákonů:

- 565/1990 Sb., - Zákon o místních poplatcích,
- 280/2009 Sb., - Daňový řád,
- 634/2004 Sb., - Zákon o správních poplatcích,
- 128/2000 Sb., - Zákon o obcích,
- 182/2006 Sb., - Insolvenční zákon

Všechny místní poplatky jsou uloženy v příslušných šanonech -pokladna, inventury, místní poplatky-psi, nájmy pozemků v daném roce, místní poplatky jsou ukládány též v digitální podobě v počítači úředníka finančního odboru, program Helios-Fenix, pokladna, pohledávky a Excel a Word soubory, k dokumentu má přístup pouze úředník finančního odboru, tajemník a správce sítě. Oprávněná osoba: úředník finančního odboru.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.10. Personální agenda, zaměstnanecká agenda

Stávající stav: Osobní spisy jsou vedeny na základě Zákoníku práce, všechny smlouvy jsou uloženy v příslušném šanonu, který je označen "Zaměstnanci" a "Zaměstnanci na



VPP". Smlouvy jsou ukládány též v digitální podobě v počítači osoby tajemník, k dokumentu mají přístup - tajemník. Celé osobní spisy jsou založeny v šanonu ve skříni.

Agenda je prováděna na základě zákonů:

- 262/2006 Sb., - Zákoník práce,
- 435/2004 Sb., - Zákon o zaměstnanosti,
- 251/2005 Sb., - Zákon o inspekci práce,
- 312/2002 Sb., - Zákon o úřednících územních samosprávných celků,
- 341/2017 Sb., - Nařízení vlády o platových poměrech zaměstnanců ve veřejných službách a správě,
- 222/2010 Sb., - Nařízení vlády o katalogu prací ve veřejných službách a správě,
- 586/1992 Sb., - Zákon o daních z příjmů,
- 187/2006 Sb., - Zákon o nemocenském pojištění,
- 120/2001 Sb., - Exekuční řád,
- 182/2006 Sb., - Insolvenční zákon,
- 582/1991 Sb., - Zákon o organizaci a provádění sociálního zabezpečení,
- 589/1992 Sb., - Zákon o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- 155/1995 Sb., - Zákon o důchodovém pojištění,
- 37/2003 Sb., - Nařízení vlády o odměnách za výkon funkce členům zastupitelstev,
- 592/1992 Sb., - Zákon o pojistném na všeobecné zdravotní pojištění,
- 128/2000 Sb., - Zákon o obcích.

Oprávněná osoba: tajemník, úředník finančního odboru, vedoucí odboru místního hospodářství.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.11. Pronájem nebytových prostor

Stávající stav: Smlouvy jsou evidovány na základě občanského zákoníku a na základě zákona č.:

- 128/2000 Sb., - Zákon o obcích,
- 89/2012 Sb., - Občanský zákoník,
- 563/1991 Sb., - Zákon o účetnictví".

Všechny smlouvy jsou uloženy v příslušném šanonu, který je označen Pronájem prostor sloužících k podnikání. Seznam smluv je též ukládán v digitální podobě v počítači u osoby tajemníka, k dokumentu má přístup tajemník a správce sítě. Platby těchto smluv jsou vedeny v pohledávkách programu Helios-Fenix v počítači úředníka



finančních odborů. Oprávněná osoba: úředník finančního odboru, tajemník, vedoucí odboru místního hospodářství.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.12. Spisová služba

Stávající stav: Spisová služba se provádí v digitální podobě. Digitální data jsou umístěna na serveru a zobrazována v počítačích ve všech kancelářích s různě omezeným režimem. Agenda je vedena na základě zákona:

- 499/2004 Sb., - Zákon o archivnictví a spisové službě a o změně některých zákonů

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.13. Účetnictví

Stávající stav: Účetnictví je zpracováváno na základě těchto zákonů

- 128/2000 Sb., - Zákon o obcích,
- 563/1991 Sb., - Zákon o účetnictví,
- 235/2004 Sb., - Zákon o dani z přidané hodnoty,
- 250/2000 Sb., - Zákon o rozpočtových pravidlech územních rozpočtů,
- 219/2000 Sb., - Zákon o majetku ČR a jejím vystupování v právních vztazích,
- 220/2013 Sb., - Vyhláška o požadavcích na schvalování účetních závěrek některých vybraných účetních jednotek,

Všechny podklady účetnictví jsou uloženy v příslušném šanonu, který je označen "Účetnictví a banka", "DPH", "Ostatní daně", agenda je též vedena v programu Helios-Fenix , účetnictví, výkaznictví, přijaté a vydané faktury,



pohledávky, rozpočet, v počítači úředníky finančního odboru k dokumentům má přístup úředník finančního odboru, tajemník a správce sítě.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.14. Vedení obecné kroniky

Stávající stav: Na základě zákona č.:

- 132/2006 Sb., Zákon o kronikách vedení kroniky v listinné podobě.

Uloženo v archivu č. 9 a vede kronikářka.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to pouze v listinné podobě. Kronika není vedena v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

8.15. Volební systém

Stávající stav: Volby se provádí v digitální podobě v počítači v kanceláři č. 4, oprávněnou osobou je úředník správy majetku obce (v zastoupení i tajemník nebo úředník finančního odboru). Papírové dokumenty jsou uloženy v krabicích v kanceláři č. 4 a následně archivovány v archivu. Agenda je vedena na základě zákona:

- 130/2000 Sb., - Zákon o volbách do zastupitelstev krajů,
- 491/2001 Sb., - Zákon o volbách do zastupitelstev obcí,
- 247/1995 Sb., - Zákon o volbách do Parlamentu České republiky,
- 62/2003 Sb., - Zákon o volbách do Evropského parlamentu,
- 275/2012 Sb., - Zákon o volbě prezidenta republiky,
- 22/2004 Sb., - Zákon o místním referendu,
- 1/1993 Sb., - Ústava České republiky,
- 2/1993 Sb., - Listina základních práv a svobod,
- 128/2000 Sb., - Zákon o obcích,

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne



9. Pověřenec pro ochranu osobních údajů

9.1. 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, řízení procesů, 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 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.

9.2. Obec má řádně jmenovaného pověřence pro ochranu osobních údajů, který není ve střetu zájmů.

9.3. Obec v postavení správce jmenováním řádného pověřence splňuje požadavky nařízení GDPR a vhodně snižuje rizika, která by mohla nastat v souvislosti s ochranou osobních údajů.

9.4. Pověřenec pro obec zajišťuje tyto činnosti:

- 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 proškoleny v oblasti ochrany osobních údajů.
- 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.

10. Závěrečná ustanovení – zhodnocení souladu s nařízením GDPR

10.1. Zpracovatel tohoto dokumentu hodnotí všechny postupy správce osobních údajů jako postupy prováděné v souladu s nařízením GDPR. Dle výše uvedených informací správce postupuje při zpracování osobních údajů řádně, transparentně a s dostatečným ohledem na zabezpečení osobních údajů.

10.2. Správce osobních údajů přijal vhodná technická a organizační opatření. Detailní popis těchto opatření je uveden na každé jednotlivé kartě příslušné agendy. Vzhledem ke skutečnosti, že správce neprovádí rizikové zpracování, jsou všechna přijatá opatření hodnocena jako přiměřená.



- 10.3. Správce osobních údajů řádně jmenoval pověřence pro ochranu osobních údajů. Správce tak splnil povinnost, která byla stanovena nařízením GDPR. Jmenovaný správce není ve střetu zájmů a může tak činnost vykonávat.
- 10.4. Správce osobních údajů řádně zpracoval záznamy o činnostech zpracování. Správce tak splnil svou povinnost, která byla stanovena nařízením GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě. Tento postup zajišťuje vysokou míru transparentnost při nakládání s osobními údaji.
- 10.5. Správce osobních údajů řádně zpracoval karty agend. Správce tak splnil svou povinnost stanovenou nařízením GDPR. Zpracování těchto karet je klíčovou činností každého správce a slouží zejména k prokázání souladu zpracování s nařízením GDPR.
- 10.6. Správce osobních údajů dlouhodobě klade důraz na bezpečné uchovávání a nakládání s osobními údaji. Tuto skutečnost potvrzuje fakt, že správce nebyl v minulosti vystaven sankci za porušení zákona o ochraně osobních údajů či jiných právních předpisů.
- 10.7. Správci lze dlouhodobě doporučit pokračování ve stávající úrovni zabezpečení a prohlubování znalostí nařízení GDPR a dalších právních předpisů.
- 10.8. Správci lze dlouhodobě doporučit průběžně aktualizovat karty agend v případě změn.
- 10.9. Správci lze dlouhodobě doporučit aktualizaci tohoto dokumentu.
- 10.10. Porušení nařízení GDPR při činnosti správce: **nebylo zjištěno.**
- 10.11. Závažné hrozby/rizika v souvislosti se zpracováním: **nezjištěno.**

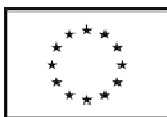
11. Konečné hodnocení

- 11.1. **Správce vykonává svou činnost v souladu s nařízením GDPR.**

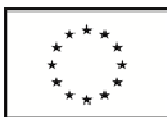
12. Seznam vedených agend

Zpracovatel analýzy přikládá přehled správcem vedených agend s vyhodnocením rizik.

Dokument/seznam/doklad	Účel zpracování	Údaje	Příjemce	Zákon	Komentář	Rizikový
------------------------	-----------------	-------	----------	-------	----------	----------



Czech Point	Právní povinnost, státní správa, služby subjektům (výkon státní správy)	Jméno, příjmení, rodné číslo, datum a místo narození, adresa, IČ, DIČ, číslo dokladu totožnosti, podpis	žadatel	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, 364/2009 Sb., vyhláška o kontaktních místech veřejné správy		NE
Evidence nálezců a majitelů nalezených věcí	Evidence nálezců a majitelů nalezených věcí, výkon činnosti dle občanského zákoníku/ zákona o obcích	Jméno, příjmení, trvalé bydliště, místo pobytu, telefon, podpis	Fyzické osoby (majitelé, nálezci), správce	Zákon č. 89/2012 Sb., Občanský zákoník, zákon č. 128/2000 Sb., o obcích		NE
Evidence obyvatel	Vedení a zpracování evidence obyvatel, právní povinnost, výkon státní správy	Jméno, příjmení, IČ, DIČ, rodné číslo, adresa, datum a místo narození, číslo dokladu totožnosti, podpis, rodné příjmení, stav	Žadatel, subjekty z rozhodnutí, státní správa	Zákon č.111/2009 Sb., o základních registrech, zákon č.133/2000Sb. , o evidenci obyvatel,296/2004Sb.,- vyhláška, kterou se provádí zákon o evidenci obyvatel, zákon č. 500/2004 Sb.,- Správní řád, zákon č. 634/2004 Sb., o správních		NE



				poplatcích		
Hospodářské smlouvy	Evidence smluv, plnění smluv, uplatňování práv a povinností ze smluv	Jméno, příjmení, IČ, DIČ, rodné číslo, datum narození, adresa	Dodavatel, odběratel, žadatel, smluvní strana	Obchodní a občanský zákoník		NE
Poskytování informací dle zákona č. 106/1999 Sb.	Vyřizování žádostí o informaci dle zákona č. 160/1990 Sb., archivace žádostí	Jméno, příjmení, titul, datum narození, trvalé bydliště, e-mail, datová schránka, podpis	Žadatel, rozhodnutí, obec, okresní archiv, krajský úřad, úřední deska – všichni	Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, zákon o obcích		NE
Kácení stromů	Evidence činnosti ve vztahu ke kácení stromů a vedení související agendy na základě zákona	Jméno, příjmení, titul, rodné číslo, trvalé bydliště, datum narození, datová schránka	Subjekt oprávněný z rozhodnutí, obec, okresní archiv, krajský úřad	Zákon č. 114/1992 Sb., o ochraně přírody a krajiny, vyhláška č. 175/2006, kterou se provádějí některá ustanovení zákona o ochraně přírody a krajiny		NE
Katastr nemovitostí	Vedení agendy katastru nemovitostí, právní povinnost, státní správa,	Jméno, příjmení, IČ, DIČ, rodné číslo, datum a místo	Žadatel	Zákon č. 365/2000 Sb. – zákon o informačních systémech veřejné		NE



	služby subjektům	narození, adresa, číslo dokladu totožnosti, podpis, rodné příjmení		správy, zákon č. 364/2009 Sb. – vyhláška o kontaktních místech veřejné správy		
Knihovna	Vedení agendy související s činností obecní knihovny, evidence čtenářů, výpůjček a činnosti související	Jméno, příjmení, trvalé bydliště, datum narození, podpis	Správce, fyzické osoby evidované na základě vlastní žádosti	Zákon č. 257/2001 Sb., - o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon), zákon č. 128/2000 Sb., - o obcích		NE
Místní poplatky	Evidence a vymáhání místních poplatků na základě zákona	Jméno, příjmení, rodné číslo, trvalý pobyt, datum narození, IČ, adresa provozovny	Plátce, příjemce (FO a PO)	Zákon o místních poplatcích		NE
Personální agenda, zaměstnanecká agenda	Zpracování personální agendy na základě pracovních smluv, plnění povinností na základě zákoníku práce, zákona o účetnictví	jméno, příjmení, titul, datum narození, rodné číslo, trvalé bydliště, e- mail, telefon, místo	Zaměstnan ec, kontrolní orgány, orgány provádějící další zpracování (zdravotní pojišťovny,	Zákon č. 262/2006 Sb.,- zákoník práce, zákon č. 435/2004 Sb., - zákon o zaměstnanosti , zákon č. 251/2005 Sb.,- zákon o		NE



		narození, stát narození, státní příslušnost, zdravotní pojišťovna, bankovní spojení, předchozí zaměstnav atel, stav, rodinný příslušník, děti, doklady o vzdělání, doklady o důchodu, výpis z rejstříku trestů, zdravotní prohlídky, zdravotní znevýhodn ění, údaje o zdravotním stavu	orgány činné v sociálním zabezpečení i)	inspekci práce, zákon č. 586/1992 zákon o daních z příjmu		
Pronájem nebytových prostor	Evidence pronájmů a vymáhání pohledávek z pronájmu nebytových prostor, evidence nájemců	Jméno, příjmení, IČ, DIČ, rodné číslo, adresa provozovny , datum narození	Dodavatel, odběratel, žadatel, smluvní strana	Občanský zákoník		NE
Spisová služba	Vedení spisové služby na základě zákonné povinnosti, evidence	Osobní údaje (jméno, příjmení, adresa,	Správce, orgány veřejné správy	Zákon č. 499/2004 Sb., - o archivnictví a spisové službě a o		NE



	přijatých a odeslaných dokumentů	rodné číslo, vyjma citlivých osobních údajů)		změně některých zákonů		
Účetnictví	Vedení účetnictví obce na základě zákona o účetnictví a souvisejících předpisů	Jméno, příjmení, titul, rodné číslo, datum narození, IČ, DIČ, adresa, sídlo podnikání, datová schránka, bankovní spojení, podpis	Dodavatel, odběratel, žadatel, smluvní strana, ministerstv o financí, obecní úřad	Zákon o účetnictví, zákon o obcích		NE
Vedení obecní kroniky	Zaznamenávání historie obce na základě zákonné povinnosti	Jméno, příjmení, datum narození, adresa	Každá fyzická či právnická osoba	zákon o kronikách obcí		NE
Volební systém	Organizace a zajištění průběhu voleb na základě zákonné povinnosti	Jméno, příjmení, narození, věk, trvalé bydliště, omezená svéprávnost , podpis, údaje o zdravotním stavu	Žadatel, orgány veřejné správy, statistika, obecní úřad	Zákon č. 130/2000 Sb.,- o volbách do zastupitelstva krajů, zákon č. 491/2001 Sb.,- o volbách do zastupitelstva obcí, zákon č. 275/2012 Sb.,- o volbě prezidenta republiky, zákon č. 1/1993 Sb., - Ústava České		NE



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

				republiky		
--	--	--	--	-----------	--	--



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

12.2 Analýza rizik obce Hory



Obec Hory, Hory 47, 360 01 Hory

Analýza rizik

zpracovaná v souladu s Nařízením 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 (dále jen „GDPR“), zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“) a dle zákona o zpracování osobních údajů č. 110/2019 Sb.,

Správce:

Obec Hory

Hory 47

360 01 Hory

IČ: 49750500



13. Úvodní ustanovení

13.1. 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 povinná 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.

13.2. Vymezení a definice správce v postavení obce

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 vyplývajících, 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.

13.3. Definice pojmu 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.

13.4. Definice pojmu 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.

13.5. Definice pojmu 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.

13.6. 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.

14. Obecné informace

14.1. Metoda zpracování analýzy

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, a to s ohledem na posuzování hodnoty aktiv, hrozeb a



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

Zpracovatel ve spolupráci se správcem osobních údajů zvolil metodu zhodnocení každé zpracovávané agendy, která osahuje osobní údaje. V rámci tohoto zhodnocení došlo k ohodnocení primárních aktiv dle jejich kritičnosti, a to v souladu s nařízením GDPR. Vzhledem ke skutečnosti, že GDPR nepředepisuje povinný formát analýzy rizik a taktéž nikterak neuvažuje hodnotu rizika, hodnotil správce riziko z pohledu ohrožení práv subjektů údajů.

Samotná definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u každé agendy je popsána v příslušném agendovém listu (dokument, který byl vypracován ke každé agendě zvlášť). Tyto údaje budou rovněž uvedeny v tomto dokumentu, v oddílu s názvem: „Řešení zabezpečení jednotlivých agend“.

Zpracovatel analýzy rizik předkládá agendový list jako přílohu této analýzy (**příloha č. 1**)

14.2. **Metoda určení a hodnocení aktiv**

Zhotovitel určí primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení. Aktivum je chápáno jako objekt (dokument, informační systém, kartotéka, spisovna, portál, evidence či jiné listinné nebo elektronické úložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR. Každá agenda pak obsahuje více těchto aktiv.

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.

14.3. **Účel zpracování dokumentu**

Tento dokument s názvem „Analýza rizik“ je zpracován v souladu s Nařízením 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 (dále jen „GDPR“), zejména dle článku 24 a článku 25.

Dokument představuje ucelený souhrn informací týkající se implementace GDPR do vnitřních i vnějších procesů obce. Osoby, které vystupují v obci v postavení správce, jsou s tímto dokumentem plně seznámeny.

Dokument popisuje vyhodnocení rizik, která vznikají správci v souvislosti se zpracováním údajů o subjektech údajů. Na základě vyhodnocených rizik přijal správce vhodná opatření, které jsou v tomto dokumentu rovněž popsána.

Opatření přijatá správcem

Správce osobních údajů přijal všechna opatření vhodná ke snížení/vyloučení rizik, která vyhodnotil jako přiměřená a v souladu s GPDR. Přijatá opatření budou podrobně popsána v tomto dokumentu.



15. Charakteristika posuzovaného subjektu – správce osobních údajů

15.1. Identifikační údaje správce

Název: Obec Hory

Sídlo: Hory 47, 360 01 Hory

IČ: 4975500

Telefon: +420 353 222 148

e-mail: podatelna@obec-hory.cz

Profil zadavatele: https://ezak.olivius.cz/profile_display_92.html

Webové stránky: <http://obec-hory.cz/>

Počet členů zastupitelstva: 7 členů

Počet obyvatel: 224⁶

15.2. Struktura obecního úřadu

Obecní úřad tvoří starosta, místostarosta a zaměstnanec obce zařazený do obecního úřadu.

Úřední hodiny obecního úřadu jsou:

Po 10.00 – 12.00 hod. a 15.00 – 17.00 hod.

St 10.00 – 12.00 hod. a 15.00 – 17.00 hod.

15.3. Zveřejňování informací

Obec zveřejňuje informace na webových stránkách obce, a to včetně informací povinně zveřejňovaných dle jiného právního předpisu. Obec dále zveřejňuje informace na úřední desce obce, a to jak na úřední desce elektronické, tak fyzické. Při zveřejňování informací obec dlouhodobě dodržuje ustanovení zákona o ochraně osobních údajů (zákon č. 101/2000 Sb.). Obec při zveřejňování všech informací dbá na dodržení nařízení GDPR. Informace, o kterých není známo, zda podléhají ochraně dle GDPR, jsou konzultovány před zveřejněním s pověřencem pro ochranu osobních údajů. Správce osobních údajů rovněž poskytuje informace písemně a ústně, vše při dodržování nařízení GDPR.

16. Obecná struktura uchovávání osobních údajů v obci

16.1. Evidence údajů nahlášená Úřadu pro ochranu osobních údajů

V současné době nevede správce žádnou evidenci, která by podléhala nahlášení Úřadu pro ochranu osobních údajů.

⁶ Tento údaj je pouze orientační.



16.2. **Technické a organizační opatření**

Správce osobních údajů přijal organizační a technická opatření v souladu s GDPR. Správce osobních údajů soustavně pracuje na modernizaci organizačních i technických opatření tak, aby bylo zajištěno maximální zabezpečení všech zpracovávaných údajů.

16.3. **Předpisy obce**

Technicko-organizační opatření ve formě předpisu k ochraně osobních údajů: ne
Obec v postavení správce osobních údajů se řídí těmito vnitřními předpisy:

- organizační řád
- spisový a skartační řád schválený věcně a místně příslušným archivem
- vnitřní organizační směrnice pro používání IT
- směrnice...
- vnitřní předpis...

16.4. **Elektronické zdroje/evidence**

16.5. Za zajištění jednotlivých informačních systémů odpovídá správce informačního systému.

16.6. Poskytovatelem internetového připojení je společnost: Lithium Pro, s. r. o., se sídlem: Nová Kyselka 8, 362 77 Kyselka. Internetové připojení není poskytováno veřejně.

16.7. Elektronické zdroje popisují programové vybavení (software) využívané správcem při zpracování a evidenci údajů dle GDPR.

16.8. Veškeré programové vybavení (software) bylo pořízeno legálně a je pravidelně aktualizováno. Správce dbá na to, aby poskytovatel software zpracovával osobní údaje v souladu s GDPR.

16.9. Správce používá při své činnosti tyto elektronické zdroje/evidence:

- **Účetní program** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program evidence obyvatel** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program pokladny** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program evidence majetku** (doplnit název) – zpracovatel, společnost GORDIC spol. s r. o. se sídlem: Erbenova 4, 586 04 Jihlava, nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Kancelářské programy Office** – jedná se o běžné kancelářské programy „Office“ od společnosti Microsoft.



16.10. Zaměstnanci obce mohou zpracovávat elektronické evidence s povahou zpracování pro osobní potřebu (např. adresáře). Tyto evidence nespádají pod působnost GDPR.

16.11. Listinné zdroje/evidence

Veškeré listinné zdroje/evidence jsou řádně uloženy v příslušných označených šanonech. Každá listinná evidence je vedena v rámci příslušné agendy. Ke každé agendě byl vypracován řádný agendový list. Pro přehled agend byl vypracován dokument s povahou soupisu agend, který obsahuje přehledné informace o vedených agendách (listinných i elektronických).

Veškeré listinné zdroje/evidence jsou uloženy v zamčených skříních/uzavřených skříních/policích vždy tak, aby k nim neměla přístup žádná třetí osoba. V případě, že je dokument uložen v kanceláři volně, dbá příslušný zaměstnanec na to, aby k němu neměla přístup žádná třetí osoba. Každá kancelář je mimo pracovní dobu uzamčena. Budova úřadu je mimo pracovní dobu vždy uzamčena a zabezpečena.

17. Popis implementace GDPR

17.1. Správce v souladu s GDPR vytvořil ke všem vedeným agendám podrobný agendový list. Tento agendový list obsahuje vždy následující údaje:

- **Název a popis agendy**
- **Účel zpracování**
- **Forma zpracování (listinná/elektronická)**
- **Forma zpracování (strukturovaná/nestrukturovaná)**
- **Podobný popis způsobu zpracování**
- **Kategorie subjektu údajů**
- **Kategorie příjemců**
- **Informaci o tom, zda jsou údaje předávány do třetích zemí**
- **Označení správce a zpracovatele**
- **Označení pověřence pro ochranu osobních údajů**
- **Označení dokladu (nosiče údajů)**
- **Určení doby zpracování**
- **Informaci o tom, zda je zpracování rizikové**
- **Informaci o tom, zda je informace zpracovávána na základě zákona**
- **Popis technických a organizačních opatření**
- **Komentář**

17.2. Vypracovaný dokument slouží správci rovněž pro posouzení, zda je zpracování v souladu s GDPR. V případě, že byl správcem vyhodnocen nesoulad, bylo přijato opatření k nápravě. Na základě vypracovaných agendových listů byl vytvořen seznam agend. Seznam agend poskytuje ucelený přehled o všech agendách, které správce zpracovává.



- 17.3. Při zpracování agendových listů nebyl správcem vyhodnocen nesoulad s nařízením GDPR.
- 17.4. Při zpracování agendových listů nevyhodnotil správce žádnou agendu jako rizikovou (obsahující citlivé osobní údaje o náboženském vyznání, sexuální orientaci, politickém přesvědčení apod.)
- 17.5. Postup správce osobních údajů při zpracování agendových listů byl vyhodnocen jako zcela legitimní, v souladu s požadavky GDPR.
- 17.6. **Záznamy o zpracování osobních údajů**
Správce vede záznamy o zpracování osobních údajů. Tyto záznamy popisují důležité skutečnosti, které se ke zpracování osobních údajů vztahují. Tuto činnost vykonává správce na základě čl. 30 nařízení GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě zvlášť a obsahují všechny informace obsažené v čl. 30 nařízení GDPR (např. údaje o správci, účel zpracování, popis kategorií subjektů údajů apod.). Všechny tyto záznamy budou pravidelně aktualizovány.
- 17.7. **Návrh na doplnění vnitřních předpisů**
Správci osobních údajů lze doporučit přijetí směrnice, která by upravovala zpracování osobních údajů dle nařízení GDPR (směrnice na ochranu osobních údajů). Vzhledem ke skutečnosti, že přijetí směrnice není povinností obce, nelze přijetí takovéto směrnice autoritativně nařídit.
Další doporučení nejsou navrhována. Správce zpracovává osobní údaje zcela v souladu s nařízením GDPR.

18. Riziková zpracování

- 18.1. Obec zpracovává většinu osobních údajů na základě čl. 6 odst. 1 písm. c), tedy za plnění zákonné povinnosti obce, případně písm. e), kdy dochází ke zpracování veřejného zájmu nebo písm. b) na základě plnění smlouvy. V minimální míře pak obec zpracovává osobní údaje na základě souhlasu a oprávněného zájmu správce.
- 18.2. Na základě pečlivého studia dokumentů v rámci ochrany osobních údajů **nebyly zjištěny agendy, které vykazují vyšší míru rizika incidentních hrozeb.**
- 18.3. Obec v minulosti nezaznamenala ztrátu nebo odcizení osobních údajů.
- 18.4. Obec v minulosti nebyla sankcionována Úřadem pro ochranu osobních údajů, pro porušení povinností souvisejících s ochranou osobních údajů.
- 18.5. **Žádné ze zpracovávaných osobních údajů nespádají do zvláštní kategorie osobních údajů ve smyslu čl. 9 nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (dále jen GDPR). Výjimku představují nanejvýš osobní údaje zaměstnanců vyžadované právními předpisy za účelem plnění zákonných povinností zaměstnavatele (např. údaje o zdravotním stavu zaměstnanců).**



19. Obecný popis technických a organizačních opatření

19.1. Technická opatření obce

Technická opatření obce jsou navržena tak, aby splňovala veškeré nároky nařízení GDPR. V první řadě jsou všechny počítače v budově úřadu zabezpečeny proti neoprávněnému přístupu heslem. Použité heslo je kombinací znaků a čísel a je pravidelně aktualizováno. Použité heslo k samotnému přístupu do PC (po zapnutí) zná vždy jen konkrétní zaměstnanec, který s PC pracuje. Zároveň obec dbá na to, aby k žádnému počítači neměla přístup třetí osoba. Z obecného hlediska lze říci, že veškerý používaný software je pravidelně aktualizován. Veškerý software byl také legálně zakoupen a je užíván dle příslušných uživatelských příruček a dokumentů obdobných. Správce dbá na to, aby případný zpracovatel (který je zároveň poskytovatelem software) dbal na ochranu osobních údajů v souladu s nařízením GDPR.

Správce dlouhodobě využívá příslušný antivirový program. Každý počítač je také chráněn branou firewall. Každý zaměstnanec při práci využívá pouze ověřené a důvěryhodné zdroje.

Správce má s tímto zabezpečením dlouhodobě dobré zkušenosti. V minulosti nikdy nedošlo k úniku dat z důvodu nedostatečného technického zabezpečení na straně správce (či zpracovatele). Riziko bylo vyhodnoceno jako minimální/žádné.

19.1.1. Dodavatelé IT software a programů

Pro elektronické zdroje je zajištěna dokumentace všech IT programů, které obecní úřad používá a postupnými kroky se zároveň bude chystat systémová příručka. V systémové příručce obce budou následující body:

1. Popis implementovaného systému nebo programu (nutné podmínky pro instalaci a následný provoz)
2. Licenční podmínky
3. Popis podpory uživatele (hot-line, helpdesk)
4. Bezpečnostní podmínky (jak je systém zabezpečen – přístupy, šifrování, zálohování a bezpečnostní kopie).
5. Popisy systémem vytvářených logů – systémových a transakčních
6. Zprávy a výsledky testů a certifikací, které informační systém nebo program získal
7. Případně cloudové služby

V současné době obec nevyužívá cloudové služby a nemá to ani v plánu. Pokud ale po změně vedení, případně jiného vedení, obec tyto služby začne používat, obec si vyžádá informace o tom, kde se úložiště nachází a že úložiště je zabezpečeno podle GDPR.

19.1.2. Smluvní vztahy s dodavateli software

Správce se v rámci svých elektronických zdrojů a informačních systémů písemně dotázal dodavatelů IS programů, zda jeho systém je na GDPR připraven. Smluvní strany jsou připraveny spolupracovat s pověřencem pro ochranu osobních údajů,



včetně kooperace s případnými kontrolami. Správce uzavřel / uzavře s poskytovateli IS dodatek ke smlouvě, který bude zaručovat odpovědnost zpracovatele za nakládání s os. údaji.

Správce po dodavateli IT softwaru požaduje závazek:

- spolupracovat s pověřencem pro ochranu os. údajů
- subjekt údajů bude mít dobrou dostupnost k informacím o zpracování svých údajů
- možnost realizovat právo subjektu na opravu nebo výmaz údajů s tím, že se uvede, v jaké formě (nejlépe v písemné formě),
- možnost realizovat právo na omezení zpracování,
- možnost subjektu poskytnout kopii zpracovávaných osobních údajů,
- možnost výkonu práva na přenositelnost údajů,
- zajištění podpory logování v čitelné formě s vazbou na uživatele a jeho činnosti,
- zajištění ochrany dat po ukončení smlouvy.

Dále správce zreviduje/zrevidoval smlouvy, které obsahují osobní údaje následujícím způsobem:

- Zajištění mlčenlivosti osob, které přijdou do styku s osobními údaji (u externích dodavatelů, případně tam, kde není zákonná povinnost)
- Zajištění a nastavení podmínek pro zapojení dalšího zpracovatele dle nařízení GDPR
- Zajistit práva subjektu údajů (informace o vedených údajích apod., dle GDPR)
- Zajistit podporu pověřence pro ochranu osobních údajů
- Zajistit ujednání o náhradě škody, včetně regresních nároků (s pozorností na smluvní pokuty, aby nevylučovaly náhradu škody).
- Zajistit po ukončení smlouvy odstranění kopií, zničení kopií, případně předání osobních údajů.

19.1.3. Obecný návrh opatření

Považuje se za vhodné zajistit pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Tento proces by měl být náležitě popsán (případně zaznamenán do systémové příručky/analýzy rizik), tak aby kontrola a realizace procesu byla součástí provozního testování, posuzování a hodnocení účinnosti zavedených opatření.

Správce bude nadále pokračovat v zajišťování souladu s GDPR. Správce bude postupně implementovat do všech dokumentací, vnitřních předpisů a nařízení ustanovení, která budou sloužit k:

- pseudoanonymizaci a šifrování osobních údajů k zajištění, aby tyto postupy byly běžnou součástí každodenního výkonu činností správce,
- zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování,



- schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů.

19.2. Organizační opatření obce

Organizační opatření správce spočívají v zajištění ochrany osobních údajů, které správce uchovává v listinné podobě (případně na fyzických datových nosičích). Toto zajištění spočívá zejména ve znemožnění třetím osobám k volnému přístupu k dokumentům, které obsahují osobní údaje. Správce provádí toto opatření zejména tak, že uzamyká budovu úřadu mimo úřední hodiny. Stejně jako budova obecního úřadu jsou uzamčeny i všechny kanceláře. V pracovní době jsou všechny výše uvedené nosiče dat pod dozorem příslušného pracovníka úřadu. Některé významné dokumenty jsou uchovány v trezoru úřadu. Zaměstnanci obce mají rovněž možnost dokumenty ukládat do uzamykatelných skříní.

Správce v minulosti nezaznamenal žádné porušení bezpečnosti, které by vedlo ke ztrátě či zneužití spravovaných údajů. Všichni zaměstnanci obce jsou řádně proškoleni.

Správce má s výše uvedeným zabezpečením dlouhodobě dobré zkušenosti. Riziko bylo vyhodnoceno jako minimální/žádné.

19.3. Personální opatření obce

Personální opatření obce, v postavení správce, spočívá v proškolení všech stávajících zaměstnanců a osob, které přichází do kontaktu s osobními údaji. Všichni zaměstnanci správce jsou řádně proškoleni na prezenčních školeních. V případě neznalosti některé problematiky se mohou obrátit na pověřence pro ochranu osobních údajů. Zároveň správce do budoucna plánuje další školení, která budou utvrzovat vzdělání všech dotčených osob v daném směru.

Správce považuje přijatá opatření za naprosto dostatečná. Riziko úniku osobních údajů subjektů údajů v důsledku neznalosti dotčených osob bylo vyhodnoceno jako minimální/žádné.

20. Řešení zabezpečení jednotlivých agend

20.1. Mzdová a personální agenda

Stávající stav: Mzdová a personální agenda je vedena na základě zákoníku práce, dalších pracovněprávních předpisů a zákona o účetnictví. Všechny dokumenty jsou uloženy v písemné formě v příslušném šanonu, který je označen OÚ/01 a v digitální podobě v počítači Ing. Věra Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing. Věra Javůrková a zaměstnanci společnosti Vikaflex s.r.o., Svatava, kteří měsíčně zpracovávají odměny a platy.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce má se zpracovatelem uzavřenou řádnou smlouvu. Zpracovatel se zavázal k dodržování zásad GDPR písemným dodatkem k výše uvedené smlouvě.

Rizikové zpracování: ne



Zpracování citlivých osobních údajů: ne

20.2. Smlouvy

Stávající stav: Smlouvy jsou evidovány na základě občanského zákoníku a na základě zákona o účetnictví. Rovněž na základě zákona o obcích. Všechny smlouvy jsou uloženy v písemné formě v příslušném šanonu, který je označen OÚ/02 a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Smlouvy jsou zveřejňovány na profilu zadavatele veřejných zakázek. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing. Věra Javůrková. Na profilu zadavatele nejsou zveřejňovány údaje nad rámec údajů zveřejňovaných v obchodním / živnostenském rejstříku.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.3. Daňové doklady, faktury

Stávající stav: Daňové doklady a faktury jsou evidovány na základě zákona o účetnictví. Všechny jsou uloženy v písemné formě v příslušném šanonu, který je označen OÚ/03 a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k nim má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoba oprávněná ke zpracování je Ing. Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.4. Žádosti

Stávající stav: Žádosti jsou evidovány na základě zákonů vztahujících se k jednotlivým druhům žádostí. Žádosti jsou uloženy v písemné formě v příslušných šanonech, které jsou označeny OÚ/04 a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing. Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.



Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.5. **Správní rozhodnutí/rozhodování**

Stávající stav: Správní rozhodnutí jsou evidována na základě správního řádu a zákonů vztahujících se k jednotlivým druhům žádostí. Rozhodnutí jsou uložena v písemné formě v příslušných šanonech, které jsou označeny OÚ/05 a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing, Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.6. **Dary**

Stávající stav: Darovací smlouvy jsou evidovány na základě zákona o obcích a občanského zákoníku. Žádosti jsou uloženy v písemné formě v příslušných šanonech, které jsou označeny OÚ/06 a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing, Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.7. **Dotace**

Stávající stav: Žádosti o dotaci jsou evidovány na základě zákona o obcích a zákona o rozpočtových pravidlech územních samosprávných celků. Žádosti jsou uloženy v písemné formě v příslušných šanonech, které jsou označeny OÚ/07 a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing, Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.



Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.8. Územní plán

Stávající stav: Územní plán obce je veden na základě stavebního zákona. Všechny dokumenty související s jeho tvorbou a změnami jsou uloženy v písemné formě v příslušném šanonu, který je označen OÚ/08 a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing, Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.9. Evidence psů

Stávající stav: Evidence psů je evidována na základě zákona o místních poplatcích. Evidence je uložena v písemné formě v příslušném šanonu, který je označen OÚ/09 a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing, Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.10. Klíče

Stávající stav: Seznam klíčů a osob je evidován na základě organizačně technického opatření a je uložen v příslušném šanonu, který je označen OÚ/10. K dokumentu má přístup Milan Pokorný a Ing. Věra Javůrková. Seznam je veden za účelem ochrany majetku (oprávněný zájem obce a povinnost obce pečovat o majetek s péčí řádného hospodáře.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR. Agenda není vedena v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne



20.11. **Razítka**

Stávající stav: Seznam razítek je evidován na základě vnitřní směrnice a zákona o archivnictví. Seznam je uložen v příslušném šanonu, který je označen OÚ/11. K dokumentu má přístup Milan Pokorný a Ing. Věra Javůrková.

Návrh opatření: Agenda je zpracovávána v souladu s GDPR. Agenda není vedena v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.12. **Adresáře**

Stávající stav: Adresáře jsou evidovány k plnění veřejné správy - např. případy havárií, agenda poplatků. Adresáře jsou uloženy v souboru kontaktů, který je označen OÚ/12. K adresářům má přístup Milan Pokorný a Ing. Věra Javůrková. Adresáře jsou vedeny částečně za účelem osobní potřeby - soukromé zpracování osobních údajů, kterého se nedotýká právní úprava.

Návrh opatření: Žádné – agenda spadá svou povahou do zpracování pro osobní potřeby.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.13. **Ověřování (vidimace a legalizace)**

Stávající stav: Vidimace a legalizace je vedena na základě zákona o ověřování shody opisu nebo kopie s listinou a ověřování pravosti. Dokumenty jsou uloženy v písemné formě v příslušném šanonu, který je označen OÚ/13 a v digitální podobě v počítači Ing. Věra Javůrkové. Ověřovací kniha je uložena v uzamykatelné skříni v kanceláři úřadu. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný a Ing. Věra Javůrková. Při zpracování agendy je dbáno na zvýšenou ochranu údajů o subjektech údajů.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.14. **Evidence obyvatel**

Stávající stav: Registratura, kterou tvoří přihlašovací lístky k trvalému pobytu, je tvořena na základě zákona o evidenci obyvatel a rodných číslech. Přihlašovací lístky jsou v písemné formě uloženy v pouzdech, které jsou označeny OÚ/14. Evidence obyvatel v digitální podobě je vedena v počítači Ing. Věry Javůrkové. Přístup k ní má starosta Milan Pokorný a zaměstnankyně úřadu Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing. Věra Javůrková.



Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem. Dokumenty, které jsou v elektronické podobě přístupné pouze v konkrétním programu jsou chráněny proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.15. **Kronika**

Stávající stav: Kronika je tvořena na základě zákona o kronikách obcí v písemné podobě. Je uložena v kanceláři obecního úřadu pod označením OÚ/15. . Přístup k ní má starosta Milan Pokorný a zaměstnankyně úřadu Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Zdeňka Mňatinohová – kronikářka.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR v listinné podobě. Kronika není vedena v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.16. **Přestupky**

Stávající stav: Oznámení o přestupku jsou bezodkladně zasílána na základě uzavřené veřejnoprávní smlouvy magistrátu města k vyřízení. Do doby odeslání jsou dokumenty uloženy v písemné formě v příslušném svazku s označením OÚ/16.. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný, Ing. Věra Javůrková a zaměstnanec Magistrátu města Karlovy Vary.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR v listinné podobě. Kronika není vedena v elektronické podobě. Povinnost k ochraně osobních údajů se přenáší na zpracovatele (Magistrát města Karlovy Vary) a to vzhledem ke skutečnosti, že nejsou u správce dlouhodobě uchovávány.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.17. **Volby**

Stávající stav: Seznam voličů je veden na základě zákona o volbách do parlamentu, do zastupitelstev obcí, do zastupitelstev krajů, prezidenta republiky a do Evropského parlamentu. Dokumenty jsou uloženy v písemné formě v příslušném šanonu, který je označen OÚ/17 a v digitální podobě v počítači Ing. Věra Javůrkové. Přístup k dokumentům má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoby oprávněné k zpracování jsou: Milan Pokorný a Ing. Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené



v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

20.18. Plné moci

Stávající stav: Plné moci jsou evidovány na základě trestního řádu, občanského soudního řádu, správního řádu, správního řádu soudního, zákona o zvláštních řízeních soudních, občanského zákoníku, zákon o obchodních společnostech a družstvech, insolvenčního zákona, daňových právních předpisů a zákoníku práce. Všechny dokumenty jsou uloženy v písemné formě v příslušném šanonu, který je označen OÚ/18. a v digitální podobě v počítači Ing. Věry Javůrkové. Přístup k nim má starosta Milan Pokorný a účetní Ing. Věra Javůrková. Osoba oprávněná ke zpracování je Ing. Věra Javůrková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

21. Pověřenec pro ochranu osobních údajů

21.1. 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, řízení procesů, 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 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.

21.2. **Obec má řádně jmenovaného pověřence pro ochranu osobních údajů, který není ve střetu zájmů.**

21.3. **Obec v postavení správce jmenováním řádného pověřence splňuje požadavky nařízení GDPR a vhodně snižuje rizika, která by mohla nastat v souvislosti s ochranou osobních údajů.**

21.4. Pověřenec pro obec zajišťuje tyto činnosti:

- 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 proškoleny v oblasti ochrany osobních údajů.
- 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.

22. Závěrečná ustanovení – zhodnocení souladu s nařízením GDPR

- 22.1. Zpracovatel tohoto dokumentu hodnotí všechny postupy správce osobních údajů jako postupy prováděné v souladu s nařízením GDPR. Dle výše uvedených informací správce postupuje při zpracování osobních údajů řádně, transparentně a s dostatečným ohledem na zabezpečení osobních údajů.
- 22.2. Správce osobních údajů přijal vhodná technická a organizační opatření. Detailní popis těchto opatření je uveden na každé jednotlivé kartě příslušné agendy. Vzhledem ke skutečnosti, že správce neprovádí rizikové zpracování, jsou všechna přijatá opatření hodnocena jako přiměřená.
- 22.3. Správce osobních údajů řádně jmenoval pověřence pro ochranu osobních údajů. Správce tak splnil povinnost, která byla stanovena nařízením GDPR. Jmenovaný správce není ve střetu zájmů a může tak činnost vykonávat.
- 22.4. Správce osobních údajů řádně zpracoval záznamy o činnostech zpracování. Správce tak splnil svou povinnost, která byla stanovena nařízením GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě. Tento postup zajišťuje vysokou míru transparentnosti při nakládání s osobními údaji.
- 22.5. Správce osobních údajů řádně zpracoval karty agend. Správce tak splnil svou povinnost stanovenou nařízením GDPR. Zpracování těchto karet je klíčovou činností každého správce a slouží zejména k prokázání souladu zpracování s nařízením GDPR.
- 22.6. Správce osobních údajů dlouhodobě klade důraz na bezpečné uchovávání a nakládání s osobními údaji. Tuto skutečnost potvrzuje fakt, že správce nebyl v minulosti vystaven sankci za porušení zákona o ochraně osobních údajů či jiných právních předpisů.
- 22.7. Správci lze dlouhodobě doporučit pokračování ve stávající úrovni zabezpečení a prohlubování znalostí nařízení GDPR a dalších právních předpisů.
- 22.8. Správci lze dlouhodobě doporučit průběžně aktualizovat karty agend v případě změn.
- 22.9. Správci lze dlouhodobě doporučit aktualizaci tohoto dokumentu.
- 22.10. Porušení nařízení GDPR při činnosti správce: **nebylo zjištěno.**
- 22.11. Závažné hrozby/rizika v souvislosti se zpracováním: **nezjištěno.**



23. Konečné hodnocení

23.1. Správce vykonává svou činnost v souladu s nařízením GDPR.

24. Seznam vedených agend

Zpracovatel analýzy přikládá přehled správcem vedených agend s vyhodnocením rizik.

Dokument/seznam/doklad	Účel zpracování	Údaje	Příjemce	Zákon	Komentář	Rizikový
Mzdová a personální agenda	plnění smluv, vedení personální evidence zaměstnanců pro účely plnění pracovních smluv a povinností dle zákoníku práce a dalších předpisů	Jméno, příjmení, rodné číslo, datum narození, adresa,	polečnost Vikaflex, s. r. o. a dozorové orgány	zákoník práce, zákon o daních z příjmu, zákon o pojistném na veřejné zdravotní pojištění, zákon o sociálním zabezpečení a příspěvku na státní politiku zaměstnanosti		NE
Smlouvy	shromažďování údajů za účelem plnění smluv, evidence smluv, archivace údajů za účelem vymáhání případných nároků ze smluv	Jméno, příjmení, rodné číslo, datum narození, IČ, DIČ, adresa,	Smluvní strana	Zákon č. 128/2000 o obcích (obecní zřízení); zákon č. 89/2012 občanský zákoník	o dílo, pronájmy, ... Vytváří se na PC a tisknou se, zakládají	NE
Faktury	zpracování Ekonomické	Jméno, příjmení,	Dodavatel,	zákon o		NE



	agendy obce, vedení účetnictví obce	IČ, DIČ, adresa,	odběratel	účetnictví		
Žádosti	správní rozhodován í úřadu, rozhodován í obce, zpracování žádostí od občanů obce a třetích osob	Jméno, příjmení, datum narození, adresa,	Žadatel v postavení fyzické osoby, či právnícké osoby (dažadující orgány), státní archiv, stavební úřad apod.	zákon o ochraně přírody a krajiny, stavební zákon, zákon o vodovodech a kanalizacích apod.		NE
Správní rozhodnutí	Výkon státní správy, evidence a vydávání správních rozhodnutí	Jméno, příjmení, datum narození, adresa,	Žadatel o rozhodnutí	správní řád, zákon o ochraně přírody a krajiny, stavební zákon, zákon o vodovodech a kanalizacích, zákon o obcích		NE
Dary	Správní rozhodnutí úřadu, rozhodován í obce	Jméno, příjmení, datum narození, adresa,	Žadatel v postavení obarovaneh o (subjekt údajů), dále zpracovatel, dárce (fyzická nebo právnícká osoba)	občanský zákoník, zákon o obcích		NE
Dotace	Evidence a vyřizování žádostí o	Jméno, příjmení, datum narození,	Žadatel o dotaci	Zákon č. 250/2000 Sb., o rozpočtových pravidlech		NE



	dotaci	adresa,		územních rozpočtů, zákon č. 500/2004 Sb., správní řád, zákon č.89/2012 Sb., občanský zákoník, zákon č.128/2000 Sb., o obcích		
Územní plán	Tvorba a změny plánu	Jméno, příjmení, adresa	občan obce, příslušný stavební úřad	stavební zákon, zákon o obcích		NE
Evidence psů	kontakt při ztrátě psa, vymáhání pohledávek za poplatky ze psů	Jméno, příjmení, adresa, telefon	Referent úřadu	zákon o místních poplatcích		NE
Klíče	Zabezpečení prostoru obecního úřadu.	jméno, příjmení	starosta, referent úřadu	Organizačně technické opatření		NE
Razítka	Evidence dle spisového řádu	číslo razítka, jméno, příjmení	starosta, referent úřadu	Zákon o archivnictví, vnitřní směrnice		NE
Adresáře	Pro komunikaci při výkonu veřejné správy	Jméno, příjmení, kontakt (tel/email)	starosta, referent úřadu		nepodléhá GDPR	NE
Ověřování	Czech Point, ověřovací kniha - zajišťování vidimace a legalizace	Jméno, příjmení, rodné číslo, datum narození,	Žadatel, Fyzická osoba	Zákon o ověřování shody opisu nebo kopie s listinou a o ověřování		NE



		adresa, číslo OP, IČ, DIČ		pravosti		
Evidence obyvatel	Vedení seznamu obyvatel / zpracování evidence obyvatel	Jméno, příjmení, datum narození, rodné číslo, místo trvalého pobytu	Referent úřadu, starosta	zákon o evidenci obyvatel a rodných číslech		NE
Kronika	Zachycení událostí v obci	Jméno, příjmení	Kronikářka, Fyzické osoby požadující nahlédnutí dle zákona	zákon o kronikách obcí		NE
Přestupky	Vedení evidence přestupků, naplnění zákona o přestupcích	Jméno, příjmení, datum narození, bydliště,	referent úřadu, starosta	zákon o odpovědnosti za přestupky a řízení o nich č. 250/2016 Sb.		NE
Volby	Organizace voleb na základě zákona	Jméno, příjmení, datum narození, bydliště	volební komise, referent úřadu	Zákon o volbách do parlamentu, do zastupitelstev obcí, do zastupitelstev krajů, prezidenta republiky, do Evropského parlamentu .		NE
Plná moc	Zastupování obce	Jméno, příjmení, datum narození, bydliště,	starosta, referent úřadu	trestní řád, občanský soudní řád, správní řád, správní řád soudní, zákon o		NE



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

		IČ, adresa		zvláštních řízeních soudních, občanský zákoník, zákon o obchodních společnostech a družstvech, insolvenční zákon, daňové právní předpisy, zákoník práce.		
--	--	------------	--	--	--	--



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

12.3 Analýza rizik obce Jenišov



Obec Jenišov, Jenišov 88, 360 01 Jenišov

Analýza rizik

zpracovaná v souladu s Nařízením 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 (dále jen „GDPR“), zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“) a dle zákona o zpracování osobních údajů č. 110/2019 Sb.,

Správce:

Obec Jenišov

Jenišov 88

362 11 Jenišov

IČ: 00573248



25. Úvodní ustanovení

25.1. 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 povinná 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.

25.2. Vymezení a definice správce v postavení obce

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 vyplývajících, 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.

25.3. Definice pojmu 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.

25.4. Definice pojmu 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.

25.5. Definice pojmu 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.

25.6. 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.

25.7. Definice pojmu rizikové zpracování

Posouzení vlivu na ochranu osobních údajů musí provést správce, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, bude představovat vysoké riziko pro práva a svobody fyzických osob. Posouzení se musí provést před započítím předmětného zpracování. Pokud byl ustanoven pověřenec pro ochranu osobních údajů, vyžádá si správce jeho posudek. Posouzení vlivu na ochranu osobních údajů se vyžaduje především:

- u systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování,



včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky

- u rozsáhlého zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech
- u rozsáhlého systematického monitorování veřejně přístupných prostorů

Správci osobních údajů budou povinni sami vést záznamy o činnostech zpracování (čl. 30), v případě vysoce rizikových zpracování provést posouzení vlivu na ochranu osobních údajů (čl. 35), a teprve v případě, že vysoká rizika nelze eliminovat, obrátit se na Úřad s žádostí o konzultaci (čl. 36).

26. Obecné informace

26.1. Metoda zpracování analýzy

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, a to s ohledem na posuzování hodnoty aktiv, hrozeb a stanovení dalších parametrů analýzy rizik z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

Zpracovatel ve spolupráci se správcem osobních údajů zvolil metodu zhodnocení každé zpracovávané agendy, která osahuje osobní údaje. V rámci tohoto zhodnocení došlo k ohodnocení primárních aktiv dle jejich kritičnosti, a to v souladu s nařízením GDPR. Vzhledem ke skutečnosti, že GDPR nepředepisuje povinný formát analýzy rizik a taktéž nikterak neuvažuje hodnotu rizika, hodnotil správce riziko z pohledu ohrožení práv subjektů údajů.

Samotná definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u každé agendy je popsána v příslušném agendovém listu (dokument, který byl vypracován ke každé agendě zvlášť). Tyto údaje budou rovněž uvedeny v tomto dokumentu, v oddílu s názvem: „Řešení zabezpečení jednotlivých agend“.

Zpracovatel analýzy rizik předkládá agendový list jako přílohu této analýzy (**příloha č. 1**)

26.2. Metoda určení a hodnocení aktiv

Zhotovitel určí primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení. Aktivum je chápáno jako objekt (dokument, informační systém, kartotéka, spisovna, portál, evidence či jiné listinné nebo elektronické úložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR. Každá agenda pak obsahuje více těchto aktiv.

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.



26.3. Účel zpracování dokumentu

Tento dokument s názvem „Analýza rizik“ je zpracován v souladu s Nařízením 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 (dále jen „GDPR“), zejména dle článku 24 a článku 25.

Dokument představuje ucelený souhrn informací týkající se implementace GDPR do vnitřních i vnějších procesů obce. Osoby, které vystupují v obci v postavení správce, jsou s tímto dokumentem plně seznámeny.

Dokument popisuje vyhodnocení rizik, která vznikají správci v souvislosti se zpracováním údajů o subjektech údajů. Na základě vyhodnocených rizik přijal správce vhodná opatření, které jsou v tomto dokumentu rovněž popsána.

Opatření přijatá správcem

Správce osobních údajů přijal všechna opatření vhodná ke snížení/vyloučení rizik, která vyhodnotil jako přiměřená a v souladu s GDPR. Přijatá opatření budou podrobně popsána v tomto dokumentu.

27. Charakteristika posuzovaného subjektu – správce osobních údajů

27.1. Identifikační údaje správce

Název: Obec Jenišov

Sídlo: Jenišov 88, 362 11 Jenišov

IČ: 00573248

Telefon: +420 739 506 842

+420 739 506 841

e-mail: info@jenisov.cz

Webové stránky: <http://www.jenisov.cz>

Počet členů zastupitelstva: 7 členů

Počet obyvatel: 978⁷

27.2. Struktura obecního úřadu

Obecní úřad tvoří starosta, místostarosta a zaměstnanci obce zařazení do obecního úřadu.

Úřední hodiny obecního úřadu jsou:

Pondělí: 7:30 – 12:00

Úterý: 14:00 – 17:00

Středa: 7:30 – 12:00

Čtvrtek: 14:00 – 17:00

Pátek: 7:30 – 12:00

⁷ Tento údaj je pouze orientační.



27.3. Zveřejňování informací

Obec zveřejňuje informace na webových stránkách obce, a to včetně informací povinně zveřejňovaných dle jiného právního předpisu. Obec dále zveřejňuje informace na úřední desce obce, a to jak na úřední desce elektronické, tak fyzické. Při zveřejňování informací obec dlouhodobě dodržuje ustanovení zákona o ochraně osobních údajů (zákon č. 101/2000 Sb.). Obec při zveřejňování všech informací dbá na dodržení nařízení GDPR. Informace, o kterých není známo, zda podléhají ochraně dle GDPR, jsou konzultovány před zveřejněním s pověřencem pro ochranu osobních údajů. Správce osobních údajů rovněž poskytuje informace písemně a ústně, vše při dodržování nařízení GDPR.

28. Obecná struktura uchovávání osobních údajů v obci

28.1. Evidence údajů nahlášená Úřadu pro ochranu osobních údajů

V současné době nevede správce žádnou evidenci, která by podléhala nahlášení Úřadu pro ochranu osobních údajů.

28.2. Technické a organizační opatření

Správce osobních údajů přijal organizační a technická opatření v souladu s GDPR. Správce osobních údajů soustavně pracuje na modernizaci organizačních i technických opatření tak, aby bylo zajištěno maximální zabezpečení všech zpracovávaných údajů.

28.3. Předpisy obce

Technicko-organizační opatření ve formě předpisu k ochraně osobních údajů: ne
Obec v postavení správce osobních údajů se řídí těmito vnitřními předpisy:

- organizační řád
- spisový a skartační řád schválený věcně a místně příslušným archivem
- vnitřní organizační směrnice pro používání IT
- směrnice...
- vnitřní předpis...

28.4. Elektronické zdroje/evidence

28.5. Za zajištění jednotlivých informačních systémů odpovídá správce informačního systému.

28.6. Poskytovatelem internetového připojení je společnost: (doplnit název). Internetové připojení není poskytováno veřejně.

28.7. Elektronické zdroje popisují programové vybavení (software) využívané správcem při zpracování a evidenci údajů dle GDPR.

28.8. Veškeré programové vybavení (software) bylo pořízeno legálně a je pravidelně aktualizováno. Správce dbá na to, aby poskytovatel software zpracovával osobní údaje v souladu s GDPR.

28.9. Správce používá při své činnosti tyto elektronické zdroje/evidence:



- **Účetní program** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program evidence obyvatel** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program pokladny** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program evidence majetku** (doplnit název) – zpracovatel, (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Kancelářské programy Office** – jedná se o běžné kancelářské programy „Office“ od společnosti Microsoft.

28.10. Zaměstnanci obce mohou zpracovávat elektronické evidence s povahou zpracování pro osobní potřebu (např. adresáře). Tyto evidence nespádají pod působnost GDPR.

28.11. Listinné zdroje/evidence

Veškeré listinné zdroje/evidence jsou řádně uloženy v příslušných označených šanonech. Každá listinná evidence je vedena v rámci příslušné agendy. Ke každé agendě byl vypracován řádný agendový list. Pro přehled agend byl vypracován dokument s povahou soupisu agend, který obsahuje přehledné informace o vedených agendách (listinných i elektronických).

Veškeré listinné zdroje/evidence jsou uloženy v zamčených skříních/uzavřených skříních/policích vždy tak, aby k nim neměla přístup žádná třetí osoba. V případě, že je dokument uložen v kanceláři volně, dbá příslušný zaměstnanec na to, aby k němu neměla přístup žádná třetí osoba. Každá kancelář je mimo pracovní dobu uzamčena. Budova úřadu je mimo pracovní dobu vždy uzamčena a zabezpečena.

29. Popis implementace GDPR

29.1. Správce v souladu s GDPR vytvořil ke všem vedeným agendám podrobný agendový list. Tento agendový list obsahuje vždy následující údaje:

- **Název a popis agendy**
- **Účel zpracování**
- **Forma zpracování (listinná/elektronická)**
- **Forma zpracování (strukturovaná/nestrukturovaná)**
- **Podobný popis způsobu zpracování**
- **Kategorie subjektu údajů**
- **Kategorie příjemců**
- **Informaci o tom, zda jsou údaje předávány do třetích zemí**



- **Označení správce a zpracovatele**
- **Označení pověřence pro ochranu osobních údajů**
- **Označení dokladu (nosiče údajů)**
- **Určení doby zpracování**
- **Informaci o tom, zda je zpracování rizikové**
- **Informaci o tom, zda je informace zpracovávána na základě zákona**
- **Popis technických a organizačních opatření**
- **Komentář**

29.2. Vypracovaný dokument slouží správci rovněž pro posouzení, zda je zpracování v souladu s GDPR. V případě, že byl správcem vyhodnocen nesoulad, bylo přijato opatření k nápravě. Na základě vypracovaných agendových listů byl vytvořen seznam agend. Seznam agend poskytuje ucelený přehled o všech agendách, které správce zpracovává.

29.3. Při zpracování agendových listů nebyl správcem vyhodnocen nesoulad s nařízením GDPR.

29.4. Při zpracování agendových listů nevyhodnotil správce žádnou agendu jako rizikovou (obsahující citlivé osobní údaje o náboženském vyznání, sexuální orientaci, politickém přesvědčení apod.)

29.5. Postup správce osobních údajů při zpracování agendových listů byl vyhodnocen jako zcela legitimní, v souladu s požadavky GDPR.

29.6. **Záznamy o zpracování osobních údajů**

Správce vede záznamy o zpracování osobních údajů. Tyto záznamy popisují důležité skutečnosti, které se ke zpracování osobních údajů vztahují. Tuto činnost vykonává správce na základě čl. 30 nařízení GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě zvlášť a obsahují všechny informace obsažené v čl. 30 nařízení GDPR (např. údaje o správci, účel zpracování, popis kategorií subjektů údajů apod.). Všechny tyto záznamy budou pravidelně aktualizovány.

29.7. **Návrh na doplnění vnitřních předpisů**

Správci osobních údajů lze doporučit přijetí směrnice, která by upravovala zpracování osobních údajů dle nařízení GDPR (směrnice na ochranu osobních údajů). Vzhledem ke skutečnosti, že přijetí směrnice není povinností obce, nelze přijetí takovéto směrnice autoritativně nařídit.

Další doporučení nejsou navrhována. Správce zpracovává osobní údaje zcela v souladu s nařízením GDPR.



30. Riziková zpracování

- 30.1. Obec zpracovává většinu osobních údajů na základě čl. 6 odst. 1 písm. c), tedy za plnění zákonné povinnosti obce, případně písm. e), kdy dochází ke zpracování veřejného zájmu nebo písm. b) na základě plnění smlouvy. V minimální míře pak obec zpracovává osobní údaje na základě souhlasu a oprávněného zájmu správce.
- 30.2. Na základě pečlivého studia dokumentů v rámci ochrany osobních údajů **nebyly zjištěny agendy, které vykazují vyšší míru rizika incidentních hrozeb.**
- 30.3. Obec v minulosti nezaznamenala ztrátu nebo odcizení osobních údajů.
- 30.4. Obec v minulosti nebyla sankcionována Úřadem pro ochranu osobních údajů, pro porušení povinností souvisejících s ochranou osobních údajů.
- 30.5. **Žádné ze zpracovávaných osobních údajů nespádají do zvláštní kategorie osobních údajů ve smyslu čl. 9 nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (dále jen GDPR). Výjimku představují nanejvýš osobní údaje zaměstnanců vyžadované právními předpisy za účelem plnění zákonných povinností zaměstnavatele (např. údaje o zdravotním stavu zaměstnanců).**

31. Obecný popis technických a organizačních opatření

31.1. Technická opatření obce

Technická opatření obce jsou navržena tak, aby splňovala veškeré nároky nařízení GDPR. V první řadě jsou všechny počítače v budově úřadu zabezpečeny proti neoprávněnému přístupu heslem. Použité heslo je kombinací znaků a čísel a je pravidelně aktualizováno. Použité heslo k samotnému přístupu do PC (po zapnutí) zná vždy jen konkrétní zaměstnanec, který s PC pracuje. Zároveň obec dbá na to, aby k žádnému počítači neměla přístup třetí osoba. Z obecného hlediska lze říci, že veškerý používaný software je pravidelně aktualizován. Veškerý software byl také legálně zakoupen a je užíván dle příslušných uživatelských příruček a dokumentů obdobných. Správce dbá na to, aby případný zpracovatel (který je zároveň poskytovatelem software) dbal na ochranu osobních údajů v souladu s nařízením GDPR.

Správce dlouhodobě využívá příslušný antivirový program. Každý počítač je také chráněn branou firewall. Každý zaměstnanec při práci využívá pouze ověřené a důvěryhodné zdroje.

Správce má s tímto zabezpečením dlouhodobě dobré zkušenosti. V minulosti nikdy nedošlo k úniku dat z důvodu nedostatečného technického zabezpečení na straně správce (či zpracovatele). Riziko bylo vyhodnoceno jako minimální/žádné.

31.1.1. Dodavatelé IT software a programů

Pro elektronické zdroje je zajištěna dokumentace všech IT programů, které obecní úřad používá a postupnými kroky se zároveň bude chystat systémová příručka. V systémové příručce obce budou následující body:



1. Popis implementovaného systému nebo programu (nutné podmínky pro instalaci a následný provoz)
2. Licenční podmínky
3. Popis podpory uživatele (hot-line, helpdesk)
4. Bezpečnostní podmínky (jak je systém zabezpečen – přístupy, šifrování, zálohování a bezpečnostní kopie).
5. Popisy systémem vytvářených logů – systémových a transakčních
6. Zprávy a výsledky testů a certifikací, které informační systém nebo program získal
7. Případně cloudové služby

V současné době obec nevyužívá cloudové služby a nemá to ani v plánu. Pokud ale po změně vedení, případně jiného vedení, obec tyto služby začne používat, obec si vyžádá informace o tom, kde se úložiště nachází a že úložiště je zabezpečeno podle GDPR.

31.1.2. Smluvní vztahy s dodavateli software

Správce se v rámci svých elektronických zdrojů a informačních systémů písemně dotázal dodavatelů IS programů, zda jeho systém je na GDPR připraven. Smluvní strany jsou připraveny spolupracovat s pověřencem pro ochranu osobních údajů, včetně kooperace s případnými kontrolami. Správce uzavřel / uzavře s poskytovateli IS dodatek ke smlouvě, který bude zaručovat odpovědnost zpracovatele za nakládání s os. údaji.

Správce po dodavateli IT softwaru požaduje závazek:

- spolupracovat s pověřencem pro ochranu os. údajů
- subjekt údajů bude mít dobrou dostupnost k informacím o zpracování svých údajů
- možnost realizovat právo subjektu na opravu nebo výmaz údajů s tím, že se uvede, v jaké formě (nejlépe v písemné formě),
- možnost realizovat právo na omezení zpracování,
- možnost subjektu poskytnout kopii zpracovávaných osobních údajů,
- možnost výkonu práva na přenositelnost údajů,
- zajištění podpory logování v čitelné formě s vazbou na uživatele a jeho činnosti,
- zajištění ochrany dat po ukončení smlouvy.

Dále správce zreviduje/zrevidoval smlouvy, které obsahují osobní údaje následujícím způsobem:

- Zajištění mlčenlivosti osob, které přijdou do styku s osobními údaji (u externích dodavatelů, případně tam, kde není zákonná povinnost)
- Zajištění a nastavení podmínek pro zapojení dalšího zpracovatele dle nařízení GDPR
- Zajistit práva subjektu údajů (informace o vedených údajích apod., dle GDPR)
- Zajistit podporu pověřence pro ochranu osobních údajů
- Zajistit ujednání o náhradě škody, včetně regresních nároků (s pozorností na smluvní pokuty, aby nevykloučovaly náhradu škody).



- Zajistit po ukončení smlouvy odstranění kopií, zničení kopií, případně předání osobních údajů.

31.1.3. Obecný návrh opatření

Považuje se za vhodné zajistit pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Tento proces by měl být náležitě popsán (případně zaznamenán do systémové příručky/analýzy rizik), tak aby kontrola a realizace procesu byla součástí provozního testování, posuzování a hodnocení účinnosti zavedených opatření.

Správce bude nadále pokračovat v zajišťování souladu s GDPR. Správce bude postupně implementovat do všech dokumentací, vnitřních předpisů a nařízení ustanovení, která budou sloužit k:

- pseudoanonymizaci a šifrování osobních údajů k zajištění, aby tyto postupy byly běžnou součástí každodenního výkonu činností správce,
- zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování,
- schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů.

31.2. Organizační opatření obce

Organizační opatření správce spočívají v zajištění ochrany osobních údajů, které správce uchovává v listinné podobě (případně na fyzických datových nosičích). Toto zajištění spočívá zejména ve znemožnění třetím osobám kvolnému přístupu k dokumentům, které obsahují osobní údaje. Správce provádí toto opatření zejména tak, že uzamyká budovu úřadu mimo úřední hodiny. Stejně jako budova obecního úřadu jsou uzamčeny i všechny kanceláře. V pracovní době jsou všechny výše uvedené nosiče dat pod dozorem příslušného pracovníka úřadu. Některé významné dokumenty jsou uchovány v trezoru úřadu. Zaměstnanci obce mají rovněž možnost dokumenty ukládat do uzamykatelných skříní.

Správce v minulosti nezaznamenal žádné porušení bezpečnosti, které by vedlo ke ztrátě či zneužití spravovaných údajů. Všichni zaměstnanci obce jsou řádně proškoleni.

Správce má s výše uvedeným zabezpečením dlouhodobě dobré zkušenosti. Riziko bylo vyhodnoceno jako minimální/žádné.

31.3. Personální opatření obce

Personální opatření obce, v postavení správce, spočívá v proškolení všech stávajících zaměstnanců a osob, které přichází do kontaktu s osobními údaji. Všichni zaměstnanci správce jsou řádně proškoleni na prezenčních školeních. V případě neznalosti některé problematiky se mohou obrátit na pověřence pro ochranu osobních údajů. Zároveň správce do budoucna plánuje další školení, která budou utvrzovat vzdělání všech dotčených osob v daném směru.



Správce považuje přijatá opatření za naprosto dostatečná. Riziko úniku osobních údajů subjektů údajů v důsledku neznalosti dotčených osob bylo vyhodnoceno jako minimální/žádné.

32. Řešení zabezpečení jednotlivých agend

32.1. Mzdová a personální agenda

Stávající stav: (Doplnit)

Návrh opatření: (Doplnit)

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

32.2. Smlouvy

Stávající stav: Smlouvy jsou evidovány na základě občanského zákoníku, na základě zákona o účetnictví a na základě zákona o obcích. Všechny smlouvy jsou uloženy v písemné formě v příslušném šanonu, který je označen „Smlouvy 2018“ a v digitální podobě na serveru O:/Dokumenty/Smlouvy. Přístup k dokumentům mají starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková. Smlouvy jsou zveřejňovány na profilu zadavatele veřejných zakázek. Osoby oprávněné k zpracování jsou: V. Brujová, P. Zámková, D. Tomková. Na profilu zadavatele nejsou zveřejňovány údaje nad rámec údajů zveřejňovaných v obchodním/živnostenském rejstříku.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

32.3. Daňové doklady, faktury

Stávající stav: Daňové doklady a faktury jsou evidovány na základě zákona o účetnictví. Všechny jsou uloženy v písemné formě v příslušném šanonu, který je označen „Účetní doklady“ a v digitální podobě v počítači účetní J. Arnoldové. Přístup k dokumentům mají starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková. Přístup k počítači účetní J. Arnoldová. Osoba oprávněná ke zpracování je J. Arnoldová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne



32.4. **Žádosti**

Stávající stav: Žádosti jsou evidovány na základě zákonů, vztahujících se k jednotlivým druhům žádostí. Žádosti jsou uloženy v písemné formě v příslušných šanonech, které jsou označeny „Agenda starosty“, „Vyjádření obce“, „Evidence obyvatel“ a v digitální podobě v počítači O:/Dokumenty/Korespondence a ve spisové službě Ahena. Přístup k dokumentům má starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková. Osoby oprávněné k zpracování jsou: starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

32.5. **Správní rozhodnutí/rozhodování**

Stávající stav: Správní rozhodnutí jsou evidována na základě správního řádu a zákonů vztahujících se k jednotlivým druhům žádostí. Rozhodnutí jsou uložena v písemné formě v příslušných šanonech, které jsou označeny „Zrušení pobytu“, „Přestupky“, „Sjezdy“, „Zvláštní užívání“, „Kácení 2018“ a v digitální podobě v počítači O:/Dokumenty/Korespondence, v počítači referentky D. Tomkové, ve spisové službě Athena. Přístup k dokumentům má starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková. Osoby oprávněné k zpracování jsou: starostka V. Brujová, místostarostka P. Zámková, referentka D. Tomková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

32.6. **Dotace**

Stávající stav: Žádosti o dotaci jsou evidovány na základě zákona o obcích a zákona o rozpočtových pravidlech územních samosprávných celků. Žádosti jsou uloženy v písemné formě v příslušných šanonech a v digitální podobě v počítači účetní J. Arnoldové a na O:/Dokumenty/Smlouvy. Přístup k dokumentům má starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková. Osoby oprávněné k zpracování jsou: starostka V. Brujová, místostarostka P. Zámková, referentka D. Tomková, účetní J. Arnoldová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené



v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

32.7. Územní plán obce

Stávající stav: Územní plán obce je veden na základě stavebního zákona. Všechny dokumenty související s jeho tvorbou a změnami jsou uloženy v písemné formě v příslušném šanonu, který je označen „Územní plán“ a v digitální podobě O:/Dokumenty/územní plán. Přístup k dokumentům má starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková. Osoby oprávněné k zpracování jsou: starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

32.8. Evidence psů

Stávající stav: Evidence psů je evidována na základě zákona o místních poplatcích. Evidence je uložena v písemné formě ve složce „Poplatky ze psů“ a v digitální podobě v počítači účetní J. Arnoldové. Přístup k dokumentům má starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková. Osoby oprávněné k zpracování jsou: starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

32.9. Klíče

Stávající stav: Seznam klíčů a osob je evidován na základě organizačně technického opatření a je uložen na obecním úřadě. K dokumentu má přístup starostka V. Brujová, místostarostka P. Zámková, účetní J. Arnoldová, referentka D. Tomková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR. Agenda není vedena v elektronické podobě.



Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

33. Pověřenec pro ochranu osobních údajů

- 33.1. 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, řízení procesů, 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 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.
- 33.2. **Obec má řádně jmenovaného pověřence pro ochranu osobních údajů, který není ve střetu zájmů.**
- 33.3. **Obec v postavení správce jmenováním řádného pověřence splňuje požadavky nařízení GDPR a vhodně snižuje rizika, která by mohla nastat v souvislosti s ochranou osobních údajů.**
- 33.4. Pověřenec pro obec zajišťuje tyto činnosti:
- 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 proškoleny v oblasti ochrany osobních údajů.
 - 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.

34. Závěrečná ustanovení – zhodnocení souladu s nařízením GDPR

- 34.1. Zpracovatel tohoto dokumentu hodnotí všechny postupy správce osobních údajů jako postupy prováděné v souladu s nařízením GDPR. Dle výše uvedených informací správce postupuje při zpracování osobních údajů řádně, transparentně a s dostatečným ohledem na zabezpečení osobních údajů.



- 34.2. Správce osobních údajů přijal vhodná technická a organizační opatření. Detailní popis těchto opatření je uveden na každé jednotlivé kartě příslušné agendy. Vzhledem ke skutečnosti, že správce neprovádí rizikové zpracování, jsou všechna přijatá opatření hodnocena jako přiměřená.
- 34.3. Správce osobních údajů řádně jmenoval pověřence pro ochranu osobních údajů. Správce tak splnil povinnost, která byla stanovena nařízením GDPR. Jmenovaný správce není ve střetu zájmů a může tak činnost vykonávat.
- 34.4. Správce osobních údajů řádně zpracoval záznamy o činnostech zpracování. Správce tak splnil svou povinnost, která byla stanovena nařízením GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě. Tento postup zajišťuje vysokou míru transparentnosti při nakládání s osobními údaji.
- 34.5. Správce osobních údajů řádně zpracoval karty agend. Správce tak splnil svou povinnost stanovenou nařízením GDPR. Zpracování těchto karet je klíčovou činností každého správce a slouží zejména k prokázání souladu zpracování s nařízením GDPR.
- 34.6. Správce osobních údajů dlouhodobě klade důraz na bezpečné uchovávání a nakládání s osobními údaji. Tuto skutečnost potvrzuje fakt, že správce nebyl v minulosti vystaven sankci za porušení zákona o ochraně osobních údajů či jiných právních předpisů.
- 34.7. Správci lze dlouhodobě doporučit pokračování ve stávající úrovni zabezpečení a prohlubování znalostí nařízení GDPR a dalších právních předpisů.
- 34.8. Správci lze dlouhodobě doporučit průběžně aktualizovat karty agend v případě změn.
- 34.9. Správci lze dlouhodobě doporučit aktualizaci tohoto dokumentu.
- 34.10. Porušení nařízení GDPR při činnosti správce: **nebylo zjištěno**.
- 34.11. Závažné hrozby/rizika v souvislosti se zpracováním: **nezjištěno**.

35. Konečné hodnocení

- 35.1. **Správce vykonává svou činnost v souladu s nařízením GDPR.**

36. Seznam vedených agend

Zpracovatel analýzy přikládá přehled správcem vedených agend s vyhodnocením rizik.

Dokument/seznam/doklad	Účel zpracování	Údaje	Příjemce	Zákon	Komentář	Riziko vý
Mzdová a personální agenda	(Doplnit)	(Doplnit)	(Doplnit)	(Doplnit)		NE
Smlouvy	Plnění smluv, vymáhání nároků ze	Jméno, příjmení, rodné číslo,	Druhá smluvní strana v postavení	Zákon č. 128/2000 o obcích (obecní zřízení); zákon		NE



	smluv, archivnictví	datum narození, IČ, DIČ, adresa,	dodavatele/ odběratele/ zhotovitele apod.	č. 89/2012 občanský zákoník, zákon o archivnictví a spisové službě		
Faktury	zpracování Ekonomické agendy	Jméno, příjmení, IČ, DIČ, adresa,	Dodavatel, odběratel	zákon o účetnictví		NE
Žádosti	správní rozhodován í úřadu, rozhodován í obce, zpracování žádostí od občanů obce a třetích osob	Jméno, příjmení, datum, narození, adresa,	Žadatel v postavení fyzické osoby, či právnícké osoby (dožadující orgány), státní archiv, stavební úřad apod.	zákon o ochraně přírody a krajiny, stavební zákon, zákon o vodovodech a kanalizacích apod.		NE
Správní rozhodnutí	Výkon státní správy, evidence a vydávání správních rozhodnutí	Jméno, příjmení, datum narození, adresa,	Žadatel o rozhodnutí	správní řád, zákon o ochraně přírody a krajiny, stavební zákon, zákon o vodovodech a kanalizacích, zákon o obcích		NE
Dotace	Evidence a vyřizování žádostí o dotaci	Jméno, příjmení, datum narození, adresa,	Žadatel o dotaci	Zákon o obcích, zákon o rozpočtových pravidlech územních rozpočtů		NE
Územní plán	Sestavení a změny plánu – k dispozici	Jméno, příjmení, adresa	Občan obce, příslušný stavební	Stavební zákon, zákon o obcích		NE

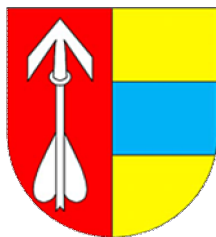


	občanům		úřad			
Evidence psů	Kontakt při ztrátě psa, vymáhání pohledávek za poplatky psů	Jméno, příjmení, adresa, telefon	Referent úřadu	Zákon o místních poplatcích		NE
Klíče	Zabezpečení prostoru obecního úřadu	Jméno, příjmení, telefon	Starosta, referent úřadu	Organizačně technické opatření	Agenda je zpracovávána na základě organizačně technického opatření, agenda neobsahuje údaje o subjektech údajů, který k tomuto vyjádřili souhlas.	NE



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

12.4 Analýza rizik obce Lomnice



Obec Lomnice, Kraslická 44, 356 01 Lomnice

Analýza rizik

zpracovaná v souladu s Nařízením 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 (dále jen „GDPR“), zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“) a dle zákona o zpracování osobních údajů č. 110/2019 Sb.,

Správce:

Obec Lomnice

Kraslická 44

356 01 Lomnice

IČ: 00259497



Úvodní ustanovení

36.1. 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.

36.2. Vymezení a definice správce v postavení obce

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 vyplývajících, 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.

36.3. Definice pojmu 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.

36.4. Definice pojmu 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.

36.5. Definice pojmu 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.

36.6. 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.

36.7. Definice pojmu rizikové zpracování

Posouzení vlivu na ochranu osobních údajů musí provést správce, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, bude představovat vysoké riziko pro práva a svobody fyzických osob. Posouzení se musí provést před započítím předmětného zpracování. Pokud byl ustanoven pověřenec pro ochranu osobních údajů, vyžádá si správce jeho posudek. Posouzení vlivu na ochranu osobních údajů se vyžaduje především:



- u systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky
 - u rozsáhlého zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech
 - u rozsáhlého systematického monitorování veřejně přístupných prostorů
- Správci osobních údajů budou povinni sami vést záznamy o činnostech zpracování (čl. 30), v případě vysoce rizikových zpracování provést posouzení vlivu na ochranu osobních údajů (čl. 35), a teprve v případě, že vysoká rizika nelze eliminovat, obrátit se na Úřad s žádostí o konzultaci (čl. 36).

37. Obecné informace

37.1. Metoda zpracování analýzy

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, a to s ohledem na posuzování hodnoty aktiv, hrozeb a stanovení dalších parametrů analýzy rizik z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

Zpracovatel ve spolupráci se správcem osobních údajů zvolil metodu zhodnocení každé zpracovávané agendy, která osahuje osobní údaje. V rámci tohoto zhodnocení došlo k ohodnocení primárních aktiv dle jejich kritičnosti, a to v souladu s nařízením GDPR. Vzhledem ke skutečnosti, že GDPR nepředepisuje povinný formát analýzy rizik a taktéž nikterak neuvažuje hodnotu rizika, hodnotil správce riziko z pohledu ohrožení práv subjektů údajů.

Samotná definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u každé agendy je popsána v příslušném agendovém listu (dokument, který byl vypracován ke každé agendě zvlášť). Tyto údaje budou rovněž uvedeny v tomto dokumentu, v oddílu s názvem: „Řešení zabezpečení jednotlivých agend“.

Zpracovatel analýzy rizik předkládá agendový list jako přílohu této analýzy (**příloha č. 1**)

37.2. Metoda určení a hodnocení aktiv

Zhotovitel určí primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení. Aktivum je chápáno jako objekt (dokument, informační systém, kartotéka, spisovna, portál, evidence či jiné listinné nebo



elektronické úložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR. Každá agenda pak obsahuje více těchto aktiv.

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.

37.3. Účel zpracování dokumentu

Tento dokument s názvem „Analýza rizik“ je zpracován v souladu s Nařízením 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 (dále jen „GDPR“), zejména dle článku 24 a článku 25.

Dokument představuje ucelený souhrn informací týkající se implementace GDPR do vnitřních i vnějších procesů obce. Osoby, které vystupují v obci v postavení správce, jsou s tímto dokumentem plně seznámeny.

Dokument popisuje vyhodnocení rizik, která vznikají správci v souvislosti se zpracováním údajů o subjektech údajů. Na základě vyhodnocených rizik přijal správce vhodná opatření, které jsou v tomto dokumentu rovněž popsána.

Opatření přijatá správcem

Správce osobních údajů přijal všechna opatření vhodná ke snížení/vyloučení rizik, která vyhodnotil jako přiměřená a v souladu s GDPR. Přijatá opatření budou podrobně popsána v tomto dokumentu.

38. Charakteristika posuzovaného subjektu – správce osobních údajů

38.1. Identifikační údaje správce

Název: Obec Lomnice

Sídlo: Kraslická 44, 356 01 Lomnice

IČ: 00259497

Telefon: +420 352 621 359

+420 352 627 942

e-mail: obec@obeclomnice.cz

Webové stránky: <http://www.obeclomnice.cz>

Počet členů zastupitelstva: 13 členů

Počet obyvatel: 1202⁸

38.2. Struktura obecního úřadu

Obecní úřad tvoří starosta, místostarosta a zaměstnanci obce zařazený do obecního úřadu.

⁸ Tento údaj je pouze orientační.



Úřední hodiny obecního úřadu jsou:

Pondělí: 7:30 – 11:30 | 12:00 – 17:30

Úterý: 7:30 – 11:30 | 12:00 – 14:30

Středa: 7:30 – 11:30 | 12:00 – 17:30

Čtvrtek: 7:30 – 11:30 | 12:00 – 14:30

Pátek: 7:30 – 11:30 | 12:00 – 14:00

38.3. Zveřejňování informací

Obec zveřejňuje informace na webových stránkách obce, a to včetně informací povinně zveřejňovaných dle jiného právního předpisu. Obec dále zveřejňuje informace na úřední desce obce, a to jak na úřední desce elektronické, tak fyzické. Při zveřejňování informací obec dlouhodobě dodržuje ustanovení zákona o ochraně osobních údajů (zákon č. 101/2000 Sb.). Obec při zveřejňování všech informací dbá na dodržení nařízení GDPR. Informace, o kterých není známo, zda podléhají ochraně dle GDPR, jsou konzultovány před zveřejněním s pověřencem pro ochranu osobních údajů. Správce osobních údajů rovněž poskytuje informace písemně a ústně, vše při dodržování nařízení GDPR.

39. Obecná struktura uchovávání osobních údajů v obci

39.1. Evidence údajů nahlášená Úřadu pro ochranu osobních údajů

V současné době nevede správce žádnou evidenci, která by podléhala nahlášení Úřadu pro ochranu osobních údajů.

39.2. Technické a organizační opatření

Správce osobních údajů přijal organizační a technická opatření v souladu s GDPR. Správce osobních údajů soustavně pracuje na modernizaci organizačních i technických opatření tak, aby bylo zajištěno maximální zabezpečení všech zpracovávaných údajů.

39.3. Předpisy obce

Technicko-organizační opatření ve formě předpisu k ochraně osobních údajů: ne
Obec v postavení správce osobních údajů se řídí těmito vnitřními předpisy:

- organizační řád
- spisový a skartační řád schválený věcně a místně příslušným archivem
- vnitřní organizační směrnice pro používání IT
- směrnice...
- vnitřní předpis...

39.4. Elektronické zdroje/evidence

39.5. Za zajištění jednotlivých informačních systémů odpovídá správce informačního systému.

39.6. Poskytovatelem internetového připojení je společnost: (doplnit název). Internetové připojení není poskytováno veřejně.



- 39.7. Elektronické zdroje popisují programové vybavení (software) využívané správcem při zpracování a evidenci údajů dle GDPR.
- 39.8. Veškeré programové vybavení (software) bylo pořízeno legálně a je pravidelně aktualizováno. Správce dbá na to, aby poskytovatel software zpracovával osobní údaje v souladu s GDPR.
- 39.9. Správce používá při své činnosti tyto elektronické zdroje/evidence:
- **Účetní program** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
 - **Program evidence obyvatel** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
 - **Program pokladny** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
 - **Program evidence majetku** (doplnit název) – zpracovatel, (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
 - **Kancelářské programy Office** – jedná se o běžné kancelářské programy „Office“ od společnosti Microsoft.
- 39.10. Zaměstnanci obce mohou zpracovávat elektronické evidence s povahou zpracování pro osobní potřebu (např. adresáře). Tyto evidence nespádají pod působnost GDPR.
- 39.11. **Listinné zdroje/evidence**
- Veškeré listinné zdroje/evidence jsou řádně uloženy v příslušných označených šanonech. Každá listinná evidence je vedena v rámci příslušné agendy. Ke každé agendě byl vypracován řádný agendový list. Pro přehled agend byl vypracován dokument s povahou soupisu agend, který obsahuje přehledné informace o vedených agendách (listinných i elektronických).
- Veškeré listinné zdroje/evidence jsou uloženy v zamčených skříních/uzavřených skříních/policích vždy tak, aby k nim neměla přístup žádná třetí osoba. V případě, že je dokument uložen v kanceláři volně, dbá příslušný zaměstnanec na to, aby k němu neměla přístup žádná třetí osoba. Každá kancelář je mimo pracovní dobu uzamčena. Budova úřadu je mimo pracovní dobu vždy uzamčena a zabezpečena.

40. Popis implementace GDPR

- 40.1. Správce v souladu s GDPR vytvořil ke všem vedeným agendám podrobný agendový list. Tento agendový list obsahuje vždy následující údaje:
- **Název a popis agendy**
 - **Účel zpracování**



- **Forma zpracování (listinná/elektronická)**
- **Forma zpracování (strukturovaná/nestrukturovaná)**
- **Podobný popis způsobu zpracování**
- **Kategorie subjektu údajů**
- **Kategorie příjemců**
- **Informaci o tom, zda jsou údaje předávány do třetích zemí**
- **Označení správce a zpracovatele**
- **Označení pověřence pro ochranu osobních údajů**
- **Označení dokladu (nosiče údajů)**
- **Určení doby zpracování**
- **Informaci o tom, zda je zpracování rizikové**
- **Informaci o tom, zda je informace zpracovávána na základě zákona**
- **Popis technických a organizačních opatření**
- **Komentář**

40.2. Vypracovaný dokument slouží správci rovněž pro posouzení, zda je zpracování v souladu s GDPR. V případě, že byl správcem vyhodnocen nesoulad, bylo přijato opatření k nápravě. Na základě vypracovaných agendových listů byl vytvořen seznam agend. Seznam agend poskytuje ucelený přehled o všech agendách, které správce zpracovává.

40.3. Při zpracování agendových listů nebyl správcem vyhodnocen nesoulad s nařízením GDPR.

40.4. Při zpracování agendových listů nevyhodnotil správce žádnou agendu jako rizikovou (obsahující citlivé osobní údaje o náboženském vyznání, sexuální orientaci, politickém přesvědčení apod.)

40.5. Postup správce osobních údajů při zpracování agendových listů byl vyhodnocen jako zcela legitimní, v souladu s požadavky GDPR.

40.6. **Záznamy o zpracování osobních údajů**

Správce vede záznamy o zpracování osobních údajů. Tyto záznamy popisují důležité skutečnosti, které se ke zpracování osobních údajů vztahují. Tuto činnost vykonává správce na základě čl. 30 nařízení GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě zvlášť a obsahují všechny informace obsažené v čl. 30 nařízení GDPR (např. údaje o správci, účel zpracování, popis kategorií subjektů údajů apod.). Všechny tyto záznamy budou pravidelně aktualizovány.

40.7. **Návrh na doplnění vnitřních předpisů**

Správci osobních údajů lze doporučit přijetí směrnice, která by upravovala zpracování osobních údajů dle nařízení GDPR (směrnice na ochranu osobních údajů). Vzhledem ke skutečnosti, že přijetí směrnice není povinností obce, nelze přijetí takovéto směrnice autoritativně nařídit.

Další doporučení nejsou navrhována. Správce zpracovává osobní údaje zcela v souladu s nařízením GDPR.



41. Riziková zpracování

- 41.1. Obec zpracovává většinu osobních údajů na základě čl. 6 odst. 1 písm. c), tedy za plnění zákonné povinnosti obce, případně písm. e), kdy dochází ke zpracování veřejného zájmu nebo písm. b) na základě plnění smlouvy. V minimální míře pak obec zpracovává osobní údaje na základě souhlasu a oprávněného zájmu správce.
- 41.2. Na základě pečlivého studia dokumentů v rámci ochrany osobních údajů **nebyly zjištěny agendy, které vykazují vyšší míru rizika incidentních hrozeb.**
- 41.3. Obec v minulosti nezaznamenala ztrátu nebo odcizení osobních údajů.
- 41.4. Obec v minulosti nebyla sankcionována Úřadem pro ochranu osobních údajů, pro porušení povinností souvisejících s ochranou osobních údajů.
- 41.5. **Žádné ze zpracovávaných osobních údajů nespádají do zvláštní kategorie osobních údajů ve smyslu čl. 9 nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (dále jen GDPR). Výjimku představují nanejvýš osobní údaje zaměstnanců vyžadované právními předpisy za účelem plnění zákonných povinností zaměstnavatele (např. údaje o zdravotním stavu zaměstnanců).**

42. Obecný popis technických a organizačních opatření

42.1. Technická opatření obce

Technická opatření obce jsou navržena tak, aby splňovala veškeré nároky nařízení GDPR. V první řadě jsou všechny počítače v budově úřadu zabezpečeny proti neoprávněnému přístupu heslem. Použité heslo je kombinací znaků a čísel a je pravidelně aktualizováno. Použité heslo k samotnému přístupu do PC (po zapnutí) zná vždy jen konkrétní zaměstnanec, který s PC pracuje. Zároveň obec dbá na to, aby k žádnému počítači neměla přístup třetí osoba. Z obecného hlediska lze říci, že veškerý používaný software je pravidelně aktualizován. Veškerý software byl také legálně zakoupen a je užíván dle příslušných uživatelských příruček a dokumentů obdobných. Správce dbá na to, aby případný zpracovatel (který je zároveň poskytovatelem software) dbal na ochranu osobních údajů v souladu s nařízením GDPR.

Správce dlouhodobě využívá příslušný antivirový program. Každý počítač je také chráněn branou firewall. Každý zaměstnanec při práci využívá pouze ověřené a důvěryhodné zdroje.

Správce má s tímto zabezpečením dlouhodobě dobré zkušenosti. V minulosti nikdy nedošlo k úniku dat z důvodu nedostatečného technického zabezpečení na straně správce (či zpracovatele). Riziko bylo vyhodnoceno jako minimální/žádné.

42.1.1. Dodavatelé IT software a programů

Pro elektronické zdroje je zajištěna dokumentace všech IT programů, které obecní úřad používá a postupnými kroky se zároveň bude chystat systémová příručka. V systémové příručce obce budou následující body:



1. Popis implementovaného systému nebo programu (nutné podmínky pro instalaci a následný provoz)
2. Licenční podmínky
3. Popis podpory uživatele (hot-line, helpdesk)
4. Bezpečnostní podmínky (jak je systém zabezpečen – přístupy, šifrování, zálohování a bezpečnostní kopie).
5. Popisy systémem vytvářených logů – systémových a transakčních
6. Zprávy a výsledky testů a certifikací, které informační systém nebo program získal
7. Případně cloudové služby

V současné době obec nevyužívá cloudové služby a nemá to ani v plánu. Pokud ale po změně vedení, případně jiného vedení, obec tyto služby začne používat, obec si vyžádá informace o tom, kde se úložiště nachází a že úložiště je zabezpečeno podle GDPR.

42.1.2. Smluvní vztahy s dodavateli software

Správce se v rámci svých elektronických zdrojů a informačních systémů písemně dotázal dodavatelů IS programů, zda jeho systém je na GDPR připraven. Smluvní strany jsou připraveny spolupracovat s pověřencem pro ochranu osobních údajů, včetně kooperace s případnými kontrolami. Správce uzavřel / uzavře s poskytovateli IS dodatek ke smlouvě, který bude zaručovat odpovědnost zpracovatele za nakládání s os. údaji.

Správce po dodavateli IT softwaru požaduje závazek:

- spolupracovat s pověřencem pro ochranu os. údajů
- subjekt údajů bude mít dobrou dostupnost k informacím o zpracování svých údajů
- možnost realizovat právo subjektu na opravu nebo výmaz údajů s tím, že se uvede, v jaké formě (nejlépe v písemné formě),
- možnost realizovat právo na omezení zpracování,
- možnost subjektu poskytnout kopii zpracovávaných osobních údajů,
- možnost výkonu práva na přenositelnost údajů,
- zajištění podpory logování v čitelné formě s vazbou na uživatele a jeho činnosti,
- zajištění ochrany dat po ukončení smlouvy.

Dále správce zreviduje/zrevidoval smlouvy, které obsahují osobní údaje následujícím způsobem:

- Zajištění mlčenlivosti osob, které přijdou do styku s osobními údaji (u externích dodavatelů, případně tam, kde není zákonná povinnost)
- Zajištění a nastavení podmínek pro zapojení dalšího zpracovatele dle nařízení GDPR
- Zajistit práva subjektu údajů (informace o vedených údajích apod., dle GDPR)
- Zajistit podporu pověřence pro ochranu osobních údajů
- Zajistit ujednání o náhradě škody, včetně regresních nároků (s pozorností na smluvní pokuty, aby nevykloučovaly náhradu škody).



- Zajistit po ukončení smlouvy odstranění kopií, zničení kopií, případně předání osobních údajů.

42.1.3. Obecný návrh opatření

Považuje se za vhodné zajistit pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Tento proces by měl být náležitě popsán (případně zaznamenán do systémové příručky/analýzy rizik), tak aby kontrola a realizace procesu byla součástí provozního testování, posuzování a hodnocení účinnosti zavedených opatření.

Správce bude nadále pokračovat v zajišťování souladu s GDPR. Správce bude postupně implementovat do všech dokumentací, vnitřních předpisů a nařízení ustanovení, která budou sloužit k:

- pseudoanonymizaci a šifrování osobních údajů k zajištění, aby tyto postupy byly běžnou součástí každodenního výkonu činností správce,
- zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování,
- schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů.

42.2. Organizační opatření obce

Organizační opatření správce spočívají v zajištění ochrany osobních údajů, které správce uchovává v listinné podobě (případně na fyzických datových nosičích). Toto zajištění spočívá zejména ve znemožnění třetím osobám kvolnému přístupu k dokumentům, které obsahují osobní údaje. Správce provádí toto opatření zejména tak, že uzamyká budovu úřadu mimo úřední hodiny. Stejně jako budova obecního úřadu jsou uzamčeny i všechny kanceláře. V pracovní době jsou všechny výše uvedené nosiče dat pod dozorem příslušného pracovníka úřadu. Některé významné dokumenty jsou uchovány v trezoru úřadu. Zaměstnanci obce mají rovněž možnost dokumenty ukládat do uzamykatelných skříní.

Správce v minulosti nezaznamenal žádné porušení bezpečnosti, které by vedlo ke ztrátě či zneužití spravovaných údajů. Všichni zaměstnanci obce jsou řádně proškoleni.

Správce má s výše uvedeným zabezpečením dlouhodobě dobré zkušenosti. Riziko bylo vyhodnoceno jako minimální/žádné.

42.3. Personální opatření obce

Personální opatření obce, v postavení správce, spočívá v proškolení všech stávajících zaměstnanců a osob, které přichází do kontaktu s osobními údaji. Všichni zaměstnanci správce jsou řádně proškoleni na prezenčních školeních. V případě neznalosti některé problematiky se mohou obrátit na pověřence pro ochranu osobních údajů. Zároveň správce do budoucna plánuje další školení, která budou utvrzovat vzdělání všech dotčených osob v daném směru.



Správce považuje přijatá opatření za naprosto dostatečná. Riziko úniku osobních údajů subjektů údajů v důsledku neznalosti dotčených osob bylo vyhodnoceno jako minimální/žádné.

43. Řešení zabezpečení jednotlivých agend

43.1. Dary

Stávající stav: Darovací smlouvy a sponzorské dary jsou evidovány na základě zákona o obcích a občanského zákoníku. Žádosti jsou uloženy v písemné formě v příslušných šanonech, které jsou označeny Darovací smlouvy a Sponzorské dary v digitální podobě v počítači Jitky Půtové. Přístup k dokumentům má starosta Miloslav Matoušek a Jitka Půtová.

Osoby oprávněné k zpracování jsou: Miloslav Matoušek, Jitka Půtová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.2. Datové schránky

Stávající stav: Zpracování žádosti podle zákona 300/2008 Sb., - Zákon o elektronických úkonech a autorizované konverzi dokumentů, Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování Informačního systému datových schránek, 111/2009 Sb., - zákon o základních registrech. Přístup zabezpečený kvalifikovaným certifikátem a heslem má Miloslav Matoušek, Eva Hilková, Jana Glosová a Jitka Půtová. Osoby oprávněné k zpracování jsou: Miloslav Matoušek, Eva Hilková, Jana Glosová a Jitka Půtová. Po zpracování žádosti jsou písemné výstupy uloženy v šanonech pod příslušným názvem agendy.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.3. Evidence obyvatel

Stávající stav: Zpracování žádosti podle zákona

- 111/2009 Sb., - Zákon o základních registrech,
- 133/2000 Sb., - Zákon o evidenci obyvatel,
- 296/2004 Sb., - Vyhláška, kterou se provádí zákon o evidenci obyvatel,
- 500/2004 Sb., - Správní řád,



- 634/2004 Sb., - Zákon o správních poplatcích,
- 561/2004 Sb., - Školský zákon.

Přihlašovací karty jsou zpracovány, data jsou uložena do ISDS prostřednictvím základních registrů. Dále jsou abecedně uloženy do trezorových šuplíků - kartotéky. Trezorové šuplíky jsou uzamykatelné, klíč má pouze Eva Hilková, matrikářka. Výsledky žádostí o zpracování dat prostřednictvím ISDS zpracovává Eva Hilková, matrikářka, data uloží do evidence obyvatel v programu Fenix, v písemné podobě založí do šanonu označeného "Výsledek žádosti o zpracování dat" do uzamykatelné skříně v kanceláři.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.4. **Emailová a telefonická komunikace s občany**

Stávající stav: Zpracování podle zákona 8128/2000 Sb., - Zákon o obcích.

Standartní postup vyřizování telefonických hovorů s možností zápisů údajů o volané osobě, vč. tel. kontaktu. Provádí všichni zaměstnanci OÚ.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.5. **Hřbitovní agendy**

Stávající stav: Zpracování podle zákona

- 256/2001 Sb., - Zákon o pohřebnictví,
- 128/2000 Sb., - Zákon o obcích,

Na základě ústní žádosti o pronájem hrobového místa je vyhotovena smlouva o pronájmu, která je zaevidována a uložena v šanonu "Pronájem hroby". Šanon je uložen v uzamykatelné skříně v kanceláři Evy Hilkové.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne



43.6. **Kniha úrazů**

Stávající stav: Zpracování podle zákona:

- Nařízení vlády č. 201/2010 Sb., o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu,
- 262/2006 Sb., - Zákoník práce.

Do knihy úrazů je zapsán den a hodina vzniku úrazu, údaje zraněné osoby, popis zranění a výsledek dechové zkoušky. Kniha úrazů je uložena v kanceláři Jitky Půtové.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.7. **Knihovna**

Stávající stav: Zpracování podle zákona

- 257/2001 Sb., - Knihovní zákon,
- 128/2000 Sb., - Zákon o obcích

Knihovnice Jiřina Němečková při zápisu nového čtenáře vyplní osobní kartu čtenáře, vč. tel. kontaktu a nechá podepsat. Osobní karty jsou uloženy v uzamykatelném šuplíku v knihovně.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.8. **Majetkoprávní transakce, kupní smlouvy**

Stávající stav: Zpracování podle zákona

- 128/2000 Sb., - Zákon o obcích,
- 89/2012 Sb., - Občanský zákoník,
- 256/2013 Sb., - Katastrální zákon

Sepsání kupní smlouvy na základě žádosti a schválení zastupitelů obce. Po kompletaci všech dokumentů se smlouvou souvisejících, je vše uloženo do šanonu označeného "Notářské zápisy" v kanceláři Jitky Půtové.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené



v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.9. Místní poplatky

Stávající stav: Zpracování podle zákona

- 565/1990 Sb., - Zákon o místních poplatcích,
- 128/2000 Sb., - Zákon o obcích,
- 280/2009 Sb., - Daňový řád,
- 634/2004 Sb., - Zákon o správních poplatcích,

Podklady pro výběr poplatků příp. nedoplatků jsou evidovány v tabulce excel, dále v listinné podobě, uloženy v šanonu "Poplatky" uložené v uzamykatelné skříni a PC v kanceláři Jany Glovové.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.10. Provoz kamerového dohlížecího systému

Stávající stav: Zpracování podle zákona

89/2012 Sb., - Občanský zákoník,
128/2000 Sb., Zákon o obcích.

Pořizování automatického záznamu návsi a budovy obecního úřadu, schodiště.

Nahrávací zařízení je umístěno v kanceláři Jitky Půtové. V době jejich nepřítomnosti je kancelář uzamčena. K záznamům nemá přístup žádná třetí osoba.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.11. Povolení zvláštního užívání komunikací

Stávající stav: Zpracování podle zákona

- 13/1997 Sb., - Zákon o pozemních komunikacích,
- 128/2000 Sb., - Zákon o obcích,
- 634/2004 Sb., - Zákon o správních poplatcích,



- 500/2004 Sb., - Správní řád,
- 89/2012 Sb., - Občanský zákoník.

Na základě žádosti je po posouzení žádosti a všech povinných příloh vyhotoveno Rozhodnutí dle správního řádu. Rozhodnutí je předáno žadateli a zasláno datovou správou na dopravní inspektorát Policie Sokolov.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.12. **Pojistné události**

Stávající stav: Zpracování podle zákona

- 128/2000 Sb., - Zákon o obcích,
- 89/2012 Sb., - Občanský zákoník.

Pojistné smlouvy a dokumenty související jsou uloženy v šanonu "Pojistné smlouvy" a uloženy v kanceláři Miroslavy Löwové v uzamykatelné skříni.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.13. **Obchodní vztahy (dodavatelské, odběratelské)**

Stávající stav: Zpracování podle zákona

- 28/2000 Sb., - Zákon o obcích,
- 89/2012 Sb., - Občanský zákoník,
- 250/2000 Sb., - Zákon o rozpočtových pravidlech územních rozpočtů,
- 134/2016 Sb., - Zákon o zadávání veřejných zakázek,
- 340/2015 Sb., - Zákon o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

Veškeré smlouvy jsou uloženy v šanonu Smlouvy s označením příslušného roku vzniku a uloženy v uzamykatelné skříni v kanceláři starosty obce.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne



Zpracování citlivých osobních údajů: ne

43.14. **Nájemní smlouvy**

Stávající stav: Nájemní smlouvy jsou evidovány na základě zákona o obcích a občanského zákoníku a zákonu o účetnictví. Žádosti jsou uloženy v písemné formě v příslušných šanonech, které jsou označeny Nájemní smlouvy v digitální podobě v počítači Evy Hilkové. Přístup k dokumentům má starosta Miloslav Matoušek a Eva Hilková. Osoby oprávněné k zpracování jsou: Miloslav Matoušek, Eva Hilková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

43.15. **Mzdová agenda**

Stávající stav: Zpracování podle zákona

- 262/2006 Sb., - Zákoník práce,
- 435/2004 Sb., - Zákon o zaměstnanosti,
- 251/2005 Sb., - Zákon o inspekci práce,
- 312/2002 Sb., - Zákon o úřednících územních samosprávných celků,
- 341/2017 Sb., - Nařízení vlády o platových poměrech zaměstnanců ve veřejných službách a správě,
- 222/2010 Sb., - Nařízení vlády o katalogu prací ve veřejných službách a správě,
- 586/1992 Sb., - Zákon o daních z příjmů,
- 187/2006 Sb., - Zákon o nemocenském pojištění,
- 120/2001 Sb., - Exekuční řád,
- 182/2006 Sb., - Insolvenční zákon,
- 582/1991 Sb., - Zákon o organizaci a provádění sociálního zabezpečení,
- 589/1992 Sb., - Zákon o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- 155/1995 Sb., - Zákon o důchodovém pojištění,
- 37/2003 Sb., - Nařízení vlády o odměnách za výkon funkce členům zastupitelstev,
- 592/1992 Sb., - Zákon o pojistném na všeobecné zdravotní pojištění,
- 128/2000 Sb., - Zákon o obcích.

Pracovní smlouvy, platové výměry a ostatní dokumenty personální agendy jsou uloženy ve spisech jednotlivých zaměstnanců a uloženy v trezorové skříni v kanceláři Miroslavy Löwové a Jitky Půtové.



Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

44. Pověřenec pro ochranu osobních údajů

44.1. 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, řízení procesů, 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 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.

44.2. **Obec má řádně jmenovaného pověřence pro ochranu osobních údajů, který není ve střetu zájmů.**

44.3. **Obec v postavení správce jmenováním řádného pověřence splňuje požadavky nařízení GDPR a vhodně snižuje rizika, která by mohla nastat v souvislosti s ochranou osobních údajů.**

44.4. Pověřenec pro obec zajišťuje tyto činnosti:

- 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 proškoleny v oblasti ochrany osobních údajů.
- 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.



45. Závěrečná ustanovení – zhodnocení souladu s nařízením GDPR

- 45.1. Zpracovatel tohoto dokumentu hodnotí všechny postupy správce osobních údajů jako postupy prováděné v souladu s nařízením GDPR. Dle výše uvedených informací správce postupuje při zpracování osobních údajů řádně, transparentně a s dostatečným ohledem na zabezpečení osobních údajů.
- 45.2. Správce osobních údajů přijal vhodná technická a organizační opatření. Detailní popis těchto opatření je uveden na každé jednotlivé kartě příslušné agendy. Vzhledem ke skutečnosti, že správce neprovádí rizikové zpracování, jsou všechna přijatá opatření hodnocena jako přiměřená.
- 45.3. Správce osobních údajů řádně jmenoval pověřence pro ochranu osobních údajů. Správce tak splnil povinnost, která byla stanovena nařízením GDPR. Jmenovaný správce není ve střetu zájmů a může tak činnost vykonávat.
- 45.4. Správce osobních údajů řádně zpracoval záznamy o činnostech zpracování. Správce tak splnil svou povinnost, která byla stanovena nařízením GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě. Tento postup zajišťuje vysokou míru transparentnosti při nakládání s osobními údaji.
- 45.5. Správce osobních údajů řádně zpracoval karty agend. Správce tak splnil svou povinnost stanovenou nařízením GDPR. Zpracování těchto karet je klíčovou činností každého správce a slouží zejména k prokázání souladu zpracování s nařízením GDPR.
- 45.6. Správce osobních údajů dlouhodobě klade důraz na bezpečné uchovávání a nakládání s osobními údaji. Tuto skutečnost potvrzuje fakt, že správce nebyl v minulosti vystaven sankci za porušení zákona o ochraně osobních údajů či jiných právních předpisů.
- 45.7. Správci lze dlouhodobě doporučit pokračování ve stávající úrovni zabezpečení a prohlubování znalostí nařízení GDPR a dalších právních předpisů.
- 45.8. Správci lze dlouhodobě doporučit průběžně aktualizovat karty agend v případě změn.
- 45.9. Správci lze dlouhodobě doporučit aktualizaci tohoto dokumentu.
- 45.10. Porušení nařízení GDPR při činnosti správce: **nebylo zjištěno.**
- 45.11. Závažné hrozby/rizika v souvislosti se zpracováním: **nezjištěno.**

46. Konečné hodnocení

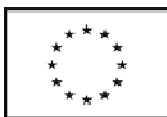
- 46.1. **Správce vykonává svou činnost v souladu s nařízením GDPR.**

47. Seznam vedených agend

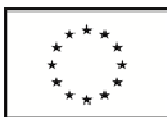
Zpracovatel analýzy přikládá přehled správcem vedených agend s vyhodnocením rizik.



Dokument/seznam/doklad	Účel zpracování	Údaje	Příjemce	Zákon	Komentář	Rizikový
Dary	Evidence poskytnutých darů	Jméno, příjmení, datum narození, adresa	Žadatel v postavení obdarovaného (subjekt údajů), dále zpracovatel, dárce (fyzická nebo právnická osoba)	Občanský zákoník, zákon o obcích		NE
Datové schránky (zřízení, zrušení, změna)	Zpracování žádosti o zřízení a zrušení dat. Schránky popř. o změnu	Jméno, příjmení, datum narození, trvalé bydliště, rodné příjmení, e-mail, telefon, podpis	Správce	300/2008 Sb., - Zákon o elektronických úkonech a autorizované konverzi dokumentů, Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, 111/2009 Sb., - zákon o základních registrech		NE
Emailová a telefonická	Evidence komunikace	Jméno, příjmení, titul, datum	Dotčené fyzické	128/2000 Sb., - Zákon o		NE



komunikace s občany	s občany obce (fyzické osoby) a PO	narození, trvalé bydliště, doručovací adresa, telefon, e-mail, datová schránka, předmět sdělení, podpis	osoby, správce	obcích		
Evidence obyvatel	Vedení evidence obyvatel na základě zákona	Jméno, příjmení, datum, narození, místo narození, rodné číslo, trvalé bydliště, doručovací adresa, předchozí pobyt, číslo OP, omezení způsobilosti, údaje o opatrovníkovi, oprávněná osoba, podpis	Dotčené fyzické osoby, správce	111/2009 Sb., - Zákon o základních registrech, 133/2000 Sb., - Zákon o evidenci obyvatel, 296/2004 Sb., - Vyhláška, kterou se provádí zákon o evidenci obyvatel, 500/2004 Sb., - Správní řád, 634/2004 Sb., - Zákon o správních poplatcích, 561/2004 Sb., - Školský zákon		NE
Hřbitovní agendy	Pronájem hrobových míst, evidence hrobových míst, poplatníků za hrobová místa	Jméno, příjmení, rodné číslo, trvalé bydliště, číslo hrobu, podpis	správce	256/2001 Sb., - Zákon o pohřebnictví 128/2000 Sb., - Zákon o obcích		NE
Kniha úrazů	Evidence pracovních úrazů	Jméno, příjmení, datum narození, datum a čas	správce	Nařízení vlády č. 201/2010 Sb., o způsobu		NE



		úrazu, druh zranění a popis zraněné části těla, místo úrazu, popis úrazového děje, zdroj a příčiny úrazu, podpis vedoucího zaměstnance a podpis zraněné osoby		evidence úrazů, hlášení a zasílání záznamu o úrazu, 262/2006 Sb., - Zákoník práce		
Knihovna	Evidence výpůjček, evidence čtenářů, knihovních poplatků a vymáhání pohledávek	Jméno, příjmení, datum narození, trvalé bydliště, e-mail, telefon, podpis	Dotčené fyzické osoby, správce	1257/2001 Sb., - Knihovní zákon, 128/2000 Sb., - Zákon o obcích		NE
Majetkoprávní transakce, kupní smlouvy	Evidence kupních smluv, plnění ze smluvních vztahů, vymáhání pohledávek	Jméno, příjmení, titul, datum narození, rodné číslo, trvalé bydliště, e-mail, telefon, datová schránka, číslo OP, bankovní spojení, bydliště, OP	smluvní strana (dotčená fyzická a právnická osoba)	128/2000 Sb., - Zákon o obcích, 89/2012 Sb., - Občanský zákoník, 256/2013 Sb., - Katastrální zákon		NE
Místní poplatky	Výběr místních poplatků, evidence plátců, vymáhání pohledávek	Jméno, příjmení, titul, datum narození, rodné číslo, trvalé bydliště, e-mail, telefon, datová schránka, místo pobytu, průkaz totožnosti, bankovní spojení, výměry důchodů, kopie průkazu	Plátce, příjemce	565/1990 Sb., - Zákon o místních poplatcích, 128/2000 Sb., - Zákon o obcích, 280/2009 Sb., - Daňový řád, 634/2004 Sb., - Zákon o správních		NE



		ZTP, TP		poplatcích,		
Mzdová agenda	Zpracování mezd, odměňování zaměstnanců	Jméno, příjmení, titul, datum narození, rodné číslo, trvalé bydliště, e-mail, telefon, místo narození, stát narození, státní příslušnost, místo pobytu, zdravotní pojišťovna, bankovní spojení, rodné příjmení, předchozí zaměstnavatel, stav, rodinný příslušník, děti, doklady o vzdělání, doklady o důchodu, osobní spis, platový výměr, výpis z rejstříku trestů, zdravotní prohlídka, invalidita, zdravotní znevýhodnění, žádost o příspěvky, potvrzení o pracovní neschopnosti, prohlášení poplatníka k dani z příjmu ze závislé činnosti, podpis, údaje o zdravotním stavu	zaměstnanec	262/2006 Sb., - Zákoník práce, 435/2004 Sb., - Zákon o zaměstnanosti , 251/2005 Sb., - Zákon o inspekci práce, 312/2002 Sb., - Zákon o úřednících územních samosprávných celků, 341/2017 Sb., - Nařízení vlády o platových poměrech zaměstnanců ve veřejných službách a správě, 586/1992 Sb., - Zákon o daních z příjmů, 120/2001 Sb., - Exekuční řád, 182/2006 Sb., - Insolvenční zákon, 582/1991 Sb., - Zákon o organizaci a provádění sociálního zabezpečení, 589/1992 Sb., - Zákon o pojistném na		



				sociální zabezpečení a příspěvku na státní politiku zaměstnanosti ,592/1992 Sb., - Zákon o pojistném na všeobecné zdravotní pojištění,		
Nájemní smlouvy	Evidence nájemních smluv, vymáhání pohledávek, plnění smluv	Jméno, příjmení, titul, datum narození, místo narození, rodné číslo, trvalé bydliště, místo pobytu, typ místa pobytu, státní příslušnost, e- mail, telefon, datová schránka, zaměstnavatel, výše příjmu, osoby sdílející společnou domácnost, nesvéprávnost, insolvence, stav, příbuzenský vztah, průkaz totožnosti, žádost o nájem, podpis, údaje o zdravotním stavu	Nájemce (fyzická osoba)	89/2012 Sb., Občanský zákoník, 128/2000 Sb Zákon o obcích, 563/1991 Sb. Zákon o účetnictví		NE
Obchodní vztahy (dodavatelské , odběratelské)	Plnění smluv, vymáhání pohledávek, evidence smluv	Jméno, příjmení, titul, datum narození, trvalé bydliště, kontaktní adresa, emial, telefon, datová schránka,	Dotčená smluvní strana (FO a PO), správce	28/2000 Sb., - Zákon o obcích, 89/2012 Sb., - Občanský zákoník,		NE



		bankovní spojení, IČO/DIČ, podpis, smlouva, objednávka, faktura,		250/2000 Sb., - Zákon o rozpočtových pravidlech územních rozpočtů, 134/2016 Sb., - Zákon o zadávání veřejných zakázek, 340/2015 Sb., - Zákon o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv)		
Pojistné události	Evidence pojistných událostí, plnění z pojistných smluv, evidence pojištění	Jméno, příjmení, titul, datum narození, trvalé bydliště, místo pobytu, e-mail, telefon, datová schránka, bankovní spojení, číslo pojistné smlouvy, průkaz totožnosti - kopie, technický průkaz vozidla, spis pojistné události, podpis	kontrolní orgány, orgány provádějící další zpracování (zdravotní pojišťovny, orgány činné v sociálním zabezpečení	128/2000 Sb., - Zákon o obcích, 89/2012 Sb., - Občanský zákoník		NE



Povolení zvláštního užívání komunikací	Evidence a zpracování agendy vydaných povolení	Jméno, příjmení, titul, datum narození, trvalé bydliště, e-mail, telefon, datová schránka, místo pobytu, podpis, spis řízení	Žadatel, správce	13/1997 Sb., - Zákon o pozemních komunikacích, 128/2000 Sb., - Zákon o obcích, 634/2004 Sb., - Zákon o správních poplatcích, 500/2004 Sb., - Správní řád, 89/2012 Sb., - Občanský zákoník		NE
Provoz kamerového dohlížecího systému	Ochrana majetku občanů obce, ochrana zdraví občanů obce, prevence kriminality	Podobizna	správce	89/2012 Sb., - Občanský zákoník, 128/2000 Sb., Zákon o obcích	Údaje jsou zpracovávány na základě oprávněného zájmu správce. Zároveň na základě práva na ochranu majetku a zdraví občanů obce.	NE



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

12.5 Analýza rizik obce Staré Sedlo



Obec Staré Sedlo, Zámecká 100, 357 46 Staré Sedlo

Analýza rizik

zpracovaná v souladu s Nařízením 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 (dále jen „GDPR“), zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“) a dle zákona o zpracování osobních údajů č. 110/2019 Sb.,

Správce:

Obec Staré Sedlo

Zámecká 100

357 46 Staré Sedlo

IČ: 00259608



48. Úvodní ustanovení

48.1. 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.

48.2. Vymezení a definice správce v postavení obce

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 vyplývajících, 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.

48.3. Definice pojmu 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.

48.4. Definice pojmu 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.

48.5. Definice pojmu 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.

48.6. 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.

48.7. Definice pojmu rizikové zpracování

Posouzení vlivu na ochranu osobních údajů musí provést správce, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, bude představovat vysoké riziko pro práva a svobody fyzických osob. Posouzení se musí provést před započítím předmětného zpracování. Pokud byl ustanoven pověřenec pro ochranu osobních údajů, vyžádá si správce jeho posudek. Posouzení vlivu na ochranu osobních údajů se vyžaduje především:

- u systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování,



včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky

- u rozsáhlého zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech
- u rozsáhlého systematického monitorování veřejně přístupných prostorů

Správci osobních údajů budou povinni sami vést záznamy o činnostech zpracování (čl. 30), v případě vysoce rizikových zpracování provést posouzení vlivu na ochranu osobních údajů (čl. 35), a teprve v případě, že vysoká rizika nelze eliminovat, obrátit se na Úřad s žádostí o konzultaci (čl. 36).

49. Obecné informace

49.1. Metoda zpracování analýzy

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, a to s ohledem na posuzování hodnoty aktiv, hrozeb a stanovení dalších parametrů analýzy rizik z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

Zpracovatel ve spolupráci se správcem osobních údajů zvolil metodu zhodnocení každé zpracovávané agendy, která osahuje osobní údaje. V rámci tohoto zhodnocení došlo k ohodnocení primárních aktiv dle jejich kritičnosti, a to v souladu s nařízením GDPR. Vzhledem ke skutečnosti, že GDPR nepředepisuje povinný formát analýzy rizik a taktéž nikterak neuvažuje hodnotu rizika, hodnotil správce riziko z pohledu ohrožení práv subjektů údajů.

Samotná definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u každé agendy je popsána v příslušném agendovém listu (dokument, který byl vypracován ke každé agendě zvlášť). Tyto údaje budou rovněž uvedeny v tomto dokumentu, v oddílu s názvem: „Řešení zabezpečení jednotlivých agend“.

Zpracovatel analýzy rizik předkládá agendový list jako přílohu této analýzy (**příloha č. 1**)

49.2. Metoda určení a hodnocení aktiv

Zhotovitel určí primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení. Aktivum je chápáno jako objekt (dokument, informační systém, kartotéka, spisovna, portál, evidence či jiné listinné nebo elektronické úložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR. Každá agenda pak obsahuje více těchto aktiv.

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.



49.3. Účel zpracování dokumentu

Tento dokument s názvem „Analýza rizik“ je zpracován v souladu s Nařízením 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 (dále jen „GDPR“), zejména dle článku 24 a článku 25.

Dokument představuje ucelený souhrn informací týkající se implementace GDPR do vnitřních i vnějších procesů obce. Osoby, které vystupují v obci v postavení správce, jsou s tímto dokumentem plně seznámeny.

Dokument popisuje vyhodnocení rizik, která vznikají správci v souvislosti se zpracováním údajů o subjektech údajů. Na základě vyhodnocených rizik přijal správce vhodná opatření, které jsou v tomto dokumentu rovněž popsána.

Opatření přijatá správcem

Správce osobních údajů přijal všechna opatření vhodná ke snížení/vyloučení rizik, která vyhodnotil jako přiměřená a v souladu s GDPR. Přijatá opatření budou podrobně popsána v tomto dokumentu.

50. Charakteristika posuzovaného subjektu – správce osobních údajů

50.1. Identifikační údaje správce

Název: Obec Staré Sedlo
Sídlo: Zámecká 100, 357 46 Staré Sedlo
IČ: 00259608
Telefon: +420 352 684 055
e-mail: oustaresedlo@cbox.cz
Profil zadavatele:
Webové stránky: <http://www.staresedlo.cz/>
Počet členů zastupitelstva: 9 členů
Počet obyvatel: 838⁹

50.2. Struktura obecního úřadu

Obecní úřad tvoří starosta, místostarosta a zaměstnanci obce zařazení do obecního úřadu.

Úřední hodiny obecního úřadu jsou:

Po 7:00-17:00
Út 7:00-15:00
St 7:00-17:00
Čt 7:00-15:00
Pá 7:00-15:00

⁹ Tento údaj je pouze orientační.



50.3. Zveřejňování informací

Obec zveřejňuje informace na webových stránkách obce, a to včetně informací povinně zveřejňovaných dle jiného právního předpisu. Obec dále zveřejňuje informace na úřední desce obce, a to jak na úřední desce elektronické, tak fyzické. Při zveřejňování informací obec dlouhodobě dodržuje ustanovení zákona o ochraně osobních údajů (zákon č. 101/2000 Sb.). Obec při zveřejňování všech informací dbá na dodržení nařízení GDPR. Informace, o kterých není známo, zda podléhají ochraně dle GDPR, jsou konzultovány před zveřejněním s pověřencem pro ochranu osobních údajů. Správce osobních údajů rovněž poskytuje informace písemně a ústně, vše při dodržování nařízení GDPR.

51. Obecná struktura uchovávání osobních údajů v obci

51.1. Evidence údajů nahlášená Úřadu pro ochranu osobních údajů

V současné době nevede správce žádnou evidenci, která by podléhala nahlášení Úřadu pro ochranu osobních údajů.

51.2. Technické a organizační opatření

Správce osobních údajů přijal organizační a technická opatření v souladu s GDPR. Správce osobních údajů soustavně pracuje na modernizaci organizačních i technických opatření tak, aby bylo zajištěno maximální zabezpečení všech zpracovávaných údajů.

51.3. Předpisy obce

Technicko-organizační opatření ve formě předpisu k ochraně osobních údajů: ne
Obec v postavení správce osobních údajů se řídí těmito vnitřními předpisy:

- organizační řád
- spisový a skartační řád schválený věcně a místně příslušným archivem
- vnitřní organizační směrnice pro používání IT
- směrnice...
- vnitřní předpis...

51.4. Elektronické zdroje/evidence

51.5. Za zajištění jednotlivých informačních systémů odpovídá správce informačního systému.

51.6. Poskytovatelem internetového připojení je společnost: (doplnit název)

51.7. Elektronické zdroje popisují programové vybavení (software) využívané správcem při zpracování a evidenci údajů dle GDPR.

51.8. Veškeré programové vybavení (software) bylo pořízeno legálně a je pravidelně aktualizováno. Správce dbá na to, aby poskytovatel software zpracovával osobní údaje v souladu s GDPR.

51.9. Správce používá při své činnosti tyto elektronické zdroje/evidence:



- **Účetní program** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program evidence obyvatel** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program pokladny** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Program evidence majetku** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
- **Kancelářské programy Office** – jedná se o běžné kancelářské programy „Office“ od společnosti Microsoft.

51.10. Zaměstnanci obce mohou zpracovávat elektronické evidence s povahou zpracování pro osobní potřebu (např. adresáře). Tyto evidence nespádají pod působnost GDPR.

51.11. Listinné zdroje/evidence

Veškeré listinné zdroje/evidence jsou řádně uloženy v příslušných označených šanonech. Každá listinná evidence je vedena v rámci příslušné agendy. Ke každé agendě byl vypracován řádný agendový list. Pro přehled agend byl vypracován dokument s povahou soupisu agend, který obsahuje přehledné informace o vedených agendách (listinných i elektronických).

Veškeré listinné zdroje/evidence jsou uloženy v zamčených skříních/uzavřených skříních/policích vždy tak, aby k nim neměla přístup žádná třetí osoba. V případě, že je dokument uložen v kanceláři volně, dbá příslušný zaměstnanec na to, aby k němu neměla přístup žádná třetí osoba. Každá kancelář je mimo pracovní dobu uzamčena. Budova úřadu je mimo pracovní dobu vždy uzamčena a zabezpečena.

52. Popis implementace GDPR

52.1. Správce v souladu s GDPR vytvořil ke všem vedeným agendám podrobný agendový list. Tento agendový list obsahuje vždy následující údaje:

- **Název a popis agendy**
- **Účel zpracování**
- **Forma zpracování (listinná/elektronická)**
- **Forma zpracování (strukturovaná/nestrukturovaná)**
- **Podobný popis způsobu zpracování**
- **Kategorie subjektu údajů**
- **Kategorie příjemců**
- **Informaci o tom, zda jsou údaje předávány do třetích zemí**



- **Označení správce a zpracovatele**
- **Označení pověřence pro ochranu osobních údajů**
- **Označení dokladu (nosiče údajů)**
- **Určení doby zpracování**
- **Informaci o tom, zda je zpracování rizikové**
- **Informaci o tom, zda je informace zpracovávána na základě zákona**
- **Popis technických a organizačních opatření**
- **Komentář**

52.2. Vypracovaný dokument slouží správci rovněž pro posouzení, zda je zpracování v souladu s GDPR. V případě, že byl správcem vyhodnocen nesoulad, bylo přijato opatření k nápravě. Na základě vypracovaných agendových listů byl vytvořen seznam agend. Seznam agend poskytuje ucelený přehled o všech agendách, které správce zpracovává.

52.3. Při zpracování agendových listů nebyl správcem vyhodnocen nesoulad s nařízením GDPR.

52.4. Při zpracování agendových listů nevyhodnotil správce žádnou agendu jako rizikovou (obsahující citlivé osobní údaje o náboženském vyznání, sexuální orientaci, politickém přesvědčení apod.)

52.5. Postup správce osobních údajů při zpracování agendových listů byl vyhodnocen jako zcela legitimní, v souladu s požadavky GDPR.

52.6. **Záznamy o zpracování osobních údajů**

Správce vede záznamy o zpracování osobních údajů. Tyto záznamy popisují důležité skutečnosti, které se ke zpracování osobních údajů vztahují. Tuto činnost vykonává správce na základě čl. 30 nařízení GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě zvlášť a obsahují všechny informace obsažené v čl. 30 nařízení GDPR (např. údaje o správci, účel zpracování, popis kategorií subjektů údajů apod.). Všechny tyto záznamy budou pravidelně aktualizovány.

52.7. **Návrh na doplnění vnitřních předpisů**

Správci osobních údajů lze doporučit přijetí směrnice, která by upravovala zpracování osobních údajů dle nařízení GDPR (směrnice na ochranu osobních údajů). Vzhledem ke skutečnosti, že přijetí směrnice není povinností obce, nelze přijetí takovéto směrnice autoritativně nařídit.

Další doporučení nejsou navrhována. Správce zpracovává osobní údaje zcela v souladu s nařízením GDPR.

53. **Riziková zpracování**

53.1. Obec zpracovává většinu osobních údajů na základě čl. 6 odst. 1 písm. c), tedy za plnění zákonné povinnosti obce, případně písm. e), kdy dochází ke zpracování



veřejného zájmu nebo písm. b) na základě plnění smlouvy. V minimální míře pak obec zpracovává osobní údaje na základě souhlasu a oprávněného zájmu správce.

- 53.2. Na základě pečlivého studia dokumentů v rámci ochrany osobních údajů **nebyly zjištěny agendy, které vykazují vyšší míru rizika incidentních hrozeb.**
- 53.3. Obec v minulosti nezaznamenala ztrátu nebo odcizení osobních údajů.
- 53.4. Obec v minulosti nebyla sankcionována Úřadem pro ochranu osobních údajů, pro porušení povinností souvisejících s ochranou osobních údajů.
- 53.5. **Žádné ze zpracovávaných osobních údajů nespadají do zvláštní kategorie osobních údajů ve smyslu čl. 9 nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (dále jen GDPR). Výjimku představují nanejvýš osobní údaje zaměstnanců vyžadované právními předpisy za účelem plnění zákonných povinností zaměstnavatele (např. údaje o zdravotním stavu zaměstnanců).**

54. Obecný popis technických a organizačních opatření

54.1. Technická opatření obce

Technická opatření obce jsou navržena tak, aby splňovala veškeré nároky nařízení GDPR. V první řadě jsou všechny počítače v budově úřadu zabezpečeny proti neoprávněnému přístupu heslem. Použité heslo je kombinací znaků a čísel a je pravidelně aktualizováno. Použité heslo k samotnému přístupu do PC (po zapnutí) zná vždy jen konkrétní zaměstnanec, který s PC pracuje. Zároveň obec dbá na to, aby k žádnému počítači neměla přístup třetí osoba. Z obecného hlediska lze říci, že veškerý používaný software je pravidelně aktualizován. Veškerý software byl také legálně zakoupen a je užíván dle příslušných uživatelských příruček a dokumentů obdobných. Správce dbá na to, aby případný zpracovatel (který je zároveň poskytovatelem software) dbal na ochranu osobních údajů v souladu s nařízením GDPR.

Správce dlouhodobě využívá příslušný antivirový program. Každý počítač je také chráněn branou firewall. Každý zaměstnanec při práci využívá pouze ověřené a důvěryhodné zdroje.

Správce má s tímto zabezpečením dlouhodobě dobré zkušenosti. V minulosti nikdy nedošlo k úniku dat z důvodu nedostatečného technického zabezpečení na straně správce (či zpracovatele). Riziko bylo vyhodnoceno jako minimální/žádné.

54.1.1. Dodavatelé IT software a programů

Pro elektronické zdroje je zajištěna dokumentace všech IT programů, které obecní úřad používá a postupnými kroky se zároveň bude chystat systémová příručka. V systémové příručce obce budou následující body:

1. Popis implementovaného systému nebo programu (nutné podmínky pro instalaci a následný provoz)
2. Licenční podmínky
3. Popis podpory uživatele (hot-line, helpdesk)



4. Bezpečnostní podmínky (jak je systém zabezpečen – přístupy, šifrování, zálohování a bezpečnostní kopie).

5. Popisy systémem vytvářených logů – systémových a transakčních

6. Zprávy a výsledky testů a certifikací, které informační systém nebo program získal

7. Případně cloudové služby

V současné době obec nevyužívá cloudové služby a nemá to ani v plánu. Pokud ale po změně vedení, případně jiného vedení, obec tyto služby začne používat, obec si vyžádá informace o tom, kde se úložiště nachází a že úložiště je zabezpečeno podle GDPR.

54.1.2. Smluvní vztahy s dodavateli software

Správce se v rámci svých elektronických zdrojů a informačních systémů písemně dotázal dodavatelů IS programů, zda jeho systém je na GDPR připraven. Smluvní strany jsou připraveny spolupracovat s pověřencem pro ochranu osobních údajů, včetně kooperace s případnými kontrolami. Správce uzavřel / uzavře s poskytovateli IS dodatek ke smlouvě, který bude zaručovat odpovědnost zpracovatele za nakládání s os. údaji.

Správce po dodavateli IT softwaru požaduje závazek:

- spolupracovat s pověřencem pro ochranu os. údajů
- subjekt údajů bude mít dobrou dostupnost k informacím o zpracování svých údajů
- možnost realizovat právo subjektu na opravu nebo výmaz údajů s tím, že se uvede, v jaké formě (nejlépe v písemné formě),
- možnost realizovat právo na omezení zpracování,
- možnost subjektu poskytnout kopii zpracovávaných osobních údajů,
- možnost výkonu práva na přenositelnost údajů,
- zajištění podpory logování v čitelné formě s vazbou na uživatele a jeho činnosti,
- zajištění ochrany dat po ukončení smlouvy.

Dále správce zreviduje/zrevidoval smlouvy, které obsahují osobní údaje následujícím způsobem:

- Zajištění mlčenlivosti osob, které přijdou do styku s osobními údaji (u externích dodavatelů, případně tam, kde není zákonná povinnost)
- Zajištění a nastavení podmínek pro zapojení dalšího zpracovatele dle nařízení GDPR
- Zajistit práva subjektu údajů (informace o vedených údajích apod., dle GDPR)
- Zajistit podporu pověřence pro ochranu osobních údajů
- Zajistit ujednání o náhradě škody, včetně regresních nároků (s pozorností na smluvní pokuty, aby nevylučovaly náhradu škody).
- Zajistit po ukončení smlouvy odstranění kopií, zničení kopií, případně předání osobních údajů.



54.1.3. Obecný návrh opatření

Považuje se za vhodné zajistit pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Tento proces by měl být náležitě popsán (případně zaznamenán do systémové příručky/analýzy rizik), tak aby kontrola a realizace procesu byla součástí provozního testování, posuzování a hodnocení účinnosti zavedených opatření.

Správce bude nadále pokračovat v zajišťování souladu s GDPR. Správce bude postupně implementovat do všech dokumentací, vnitřních předpisů a nařízení ustanovení, která budou sloužit k:

- pseudoanonymizaci a šifrování osobních údajů k zajištění, aby tyto postupy byly běžnou součástí každodenního výkonu činností správce,
- zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování,
- schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů.

54.2. Organizační opatření obce

Organizační opatření správce spočívají v zajištění ochrany osobních údajů, které správce uchovává v listinné podobě (případně na fyzických datových nosičích). Toto zajištění spočívá zejména ve znemožnění třetím osobám k volnému přístupu k dokumentům, které obsahují osobní údaje. Správce provádí toto opatření zejména tak, že uzamyká budovu úřadu mimo úřední hodiny. Stejně jako budova obecního úřadu jsou uzamčeny i všechny kanceláře. V pracovní době jsou všechny výše uvedené nosiče dat pod dozorem příslušného pracovníka úřadu. Některé významné dokumenty jsou uchovány v trezoru úřadu. Zaměstnanci obce mají rovněž možnost dokumenty ukládat do uzamykatelných skříní.

Správce v minulosti nezaznamenal žádné porušení bezpečnosti, které by vedlo ke ztrátě či zneužití spravovaných údajů. Všichni zaměstnanci obce jsou řádně proškoleni.

Správce má s výše uvedeným zabezpečením dlouhodobě dobré zkušenosti. Riziko bylo vyhodnoceno jako minimální/žádné.

54.3. Personální opatření obce

Personální opatření obce, v postavení správce, spočívá v proškolení všech stávajících zaměstnanců a osob, které přichází do kontaktu s osobními údaji. Všichni zaměstnanci správce jsou řádně proškoleni na prezenčních školeních. V případě neznalosti některé problematiky se mohou obrátit na pověřence pro ochranu osobních údajů. Zároveň správce do budoucna plánuje další školení, která budou utvrzovat vzdělání všech dotčených osob v daném směru.



Správce považuje přijatá opatření za naprosto dostatečná. Riziko úniku osobních údajů subjektů údajů v důsledku neznalosti dotčených osob bylo vyhodnoceno jako minimální/žádné.

55. Řešení zabezpečení jednotlivých agend

55.1. Czech Point

Stávající stav: Žádosti jsou uloženy v deskách označených "Výstupy z CzechPoint" v šanonu Pošta v uzamykatelné skříňce, dále jsou žádosti ukládány na PC osob Venuše Štáhlovská a Romana Hořková, tyto PC jsou chráněny heslem. K dokumentům mají přístup R. Hořková, V. Štáhlovská, místostarosta Josef Kořínek a starosta Miroslav Toncar.

Osoby oprávněné ke zpracování jsou V. Štáhlovská, R. Hořková, M. Toncar, J. Kořínek.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.2. Evidence obyvatel

Stávající stav: Přihlašovací lístky k trvalému pobytu jsou evidovány na základě zákona o evidenci obyvatel, všechny karty jsou uloženy v uzamykatelné kartotéce, evidence obyvatel je vedena v programu Helios Fenix v PC osob Hořková Romana, Štáhlovská Venuše. K dokumentům mají přístup R. Hořková, V. Štáhlovská, místostarosta Josef Kořínek a starosta Miroslav Toncar.

Osoby oprávněné ke zpracování jsou V. Štáhlovská, R. Hořková, M. Toncar, J. Kořínek.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.3. Fond rozvoje bydlení

Stávající stav: Žádosti, smlouvy, Ručitelské prohlášení, faktury k proplacení týkající se FRB jsou v tištěné formě uloženy v šanonu "Půjčky z FRB", dále je vždy poslední smlouva a ručitelské prohlášení uloženo v PC osob Venuše Štáhlovská a Romana Hořková, tyto PC jsou chráněny heslem. K dokumentům mají přístup R. Hořková, V. Štáhlovská, místostarosta Josef Kořínek a starosta Miroslav Toncar.

Osoby oprávněné ke zpracování jsou V. Štáhlovská, R. Hořková, M. Toncar, J. Kořínek. Smlouva je předkládána v Komerční bance vypůjčitelem pro zřízení účtu k půjčce.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak



v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.4. **Pohřebnictví**

Stávající stav: Smlouvy o nájmu hrobových míst jsou uloženy v šanonech "Urnový háj - smlouvy a Hroby - smlouvy" spolu s Hřbitovní knihou a Knihou pohledávek v uzamykatelné skříňce, evidenční karty hrobů a uren jsou uloženy v uzamykatelné kartotéce, dále Evidence zemřelých s uvedením plátce, evidenční karty a vždy poslední smlouva o pronájmu hrobového místa jsou ukládány na PC osoby Romany Hořkové, tento PC je chráněn heslem. Evidence je ještě zpracovávána ve webovém prostředí na stránkách www.ceskehřbitovy.cz - kde jsou dány přihlašovací údaje. K dokumentům mají přístup R. Hořková, V. Štáhlavská, místostarosta Josef Kořínek a starosta Miroslav Toncar.

Osoby oprávněné ke zpracování jsou V. Štáhlavská, R. Hořková, M. Toncar, J. Kořínek.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.5. **Kamerový systém**

Stávající stav: Kamerový záznam je uložen ve vnitřní paměti kamery a lze jej dálkově přehrát v zařízeních, které mají nainstalovaný daný program. Obec Staré Sedlo přehrává a je tu i možnost uložení do zaheslovaného počítače osoby Romany Hořkové do té doby, než bude záznam přemazán z důvodu kapacity paměti kamery. Kamerový záznam není dlouhodobě zpracováván (uchováván).

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.6. **Odpadové hospodářství**

Stávající stav: Smlouvy jsou evidovány na základě zákona o odpadech a OZV č. 1/2015, všechny smlouvy jsou uloženy v příslušném šanonu, který je označen "Odpady", poslední smlouva je ukládána též v digitální podobě v počítači osob Hořková Romana,



Štáhlovská Venuše. Pohledávky jsou vedeny písemnou formou i v PC, pokladní doklady jsou vedeny v písemné formě v šanonu Pokladna, výpisy z účtu jsou vedeny v písemné formě v šanonu "Účetní doklady" a Výkazy jsou vedeny v písemné formě v šanonu "Odpady-výkazy". K dokumentům mají přístup R. Hořková, V. Štáhlovská, místostarosta Josef Kořínek a starosta Miroslav Toncar.

Osoby oprávněné ke zpracování jsou V. Štáhlovská, R. Hořková, M. Toncar, J. Kořínek.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.7. **Mzdová a personální agenda**

Stávající stav: Mzdová a personální agenda je vedena na základě zákoníku práce, dalších pracovněprávních předpisů a zákona o účetnictví. Všechny dokumenty jsou uloženy v písemné formě v příslušném šanonu, který je označen "Zaměstnanci" a v digitální podobě v počítači Venuše Štáhlovské. Přístup k dokumentům má starosta Miroslav Toncar a účetní Venuše Štáhlovská a Romana Hořková.

Osoby oprávněné ke zpracování jsou Miroslav Toncar, Venuše Štáhlovská, Romana Hořková a zaměstnanci společnosti Ing. Jan Klouda, Mánesova 1654, Sokolov, kteří měsíčně zpracovávají odměny a platy.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.8. **Smlouvy**

Stávající stav: Smlouvy jsou uloženy v šanonech označených "Kupní smlouvy", "Veřejnoprávní smlouvy", "Darovací smlouvy", "Pronájem pozemků", "Smlouvy o pronájem nebytových prostor", "Smlouvy o zřízení věcného břemene" v uzamykatelné skříňce, dále je vždy poslední smlouva uložena v PC osob Venuše Štáhlovská a Romana Hořková, tyto PC jsou chráněny heslem. K dokumentům mají přístup R. Hořková, V. Štáhlovská, místostarosta Josef Kořínek a starosta Miroslav Toncar.

Osoby oprávněné ke zpracování jsou V. Štáhlovská, R. Hořková, M. Toncar, J. Kořínek. Smlouvy veřejnoprávní s poskytnutím dotace nad 50.000,- Kč jsou dle zákona zveřejňovány na úřední desce internetových stránek obce.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně



proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.9. Správní řízení

Stávající stav: Spisová dokumentace je vedena v písemné formě dle spisu v šanonu správní řízení, v elektronické podobě pouze poslední správní řízení v dané oblasti.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.10. Účetnictví

Stávající stav: Bankovní výpisy, pokladní doklady, faktury, vnitřní účetní doklady, pohledávky, závazky, veškeré doklady k platbám jsou uloženy v šanonech a v uzamykatelné skříni. Data jsou ukládána na PC osoby Romany Hořkové a Venuše Štáhlavské, tyto PC jsou chráněny heslem. Účetnictví je zpracováváno v programu Helios Fenix od firmy Asseco Solutions, do kterého se lze přihlásit pouze pod heslem, kam mají přístup R. Hořková, V. Štáhlavská.

Osoby oprávněné ke zpracování jsou V. Štáhlavská, R. Hořková, M. Toncar, J. Kořínek. Doklady kontroluje finanční výbor.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům, byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

55.11. Vedení obecní kroniky

Stávající stav: Kronika je vedena na základě Zákona o kronikách. Je vedena v písemné formě a je uložena v trezoru v kanceláři starosty. Přístup k dokumentům má starosta Miroslav Toncar a účetní Venuše Štáhlavská a Romana Hořková. Klíče od trezoru mají V. Štáhlavská a R. Hořková.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to pouze v listinné podobě. Kronika není vedena v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne



55.12. Volební dokumentace

Stávající stav: Volební dokumentace - voličské průkazy + evidence, jmenování členů okrskové volební komise, průkazy zapisovatele a členů volební komise, volební seznamy, výpisy z volebních seznamů a další. Vedeno v písemné formě v označené krabici, která je uložena v uzamykatelné skříni. Přístup k dokumentům má starosta Miroslav Toncar a účetní Venuše Štálovská a Romana Hořková.

Osoby oprávněné ke zpracování jsou V. Štáhlavská, R. Hořková, M. Toncar, J. Kořínek.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to pouze v listinné podobě. Kronika není vedena v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

56. Pověřenec pro ochranu osobních údajů

56.1. 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, řízení procesů, 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 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.

56.2. **Obec má řádně jmenovaného pověřence pro ochranu osobních údajů, který není ve střetu zájmů.**

56.3. **Obec v postavení správce jmenováním řádného pověřence splňuje požadavky nařízení GDPR a vhodně snižuje rizika, která by mohla nastat v souvislosti s ochranou osobních údajů.**

56.4. Pověřenec pro obec zajišťuje tyto činnosti:

- 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 proškoleny v oblasti ochrany osobních údajů.
- 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.

57. Závěrečná ustanovení – zhodnocení souladu s nařízením GDPR

- 57.1. Zpracovatel tohoto dokumentu hodnotí všechny postupy správce osobních údajů jako postupy prováděné v souladu s nařízením GDPR. Dle výše uvedených informací správce postupuje při zpracování osobních údajů řádně, transparentně a s dostatečným ohledem na zabezpečení osobních údajů.
- 57.2. Správce osobních údajů přijal vhodná technická a organizační opatření. Detailní popis těchto opatření je uveden na každé jednotlivé kartě příslušné agendy. Vzhledem ke skutečnosti, že správce neprovádí rizikové zpracování, jsou všechna přijatá opatření hodnocena jako přiměřená.
- 57.3. Správce osobních údajů řádně jmenoval pověřence pro ochranu osobních údajů. Správce tak splnil povinnost, která byla stanovena nařízením GDPR. Jmenovaný správce není ve střetu zájmů a může tak činnost vykonávat.
- 57.4. Správce osobních údajů řádně zpracoval záznamy o činnostech zpracování. Správce tak splnil svou povinnost, která byla stanovena nařízením GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě. Tento postup zajišťuje vysokou míru transparentnosti při nakládání s osobními údaji.
- 57.5. Správce osobních údajů řádně zpracoval karty agend. Správce tak splnil svou povinnost stanovenou nařízením GDPR. Zpracování těchto karet je klíčovou činností každého správce a slouží zejména k prokázání souladu zpracování s nařízením GDPR.
- 57.6. Správce osobních údajů dlouhodobě klade důraz na bezpečné uchovávání a nakládání s osobními údaji. Tuto skutečnost potvrzuje fakt, že správce nebyl v minulosti vystaven sankci za porušení zákona o ochraně osobních údajů či jiných právních předpisů.
- 57.7. Správci lze dlouhodobě doporučit pokračování ve stávající úrovni zabezpečení a prohlubování znalostí nařízení GDPR a dalších právních předpisů.
- 57.8. Správci lze dlouhodobě doporučit průběžně aktualizovat karty agend v případě změn.
- 57.9. Správci lze dlouhodobě doporučit aktualizaci tohoto dokumentu.
- 57.10. Porušení nařízení GDPR při činnosti správce: **nebylo zjištěno.**
- 57.11. Závažné hrozby/rizika v souvislosti se zpracováním: **nezjištěno.**

58. Konečné hodnocení

- 58.1. **Správce vykonává svou činnost v souladu s nařízením GDPR.**

59. Seznam vedených agend

Zpracovatel analýzy přikládá přehled správcem vedených agend s vyhodnocením rizik.



Dokument/seznam/doklad	Účel zpracování	Údaje	Příjemce	Zákon	Komentář	Rizikový
Czech Point	Právní povinnost, státní správa, vedení agendy Czech Point pro FO a PO	Jméno, příjmení, rodné číslo, datum a místo narození, rodné příjmení, trvalé bydliště, číslo dokladu totožnosti, podpis	Žadatel – fyzická osoba	Zákon o obcích, o provozu pozemních komunikacích, o rejstříku trestů, o evidenci obyvatel, o katastru nemovitostí, o informačních systémech veřejné správy, o kontaktních místech VS, správní řád		NE
Evidence obyvatel	Vedení evidence obyvatel na základě povinnosti ze zákona	Jméno, příjmení, datum a místo narození, rodné číslo, trvalé bydliště, doručovací adresa, předchozí pobyt, číslo OP, omezení způsobilosti, údaje o opatrovníkovi, oprávněná osoba, podpis	Smluvní strana	Zákon o základních registrech, zákon o evidenci obyvatel, vyhláška k zákonu o evidenci obyvatel, správní poplatky, školský zákon		NE



Fond rozvoje bydlení	Vedení agendy fondu rozvoje bydlení (plnění bytových potřeb) vycházející z právní povinnosti	Jméno, příjmení, datum narození, rodné číslo, trvalé bydliště, číslo dokladu totožnosti, podpis, tele. číslo, číslo účtu	Žadatel	Zákon o obcích, občanský zákoník		NE
Pohřebnictví	Evidence hrobových míst, výběr poplatků a služby související s pohřebnictvím, evidence zemřelých, plátců a pohledávek	Jméno, příjmení, datum narození, rodné číslo, trvalé bydliště, telefon, číslo, podpis	Osobní údaje nejsou poskytovány třetím osobám, k údajům má přístup pouze správce a dotčená FO (v omezeném rozsahu)	Zákon o obcích, o pohřebnictví		NE
Kamerový systém	Ochrana životního prostředí a ochrana majetku	Podobizna z kamerového systému (nahrávka)	Pouze správce	Zákon o obcích, zákon o odpadech, zákon o přestupcích, trestní zákoník	Údaje jsou získávány na základě oprávněného zájmu obce a zájmu na ochraně zdraví a majetku obyvatel obce	NE
Odpadové hospodářství	Vedení a evidence	Jméno, příjmení,	Správce, dotčená	Zákon o obcích, zákon		NE



	odpadového hospodářství, plnění smlouvy, vymáhání pohledávek	IČ, DIČ, rodné číslo, adresa, datum narození, číslo bankovního účtu, datová schránka, telefonní číslo	smluvní strana (FO +PO)	o účetnictví, zákon o odpadech, občanský zákoník, zákon o archivní a spisové službě		
Mzdová a personální agenda	Evidence smluv, plnění smluv, vedení personální evidence zaměstnanců pro účely plnění pracovněprávních smluv a povinností dle zákoníku práce a dalších předpisů	Jméno, příjmení, datum narození, rodné číslo, trvalé bydliště, číslo dokladu totožnosti, podpis, telefonní číslo, číslo účtu	Ing. Jan Klouda, částečně pak orgány příslušné dle jiného právního předpisu (okresní správa sociálního zabezpečení, příslušná zdravotní pojišťovna a další dotčené orgány, příslušný finanční úřad)	Zákoník práce, zákon o daních z příjmu, zákon o pojistném na veřejné zdravotní pojištění, zákon o sociálním zabezpečení a příspěvku na státní politiku zaměstnanosti		NE
Smlouvy	Evidence a plnění smluv, vymáhání pohledávek apod.	Jméno, příjmení, datum a místo narození, rodné číslo, rodné příjmení, trvalé	Správce, druhá smluvní strana (FO, PO)	Zákon o obcích, občanský zákoník		NE



		bydliště, číslo doklady totožnosti, podpis, telefonní číslo, číslo úctu				
Správní řízení	Správní rozhodování obecního úřadu, výkon správního řízení dle správního řádu, plnění zákonné povinnosti	Jméno, příjmení, datum a místo narození, rodné číslo, rodné příjmení, trvalé bydliště, číslo dokladu totožnosti, datová schránka, podpis	Účastníci správního řízení, fyzické osoby	Zákon o ochraně přírody a krajiny, o evidenci obyvatel, o svobodném přístupu k informacím, o komunikacích, správní řád, o obcích		NE
Účetnictví	Vedení účetnictví a přidružovaných agend za účelem naplnění právní povinnosti	Jméno, příjmení, datum narození, rodné číslo, trvalé bydliště, číslo telefonu, podpis, sídlo podnikání, datová schránka, IČ, DIČ, bankovní spojení	Fyzické a právní osoby, osoby dotčené vedením účetnictví obce	Zákon o obcích, o účetnictví, o rozpočtových pravidlech územních rozpočtů		NE



Vedení obecní kroniky	Vedení obecní kroniky za účelem naplnění právní povinnosti, zaznamenávání historie obce	Jméno, příjmení, datum narození, rodné číslo, trvalé bydliště	Fyzické osoby požadující nahlédnutí do kroniky dle zákona	Zákon o obecních kronikách		NE
Volební dokumentace	Organizace a zajištění řádného průběhu voleb dle zákona	Jméno, příjmení, datum narození, rodné číslo, trvalé bydliště, věk, omezení svéprávnosti, podpis, číslo OP	Fyzické osoby-voliči, správce, úřad provádějící hodnocení výsledků voleb (ČSÚ)	Zákon o volbách do Parlamentu České republiky, zákon o volbách do zastupitelstev krajů, zákon o volbách do zastupitelstev obcí, zákon o volbách do Evropského parlamentu, Zákon o volbě prezidenta republiky		NE



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

12.6 Analýza rizik obce Šabina



Obec Šabina, Šabina č. p. 80, 356 01 Šabina

Analýza rizik

zpracovaná v souladu s Nařízením 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 (dále jen „GDPR“), zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“) a dle zákona o zpracování osobních údajů č. 110/2019 Sb.,

Správce:

Obec Šabina

Šabina č. p. 80

356 01 Šabina

IČ: 00573159



60. Úvodní ustanovení

60.1. 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 povinná 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.

60.2. Vymezení a definice správce v postavení obce

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 vyplývajících, 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.

60.3. Definice pojmu 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.

60.4. Definice pojmu 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.

60.5. Definice pojmu 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.

60.6. 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.

60.7. Ostatní ujednání – výklad pojmů

Je-li v tomto dokumentu uvedeno „správce“ je tím míněn správce a jeho příspěvková organizace (mateřská škola), není-li výslovně uvedeno jinak.

61. Obecné informace

61.1. Metoda zpracování analýzy

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, a to s ohledem na posuzování hodnoty aktiv, hrozeb a stanovení dalších parametrů analýzy rizik z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

Zpracovatel ve spolupráci se správcem osobních údajů zvolil metodu zhodnocení každé zpracovávané agendy, která osahuje osobní údaje. V rámci tohoto zhodnocení došlo k ohodnocení primárních aktiv dle jejich kritičnosti, a to v souladu s nařízením GDPR. Vzhledem ke skutečnosti, že GDPR nepředepisuje povinný formát analýzy rizik a taktéž nikterak neuvažuje hodnotu rizika, hodnotil správce riziko z pohledu ohrožení práv subjektů údajů.

Samotná definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u každé agendy je popsána v příslušném agendovém listu (dokument, který byl vypracován ke každé agendě zvlášť). Tyto údaje budou rovněž uvedeny v tomto dokumentu, v oddílu s názvem: „Řešení zabezpečení jednotlivých agend“.

Zpracovatel analýzy rizik předkládá agendový list jako přílohu této analýzy (**příloha č. 1**)

61.2. **Metoda určení a hodnocení aktiv**

Zhotovitel určí primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení. Aktivum je chápáno jako objekt (dokument, informační systém, kartotéka, spisovna, portál, evidence či jiné listinné nebo elektronické úložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR. Každá agenda pak obsahuje více těchto aktiv.

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.

61.3. **Účel zpracování dokumentu**

Tento dokument s názvem „Analýza rizik“ je zpracován v souladu s Nařízením 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 (dále jen „GDPR“), zejména dle článku 24 a článku 25.

Dokument představuje ucelený souhrn informací týkající se implementace GDPR do vnitřních i vnějších procesů obce. Osoby, které vystupují v obci v postavení správce, jsou s tímto dokumentem plně seznámeny.

Dokument popisuje vyhodnocení rizik, která vznikají správci v souvislosti se zpracováním údajů o subjektech údajů. Na základě vyhodnocených rizik přijal správce vhodná opatření, které jsou v tomto dokumentu rovněž popsána.



Opatření přijatá správcem

Správce osobních údajů přijal všechna opatření vhodná ke snížení/vyloučení rizik, která vyhodnotil jako přiměřená a v souladu s GPDR. Přijatá opatření budou podrobně popsána v tomto dokumentu.

62. Charakteristika posuzovaného subjektu – správce osobních údajů

62.1. Identifikační údaje správce

Název: Obec Šabina

Sídlo: Šabina č. p. 80, 356 01 Šabina

IČ: 00573159

Telefon: +420 352 693 449

e-mail: obec@obec-sabina.cz

Profil zadavatele: <https://www.vhodne-uverejneni.cz/profil/00573159>

Webové stránky: <http://www.obec-sabina.cz/>

Počet členů zastupitelstva: 7 členů

Počet obyvatel: 319¹⁰

62.2. Identifikační údaje příspěvkové organizace správce

Název: Mateřská škola Šabina

Sídlo: Šabina č. p. 80, 356 01 Šabina

IČ: 70995982

Telefon: +420 352 693 231

e-mail: mssabina@volny.cz

Webové stránky: <http://www.mssabina.estranky.cz/>

Odpovědná osoba: Lenka Kalousová, ředitelka školy

62.3. Příspěvkové organizace zřízené správcem

Správce zřídil mateřskou školu Šabina. Tato příspěvková organizace je považována z hlediska ochrany osobních údajů za organizační složku správce (nikoliv za samostatný subjekt/samostatného správce). Důvodem pro toto rozhodnutí je téměř absolutní provázanost činnosti správce a jeho příspěvkové organizace.

Příspěvková organizace je umístěna v budově, kde vykonává svou činnost správce.

62.4. Struktura obecního úřadu

Obecní úřad tvoří starosta, místostarosta a zaměstnanec obce zařazený do obecního úřadu.

Úřední hodiny obecního úřadu jsou:

Pondělí: 8:00 - 17:00 (polední přestávka 12.00 -13.00)

¹⁰ Tento údaj je pouze orientační.



Úterý:8:00 - 12:00

Středa:8:00 - 17:00 (polední přestávka 12.00 -13.00)

Čtvrtek:13:00 - 15:00

Pátek:8:00 - 13:00

62.5. **Zveřejňování informací**

Obec zveřejňuje informace na webových stránkách obce, a to včetně informací povinně zveřejňovaných dle jiného právního předpisu. Obec dále zveřejňuje informace na úřední desce obce, a to jak na úřední desce elektronické, tak fyzické. Při zveřejňování informací obec dlouhodobě dodržuje ustanovení zákona o ochraně osobních údajů (zákon č. 101/2000 Sb.). Obec při zveřejňování všech informací dbá na dodržení nařízení GDPR. Informace, o kterých není známo, zda podléhají ochraně dle GDPR, jsou konzultovány před zveřejněním s pověřencem pro ochranu osobních údajů. Správce osobních údajů rovněž poskytuje informace písemně a ústně, vše při dodržování nařízení GDPR.

Příspěvková organizace obce zveřejňuje některé informace na svých webových stránkách. Informace jsou zveřejňovány v souladu s GDPR. Informace, o kterých není známo, zda podléhají ochraně dle GDPR, jsou konzultovány před zveřejněním s pověřencem pro ochranu osobních údajů.

63. Obecná struktura uchovávání osobních údajů v obci

63.1. **Evidence údajů nahlášená Úřadu pro ochranu osobních údajů**

V současné době nevede správce žádnou evidenci, která by podléhala nahlášení Úřadu pro ochranu osobních údajů.

63.2. **Technické a organizační opatření**

Správce osobních údajů přijal organizační a technická opatření v souladu s GDPR. Správce osobních údajů soustavně pracuje na modernizaci organizačních i technických opatření tak, aby bylo zajištěno maximální zabezpečení všech zpracovávaných údajů.

63.3. **Předpisy obce**

Technicko-organizační opatření ve formě předpisu k ochraně osobních údajů: ne
Obec v postavení správce osobních údajů se řídí těmito vnitřními předpisy:

- organizační řád
- spisový a skartační řád schválený věcně a místně příslušným archivem
- vnitřní organizační směrnice pro používání IT
- směrnice...
- vnitřní předpis...

63.4. **Elektronické zdroje/evidence**

63.5. Za zajištění jednotlivých informačních systémů odpovídá správce informačního systému.



- 63.6. Poskytovatelem internetového připojení je společnost: (doplnit), se sídlem: (doplnit). Internetové připojení není poskytováno veřejně.
- 63.7. Elektronické zdroje popisují programové vybavení (software) využívané správcem při zpracování a evidenci údajů dle GDPR.
- 63.8. Veškeré programové vybavení (software) bylo pořízeno legálně a je pravidelně aktualizováno. Správce dbá na to, aby poskytovatel software zpracovával osobní údaje v souladu s GDPR.
- 63.9. Správce používá při své činnosti tyto elektronické zdroje/evidence:
- **Účetní program** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
 - **Program evidence obyvatel** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
 - **Program pokladny** (doplnit název) – zpracovatel (doplnit název zpracovatele) nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
 - **Program evidence majetku** (doplnit název) – zpracovatel, (doplnit název zpracovatele), nakládá s osobními údaji v souladu s nařízením GDPR. Přístup do programu je zabezpečen heslem.
 - **Kancelářské programy Office** – jedná se o běžné kancelářské programy „Office“ od společnosti Microsoft.
- 63.10. Zaměstnanci obce mohou zpracovávat elektronické evidence s povahou zpracování pro osobní potřebu (např. adresáře). Tyto evidence nespadají pod působnost GDPR.

63.11. **Listinné zdroje/evidence**

Veškeré listinné zdroje/evidence jsou řádně uloženy v příslušných označených šanonech. Každá listinná evidence je vedena v rámci příslušné agendy. Ke každé agendě byl vypracován řádný agendový list. Pro přehled agend byl vypracován dokument s povahou soupisu agend, který obsahuje přehledné informace o vedených agendách (listinných i elektronických).

Veškeré listinné zdroje/evidence jsou uloženy v zamčených skříních/uzavřených skříních/policích vždy tak, aby k nim neměla přístup žádná třetí osoba. V případě, že je dokument uložen v kanceláři volně, dbá příslušný zaměstnanec na to, aby k němu neměla přístup žádná třetí osoba. Každá kancelář je mimo pracovní dobu uzamčena. Budova úřadu je mimo pracovní dobu vždy uzamčena a zabezpečena.

64. Popis implementace GDPR

- 64.1. Správce v souladu s GDPR vytvořil ke všem vedeným agendám podrobný agendový list. Tento agendový list obsahuje vždy následující údaje:



- **Název a popis agendy**
- **Účel zpracování**
- **Forma zpracování (listinná/elektronická)**
- **Forma zpracování (strukturovaná/nestrukturovaná)**
- **Podobný popis způsobu zpracování**
- **Kategorie subjektu údajů**
- **Kategorie příjemců**
- **Informaci o tom, zda jsou údaje předávány do třetích zemí**
- **Označení správce a zpracovatele**
- **Označení pověření pro ochranu osobních údajů**
- **Označení dokladu (nosiče údajů)**
- **Určení doby zpracování**
- **Informaci o tom, zda je zpracování rizikové**
- **Informaci o tom, zda je informace zpracovávána na základě zákona**
- **Popis technických a organizačních opatření**
- **Komentář**

64.2. Vypracovaný dokument slouží správci rovněž pro posouzení, zda je zpracování v souladu s GDPR. V případě, že byl správcem vyhodnocen nesoulad, bylo přijato opatření k nápravě. Na základě vypracovaných agendových listů byl vytvořen seznam agend. Seznam agend poskytuje ucelený přehled o všech agendách, které správce zpracovává.

64.3. Při zpracování agendových listů nebyl správcem vyhodnocen nesoulad s nařízením GDPR.

64.4. Při zpracování agendových listů nevyhodnotil správce žádnou agendu jako rizikovou (obsahující citlivé osobní údaje o náboženském vyznání, sexuální orientaci, politickém přesvědčení apod.)

64.5. Postup správce osobních údajů při zpracování agendových listů byl vyhodnocen jako zcela legitimní, v souladu s požadavky GDPR.

64.6. **Záznamy o zpracování osobních údajů**

Správce vede záznamy o zpracování osobních údajů. Tyto záznamy popisují důležité skutečnosti, které se ke zpracování osobních údajů vztahují. Tuto činnost vykonává správce na základě čl. 30 nařízení GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě zvlášť a obsahují všechny informace obsažené v čl. 30 nařízení GDPR (např. údaje o správci, účel zpracování, popis kategorií subjektů údajů apod.). Všechny tyto záznamy budou pravidelně aktualizovány.

64.7. **Návrh na doplnění vnitřních předpisů**

Správci osobních údajů lze doporučit přijetí směrnice, která by upravovala zpracování osobních údajů dle nařízení GDPR (směrnice na ochranu osobních údajů). Vzhledem ke skutečnosti, že přijetí směrnice není povinností obce, nelze přijetí takovéto směrnice autoritativně nařídit.



Další doporučení nejsou navrhována. Správce zpracovává osobní údaje zcela v souladu s nařízením GDPR.

65. Riziková zpracování

- 65.1. Obec zpracovává většinu osobních údajů na základě čl. 6 odst. 1 písm. c), tedy za plnění zákonné povinnosti obce, případně písm. e), kdy dochází ke zpracování veřejného zájmu nebo písm. b) na základě plnění smlouvy. V minimální míře pak obec zpracovává osobní údaje na základě souhlasu a oprávněného zájmu správce.
- 65.2. Na základě pečlivého studia dokumentů v rámci ochrany osobních údajů **nebyly zjištěny agendy, které vykazují vyšší míru rizika incidentních hrozeb.**
- 65.3. Obec v minulosti nezaznamenala ztrátu nebo odcizení osobních údajů.
- 65.4. Obec v minulosti nebyla sankcionována Úřadem pro ochranu osobních údajů, pro porušení povinností souvisejících s ochranou osobních údajů.
- 65.5. **Žádné ze zpracovávaných osobních údajů nespádají do zvláštní kategorie osobních údajů ve smyslu čl. 9 nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (dále jen GDPR). Výjimku představují nanejvýš osobní údaje zaměstnanců vyžadované právními předpisy za účelem plnění zákonných povinností zaměstnavatele (např. údaje o zdravotním stavu zaměstnanců).**

66. Obecný popis technických a organizačních opatření

66.1. Technická opatření obce

Technická opatření obce jsou navržena tak, aby splňovala veškeré nároky nařízení GDPR. V první řadě jsou všechny počítače v budově úřadu zabezpečeny proti neoprávněnému přístupu heslem. Použité heslo je kombinací znaků a čísel a je pravidelně aktualizováno. Použité heslo k samotnému přístupu do PC (po zapnutí) zná vždy jen konkrétní zaměstnanec, který s PC pracuje. Zároveň obec dbá na to, aby k žádnému počítači neměla přístup třetí osoba. Z obecného hlediska lze říci, že veškerý používaný software je pravidelně aktualizován. Veškerý software byl také legálně zakoupen a je užíván dle příslušných uživatelských příruček a dokumentů obdobných. Správce dbá na to, aby případný zpracovatel (který je zároveň poskytovatelem software) dbal na ochranu osobních údajů v souladu s nařízením GDPR.

Správce dlouhodobě využívá příslušný antivirový program. Každý počítač je také chráněn branou firewall. Každý zaměstnanec při práci využívá pouze ověřené a důvěryhodné zdroje.

Správce má s tímto zabezpečením dlouhodobě dobré zkušenosti. V minulosti nikdy nedošlo k úniku dat z důvodu nedostatečného technického zabezpečení na straně správce (či zpracovatele). Riziko bylo vyhodnoceno jako minimální/žádné.



66.1.1. Dodavatelé IT software a programů

Pro elektronické zdroje je zajištěna dokumentace všech IT programů, které obecní úřad používá a postupnými kroky se zároveň bude chystat systémová příručka. V systémové příručce obce budou následující body:

1. Popis implementovaného systému nebo programu (nutné podmínky pro instalaci a následný provoz)
2. Licenční podmínky
3. Popis podpory uživatele (hot-line, helpdesk)
4. Bezpečnostní podmínky (jak je systém zabezpečen – přístupy, šifrování, zálohování a bezpečnostní kopie).
5. Popisy systémem vytvářených logů – systémových a transakčních
6. Zprávy a výsledky testů a certifikací, které informační systém nebo program získal
7. Případně cloudové služby

V současné době obec nevyužívá cloudové služby a nemá to ani v plánu. Pokud ale po změně vedení, případně jiného vedení, obec tyto služby začne používat, obec si vyžádá informace o tom, kde se úložiště nachází a že úložiště je zabezpečeno podle GDPR.

66.1.2. Smluvní vztahy s dodavateli software

Správce se v rámci svých elektronických zdrojů a informačních systémů písemně dotázal dodavatelů IS programů, zda jeho systém je na GDPR připraven. Smluvní strany jsou připraveny spolupracovat s pověřencem pro ochranu osobních údajů, včetně kooperace s případnými kontrolami. Správce uzavřel / uzavře s poskytovateli IS dodatek ke smlouvě, který bude zaručovat odpovědnost zpracovatele za nakládání s os. údaji.

Správce po dodavateli IT softwaru požaduje závazek:

- spolupracovat s pověřencem pro ochranu os. údajů
- subjekt údajů bude mít dobrou dostupnost k informacím o zpracování svých údajů
- možnost realizovat právo subjektu na opravu nebo výmaz údajů s tím, že se uvede, v jaké formě (nejlépe v písemné formě),
- možnost realizovat právo na omezení zpracování,
- možnost subjektu poskytnout kopii zpracovávaných osobních údajů,
- možnost výkonu práva na přenositelnost údajů,
- zajištění podpory logování v čitelné formě s vazbou na uživatele a jeho činnosti,
- zajištění ochrany dat po ukončení smlouvy.

Dále správce zrevizuje/zrevizoval smlouvy, které obsahují osobní údaje následujícím způsobem:

- Zajištění mlčenlivosti osob, které přijdou do styku s osobními údaji (u externích dodavatelů, případně tam, kde není zákonná povinnost)
- Zajištění a nastavení podmínek pro zapojení dalšího zpracovatele dle nařízení GDPR
- Zajistit práva subjektu údajů (informace o vedených údajích apod., dle GDPR)



- Zajistit podporu pověřence pro ochranu osobních údajů
- Zajistit ujednání o náhradě škody, včetně regresních nároků (s pozorností na smluvní pokuty, aby nevylučovaly náhradu škody).
- Zajistit po ukončení smlouvy odstranění kopií, zničení kopií, případně předání osobních údajů.

66.1.3. Obecný návrh opatření

Považuje se za vhodné zajistit pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Tento proces by měl být náležitě popsán (případně zaznamenán do systémové příručky/analýzy rizik), tak aby kontrola a realizace procesu byla součástí provozního testování, posuzování a hodnocení účinnosti zavedených opatření.

Správce bude nadále pokračovat v zajišťování souladu s GDPR. Správce bude postupně implementovat do všech dokumentací, vnitřních předpisů a nařízení ustanovení, která budou sloužit k:

- pseudoanonymizaci a šifrování osobních údajů k zajištění, aby tyto postupy byly běžnou součástí každodenního výkonu činností správce,
- zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování,
- schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů.

66.2. Organizační opatření obce

Organizační opatření správce spočívají v zajištění ochrany osobních údajů, které správce uchovává v listinné podobě (případně na fyzických datových nosičích). Toto zajištění spočívá zejména ve znemožnění třetím osobám k volnému přístupu k dokumentům, které obsahují osobní údaje. Správce provádí toto opatření zejména tak, že uzamyká budovu úřadu mimo úřední hodiny. Stejně jako budova obecního úřadu jsou uzamčeny i všechny kanceláře. V pracovní době jsou všechny výše uvedené nosiče dat pod dozorem příslušného pracovníka úřadu. Některé významné dokumenty jsou uchovány v trezoru úřadu. Zaměstnanci obce mají rovněž možnost dokumenty ukládat do uzamykatelných skříní.

Správce v minulosti nezaznamenal žádné porušení bezpečnosti, které by vedlo ke ztrátě či zneužití spravovaných údajů. Všichni zaměstnanci obce jsou řádně proškoleni.

Správce má s výše uvedeným zabezpečením dlouhodobě dobré zkušenosti. Riziko bylo vyhodnoceno jako minimální/žádné.

66.3. Personální opatření obce

Personální opatření obce, v postavení správce, spočívá v proškolení všech stávajících zaměstnanců a osob, které přichází do kontaktu s osobními údaji. Všichni zaměstnanci



správce jsou řádně proškoleni na prezenčních školeních. V případě neznalosti některé problematiky se mohou obrátit na pověřence pro ochranu osobních údajů. Zároveň správce do budoucna plánuje další školení, která budou utvrzovat vzdělání všech dotčených osob v daném směru.

Správce považuje přijatá opatření za naprosto dostatečná. Riziko úniku osobních údajů subjektů údajů v důsledku neznalosti dotčených osob bylo vyhodnoceno jako minimální/žádné.

67. Řešení zabezpečení jednotlivých agend

67.1. Mzdová a personální agenda

Stávající stav: Mzdová a personální agenda je vedena na základě zákoníku práce, dalších pracovněprávních předpisů a zákona o účetnictví. Všechny dokumenty jsou uloženy v písemné formě v příslušném šanonu, který je označen OÚ/1 a v digitální podobě v počítači Dagmar Fischerové. Přístup k dokumentům má starosta František Pešek a účetní Dagmar Fischerová. Osoby oprávněné k zpracování jsou: Dagmar Fischerová. Údaje nejsou předávány třetím osobám (zpracovateli), pouze odpovědným orgánům, např. Finanční úřad.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.2. Smlouvy

Stávající stav: Smlouvy jsou evidovány na základě občanského zákoníku a na základě zákona o účetnictví. Rovněž na základě zákona o obcích. Všechny smlouvy jsou uloženy v písemné formě v příslušných šanonech, které jsou označeny Smlouvy různé, Nájem pozemků, Smlouvy odpad, BH - nájemní smlouvy, Smlouvy veřejnoprávní a Banka a v digitální podobě v počítači Dagmar Fischerové. Přístup k dokumentům má starosta František Pešek a účetní Dagmar Fischerová. Smlouvy na VZMR nad 500.000,- Kč jsou zveřejňovány na profilu zadavatele veřejných zakázek. Osoba oprávněná k zpracování je Dagmar Fischerová. Na profilu zadavatele nejsou zveřejňovány údaje nad rámec údajů zveřejňovaných v obchodním/živnostenském rejstříku.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané smlouvy uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.3. Daňové doklady, faktury

Stávající stav: Daňové doklady a faktury jsou evidovány na základě zákona o účetnictví. Všechny jsou uloženy v písemné formě v příslušných šanonech, které jsou



označeny Faktury, účetní doklady, pokladna, BÚ, FRB, Rozpočet, ČNB, spořicí KB a v digitální podobě v počítači Dagmar Fischerové. Přístup k nim má starosta František Pešek a účetní Dagmar Fischerová. Osoba oprávněna ke zpracování je Dagmar Fischerová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.4. **Žádosti**

Stávající stav: Žádosti jsou uloženy ve spisovně a v kanceláři obecního úřadu, kde vykonává svoji funkci starosta a úřední činnost zaměstnankyně. V době jejich nepřítomnosti je kancelář i budova uzamčena. Klíč od kanceláře mají tyto osoby: František Pešek a Dagmar Fischerová. K žádostem nemá přístup žádná třetí osoba.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, pouze v listinné podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.5. **Správní rozhodnutí/rozhodování**

Stávající stav: Správní rozhodnutí jsou evidovány na základě správního řádu a zákonů vztahujících se k jednotlivým druhům žádostí. Rozhodnutí jsou uložena v listinné formě v příslušném šanonu, který je označen Rozhodnutí a v digitální podobě v počítači Dagmar Fischerové. Přístup k dokumentům má starosta František Pešek a účetní Dagmar Fischerová. Osoby oprávněné k zpracování jsou: František Pešek a Dagmar Fischerová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.6. **Dary**

Stávající stav: Darovací smlouvy jsou evidovány na základě zákona o obcích a občanského zákoníku. Žádosti jsou uloženy v písemné formě v příslušných šanonech označených Smlouvy různé, Smlouvy veřejné finanční podpory a v digitální podobě v počítači Dagmar Fischerové. Přístup k dokumentům má starosta František Pešek a účetní Dagmar Fischerová. Osoby oprávněné k zpracování jsou: František Pešek a Dagmar Fischerová.



Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.7. **Dotace**

Stávající stav: Žádosti o dotaci jsou evidovány na základě zákona o obcích a zákona o rozpočtových pravidlech územních samosprávných celků. Žádosti jsou uloženy v listinné podobě v příslušných šanonech označených Smlouvy různé a ve složkách jednotlivých akcí, kterých se dotace týkají. V digitální podobě jsou v počítači Dagmar Fischerové. Přístup k dokumentům má starosta František Pešek a účetní Dagmar Fischerová. Osoby oprávněné k zpracování jsou: František Pešek a Dagmar Fischerová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.8. **Územní plán**

Stávající stav: Územní plán obce je veden na základě stavebního zákona. Všechny dokumenty související s jeho tvorbou a změnami jsou uloženy v písemné formě v šanonu, který je označen Územní plán obce Šabina a v digitální podobě v počítači Dagmar Fischerové. Přístup k dokumentům má starosta František Pešek a účetní Dagmar Fischerová. Osoby oprávněné k zpracování jsou: František Pešek a Dagmar Fischerová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.9. **Klíče**

Stávající stav: Seznam klíčů a osob je evidován na základě organizačně technického opatření a je uložen v kanceláři starosty obce. K dokumentu má přístup František Pešek a Dagmar Fischerová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR. Agenda není vedena v elektronické podobě.



Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.10. **Evidence obyvatel**

Stávající stav: Evidence psů a poplatků za komunální odpady je evidována na základě zákona o místních poplatcích. Evidence je uloženy písemné formě v příslušném šanonu, který je označen Odpady, psi - pohledávky a v digitální podobě v počítači Dagmar Fischerové. Přístup k dokumentům má starosta František Pešek a účetní Dagmar Fischerová. Osoby oprávněné k zpracování jsou: František Pešek a Dagmar Fischerová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR, a to jak v listinné, tak v elektronické podobě. Osoby, které mají přístup k těmto údajům byly řádně proškoleny. Správce zašifruje všechny aktuálně nevyužívané dokumenty uložené v elektronické podobě minimálně komprimací do formátu zip. Tento zip soubor pak bude chráněn proti neoprávněnému přístupu heslem. Dokumenty, které jsou v elektronické podobě přístupné pouze v konkrétním programu jsou chráněny proti neoprávněnému přístupu heslem.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.11. **Kronika**

Stávající stav: Kronika je tvořena na základě zákona o kronikách obcí v písemné podobě.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR v listinné podobě. Kronika není vedena v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.12. **Všeobecné doklady – mateřská školka**

Stávající stav: Daňové doklady a faktury jsou evidovány na základě zákona o účetnictví. Všechny jsou uloženy v písemné formě v příslušných šanonech, které jsou označeny Faktury, Pokladna. Přístup k nim má ředitelka Lenka Kalousová a účetní firma Lendo.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR v listinné podobě. Doklady nejsou vedeny v elektronické podobě. Mezi správcem a zpracovatelem je uzavřen závazek deklarující zpracování osobních údajů v souladu s GDPR.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.13. **Klíče – mateřská školka**

Stávající stav: Seznam klíčů a osob je evidován na základě organizačně technického opatření a je uložen v ředitelně školy. K dokumentu má přístup ředitelka Lenka Kalousová.



Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR v listinné podobě. Doklad není veden v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.14. **Matrika – mateřská školka**

Stávající stav: Školní matrika je vedena na základě školského zákona. Všechny údaje jsou zapsané v knize "školní matrika" a dokumenty o dětech jsou v písemné formě založeny v šanonu. Přístup k dokumentům má ředitelka Lenka Kalousová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR v listinné podobě. Doklad není veden v elektronické podobě. Dokumenty jsou uloženy v řádně uzamykatelné skříni.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.15. **Mzdy – mateřská školka**

Stávající stav: Mzdová a personální agenda je vedena na základě zákoníku práce, dalších pracovněprávních předpisů a zákona o účetnictví. Všechny dokumenty jsou uloženy v písemné formě v příslušném šanonu. Přístup k dokumentům má ředitelka Lenka Kalousová a mzdová firma p.Z.Kapešové.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR v listinné podobě. Doklady jsou vedeny rovněž v elektronické podobě. Mezi správcem a zpracovatelem je uzavřen závazek deklarující zpracování osobních údajů v souladu s GDPR.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

67.16. **Smlouvy – mateřská školka**

Stávající stav: Smlouvy jsou evidovány na základě občanského zákoníku a na základě zákona o účetnictví. Všechny smlouvy jsou uloženy v písemné podobě v příslušných šanonech. K dokumentům má přístup ředitelka Lenka Kalousová.

Návrh opatření: Údaje jsou zpracovávány v souladu s GDPR v listinné podobě. Doklady nejsou vedeny v elektronické podobě.

Rizikové zpracování: ne

Zpracování citlivých osobních údajů: ne

68. Pověřenec pro ochranu osobních údajů

- 68.1. 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, řízení procesů, 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 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.

68.2. **Obec má řádně jmenovaného pověřence pro ochranu osobních údajů, který není ve střetu zájmů.**

68.3. **Obec v postavení správce jmenováním řádného pověřence splňuje požadavky nařízení GDPR a vhodně snižuje rizika, která by mohla nastat v souvislosti s ochranou osobních údajů.**

68.4. Pověřenec pro obec zajišťuje tyto činnosti:

- 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 proškoleny v oblasti ochrany osobních údajů.
- 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.

69. Závěrečná ustanovení – zhodnocení souladu s nařízením GDPR

69.1. Zpracovatel tohoto dokumentu hodnotí všechny postupy správce osobních údajů jako postupy prováděné v souladu s nařízením GDPR. Dle výše uvedených informací správce postupuje při zpracování osobních údajů řádně, transparentně a s dostatečným ohledem na zabezpečení osobních údajů.

69.2. Správce osobních údajů přijal vhodná technická a organizační opatření. Detailní popis těchto opatření je uveden na každé jednotlivé kartě příslušné agendy. Vzhledem ke skutečnosti, že správce neprovádí rizikové zpracování, jsou všechna přijatá opatření hodnocena jako přiměřená.

69.3. Správce osobních údajů řádně jmenoval pověřence pro ochranu osobních údajů. Správce tak splnil povinnost, která byla stanovena nařízením GDPR. Jmenovaný správce není ve střetu zájmů a může tak činnost vykonávat.

69.4. Správce osobních údajů řádně zpracoval záznamy o činnostech zpracování. Správce tak splnil svou povinnost, která byla stanovena nařízením GDPR. Záznamy o činnostech zpracování jsou vedeny ke každé agendě. Tento postup zajišťuje vysokou míru transparentnosti při nakládání s osobními údaji.

69.5. Správce osobních údajů řádně zpracoval karty agend. Správce tak splnil svou povinnost stanovenou nařízením GDPR. Zpracování těchto karet je klíčovou činností každého správce a slouží zejména k prokázání souladu zpracování s nařízením GDPR.



- 69.6. Správce osobních údajů dlouhodobě klade důraz na bezpečné uchovávání a nakládání s osobními údaji. Tuto skutečnost potvrzuje fakt, že správce nebyl v minulosti vystaven sankci za porušení zákona o ochraně osobních údajů či jiných právních předpisů.
- 69.7. Správci lze dlouhodobě doporučit pokračování ve stávající úrovni zabezpečení a prohlubování znalostí nařízení GDPR a dalších právních předpisů.
- 69.8. Správci lze dlouhodobě doporučit průběžně aktualizovat karty agend v případě změn.
- 69.9. Správci lze dlouhodobě doporučit aktualizaci tohoto dokumentu.
- 69.10. Porušení nařízení GDPR při činnosti správce: **nebylo zjištěno**.
- 69.11. Závažné hrozby/rizika v souvislosti se zpracováním: **nezjištěno**.

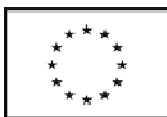
70. Konečné hodnocení

- 70.1. **Správce vykonává svou činnost v souladu s nařízením GDPR.**

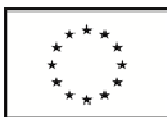
71. Seznam vedených agend

Zpracovatel analýzy přikládá přehled správcem vedených agend s vyhodnocením rizik.

Dokument/seznam/doklad	Účel zpracování	Údaje	Příjemce	Zákon	Komentář	Rizikový
Mzdová a personální agenda	plnění smluv, vedení personální evidence zaměstnanců pro účely plnění pracovních smluv a povinností dle zákoníku práce a dalších předpisů	Jméno, příjmení, rodné číslo, datum narození, adresa,	společnost – název účetní společnosti dozorové orgány	zákoník práce, zákon o daních z příjmu, zákon o pojistném na veřejné zdravotní pojištění, zákon o sociálním zabezpečení a příspěvku na státní politiku zaměstnanosti		NE
Smlouvy	shromažďování údajů za účelem plnění	Jméno, příjmení, rodné číslo,	Smluvní strana	Zákon č. 128/2000 o obcích (obecní zřízení); zákon	o dílo, pronájmy, ... Vytváří se na PC a tisknou	NE



	smluv, evidence smluv, archivace údajů za účelem vymáhání případných nároků ze smluv	datum narození, IČ, DIČ, adresa,		č. 89/2012 občanský zákoník	se, zakládají	
Faktury	zpracování Ekonomické agendy obce, vedení účetnictví obce	Jméno, příjmení, IČ, DIČ, adresa,	Dodavatel, odběratel	zákon o účetnictví		NE
Žádosti	správní rozhodován í úřadu, rozhodován í obce, zpracování žádostí od občanů obce a třetích osob	Jméno, příjmení, datum narození, adresa,	Žadatel v postavení fyzické osoby, či právnícké osoby (dažadující orgány), státní archiv, stavební úřad apod.	zákon o ochraně přírody a krajiny, stavební zákon, zákon o vodovodech a kanalizacích apod.		NE
Správní rozhodnutí	Výkon státní správy, evidence a vydávání správních rozhodnutí	Jméno, příjmení, datum narození, adresa,	Žadatel o rozhodnutí	správní řád, zákon o ochraně přírody a krajiny, stavební zákon, zákon o vodovodech a kanalizacích, zákon o obcích		NE
Dary	Správní rozhodnutí úřadu,	Jméno, příjmení, datum	Žadatel v postavení obávanéh	občanský zákoník, zákon		NE



	rozhodován í obce	narození, adresa,	o (subjekt údajů), dále zpracovatel, dárce (fyzická nebo právnícká osoba)	o obcích		
Dotace	Evidence a vyřizování žádostí o dotaci	Jméno, příjmení, datum narození, adresa,	Žadatel o dotaci	Zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, zákon č. 500/2004 Sb., správní řád, zákon č.89/2012 Sb., občanský zákoník, zákon č.128/2000 Sb., o obcích		NE
Územní plán	Tvorba a změny plánu	Jméno, příjmení, adresa	občan obce, příslušný stavební úřad	stavební zákon, zákon o obcích		NE
Klíče	Zabezpečen í prostor obecního úřadu.	jméno, příjmení	starosta, referent úřadu	Organizačně technické opatření		NE
Razítka	Evidence dle spisového řádu	číslo razítko, jméno, příjmení	starosta, referent úřadu	Zákon o archivnictví, vnitřní směrnice		NE
Adresáře	Pro komunikaci při výkonu veřejné správy	Jméno, příjmení, kontakt (tel/email)	starosta, referent úřadu		nepodléhá GDPR	NE



Evidence obyvatel	Vedení seznamu obyvatel / zpracování evidence obyvatel	Jméno, příjmení, datum narození, rodné číslo, místo trvalého pobytu	Referent úřadu, starosta	zákon o evidenci obyvatel a rodných číslech		NE
Kronika	Zachycení událostí v obci	Jméno, příjmení	Kronikářka, Fyzické osoby požadující nahlédnutí dle zákona	zákon o kronikách obcí		NE
Volby	Organizace voleb na základě zákona	Jméno, příjmení, datum narození, bydliště	volební komise, referent úřadu	Zákon o volbách do parlamentu, do zastupitelstev obcí, do zastupitelstev krajů, prezidenta republiky, do Evropského parlamentu .		NE



13. Praktická část – pověřenec pro ochranu osobních údajů

Všechny obce, pro které je tento dokument zpracováván, tedy: Hory, Jenišov, Lomnice, Staré Sedlo, Šabina a Vintířov mají jmenovaného pověřence 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, řízení procesů, 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 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.

Obec má řádně jmenovaného pověřence pro ochranu osobních údajů, který není ve střetu zájmů. Konkrétním pověřencem je společnost ABRI, s. r. o., se sídlem: Ondříčkova 537, Sokolov 356 01. Tato společnost je regionální rozvojovou agenturou, která se zabývá širokou škálou činností, od administrace žádostí o dotace, přes služby pověřence GDPR, po vedení samostatné části sociálního podniku. Společnost zastupuje jednatelka paní Linda Zemanová, která má na starost také vztahy s obcemi v postavení zákazníků a vykonává činnost osobně jako pověřenec pro ochranu osobních údajů. Služby jsou poskytovány na základě žádostí obcí, které se sami obracejí na společnost ABRI, s. r. o. s konkrétními dotazy. Jsou tedy poskytovány konzultace při řešení běžné problematiky.

Obec v postavení správce jmenováním řádného pověřence splňuje požadavky nařízení GDPR a vhodně snižuje rizika, která by mohla nastat v souvislosti s ochranou osobních údajů.



13.1 Činnost pověřence

Pověřenec pro obce zajišťuje tyto činnosti:

- 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 proškoleny v oblasti ochrany osobních údajů.
- 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.

13.2 Doporučení k činnosti pověřence

K činnosti pověřence lze doporučit aktivnější zapojení pověřence do činností, při nichž dochází ke zpracování osobních údajů. Služby pověřence jsou hrazeny paušálně a poskytovány na požádání každé jednotlivé obce. Některé případy zpracování osobních údajů tak mohou pověřenci uniknout, protože o nich není informován (není seznámen s činnostmi zpracování). Lze tedy doporučit, aby pověřenec pro ochranu osobních údajů aktivně spolupracoval s obcemi při aktualizaci Analýz rizik, při aktualizaci Záznamů o činnosti zpracování (případně při jejich vytváření) a případně také při vytvoření vnitřní směrnice pro ochranu osobních údajů, bude-li mít obec o tuto vnitřní směrnici zájem. Pověřenec pro ochranu osobních údajů by se tak měl stát aktivním pomocníkem, který zná agendy, které obec, v postavení správce, vede. Defacto jej lze postavit na rovinu zaměstnanci, který osobní údaje zpracovává.

S pověřencem pro ochranu osobních údajů by měly být dohodnuty osobní konzultace v určitém časovém horizontu (např. jednou za půl roku) a také by mělo být dohodnuto pravidelné školení zaměstnanců. Tato činnost jde možná nad rámec činností, které má



vykonávat pověřenec, přesto však při zpracování tohoto dokumentu bylo zjištěno, že společnost ABRI, s. r. o., má na poskytování školení tohoto typu dostatečnou kapacitu.

14. Praktická část – návrhy a doporučení

Návrhy a doporučení jsou závěrečnou částí dokumentu, která vhodně shrnuje a implementuje do praxe výše uvedený text. Spolu s vypracováním kompletních aktualizovaných Analýz rizik pro jednotlivé obce, tvoří vhodně propojený celek, který pomůže obcím lépe implementovat nařízení GDPR.

14.1 Přijetí a aktualizace Analýzy rizik

Analýza rizik je zpracována v souladu s Nařízením 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 (dále jen „GDPR“), zejména dle článku 24 a článku 25. Dokument představuje ucelený souhrn informací týkající se implementace GDPR do vnitřních i vnějších procesů obce. Lze tedy všem obcím doporučit přijetí tohoto dokumentu, jeho implementaci, seznámení všech dotčených pracovníků s tímto dokumentem a jeho další aktualizaci. Dále by s dokumentem měl být seznámen pověřenec pro ochranu osobních údajů, který by měl být rovněž pověřen pravidelnou aktualizací tohoto dokumentu (dle názoru autora tohoto dokumentu by postačovalo 1 ročně).

Zpracovávané agendy se totiž mohou v průběhu roku měnit, stejně tak jako se mohou měnit vhodná přijatá opatření (vždy na základě testu proporcionality), je to právě pověřenec pro ochranu osobních údajů, který by měl správci doporučovat vhodné postupy, co se týče zpracování, zabezpečení a dalších kroků.

Přijatá a aktualizovaná Analýza rizik na každé jednotlivé obci bude tvořit páteří dokument pro implementaci GDPR. Jak již bylo uvedeno výše, pro všechny zapojené obce byl tento dokument vypracován a bude jim také samostatně předán v otevřeném, strojově čitelném formátu, k dalšímu použití.



Vzhledem ke skutečnosti, že dokument nemá váhu směrnice obce, nemusí být jeho obsah schvalován zastupitelstvem obce. Může být tedy upravován, měněn a doplňován velmi pružně, v závislosti na dotvářejícím se výkladu nařízení GDPR a také v závislosti na požadavcích každé konkrétní obce. Některé velmi malé obce (např. Šabina) nelze nařízením GDPR více zatěžovat (opět dle testu proporcionality) jelikož mají jen 300 obyvatel a jednoho stálého zaměstnance, který vykonává veškerou agendu úřadu, v samostatné i přenesené působnosti. Z toho je patrné, že každá analýza rizik bude vysoce individuální.

14.2 Přijetí a aktualizace Záznamů o činnosti zpracování

Záznamy o činnosti zpracování lze označit za výstup mapování zpracování, které lze považovat za povinné (bez mapování nemůže správce přijmout adekvátní opatření). V první řadě je tedy třeba provést mapování a jeho výstupem budou právě záznamy o činnosti zpracování. Toto záznamy pak prakticky doporučujeme vést pro každou zpracovávanou agendu zvlášť, pro zvýšení přehlednosti a orientace ve zpracování.

Znalost prováděného zpracování, rozsahu zpracování, účelů zpracování, právního základu a dalších skutečností je základním předpokladem pro to, aby zpracování probíhalo v souladu s nařízením GDPR a aby byl správce tento soulad schopen prokázat (doložit).

Abychom mohli sestavit řádnou a úplnou analýzu rizik GDPR je potřeba mít postaveno na jisto, jaké agendy obec vede, jaké důvody zpracování jsou na tyto agendy vázány a jaké konkrétní osobní údaje jsou v rámci vedení agend zpracovávány. K tomuto nám slouží záznamy o činnostech zpracování, které obsahují všechny výše uvedené důležité údaje. Záznam o činnosti zpracování by měl být veden ke každé zpracovávané agendě, a to nejlépe v elektronické podobě pro snadné úpravy. Stejně jako se bude v čase měnit analýza rizik, budou se měnit i záznamy o činnostech zpracování. Zde lze však předpokládat, že aktualizace bude nutná výrazně častěji. Záznamy o činnosti zpracování byly aktualizovány v době zpracovávání tohoto dokumentu, a to externím poradcem pod dohledem pověřence pro ochranu osobních údajů.

Obcím lze v tomto směru tedy dále doporučit, aby udržovaly záznamy o činnosti zpracování aktualizované, případně jejich aktualizací pověřili pověřence pro ochranu



osobních údajů. Bez této činnosti nelze zaručit aktuální znění analýzy rizik, jejíž důležitost je uvedena výše. Stejně jako aktualizace ale musí probíhat také vyřazování nebo přidávání záznamů o činnostech zpracování, podle toho, jaké agendy zrovna obec zpracovává. Některé agendy lze totiž označit za trvalé např. evidenci obyvatel, některé za dočasné např. evidence sponzorů dětského dne.

14.3 Fyzická bezpečnost

V rámci přezkoumání fyzické bezpečnosti zpracovávaných údajů byla společně s jmenovaným pověřencem pro ochranu osobních údajů provedena revize zabezpečení údajů na jednotlivých obcích. Tímto místním šetřením bylo zjištěno, že všechny zapojené obce dbají na fyzické zabezpečení minimálně v tom rozsahu, jak byly zvyklé v době účinnosti zákona o ochraně osobních údajů.

Důležité dokumenty jsou na všech obcích uloženy v uzamykatelných skříních nebo trezorech. Dokumenty s menší mírou rizika jsou uloženy ve skříních, které nejsou uzamykatelné, vždy však je uzamykatelná kancelář a budova úřadu. Budovy úřadu jsou pak povětšinou chráněny elektronickým zabezpečovacím systémem. Všechny obce se snaží vyhýbat nešvaru „volně ložených dokumentů“ na stolech úředníků, ke kterým mají velmi snadno přístup osoby, které navštěvují úřad v úředních hodinách.

Při testu proporcionality přijatých opatření bylo vycházeno zvláště ze skutečnosti, že žádný z obecních úřadů se ve své porevoluční historii nestal předmětem vloupání. Zvláště pak nelze přepokládat, že by případné vloupání ohrozilo dokumenty v listinné podobě, které pro neznalé nemají žádnou peněžní hodnotu.

Co se týče fyzické bezpečnosti, nelze tedy striktně doporučit přijetí dalších opatření. Horší situace nastává se zabezpečením počítačů, které jsou běžnou součástí kanceláří. Tyto počítače nejen že mají pro případné „lapky“ vysokou hodnotu, ale navíc obsahují 90% údajů, se kterými úředníci obecních úřadů nakládají. Zde lze tedy jen doporučit pečlivou ochranu hardware před krádeží a vhodné zabezpečení na softwarové úrovni, o čem bude psáno níže.



14.4 IT bezpečnost

IT bezpečnost je jistě největším tématem, co se zabezpečení týče. Jak již bylo uvedeno výše, hlavním cílem všech obcí by mělo být v první řadě uchránění zařízení před fyzickou krádeží. Dále pak pokud již bude počítač odcizen, je nutné jej mít zabezpečený tak, aby neměl pro zloděje vysokou hodnotu – zamknutím dat, zamknutím úvodní obrazovky, anonymizací dat nebo jejich pseudonymizací.

V dnešní době se již nedá předpokládat, že by průměrný uživatel PC nedokázal prolomit heslo vstupní obrazovky, proto je nutné (pokud to jde) právě nad rámec tohoto anonymizovat všechna data u kterých je to nutné, nebo je pseudonymizovat. Rovněž je vhodné zamknout heslem složky ve kterých jsou údaje uloženy nebo soubory, ve kterých tyto údaje jsou.

Heslo by pak měl znát pouze konkrétní zaměstnanec, který zpracování provádí a případně jeho nadřízený. Pochopitelně není vhodné (ale stále se s tím lze setkat!) uvedení hesla na zadní stranu notebooku, na nástěnku v kanceláři a podobně.

Jako velmi vhodné se jeví práce s daty „online“, které nejsou fyzicky uloženy v počítači, ale v online rozhraní tzv. cloudu. Tento cloud je většinou výborně zabezpečen proti ztrátě či zcizení osobních údajů a práce v něm je uživatelsky přívětivá.

Pro prvotní zvýšení bezpečnosti IT vybavení, které je v obci používáno, je vhodné oslovit specializovanou firmu nebo specializovaného IT technika, který by měl být schopen navrhnout vhodné opatření. I zde je nutné stále přihlížet k testu proporcionality a mít na paměti, že jistě nelze vyžadovat stejnou úroveň zabezpečení v obci Šabina jako v Centrální národní bance.

Závěrem lze říci, že ačkoliv je fyzické zabezpečení mnohdy na velmi vysoké úrovni, na IT zabezpečení se často „zapomíná“, ačkoliv právě zabezpečení IT by mělo být primárním cílem na každé dotčené obci. Doporučujeme proto zvážení konzultace zabezpečení s odbornou obchodní korporací.

14.5 Interní předpisy a směrnice

Zpracovávané obce neměly v době zpracovávání tohoto dokumentu žádný interní předpis nebo směrnici, která by upravovala nakládání s osobními údaji. Zaměstnanci



obce vycházejí při své práci zejména ze znalosti minulé právní úpravy (zákon o ochraně osobních údajů), z nařízení GDPR, částečně též ze zákona o ochraně osobních údajů a také ze své dlouhodobé praxe.

Pro další práci zejména na větších obcích lze doporučit zpracování interního předpisu pro ochranu osobních údajů, který by upravoval sběr, zpracování a nakládání s osobními údaji. V interním předpisu by měl být uveden přehled základních pojmů, co jsou to osobní údaje, jaké operace jsou považovány za zpracování osobních údajů, kdo je správce a zpracovatel a další informace. Dále by mohl vnitřní předpis upravovat odpovědnost každého zaměstnance, který osobní údaje získává, využívá a dále zpracovává, stejně tak by vnitřní předpis mohl upravovat povinnosti tohoto zaměstnance. Další informace uvedené se mohou týkat obecných zásad zpracování osobních údajů. Nedílnou součástí je pak popis bezpečnostních opatření.

Namísto přijetí nového interního dokumentu, ať už ve formě směrnice nebo interního předpisu, lze k výše uvedenému použít vypracovanou analýzu rizik. Tato, po vhodném individuálním doplnění, bude obsahovat všechny výše navrhované body. Tento dokument pak může sloužit všem zaměstnancům, kteří se nějakým způsobem podílejí na zpracování osobních údajů, jako interní předpis pro zpracovávání osobních údajů v souladu s nařízením GDPR.

Tento postup lze na všech dotčených obcích doporučit. Vnitřní směrnice a další dokumenty jsou často opomíjeny a ztrácejí se ve velkém množství už tak přijatých vnitřních směrnic a dokumentů. Navíc analýza rizik, která byly pro obce zpracovávána, má být „živým“ pravidelně aktualizovaný dokumentem, k čemuž může právě přispět i to, že bude zároveň fungovat jako základní směrnice (pravidlo) pro práci s osobními údaji.

14.6 Kamerový systém

Většina obcí, pro které je tento dokument zpracováván, používá kamerový systém. Tento je dnes již běžnou součástí našich životů. Nesprávným používáním kamerového systému však může dojít k poškozování základního práva člověka – práva na soukromí. Provozováním kamerového systému tak může dojít k porušení práv chráněných jinými



právními předpisy, ale také při jeho provozování dochází ke zpracování osobních údajů, dle nařízení GDPR.

Správce provozující kamerový systém podle nařízení GDPR plně odpovídá za zpracování, které jeho prostřednictvím provádí. Obec, která pořizuje kamerový systém, tak bude činit zejména ze své zákonné povinnosti nakládat se svým majetkem s péčí řádného hospodáře – tedy s péčí řádného hospodáře jej též ochraňovat. Mezi způsoby ochrany pak patří pojištění a také zabezpečení, souborem různých opatření. Jedním z nich je právě zmiňovaný kamerový systém, jehož pořízení musí být pečlivě zváženo k daným okolnostem a k ochraně soukromí, která může být pořízením kamerového systému narušena.

Právním důvodem zpracování by pak mohla být zákonná povinnost, protože ochrana majetku je zákonnou povinností obce, stejně tak jako oprávněný zájem – jelikož opět ochrana majetku je nepochybně oprávněným zájmem obce. Bez právního důvodu zpracování, jak bylo uvedeno výše, nelze zpracování osobních údajů legálně provádět. Zde tedy stojí právní důvody dva, což je naprosto dostačující.

Opětovně se vracíme k testu proporcionality, kdy oprávněný zájem správce na sledování určitých prostor nebo prostranství převáží nad základním právem na soukromí každého člověka. Proporcionalita se pak poměřuje ve vztahu k účelu, kterého má být monitorováním dosaženo (zabránění krádeže, zvýšení šance dopadení pachatele apod.). Stále je ovšem nutné mít na paměti, že kamerové systémy nevyřeší všechny problémy a jejich instalace bude oprávněná pouze tam, kde sledovaný legitimní účel nelze dosáhnout jinými běžnými prostředky, které představují menší zásah do soukromí. Zvláštní problematiku pak tvoří existence kamerového systému na pracovištích, kdy kamerový systém snímá pracoviště zaměstnance. Takovýto kamerový systém ovšem žádná z dotčených obcí neprovozuje, a proto není důležité se jím dále zabývat.

Zabezpečení samotného kamerového systému pak musí odpovídat podmínkám záměrné a standardní ochrany osobních údajů, jak je to specifikováno v čl. 25 nařízení GDPR a podmínkám zabezpečení osobních údajů podle čl. 32 nařízení GDPR. Správce tedy musí vyřešit vhodné umístění zařízení, které bude obsahovat záznamy a toto zabezpečit proti neoprávněnému přístupu (přičemž není nutné záznamy šifrovat). V rámci zabezpečení také musí být konkrétně řešena přístupová práva, tj. kdo může se záznamy



manipulovat (stejně tak by mělo být jasné kdo a kdy se záznamem případně manipuloval).

Důležitou součástí při provozování kamerového systému pak tvoří informační povinnost správce, která je dána ustanovením článku 13 nařízení GDPR. S informacemi se často setkáme ve formě cedulek „prostor je snímán kamerovým systémem“ a podobně. Nařízení GDPR žádnou takovou formu nestanovuje, je tedy na vůli správce, jak dotčené osoby informuje (opět s přihlédnutím k přiměřenosti).

O kamerovém systému by pak samozřejmě měl být veden záznam o činnosti zpracování, tak, jak je to doporučováno v analýze rizik. S pořízeným záznamem by se mělo řádně a transparentně nakládat, měla by být určena doba jeho uchování a také způsob likvidace. Použití záznamů by pak mělo být vázáno pouze na situace, kdy dojde k nějakému incidentu – v takovém případě může být kamerový záznam předán Policii České republiky nebo jiným orgánům.

14.7 Proškolení zaměstnanců

Školení zaměstnanců na dotčených obcích v oblasti GDPR probíhalo v době nabytí účinnosti platnosti nařízení GDPR, tj. po květnu 2018. Poté byla přijata některá základní pravidla a provedeny základní revize, aby bylo nařízení GDPR vyhověno. Motivace k dalšímu vzdělávání pak ochladla s přijetím zákona o ochraně osobních údajů, který zcela vyloučil pokuty, které nařízení GDPR stanovovalo, pro obce a kraje.

Přesto jak bylo uvedeno výše v textu, lze všem obcím doporučit pravidelná školení k problematice ochrany osobních údajů, která se vyvíjí v čase. Zde doporučuji jednoznačně zapojit pověřence pro ochranu osobních údajů, který by měl na dotčených obcích alespoň zjistit, jak jsou na tom obce s informovaností zaměstnanců o problematice ochrany osobních údajů. Za tři roky totiž může fluktuace zaměstnanců způsobit téměř nulové seznámení s touto problematikou. Opět lze provést školení jednoduše, bez dalších nákladů tím, že bude zaměstnancům představena analýza rizik GDPR a práce s ní, vize práce s osobními údaji a představeny základní zásady nařízení GDPR na kterých je ochrana osobních údajů postavena.

Autor tohoto dokumentu navštívil osobně všechny obce a je si vědom, že výkon samostatné i přenesené působnosti je pro zaměstnance úřadů velkou zátěží i vzhledem



k stále měnící se legislativě, přesto lze však trvat na nutnosti školení alespoň jednou ročně. Samozřejmostí je, že prvotní školení by mělo být ve větším rozsahu, v dalších letech pak mohou probíhat poloformální setkávání, s výkladem novinek v oblasti ochrany osobních údajů.

Ochrana osobních údajů se dotýká různým způsobem všech agend, které jsou zpracovávány v rámci samostatné i přenesené působnosti, proto nelze ochranu osobních údajů přesunout „na okraj zájmu“ zástupců obcí.

14.8 Příklady dobré praxe / konkrétní postupy

Jako doplňková část textu tohoto dokumentu je uveřejněna dobrá praxe s praktickými postupy pro konkrétní situace. Velká většina postupů však byla upravena v přeložených analýzách rizik, případně je upravena přímo výše v textu. Údaje pro dobrou praxi / konkrétní postupy byly převzaty a upraveny ze stanovisek Ministerstva vnitra České republiky. Dokumenty jsou dostupné pod odkazem: <https://www.mvcr.cz/gdpr/clanek/modelove-situace.aspx>.

Pro účely tohoto dokumentu byly vybrány pouze relevantní situace, se kterými se obce při zpracování běžně setkávají.

14.8.1 Výkon spisové služby, ukládání a skartace dokumentů

Povinnost vést spisovou službu a pravidla pro skartační řízení upravuje zákon o archivnictví a spisové službě a vyhláška o spisové službě. V konečném důsledku zákon o archivnictví a spisové službě mimo jiné založil povinnost pro určené původce vést spisovou službu.

Dle této speciální právní úpravy je dokument vytvořený veřejnoprávním původcem součástí výkonu spisové služby. Za dokument vzniklý z činnosti původce se považuje rovněž dokument, který byl původci doručen nebo jinak předán. Povinnost uchovávat dokumenty a umožnit výběr archiválií mají také územní samosprávně celky, školy a školská zařízení s výjimkou mateřských škol, výchovných a ubytovacích zařízení a zařízení školního stravování.



Výkonem spisové služby je zajištění odborné správy dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností. Spisovou službu vykonávají všechny obce. Většina obcí se také může rozhodnout, zda spisovou službu povede v listinné nebo elektronické formě.

Posouzení z pohledu ochrany osobních údajů:

Kmenovou součástí výkonu spisové služby je i v případě obcí několik dílčích zpracování osobních údajů, které je ovšem možné posuzovat souhrnně právě jako výkon spisové služby: zákon výslovně uvádí jmenný rejstřík určený pro vyhledávání, ověřování a automatické zpracování údajů o adresách odesílatelů a adresátech dokumentů evidovaných v evidenci dokumentů spisové služby.

V kontextu nové právní úpravy ochrany osobních údajů se v rámci auditu osobních údajů provádí také revize spisového a skartačního plánu, zejména skartačních lhůt. V této souvislosti může obcím posloužit metodika vydaná Ministerstvem vnitra ČR, která obsahuje vybrané právní předpisy, stanovující povinnosti v souvislosti s ukládáním dokumentů. Po provedení revize spisového řádu by měly obce využít konzultace s příslušným archivem. Vyřazování dokumentů je povinností i v současné době. Likvidace dokumentů se realizuje až po ukončení skartačního řízení. Pro zpracování osobních údajů, na které se přímo váže skartační lhůta, platí, že nemohou být po dobu této lhůty a po dobu realizace na tuto lhůtu navazujícího skartačního řízení na základě žádosti subjektu údajů smazány. K výmazu dochází automaticky po realizaci skartačního řízení a pouze v případě, že příslušné dokumenty nebyly vybrány za archiválie a jako takové předány k archivaci příslušnému archivu. Pokud by došlo k vymazání osobních údajů během skartační doby, původce by se dopustil přestupku podle zákona o archivnictví a spisové službě.

Účel zpracování osobních údajů:

Základním účelem zpracování údajů v průběhu uložení dokumentů (a po dobu do dosažení skartační lhůty) je zajištění výkonu spisové služby v rozsahu stanoveném zákonem o archivnictví a spisové službě a případně dalšími zákony, které zpravidla stanoví rozsah a délku uchování jednotlivých částí dokumentace. Po uplynutí skartační



lhůty a následné realizaci skartačního řízení (které by mělo být podrobně popsáno ve spisovém řádu organizace) je účelem resp. operací zpracování zejména skartace dokumentů v souladu se spisovým řádem obce, který obsahuje i spisový a skartační plán. Pro skartaci je primárně využíván právní titul plnění právních povinností obce jako správce osobních údajů, tedy důvod pro zákonnost zpracování zakotvený v čl. 6 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů. Rozsah zpracovávaných osobních údajů:

Rozsah zpracování osobních údajů po dobu běhu skartační lhůty, tedy pro účely uložení dokumentů, je dán vždy rozsahem zpracování pro účely příslušné agendy obce a v průběhu období uložení dokumentů se nikterak nemění; rozsah údajů ve jmenném rejstříku údajů o odesílatelích a adresátech přitom taxativně stanoví zákon o archivnictví a spisové službě (§ 64) a obce se od tohoto rozsahu shromažďovaných a zpracovávaných osobních údajů tedy nemohou odchýlit. Po uplynutí skartační lhůty se dokumentace skartuje. V souvislosti se správným naplňováním zásady omezeného uložení osobních údajů (např. v případě zaměstnaneckých spisů) by však obec měla dbát na to, aby skartační lhůty pro jednotlivé části spisu tam, kde je to vzhledem ke správnému naplnění zásady omezeného uložení údajů vhodné a účelné, byly nastaveny diferenciovaně pro jednotlivé části spisu v návaznosti na zákonné povinnosti obce jako zaměstnavatele při uchovávání jednotlivých druhů informací vedených o bývalých zaměstnancích.

Příklady:

- Mzdové listy zaměstnanců musejí být dle zákona o účetnictví uchovány nejméně po dobu pěti let po skončení pracovního poměru.
- Všechny podklady pro účely důchodového pojištění, a to včetně mzdových listů a jiných podkladů potřebných pro účely stanovení nároku na dávky důchodového pojištění, musejí být dle zákona o důchodovém pojištění uchovány nejméně po dobu 30 let po kalendářním roce následujícím po roce, kterého se týkají. Proces zpracování osobních údajů:

Relevantními procesy zpracování jsou všechny procesy zpracování osobních údajů přímo vázané na výsledky realizace skartačního řízení, tedy zejména skartace (tedy výmaz dokumentů obsahujících i osobní údaje po uplynutí doby, po kterou je jejich



zpracování nezbytné) a výběr archiválií (tedy zpracování osobních údajů pro účely správy archiválií a jejich následné archivace, která však probíhá mimo obec jako původce archiválií). Pravidla pro zpracování osobních údajů:

V průběhu činností spojených s vedením spisové služby musí být naplněno několik zásad a požadavků GDPR:

- Doložitelnost průběhu zpracování osobních údajů
- Povinnost vést záznamy o zpracování osobních údajů
- Povinnost zavést organizační opatření pro zajištění zabezpečení zpracování osobních údajů
- Zákonnost, transparentnost a korektnost zpracování osobních údajů
- Zajištění zabezpečení zpracování osobních údajů

Práce s uloženými dokumenty může být relevantní především v případě, že subjekt údajů uplatní své právo na přístup k osobním údajům a jako odpověď na tento požadavek musí získat kompletní přehled zpracování svých osobních údajů, a to včetně těch, které jsou uchovávány ve spisovně. Je tedy důležité mít dobře zmapováno, jaké osobní údaje a za jakými účely jsou ve spisovně uloženy a jaká je lhůta, po kterou je jejich uchovávání legitimní. S procesy uchování a následné skartace dokumentů samozřejmě souvisí i právo subjektů údajů na výmaz údajů bezprostředně poté, co pomine potřeba jejich zpracování vzhledem k danému účelu zpracování. Skartační lhůty by se optimálně měly krýt s expirací právního titulu pro zpracování údajů a v rámci přípravy na účinnost obecného nařízení lze tedy jen doporučit, aby si obce zrevidovaly obecné předpisy rozhodné pro uplatnění práva na výmaz (tj. zejména spisový řád, jehož součástí by měl být i spisový a skartační plán) a současně i dbaly na důsledné plnění pravidel v jednotlivých případech. Kdo má ke zpracovávaným osobním údajům přístup:

K dokumentaci obsahující osobní údaje by v průběhu jejího uložení měl mít přístup pouze pracovník anebo úsek pověřený v rámci obecního úřadu plněním povinností na úseku archivace. Stejně jako v ostatních případech zpracování osobních údajů je třeba v rámci zachovávání zásady důvěrnosti zpracování zajistit, aby osobní údaje nebyly zpřístupňovány širšímu okruhu osob, než je vzhledem k danému účelu zpracování nezbytné.



Příklady dobré praxe při řešení modelové situace:

Ve spisovém řádu obecního úřadu byl přesně vymezen vztah povinností obce v průběhu uložení a při skartaci k realizaci práv subjektů údajů dle GDPR, tedy zejména práva na informace a přístup k údajům a na výmaz údajů.

V rámci nastavených pravidel pro výmaz údajů byly přesně vymezeny situace, kdy výmaz nelze provést pro kolizi s povinnostmi obce v oblasti spisové služby. Příklady špatné praxe při řešení modelové situace: Osobní údaje, u nichž běžela skartační lhůta, byly vymazány na základě žádosti občana ještě před uplynutím této lhůty a nebo před dokončením skartačního řízení či mimo skartačního řízení

Na základě žádosti o informace a následně uplatněnou žádost o přístup k údajům občan obdržel úplný výpis osobních údajů, které o něm obec vedla včetně informací o způsobu jejich zpracování mimo údaje, které byly v době jeho žádosti již archivovány

14.8.2 Kontrolní činnost

V rámci kontrolní činnosti je třeba se zaměřit na vzájemné postavení obce jako správce osobních údajů a současně kontrolovaného orgánu, na postavení kontrolního orgánu jako samostatného správce osobních údajů, který mimo obec jako primárního správce samostatně rozhoduje o způsobu zpracování údajů a současně na ochranu práv osob, jejichž osobní údaje jsou součástí kontrolované dokumentace, jako subjektů osobních údajů.

Posouzení z pohledu ochrany osobních údajů:

Při kontrole kontrolující přichází téměř vždy do styku s osobními údaji třetích osob, a to často i s údaji

citlivého charakteru nebo dokonce s osobními údaji zvláštních kategorií. Zatímco zpracování osobních údajů, např. jejich ověřování je pro průběh vlastní kontroly nevyhnutelné a je nutné je realizovat v rámci plnění právních povinností kontrolujícího orgánu, je velmi důležité, aby kontrolní orgán uvážil, zda je nezbytné i jejich uvádění v kontrolní zprávě. Úvodem popisu této modelové situace je zapotřebí konstatovat, že procesy zpracování osobních údajů v průběhu provádění veřejnoprávních kontrol se oproti nyní platné právní úpravě nikterak zásadně nemění.

Účel zpracování osobních údajů:



Účelem zpracování osobních údajů (za předpokladu, že k němu vůbec dochází – v řadě případů totiž kontrolní orgán pouze nahlédne do dokumentace obsahující osobní údaje a dále je v rámci provádění kontroly nezpracovává) zde bude kromě standardního zpracování osobních údajů ve spisové službě realizace kontrolní činnosti a k tomuto účelu je zapotřebí, aby obec:

- Vedla tento typ/skupinu účelů zpracování v patnosti při plnění své evidenční povinnosti
- Informovala o tomto druhu možného zpracování osobních údajů dotčené subjekty údajů, a to optimálně v obecné rovině (a to i formami umožňujícími dálkový přístup – tedy např. na webu obce).

Zákonnost zpracování osobních údajů pro účely výkonu kontrolní činnosti (pokud se veřejnoprávních kontrol týče) je dána zejména na základě právního titulu dle čl. 6 odst. 1 písm. e) GDPR – zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci. Může však dojít i k situacím, kdy právním titulem bude plnění právní povinnosti (tedy právní titul dle čl. 6 odst. 1 písm. c) GDPR) – a to v případě postupu dle § 8 písm. c) kontrolního řádu, kdy má kontrolující právo seznamovat se s podklady a kontrolní orgán naopak plní právní povinnosti poskytnout součinnost při naplňování tohoto práva.

Rozsah zpracovávaných osobních údajů:

Osobní údaje by stejně jako v rámci ostatních agend obce měly být zpracovávány pouze v rozsahu nezbytně nutném pro realizaci daného účelu zpracování, tedy pro provedení kontroly a eventuálního navazujícího správního řízení o uložení opatření k nápravě. V průběhu kontrolní činnosti je tedy

nutné, aby kontrolní orgán měl na straně jedné k dispozici veškerou dokumentaci obsahující i osobní údaje, avšak na straně druhé obvykle není nutné, aby osobní údaje dále zpracovával, natož pak např. jejich zveřejněním. I zde je tedy zapotřebí dodržovat zásadu minimalizace zpracování osobních údajů ve vztahu k efektivitě kontrolní činnosti.



Proces zpracování osobních údajů:

Relevantními procesy zpracování osobních údajů jsou zde v obecné rovině všechny úkony směřující k realizaci kontrolní činnosti. S těmi souvisí např. seznamování se s osobními údaji v průběhu kontroly nebo uvádění osobních údajů v kontrolní zprávě.

Pravidla pro zpracování osobních údajů:

Na zpracování osobních údajů v souvislosti s kontrolní činností je třeba aplikovat všechny zásady

GDPR (viz Průvodce pro přípravu obcí na GDPR).:

Každý subjekt, jehož údaje jsou shromažďovány, má právo být informován o podstatných náležitostech zpracování jeho osobních údajů. Tato informace mu může být doručena buď individuálně (osobně, e-mailem) nebo i v obecné rovině (způsobem umožňujícím dálkový přístup – např. na webu obce apod.). Obec je rovněž povinna poskytnout informace o zpracování na žádost subjektu údajů. Subjekt osobních údajů se taktéž může obrátit na pověřence pro ochranu osobních údajů (DPO) s dotazy či žádostmi o vysvětlení. Subjekt má právo na opravu nepřesných nebo doplnění neúplných údajů. Ve zvláštních případech může subjekt údajů požadovat omezení zpracování. Právo na výmaz se však na toto zpracování neuplatní (čl. 17 odst. 3 písm. b) GDPR). Rovněž se v případě tohoto zpracování neuplatní právo na přenositelnost osobních údajů k jinému správci. Na obec dopadají v obecné rovině veškeré povinnosti správce osobních údajů, zejména je povinna podrobnosti o zpracování osobních údajů pro účely kontrolní činnosti zanést do evidence zpracování (záznamů o činnostech zpracování), zajistit odpovídající zabezpečení a omezení přístupu k osobním údajům pouze pro příslušné osoby a v případě eventuálního bezpečnostního incidentu na poli ochrany osobních údajů, který by se udál v průběhu kontroly, takový incident zdokumentovat, ohlásit Úřadu pro ochranu osobních údajů a případně oznámit dotčeným subjektům.

V souvislosti s návrhem zákona o zpracování osobních údajů je zapotřebí upozornit, že se ustanovení obecného nařízení o právech subjektů údajů a povinnostech správců a zpracovatelů použijí přiměřeně nebo se splnění povinností správce nebo zpracovatele nebo uplatnění práva subjektu údajů stanovených těmito články odloží, je-li to nezbytné



a svým rozsahem přiměřené k zajištění dohledové, kontrolní nebo regulační funkce spojené s výkonem veřejné moci, tedy i k výkonu kontrolní činnosti.

Příklady:

- Zpracování osobních údajů, např. jejich ověřování, je pro průběh vlastní kontroly nevyhnutelné.
- Za předpokladu, že se např. smlouva nebo jiný dokument zahrnující i osobní údaje třetí strany stane součástí spisu, není nutné, aby byl dotčený subjekt údajů v průběhu provádění kontroly o tomto informován nebo snad aby k tomu dokonce udělil svůj souhlas. Jako relevantní právní titul pro takový způsob nakládání s osobními údaji lze použít výkon veřejné moci a na možné předání kontrolním orgánům jako příjemcům údajů pamatovat v obecné informaci určené subjektům údajů publikované na webové stránce obce nebo v ustanoveních smluv s nimi uzavíraných.
- Na druhou stranu by měl kontrolní orgán zvážit, zda je nezbytné i jejich uvádění v kontrolní zprávě. Většinou je totiž možné osobní údaje třetích osob anonymizovat, což je zvláště důležité tehdy, kdy jsou závěry kontroly projednávány veřejně, například při zasedání zastupitelstva obce.
- Zvláštní pozornost by měla být věnována zejména osobním údajům zvláštních kategorií jako citlivým osobním údajům, tedy např. údajům o zdravotním stavu, sociálním postavení třetích osob aj.

Kdo má ke zpracovávaným osobním údajům přístup:

Zpracování osobních údajů za účelem kontroly se dotýká zejména kontrolních orgánů provádějících veřejnosprávní kontrolu jako příjemců osobních údajů, jejichž ověření nebo zpracování je zapotřebí k provedení kontroly. Do kontroly jsou rovněž zapojeny ostatní oddělení nebo úseky, jichž se výkon kontroly týká.

Příklady dobré praxe při řešení modelové situace:

Ne vždy stačí anonymizovat pouze jména osob, zvláště v menších obcích je totiž možné osoby identifikovat i podle jiných znaků např. počtu dětí, zdravotního handicapu apod. Pokud je to tedy možné, publikované informace o provedení kontroly by neměly obsahovat žádné osobní údaje včetně těch, které mohou vést k nepřímé identifikaci



dotčených osob. Minimalizace osobních údajů v protokolu o kontrole spolu s jejich pseudonymizací.

Příklady špatné praxe při řešení modelové situace:

Uvedení konkrétních jmen a dalších zpracovávaných osobních údajů, případně celých kontrolovaných evidencí v protokolu o kontrole nebo jeho příloze (v případech, kdy se pro účely výsledků kontroly lze omezit na obecné konstatování o oblasti kontroly a zjištěných pochybení bez identifikace osoby

14.8.3 Správní řízení

Podle správního řádu postupují orgány územních samosprávných celků, pokud rozhodují o právech, právem chráněných zájmech nebo povinnostech, ale i při veškerých postupech v oblasti veřejné správy, které jsou výkonem veřejné moci, pokud zvláštní zákon nestanoví jiný postup. Subsidiárně se správní řád nejčastěji uplatňuje v přestupkovém řízení a nově také mohou obce ve správním řízení povolovat např. umístění hazardních her na svém území, resp. vydávat povolení k umístění herního prostoru. Obce dále vydávají celou řadu správních rozhodnutí na úseku územního a stavebního řízení, ochrany životního prostředí aj. Základní pravidla pro nakládání s osobními údaji účastníků řízení však budou pro všechny tyto typy společná a budou se řídit obecným nařízením o ochraně osobních údajů a související národní právní úpravou.

Posouzení z pohledu ochrany osobních údajů:

Ochrana osobních údajů ve správním řízení je povětšinou záležitostí obcí s rozšířenou působností, avšak musí jí věnovat pozornost i všechny ostatní obce, neb každá obec může vést správní řízení. Obce musejí pro postup podle správního řádu přijmout dostatečná technická a organizační opatření pro zajištění ochrany osobních údajů osob, vůči nimž postup směřuje. Z pohledu organizačních opatření jde především o vnitřní předpisy, které jsou blíže popsány v samostatné životní situaci, stejně tak jsou samostatně popsána technická opatření týkající se především zabezpečení zpracování osobních údajů. Úvodem popisu této modelové situace je zapotřebí konstatovat, že procesy zpracování osobních údajů v průběhu správních řízení se oproti nyní platné právní úpravě nikterak zásadně nemění.



Účel zpracování osobních údajů:

Základním účelem zpracování údajů je zde naplňování povinností obce realizovaných v rámci její působnosti ve formě správního rozhodování. Tento základní účel zpracování údajů by měl být zahrnut v evidenci zpracování údajů vedené v souladu s čl. 30 GDPR obcí jako správcem a současně tvoří základ pro zákonnost zpracování.

Ta je v průběhu správního řízení primárně dána zejména plněním právní povinnosti obce (tedy právní titul dle čl. 6 odst. 1 písm. c) obecného nařízení). V některých případech, a to tam, kde obec nemá povinnost rozhodnout o určité záležitosti ve správním řízení nebo vydat správní rozhodnutí, připadá v úvahu i provádění úkolu ve veřejném zájmu nebo při výkonu veřejné moci (tedy dle čl. 6 odst. 1 písm. e) obecného nařízení o ochraně osobních údajů).

Rozsah zpracovávaných osobních údajů:

Stejně jako i v jiných případech, je obec povinna držet se zásady minimalizace zpracování osobních údajů a osobní údaje zpracovávat pouze v rozsahu, který je nezbytně nutný pro realizaci daného řízení, resp. který je dán zákonem. V případě, kdy jsou jí předány osobní údaje v rozsahu širším, než je pro dané správní řízení nezbytné, je povinna vůbec nezahájit jejich zpracování. Jedinou výjimku tvoří např. běžné kontaktní údaje účastníků řízení (např. telefonní číslo), které může obec s vědomím účastníků držet a využívat z důvodu usnadňování výkonu veřejné moci a/nebo naplňování veřejného zájmu na usnadnění komunikace s účastníky.

Příklady:

- Pro účely správního řízení je zapotřebí samozřejmě naprosto jasně identifikovat osobu, které se rozhodnutí týká, každý z účastníků řízení tedy musí být identifikován nejméně svým jménem, příjmením, datem narození a místem trvalého pobytu, případně jiným údajem podle zvláštního zákona (viz § 18 odst. 2 správního řádu).

- V rámci správního řízení obec dále krom osobních údajů účastníků řízení zpracovává i osobní údaje dalších osob, kterými jsou např. zástupce účastníka, svědek, osoba uvedená v listině předložené k provedení důkazu, nestranná osoba přítomná u provedení důkazu, osoba uvedená v protokolu o úkonech ve správním řízení, znalec, osoba, která prokázala právní zájem nahlížet do spisu



- Pro účely rozhodování o právech a povinnostech účastníků je zapotřebí také dalších informací, které mohou obsahovat i osobní údaje, na kterých stojí správní rozhodnutí. Může jít např. o údaje o jejich ekonomické nebo rodinné situaci (pro účely rozhodnutí o poskytnutí sociální pomoci nebo dávky státní sociální podpory) nebo majetku (pro účely vydání povolení o kácení dřevin nebo stavebního povolení).

- Pro účely správního řízení obvykle nebude nutně zapotřebí pracovat s číslem účtu, telefonním číslem a dalšími obdobnými osobními údaji. Jejich zpracování buď musí obec odůvodnit nezbytností pro účely vydání správního rozhodnutí, nebo je vůbec nezpracovávat. V případě, kdy by zpracování údajů bylo vzhledem k danému účelu (realizace správního řízení) zjevně nadbytečné, obec není oprávněna údaje vůbec zpracovávat (a to ani se souhlasem dotčeného subjektu údajů, resp. účastníka správního řízení), neboť by to bylo v rozporu se zásadou minimalizace zpracování osobních údajů a principem standardní ochrany osobních údajů.

Proces zpracování osobních údajů:

Relevantní procesy zpracování jsou dány správním řádem a dalšími právními předpisy, které upravují činnost obce při správním rozhodování při výkonu jejich působnosti. Jde o všechny procesy zahrnující zpracování osobních údajů v průběhu činností spojených s daným správním řízením.

Pravidla pro zpracování osobních údajů:

V průběhu činností spojených se správním řízením musí být naplněny zejména tyto zásady a požadavky obecného nařízení o ochraně osobních údajů:

- Doložitelnost průběhu zpracování osobních údajů v rámci naplňování zásady transparentnosti zpracování údajů
- Povinnost vést záznamy o zpracování osobních údajů, resp. pracovat s typovým určením zpracování osobních údajů pro účely správního rozhodování v pravomoci obce v rámci naplňování evidenční povinnosti
- Povinnost zavést organizační opatření pro zajištění zabezpečení zpracování osobních údajů v rámci naplňování zásady bezpečnosti zpracování údajů



- Povinnost v rámci zásady minimalizace zpracování osobních údajů zpracovávat pro účely správního řízení pouze penzum osobních údajů, jejichž zpracování je ve vztahu k danému správnímu řízení nezbytné.

Subjekty údajů, resp. účastníci správních řízení také mají právo na informace o tom, jaké jeho osobní údaje a jakým způsobem obec o nich zpracovává. Tato informace jim může být doručena buď individuálně (osobně, e-mailem) nebo i v obecné rovině (způsobem umožňujícím dálkový přístup – např. na webu obce apod.). Subjekty údajů není zapotřebí znovu informovat o skutečnostech, které již ví anebo mají možnost se s nimi seznámit – pokud jsou tedy informace součástí formuláře žádosti nebo podání žadatele, není zapotřebí již znovu informaci žadateli poskytnout. V úvahu přichází také právo účastníka správního řízení na opravu či aktualizaci osobních údajů, které jsou zpracovávány nepřesně či neúplně. Naopak velmi zřídka až vůbec se nebude uplatňovat právo na výmaz údajů, neboť pro účely správního rozhodování je obec oprávněna zpracovávat údaje pouze v rozsahu nezbytně nutném pro realizaci správního řízení a uchovávat je po dobu běhu skartační lhůty podle předpisů v oblasti archivnictví a spisové služby. Tomu by měl odpovídat rozsah zpracovávaných osobních údajů i nastavená skartační lhůta. Právo na výmaz by tedy bylo možné uplatnit pouze v případech, kdy skartační lhůta nebyla dodržena.

Kdo má ke zpracovávaným osobním údajům přístup:

Pro účely správního řízení by jak k osobním údajům ve spisu obsaženým, tak i ke spisu jako takovému, měl mít přístup pouze přesně vymezený okruh osob, které se podílejí na správním rozhodování v gesci obce a do jejichž pracovní náplně spadá činnost obce v přenesené působnosti při realizaci správních řízení. Stejně jako v ostatních agendách tedy není na místě, aby k těmto informacím měl přístup neomezený okruh zaměstnanců obecního úřadu anebo okruh osob, který je širší než výčet osob, které se podílejí na správním rozhodování obce anebo jsou v souladu se správním řádem oprávněny k nahlížení do spisu.

Příklady dobré praxe při řešení modelové situace:

Úprava správního rozhodnutí před jeho zveřejněním tak, aby obsahovalo co do identifikace účastníků řízení jen nezbytné osobní údaje osoby, jíž se správní rozhodnutí týká, kterými jsou:



jméno, příjmení, datum narození a místo jejího trvalého pobytu.

U zveřejňování rozhodnutí v přestupkových věcech, pokud jsou z jakéhokoli důvodu zveřejňovány, vždy striktní anonymizace všech osobních údajů. Jedinou výjimku tvoří rozhodnutí o přestupcích veřejně činných osob (je dán veřejný zájem na sledování zákonnosti jednání voleného zástupce /veřejně činné osoby).

Příklady špatné praxe při řešení modelové situace:

Publikace úplného textu správních rozhodnutí obce včetně osobních údajů osob, jichž se správní řízení týkají, na webové stránce obce.

14.8.4 Činnost obecních knihoven

Na rozdíl od obcí, mateřských nebo základních škol nejsou obecní nebo školní knihovny orgánem veřejné moci ani veřejným subjektem ve smyslu zákona o zpracování osobních údajů. Neplatí pro ně tedy povinnost jmenovat pověřence pro ochranu osobních údajů, ale to vůbec neznamená, že se jich nařízení o ochraně osobních údajů netýká. Zvláště pokud knihovna není samostatnou právnickou osobou, ale organizační složkou obce nebo školy. Pak se pověřenec školy, resp. obce bude zabývat i způsoby, jakými knihovna zpracovává osobní údaje.

Knihovna, z podstaty nakládá s osobními údaji svých čtenářů a zaměstnanců, případně dalších osob. Zvláště v obcích a menších městech neplní knihovna jen funkci místa, kde se půjčují knihy, ale také úlohu informačního, kulturního a společenského centra obce. Podrobnosti poskytování knihovnických a informačních služeb stanoví knihovní řád (v návaznosti na § 4 zákona č. 257/2001 Sb., o knihovnách). V tomto řádu by mělo tedy být upraveno, jak knihovna a za jakým účelem eviduje půjčování knih, jak poskytuje informace, a případně i ceník služeb knihovny, pokud je poskytuje za úhradu. Současně může být v knihovním řádu upraveno i poskytování dalších služeb knihovny, například umožňování přístupu k placeným informacím na internetu, kulturní, výchovná a vzdělávací činnost, vydávání tematických publikací, poskytování reprografických služeb nebo poskytování bibliografických, referenčních a faktografických informací a rešerší. Zaplacením evidenčního poplatku uzavírá uživatel služeb smlouvu s knihovnou a je tedy velmi důležité upravit knihovní řád tak, aby umožňoval využívání služeb v rozsahu, který je v obci obvyklý a pro podmínky v dané obci žádoucí.



Účel zpracování osobních údajů:

Základním obecným účelem zpracování údajů bude „zajišťování činnosti obecní/školní knihovny“, může však být formulován i specificky jako jednotlivé činnosti knihovny spočívající ve „vedení osobních údajů pro účely evidence čtenářů a výpůjček knihovny“, „evidence čtenářů“, „výpůjční systém“, „poskytování informačních služeb“, „zajišťování vzdělávacích služeb“ apod. Takto je vhodné účely zpracování zanést do evidence zpracování. Právním titulem ke zpracování údajů bude v obecné rovině naplňování zákona o knihovnách, ve vztahu ke čtenářům a jiným návštěvníkům knihovny zejména smlouva čtenáře či jiného uživatele uzavřená s knihovnou, a to ve formě přistoupení ke knihovnímu řádu. Pro žádné ze způsobů zpracování, které jsou v souladu s výše specifikovaným základním účelem zpracování, kterým je realizace zákonem a knihovním řádem vymezených činností knihovny, tedy není zapotřebí souhlasu čtenářů jako subjektů údajů. To se může týkat např. i rozesílky pozvánek na akce knihovny, je-li tento způsob zpracováním součástí knihovního řádu, zapojení čtenářů do anket či průzkumů apod. V případech, kdy by tyto činnosti nebyly knihovním řádem upraveny, bylo by na místě získání souhlasu čtenářů k těmto způsobům zpracování jejich údajů.

Rozsah zpracovávaných osobních údajů:

Při zpracování osobních údajů čtenářů je třeba klást jako vždy důraz na to, aby byly shromažďované osobní údaje minimalizovány a aby jejich rozsah byl vždy v souladu se základním účelem jejich zpracování. Přihláška čtenáře nebo jiné formuláře a žádosti, které knihovna využívá při své činnosti, by tedy neměly obsahovat širší výčet osobních údajů, než ty osobní údaje, jejichž zpracování je nezbytné pro účely realizace činností knihovny.

Příklad:

Pro zajišťování výpůjček knihovny není např. nezbytné shromažďovat údaje o rodinné situaci čtenářů a o tom, zda jsou jejich rodinní příslušníky evidovanými čtenáři příslušné nebo i jiné knihovny. Dodatečný sběr těchto informací v anonymizované podobě lze nicméně realizovat a odůvodnit jej např. statistickými účely nebo oprávněným zájmem knihovny. Sběr statistických dat by však neměl být nedílnou součástí žádosti o zápis do seznamu čtenářů.



Proces zpracování osobních údajů:

O konkrétním způsobu zpracování údajů v rámci činnosti knihovny je třeba samozřejmě již při zahájení jejich zpracování informovat všechny její čtenáře nebo další osoby, jimž knihovna poskytuje své služby jako subjekty údajů; výjimkou jsou situace, kdy subjekt údajů o způsobu zpracování svých údajů již ví (a to jak z knihovního řádu, tak např. i z formuláře žádosti o poskytnutí příslušné služby, nebo i z vlastních zkušeností s fungováním knihovny). Čtenář jako subjekt údajů má také právo vznést námitku proti zpracování údajů na základě oprávněného zájmu správce nebo tehdy, pokud správce tvrdí, že jde o zpracování ve veřejném zájmu anebo pokud se jedná o profilování na základě oprávněného zájmu správce nebo veřejného zájmu. Toto právo hraje roli např. v případech realizovaného profilování čtenářů a adresné nabídky publikací k výpůjčce nebo dalších služeb v návaznosti na tyto čtenářské profily. V neposlední řadě má čtenář vždy právo na opravu či aktualizaci osobních údajů, které jsou zpracovávány nepřesně či neúplně. Pravidla pro zpracování osobních údajů:

Na každou situaci související s činností knihoven je třeba aplikovat všechny zásady GDPR, tedy zejména:

- Zjistit, zda je, v návaznosti na zásadu zákonnosti, pro držení jednotlivých osobních údajů čtenářů knihovny k dispozici právní titul. Ten bude vyjádřen zejm. přihláškou čtenáře do knihovny, smlouvou o jednorázovém využití služeb knihovny nebo přistoupením ke knihovnímu řádu.
- Ujistit se, že údaje jsou ve všech fázích jejich zpracování zpracovávány korektně a transparentně, tedy zejména že má čtenář k dispozici údaje o tom, jakým způsobem a k jakému účelu je s jeho osobními údaji nakládáno
- Zkontrolovat, zda je zpracování veškerých osobních údajů knihovnou v souladu s daným účelem zpracování, kterým je zejména vedení evidence čtenářů a výpůjček, eventuálně poskytování dalších služeb knihovny
- Zjistit, zda nejsou některé osobní údaje čtenářů zpracovávány déle, než je pro daný účel nutné, tedy zejména že jsou informace o bývalých čtenářích nebo návštěvnících knihovny po ukončení poskytování služeb knihovny skartovány



- Dbát na to, aby osobní údaje čtenářů byly zpracovávány pouze v rozsahu nezbytně nutném pro daný účel zpracování, tedy nevyžadovat od čtenářů a jiných návštěvníků údaje, které nejsou pro poskytnutí služeb knihovny nezbytné.

Kdo má ke zpracovávaným osobním údajům přístup: Při posuzování činnosti knihoven z pohledu ochrany osobních údajů a vymezení okruhu osob, které k osobním údajům mají přístup, je zejména třeba vycházet z toho, zda je knihovna:

- a) součástí obecního úřadu (např. v rámci úseku pečujícího o společenský život a kulturu obce v souladu s § 35 odst. 2 zákona o obcích)
- b) obcí zřizovanou právnickou osobou a nebo součástí obcí zřizované právnické osoby (např. školy)
- c) samostatnou právnickou osobou spolupracující s obcí.

V návaznosti na toto její právní postavení pak bude nutné vymezit okruh osob, které zpracovávají údaje čtenářů a vymezit jej v knihovním řádu nebo v jiném interním předpisu relevantním pro činnost knihovny. Stejně jako i u ostatních operací zpracování osobních údajů je nutné v rámci naplňování zásady důvěrnosti zpracování dbát na to, aby osobní údaje nebyly zpřístupněny osobám, které ve vztahu ke své pracovní náplni nemají nakládat s osobními údaji čtenářů a ostatních zákazníků knihovny.

Příklady:

- Pokud například knihovna informuje své uživatele o připravovaných kulturních, společenských či sportovních akcích v obci adresně, formou SMS nebo pomocí mailu, je to nutné uvést v knihovním řádu. V takovém případě knihovna rozesíláním adresných zpráv plní svou zákonnou povinnost zakotvenou v §4 knihovního zákona a není potřeba, aby ještě požadovala k takové činnosti souhlas daného uživatele služeb. Jinak pro knihovnu platí stejná pravidla pro nakládání s osobními údaji jako pro obec či školu.
- Upozornit je však třeba na to, že i seznam půjčené literatury, či seznam kopírovaných děl, případně písemností, může být za předpokladu, že z něj lze vyčíst informace o politickém či náboženském přesvědčení, sexuální orientaci nebo obsahuje jiné citlivé informace osobního charakteru, považován za osobní



údaj zvláštní kategorie a jeho jiné užití, než pro realizaci vlastních služeb by bylo v přímém rozporu s nařízením o ochraně osobních údajů.

- Po ukončení vztahu mezi knihovnou a uživatelem jejích služeb, v případě, že všechny vzájemné závazky byly vypořádány, eventuálně uplynula doba pro případné uplatnění nároku na náhradu škody, musejí být osobní údaje uživatele knihovny vymazány. Příklady dobré praxe při řešení modelové situace:

Knihovna zahájila novou činnost, která dosud nebyla součástí knihovního řádu – rozesílku pozvánek na své kulturní akce i na jiné společenské a kulturní akce obce čtenářům, kteří o to projeví zájem. Informaci obdrželi čtenáři prostřednictvím e-mailu a knihovnice se současně každého čtenáře ptala, zda má o tuto službu zájem. Pokud čtenář projevil zájem o rozesílku, byl informován, že přihlášení se k odběru kulturních novinek je zcela dobrovolné a lze je vzít kdykoli zpět.

Upomínky svým čtenářům zasílala knihovna vždy e-mailem (u prvních dvou upomínek) nebo písemně (u třetí upomínky). Informace o čtenářích, kteří nedodrželi výpůjční dobu, nikdy (a to ani na žádost jiných čtenářů) nezveřejňovala.

Příklady špatné praxe při řešení modelové situace:

Knihovna na svém webu publikovala evidenci výpůjček. Protože šlo o malou obec, v rámci evidence výpůjček zveřejňovala, a to bez souhlasu čtenářů, informace o aktuálním vypůjčitel s cílem umožnit ostatním čtenářům dohodnout si s ním, kdy knihu hodlá vrátit.

S cílem ušetřit kapacitu i finance na rozesílání upomínek knihovna na své nástěnce i na svém webu publikovala informace o čtenářích, kteří nedodrželi výpůjční dobu.

14.8.5 Pořádání kulturních akcí

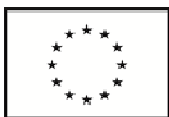
Tuto modelovou situaci je třeba posoudit ve dvou rovinách: tou první je ochrana osobních údajů v rámci propagace akce, druhou pak ex post publikace informací o proběhnuvší akci. To probíhá zejména prostřednictvím tradičních komunikačních kanálů obce – tedy webu a obecního periodika, k této tematice viz modelové situace věnované publikaci informací. Zvat na společenské, sportovní či kulturní akce je možné buď neadresně (prostřednictvím papírových plakátů, na webu obce či v obecním periodiku) nebo adresně (papírovou formou prostřednictvím letáků distribuovaných



jednotlivým občanům nebo elektronicky prostřednictvím SMS zpráv nebo e-mailem). U první formy není ochrana osobních údajů adresátů relevantní a může se týkat pouze osob na plakátech či letácích vyobrazených, jejichž práva jsou chráněna v rámci občanskoprávní ochrany osobnosti (resp. podoby a soukromí) v režimu § 84 a následujících občanského zákoníku. U adresného zasílání pozvánek prostřednictvím adresou příjemce označených písemných zásilek, e-mailů nebo SMS zpráv je zapotřebí sledovat, zda je dán právní titul pro takovou rozesílku, tedy zda lze očekávat zájem občanů o takovouto službu v souladu s místními předpoklady a s místními zvyklostmi. Pokud místní předpoklady a zvyklosti nezahrnují takový způsob komunikace s občany, bude zapotřebí pro rozesílku získat souhlas dotčených občanů. Naopak pokud místní potřeby a zvyklosti tento způsob komunikace (zejm. pokud se elektronické komunikace s občany týče) zahrnují, bude možné rozesílku posoudit jako naplňování zákonného zmocnění obce zakotvené v § 35 odst. 2 zákona o obcích – tedy vytvářet podmínky pro uspokojování potřeb svých občanů mj. v oblasti celkového kulturního rozvoje obce, a tedy plnění úkolu ve veřejném zájmu.

Účel zpracování osobních údajů:

Základním účelem zpracování osobních údajů zde bude uspořádání kulturní nebo společenské akce a s tím související nakládání s osobními údaji pozvaných a zúčastněných osob. Účel zpracování vždy souvisí s dodržением zásady zákonnosti zpracování, v případech zvaní, organizace programu akcí nebo rekapitulaci jejich výstupů je však vždy nutné věnovat pozornost tomu, zda je zpracování informací k dispozici příslušný právní titul, tedy buď zda je taková rozesílka informací v souladu s místními potřebami a zvyklostmi (a pak se lze opřít o naplňování zákona o obcích a plnění zákonné povinnosti obce – viz výše) a nebo zda, pokud místní potřeby a zvyklosti neodůvodňují takovou rozesílku, jde o rozesílku takových informací a takovým způsobem, že to lze odůvodnit oprávněným zájmem obce (a jako podklad pro zákonnost takového postupu se opřít o čl. 6 odst. 1 písm. f) obecného nařízení). V případě, že je právním titulem pro zpracování osobních údajů vyjádření oprávněného zájmu obce, je pak třeba upozornit i na možnost podat námitku proti takovému zpracování osobních údajů v souladu s čl. 21 odst. 1 obecného nařízení. V tomto ohledu je vždy třeba vycházet z přiměřenosti konkrétního způsobu oslovení pro daný účel – pokud se jedná skutečně o výjimečnou událost a písemné obeslání občanů na jejich



poštovní adresy nebo pokud je úzká komunikace (zejména malé) obce s jejími občany v souladu s místními potřebami a zvyklostmi, může postačit odkaz na zákon o obcích a obec může využít jako právního titulu naplňování veřejného zájmu, resp. činění úkolu ve veřejném zájmu. Naopak pokud se týče pravidelného oslovování s pozvánkami na společenské akce formou SMS zprávy v prostředí zejména větších obcí, odkaz na zákon o obcích velmi pravděpodobně neobstojí a k adresné rozesílce pozvánek bude zapotřebí buď přesvědčivé argumentace oprávněným zájmem obce, nebo (v prostředí velkých obcí) souhlasu oslovených osob.

Pokud se týká zapojení občanů do programu akce (tombola, zábavné soutěže apod.), je v každém případě třeba, aby občané byli odpovídajícím způsobem informováni o tom, jakým způsobem budou jejich osobní údaje zpracovány. V případech, kdy se jedná o jednorázové využití osobních údajů bez toho, aby se údaje staly součástí evidence, nejedná se o zpracování osobních údajů ve smyslu obecného nařízení o ochraně osobních údajů a pravidla pro zpracování osobních údajů se tedy na toto nakládání s osobními údaji nepoužijí. Nicméně pokud by byl seznam soutěžících po ukončení tomboly či soutěže i po jejím skončení evidován, je zapotřebí k této evidenci (která již je zpracováním osobních údajů) přiřadit odpovídající právní titul. Tím může být ochrana oprávněného zájmu obce jako pořadatele soutěže před eventuálními reklamacemi výsledků nebo uplatnění nároků osob, které v soutěži nevyhrály. I o tomto zpracování údajů je zapotřebí dotčené osoby transparentně informovat, a to buď individuálně, nebo odkazem na pravidla soutěže či tomboly a zpracování osobních údajů, ke kterému při realizaci soutěže dochází.

V rámci informací o realizovaných akcích, které jsou publikovány ve zpravodajské rubrice na webu anebo v obecním periodiku způsobem, který je obdobný novinářské činnosti, je pak možné využít zpravodajskou licenci upravenou v § 16 odst. 1 zákona o zpracování osobních údajů a ani zde tedy není zapotřebí žádat o souhlas dotčené subjekty údajů. I při této příležitosti je vhodné připomenout, že v souvislosti s publikací textových a obrazových informací (fotografií) obsahujících osobní údaje může dojít ke kombinaci režimu občanskoprávní ochrany osobnosti, resp. podoby a soukromí zakotvené v § 84 občanského zákoníku (tam, kde se jedná o publikaci fotografií nebo jiných obrazových záznamů) a režimu ochrany osobních údajů (tam, kde se jedná o mluvené či psané informace obsahující osobní údaje). U fotografií a jiných obrazových



záznamů se tak krom zpravodajské licence může uplatnit i svolení fyzické osoby s pořízením fotografie za okolností, z nichž je zřejmé, že budou dále šířeny (viz § 85 občanského zákoníku). Opět je však třeba nezapomínat na transparentní sdělení informace o způsobu publikace dotčeným subjektům údajů (v případech, kdy o něm již nejsou informovány).

Právním titulem ke zpracování údajů bude tedy obvykle plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci (čl. 6 odst. 1 písm. e) obecného nařízení) spolu s naplňováním zákonného zmocnění obce pečovat o naplňování potřeb svých občanů, a to včetně potřeb kulturních (viz § 35 odst. 2 zákona o obcích). Při publikaci informací způsobem obdobným novinářské činnosti (v obecním periodiku, v reportážní rubrice obecního webu apod.) pak postačí novinářská licence jako aditivní právní titul upravený v § 16 odst. 1 zákona o zpracování osobních údajů. V krajním případě však může být zapotřebí i souhlasu subjektu údajů (tam, kde se pracuje s individuálními kontakty, jmény anebo fotografiemi jednotlivých občanů), resp. svolení s využitím fotografie udělené v režimu pravidel pro ochranu podoby fyzické osoby upravené v občanském zákoníku (tam, kde se jedná pouze o využití fotografie).

Příklady:

- Pokud obec pořádá ples nebo sportovní utkání, obvykle na ně zve neadresně na svém webu, na obecních plakátovacích plochách a/nebo v obecním periodiku. Ať již jsou nebo nejsou součástí takové pozvánky osobní údaje konkrétních subjektů (např. jméno tanečního mistra, který povede předtančení, jméno rozhodčího u fotbalového utkání nebo jméno a fotografie vystupujícího umělce), není k tomu zapotřebí žádat o souhlas těchto osob jako subjektů údajů. Dotčené osoby by však o takovém zveřejnění svých jmen nebo podobenek měly být v rámci ochrany svých osobnostních práv informovány (tam, kde se jedná o konkrétní jména a fotografie osob). Jde-li o fotografie ilustrační, lze je přiměřeným způsobem publikovat v rámci realizace novinářské/reportážní licence.



V rámci distribuce adresné (e-maily, SMS zprávy) je nutné posoudit zda:

- a) Místní podmínky a potřeby odůvodňují takovou komunikaci s občany obce v rámci naplňování jejich kulturních potřeb v souladu se zákonem o obcích – pak by právním titulem ke zpracování údajů bylo činění úkolu obce ve veřejném zájmu.
- b) V případech, kdy místní podmínky a potřeby takový kontakt neodůvodňují, odůvodnit informování o aktuálním dění v obci prostřednictvím daného komunikačního kanálu oprávněným zájmem obce.

V obou těchto případech je třeba mít na mysli, že subjekt údajů má právo vznést námitku proti zvolenému způsobu zpracování svých osobních údajů a obec jako správce údajů by tedy byla povinna se dalšího zpracování údajů zdržet.

- V rámci organizace programu akce není nutné, aby osoby, které se stanou dobrovolně součástí akce, k tomu udělovaly svůj explicitní souhlas, neb jejich osobní údaje se obvykle nestávají součástí evidence a nejedná se tedy o zpracování údajů ve smyslu GDPR. Ani pokud by však obec uvažovala např. o publikaci jmen výherců, jmen vítězných či skórujících sportovců apod. v rámci rekapitulace výstupů z akce na svém webu nebo v obecním periodiku, která je svým obsahem obdobná novinářské činnosti, souhlasu nebude zapotřebí, neb případy jsou kryty tzv. novinářskou neboli zpravodajskou licenci.
- V případě obeslání občanů obce a bývalých občanů obce s pozvánkou na setkání rodáků lze tuto událost zahrnout pod události v životě obce, jejichž realizací obec naplňuje potřeby svých občanů a lze je tedy pokrýt naplňováním veřejným zájmu v návaznosti na zmocnění formulované v § 35 odst. 2 zákona o obcích. S využitím této argumentace lze proto účastníky obeslat i bez jejich předchozího souhlasu.

Rozsah zpracovávaných osobních údajů:

Osobní údaje lze zpracovávat pouze v rozsahu a míře přiměřené danému účelu, jímž je zde uspořádání kulturní či společenské akce včetně distribuce pozvánek na a výstupů z akce:

- Pro účely adresné distribuce pozvánek si tedy lze představit práci s poštovními i e-mailovými adresami a telefonními čísly zájemců o takové informace,



- Pro účely publikace anebo dalšího použití výstupů z akce budou nejdůležitějšími osobními údaji jméno a příjmení, případně věk a místo bydliště zúčastněných osob (pokud je to vzhledem k obsahu informace o realizované akci nezbytné) a často i jejich podoba.

Širší rozsah zpracování osobních údajů by velmi pravděpodobně mohl být posouzen jako zpracování údajů nad rámec daného účelu a tedy jako zpracování nezákonné.

Proces zpracování osobních údajů:

Príslušné procesy zpracování je vhodné pojmenovat:

- V případě adresné distribuce pozvánek jako „rozesílka informací o dění v obci (eventuálně s upřesněním - prostřednictvím jakého komunikačního kanálu)“
- V případě zveřejnění jména a/nebo fotografie subjektu údajů v rámci informování o proběhnuvších akcích jako „zveřejnění informací o průběhu akcí pořádaných obcí“

a takto je zanést do evidence zpracování. Ke konkrétnímu způsobu zpracování informací v rámci zvaní, realizace programu a zejména publikace informací o průběhu a výstupech akce je vhodné nejprve zjistit, které operace zahrnují zpracování osobních údajů. O něm je třeba samozřejmě informovat všechny subjekty údajů, jejichž osobní údaje jsou při těchto činnostech využity a nezapomínat ani na informace o předání údajů ke zpracování třetím osobám (organizátorovi akce, grafikovi, tiskárně, fotbalovému svazu apod.). Výjimkou jsou situace, kdy dotčený subjekt údajů již má informace k dispozici. V úvahu zde také přichází právo na opravu či aktualizaci osobních údajů, které jsou zpracovávány nepřesně či neúplně.

V této souvislosti je zapotřebí zmínit rozdílný přístup při opravě či aktualizaci osobních údajů, jejichž zpracování spočívá v publikaci fotografie nebo jiného obrazového záznamu obsahujícího zachycení podoby fyzické osoby. Pokud totiž takový obrazový záznam byl pořízen v režimu ochrany osobnosti resp. podoby a soukromí dle občanského zákoníku (§ 84 a následující), tedy se svolením příslušné fyzické osoby, platí i pro opravu, aktualizaci či případný výmaz režim občanského zákoníku – tedy bylo-li svolení udělené na určitou dobu odvoláno, aniž to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, nahradí odvolávající (tedy příslušná fyzická osoba) škodu z toho vzniklou osobě, které svolení udělil (tedy obci).



Pravidla pro zpracování osobních údajů:

Na každou situaci související s distribucí pozvánek, organizací programu akce i zpětném informování o jejím konání a výsledcích je třeba aplikovat všechny zásady GDPR, tedy zejména:

- Zjistit, zda je, v návaznosti na zásadu zákonnosti, pro držení osobních údajů, které se obec chystá využít při zvaní (např. telefonní čísla nebo e-mailové adresy pozvaných osob, fotografie umělců na plakáty apod.) nebo rekapitulaci výstupů akce (kde obvykle je možné spolehnout se na zpravodajskou licenci) k dispozici právní titul
- Ujistit se, že údaje byly ve všech fázích přípravy, realizace i vyhodnocení akce zpracovány korektně a transparentně, tedy zejména že jsou dotčené subjekty údajů informovány o tom, k jakému účelu a jakým způsobem byly jejich osobní údaje využity
- Zkontrolovat, zda je způsob zpracování osobních údajů v rámci zvaní, organizace programu i rekapitulace výstupů akce v souladu s daným účelem zpracování, tedy zejména že předmětné údaje nejsou využívány k jinému účelu, než je uspořádání kulturní akce. Dbát na to, aby osobní údaje byly zpracovávány resp. zveřejňovány pouze v rozsahu nezbytně nutném pro daný účel zpracování, tedy nezpracovávat osobní údaje nad rámec údajů nutných pro uspořádání akce a zpětné informování o jejím průběhu.

Kdo má ke zpracovávaným osobním údajům přístup:

K informacím souvisejícím s pořádáním kulturních a společenských akcí a tedy i k osobním údajům v nich obsaženým by měl v rámci naplňování zásady důvěrnosti zpracování osobních údajů mít přístup pouze okruh pracovníků, kteří tyto informace potřebují pro výkon svých pracovních povinností nebo své funkce – tedy obvykle pracovníků úseku obecního úřadu pověřeného realizací kulturních a jiných společenských akcí obce, úsek sportu a jiné útvary, které zajišťuje šíření pozvánek i ex post informací o realizovaných akcích.

Relevantní je spolupráce s organizátory akcí, kteří mohou být součástí struktur obce (kulturní domy, obecní sportoviště apod.), ale mohou být také subjekty externími (např.



najatá agentura) a vystupovali by tedy v pozici zpracovatelů údajů, které obec jako správce pověřuje provedením určitého druhu zpracování údajů (zde tedy adresnou distribucí pozvánek, organizací programu zahrnující pořádání soutěží či tombol nebo dokumentací a publikací výstupů z akcí). Všechny tyto osoby by měly mít přístup ke zpracovávaným osobním údajům nebo se přímo podílet na jejich zpracování. Stejně jako i u ostatních agend je v rámci zachování zásady důvěrnosti zpracování osobních údajů zapotřebí zajistit, aby zpracovávané osobní údaje (zejm. kontakty pro účely šíření adresných pozvánek na akce) nebyly zpřístupněny neomezenému okruhu osob. V případě publikace informací o proběhnuvší akci je pak naopak zpřístupnění údajů neomezenému okruhu osob nedílnou součástí jejich zveřejnění.

Příklady dobré praxe při řešení modelové situace:

Zveřejnění ilustračních fotografií z předchozího ročníku plesu na plakátech a informačních letácích

Zveřejnění fotografie konkrétního občana na pozvánce na společenskou akci s využitím svolení uděleného v režimu občanského zákoníku (§ 85 a následující)

Zveřejnění fotografie umělce nebo jiného účinkujícího na plakátu s pozvánkou na akci na základě smlouvy o účinkování na akci

Zveřejnění jmen vítězných nebo skórujících sportovců v průběhu zápasu či akce samotné z důvodu oprávněného zájmu pořadatele akce

Zveřejnění jmen výherců v tombole na společenské akci i bez jejich souhlasu na základě oprávněného zájmu pořadatele

Skartace předmětných osobních údajů výherců i zúčastnivších se osob, které nevyhrály, ihned po ukončení akce, eventuálně využití k jinému účelu na základě oprávněného zájmu obce (obhajoba v případě uplatnění nároku na náhradu škody) anebo se souhlasem zúčastněných

Zveřejnění jmen vítězných nebo skórujících sportovců nebo výherců v tombole na společenské akci v obecním periodiku a/nebo na webu obce i bez jejich souhlasu s využitím zpravodajské licence

Příklady špatné praxe při řešení modelové situace:

Zveřejnění dehonestujících fotografií občanů z obecního plesu



Rozesílka pozvánek na kulturní akci v prostředí velké obce prostřednictvím SMS a/nebo e-mailových zpráv jednotlivým občanům i po vyjádření jejich námitek proti takovému způsobu zpracování jejich osobních údajů

14.8.6 Uveřejňování dokumentů na webu obce

Při rozhodování o zveřejnění osobních údajů na webu (obvykle buď v textové podobě, nebo formou fotografií) je nejdůležitějším momentem odlišit, zda jsou vůbec údaje získány a zpracovávány na základě legitimního účelu a zda je ke konkrétnímu zpracování údajů ve formě jejich zveřejnění dán konkrétní právní titul, kterým nejčastěji bude:

- V případě povinného zveřejňování informací plnění právní povinnosti,
- V případě zveřejňování informací o aktualitách v obci veřejný zájem na zveřejnění daných informací, resp. novinářská či reportážní licence u publikace ilustračních a reportážních fotografií,
- V případě naplňování smluvních povinností obce jím může být i plnění smlouvy,
- V případě zveřejňování individuálních fotografií, jejichž zveřejnění nelze odůvodnit existencí veřejného zájmu na jejich publikaci pak v určitých případech i oprávněný zájem obce, jehož realizace se odbyvá v režimu speciální právní úpravy – občanského zákoníku – který v § 84 a následujících stanoví pravidla pro rozšiřování podoby fyzické osoby a udělení i odejmutí svolení s pořízením a šířením záznamu této podoby anebo
- Ve zcela výjimečných případech (např. v případě publikace kontaktních údajů všech zaměstnanců obecního úřadu), explicitní souhlas subjektu údajů, jehož se zveřejňované údaje týkají. Aktuální stanovisko Odboru bezpečnostní politiky MV ČR konstatuje, že u zveřejňování fotografií nenastanou oproti stávajícímu stavu žádné revoluční novinky; problematika je totiž upravena primárně v novém občanském zákoníku. Fotografii bez souhlasu je tak možné pořídit a použít pro účely vědecké či umělecké a také pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství, to však pouze za podmínky, že se tak děje přiměřeně. Totéž obdobně platí v režimu GDPR, jde-li o automatizované zpracování informací pro novinářské účely nebo o vytváření databází informací



pro tiskové účely. Zjednodušeně lze říci, že zatímco ilustrační fotografii z plesu, kde osoby tančí nebo kde jsou přítomny známé osobnosti, jsou přiměřeným zpracováním, fotografie z plesu, kde jsou zachyceny osoby v nelichotivých pozicích pod vlivem alkoholu, již přiměřeným zpracováním nejsou (leďa by se jednalo třeba o starostu a byl zde zároveň dán veřejný zájem na informování o konkrétní události, neboť veřejně činné osoby požívají zpravidla nižší míry ochrany osobnostních práv a může být přítomen i objektivní, resp. veřejný, zájem na informování, jak se úřední osoba chová i mimo výkon funkce. V zásadě si však lze vystačit s principy slušnosti, respektu k druhému (a jeho oprávněným zájmům či legitimním přáním) a zásadou přiměřenosti.

Účel zpracování osobních údajů:

Účelem zpracování osobních údajů je zde jejich zveřejnění na webu obce. Je přitom nutné ujistit se, že pro zpracování informací určených ke zveřejnění je k dispozici příslušný právní titul, tedy že údaje jsou zpracovávány na základě zákona, smlouvy s dotčeným subjektem údajů, jsou obsahem správního rozhodnutí nebo existuje veřejný zájem na jejich zpracování. A pokud žádný z těchto právních titulů neexistuje, zda je s ohledem na rozsah zpracování údajů vhodné požádat dotčený subjekt údajů o souhlas a případně prověřit, zda byl tento souhlas před zveřejněním skutečně udělen, a to v souladu s GDPR. Teprve po spolehlivém prověření právního titulu pro zpracování údajů je možné uvažovat o zveřejnění informací obsahujících i osobní údaje.

Rozsah zpracovávaných/zveřejňovaných osobních údajů:

Osobní údaje by měly být zveřejňovány vždy v rozsahu, který je nezbytně nutný k naplnění daného účelu.

Příklady:

- Je-li shledána existence zájmu veřejnosti se zveřejněním kontaktních údajů určitého pracovníka obecního úřadu, pak postačující bude zveřejnit jeho jméno, telefonní číslo a e-mailovou adresu. Není již nutné zveřejňovat jeho fotografii (tam, kde není dán veřejný zájem na jejím zpřístupnění veřejnosti), údaj o přítomnosti zaměstnance na pracovišti a/nebo ani soukromé telefonní číslo nebo e-mailovou adresu daného pracovníka.



- Existuje-li veřejný zájem na kontrole způsobu hospodaření s veřejnými financemi, postačí pro identifikaci fyzické osoby, již byl poskytnut dar, dotace nebo jiná finanční výpomoc obce, zveřejnit základní identifikační údaje obdarovaného nebo adresáta dotace či finanční výpomoci, tedy jeho jméno a příjmení, ročník narození a adresu trvalého bydliště. Tento postup je nejen v souladu se zásadou důvěrnosti zpracování osobních údajů, ale současně je i zakotven ve speciálních právních předpisech, konkrétně v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím (tam, kde se zveřejňují na žádost informace o způsobu hospodaření s majetkem obce) a v zákoně č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů (tam, kde jsou na úřední desce obce povinně publikovány informace o příjemci dotace nebo návratné finanční výpomoci obce.)

Proces zpracování osobních údajů:

Na každou situaci související se zveřejněním informací na webu obce je třeba aplikovat všechny zásady GDPR, tedy:

- Zjistit, zda je v návaznosti na zásadu zákonnosti pro držení osobních údajů, které se obec chystá zveřejnit, k dispozici právní titul
- Ujistit se, že údaje jsou zpracovávány korektně a transparentně, tedy zejména že dotčený subjekt údajů je informován o tom, že může dojít ke zveřejnění údajů formou jejich publikace na webu obce
- Zkontrolovat, zda je zpracování, resp. zveřejnění osobních údajů v souladu s účelem zpracování
- Zjistit, zda nejsou některé osobní údaje zpracovávány resp. zveřejňovány déle, než je pro daný účel nutné
- Dbát na to, aby osobní údaje byly zpracovávány resp. zveřejňovány pouze v rozsahu nezbytně nutném pro daný účel zpracování (tedy že např. u zveřejňování informací o nově narozených dětech nejsou současně zveřejňována i jména a věk jejich rodičů či jejich bydliště).
- Mít jistotu, že osobní údaje, o jejichž zveřejnění se uvažuje, jsou zpracovávány bez chyb



- Dbát na odpovědnost obce jako správce při zpracování resp. zveřejnění předmětných údajů

Pravidla pro zpracování osobních údajů:

Co do relevantních práv subjektů údajů, v úvahu zde přichází zejména právo podat námitku proti zpracování údajů i jejich zveřejnění, pokud obec údaje zpracovává na základě veřejného zájmu. Současně se aplikuje, v případech, kdy je zveřejnění založeno na souhlasu, právo občana souhlas udělit či neudělit, ale také odvolat. V neposlední řadě má občan či zaměstnanec úřadu právo na opravu či aktualizaci osobních údajů, které jsou zpracovávány nepřesně či neúplně. Je také třeba nezapomínat na to, že pokud administraci webu zajišťuje pro obec na základě smlouvy externí subjekt, mají všichni zaměstnanci i občané, jejichž osobní údaje jsou na webu zveřejňovány, právo na informace o tom, o jaký subjekt konkrétně se jedná a o tom, že jsou mu předávány jejich osobní údaje jako příjemci údajů.

V obecné rovině platí všechny povinnosti obce jako správce údajů, zejména je třeba informaci o zveřejnění údajů zanechat jako záznam do evidence zpracování a je třeba také zajistit, aby všechny dotčené subjekty údajů (zejména občané i zaměstnanci) byly již v okamžiku zahájení zpracování údajů, tedy nejpozději v okamžiku sepsání informace určené k publikaci na webu obce minimálně o zveřejnění svých údajů informovány, a to buď způsobem umožňujícím dálkový přístup a nebo i individuálně (pokud zveřejnění probíhá na základě zákona, smlouvy, z důvodů daných veřejným zájmem nebo oprávněným zájmem obce) a nebo aby k němu přímo daly souhlas (v případě výjimečných situací, kde se jedná o zveřejnění pod souhlasem subjektu údajů). V případě poskytování informace subjektům údajů je samozřejmě vhodné zachovávat zásadu, že subjekt údajů nemusí být informován o těch skutečnostech, o nichž již ví.

Kdo má ke zpracovávaným osobním údajům přístup:

Příprava informací ke zveřejnění se týká všech úseků obecního úřadu, neb každý z nich se při své činnosti setkává s informacemi určenými ke zveřejnění. Principiálně by přístup k údajům měly mít jen osoby, kterým je v rámci organizace obce svěřena daná agenda do pracovní náplně. Může jít nejen o agendu vnitřních věcí (a zveřejňování osobních údajů o zaměstnancích obecního úřadu), agendu kultury (informace z kulturního života obce obsahující osobní údaje občanů), sportu (sportovní události a



osobní údaje oceněných, vítězných nebo skórujících sportovců), ale i informace o rozhodnutích ve správním řízení v působnosti obce (více o této agendě viz situace č. 2.15 Správní řízení). Kdykoli v případech, kdy dokumenty, údaje či obrazové materiály určené ke zveřejnění na webu obce obsahují osobní údaje, je na místě pečlivá analýza toho, zda je pro to dán odpovídající právní základ v příslušných právních předpisech (tedy jak v GDPR, tak např. i v občanském zákoníku).

Zveřejněním dotčených osobních údajů na webu obce dochází k jejich zpřístupnění blíže neurčenému okruhu osob, resp. široké veřejnosti.

Příklady:

- Pokud např. zákon o obcích obcím umožňuje získávat osobní údaje o narozených dětech nebo věku, pro účely ocenění významné životní události (§36a zákona 128/2000Sb.), neznamená to, že o této události může zcela neomezeně a bez souhlasu dotčené osoby informovat na svém webu. K této záležitosti viz stanovisko ÚOOÚ ze 24. 6. 2016: Pokud jde o možnost gratulace v místním tisku bez souhlasu dotčených osob (či jejich zákonných zástupců), Úřad považuje zapřípustné, jestliže jsou ve společenských rubrikách, např. „Blahopřejeme jubilantům naší obce“ nebo „Vítáme nové občánky naší obce“ v určitém měsíci i bez souhlasu zveřejněna pouze jména a příjmení bez jakýchkoliv dalších údajů. Pokud se obec pouze pro tuto formu ocenění významné životní události rozhodne, mělo by jít v případě blahopřání seniorům o významná životní jubilea, nikoli o každoroční zveřejňování jmen a příjmení v měsíci narození bez souhlasu jejich nositelů. K zveřejňování dalších údajů, např. věku, data narození, části obce, je však nutné, aby obec disponovala souhlasem subjektu údajů či zákonného zástupce. Ke zveřejnění fotografie pak postačí svolení s použitím obrazového zpodobnění osoby udělené v souladu s § 85 občanského zákoníku.
- Právě tak pokud zákon stanoví, že některé listiny (např. zápisy ze zastupitelstev obce, rozhodnutí rady obce) musí být uloženy k nahlédnutí občanům na obecním úřadě, neznamená to, že bez ohledu na další, zejména na právo na ochranu soukromí a důstojnosti mohou být tyto, bez dalších úprav zveřejněny na jejím webu. Příkladem může být zápis z jednání zastupitelstva – ten musí být uložen



na obecním úřadě k nahlédnutí občanům obce, a priori by však neměl být zveřejňován na webu obce a pokud již je zveřejněn, osobní údaje v něm obsažené by měly být anonymizovány.

- Obec obvykle zveřejňuje jména zastupitelů mj. na svém webu, jistě je ve veřejném zájmu zveřejnit i jejich fotografie tak, aby je občané obce poznali, a důležité je, aby je bylo možné zkontaktovat minimálně prostřednictvím obecního úřadu. I oni však mají právo na své soukromí, a obec by se měla vyvarovat zveřejňování jejich soukromých telefonních čísel, e-mailových adres a fotografií z jejich soukromého života. Naproti tomu zveřejnění fotografií z jednání zastupitelstva či jakákoli jiná dokumentace vztahující se k výkonu jejich veřejné funkce souhlas ani svolení s využitím podoby dle občanského zákoníku nevyžaduje, neb jejich publikace je kryta veřejným zájmem. V úvahu přichází i pokrytí publikace těchto fotografií tzv. reportážní neboli novinářskou (někdy uváděno i jako zpravodajskou) licenci, kterou lze posoudit jako důvod veřejného zájmu svého druhu (viz § 16 odst. 1 zákona o zpracování osobních údajů) i práva na ochranu osobnosti (§ 89 občanského zákoníku).
- Složitější je situace u zaměstnanců obce a obecního úřadu. Je nepochybné, že u obslužných profesí (řidiči, účetní, IT specialisté apod.) převládá ochrana jejich soukromí, a jejich fotografie či soukromé kontaktní údaje obec na svém webu zveřejňovat nemůže, eventuálně ke zveřejnění přistoupit může s jejich souhlasem, u jehož udělení by však obec měla přísně dbát na to, aby bylo možné jej posoudit jako svobodně udělený. Podobná situace je u všech zaměstnanců obecního úřadu, kteří zastávají pracovní pozici, u níž není z důvodu veřejného zájmu vhodné nebo nutné, aby je mohla veřejnost kontaktovat přímo. Naproti tomu tajemník nebo vedoucí pracovník, který řídí určitou agendu obce, eventuálně i pracovník, který není v řídicí pozici, avšak vykonává specifickou agendu (např. obecní strážník), mohou být v pozici, kdy je dán veřejný zájem na možnosti takového pracovníka přímo kontaktovat. Je-li tedy v zájmu veřejnosti, aby mohla daného pracovníka přímo kontaktovat, má za to, že veřejný zájem občanů převládá nad jejich právem na ochranu soukromí (viz judikatura nejvyššího soudu či zákon 159/2006 Sb. o střetu zájmů). Jejich kontakt a, je-li to



vzhledem k okolnostem vhodné či nutné, a je v zájmu veřejnosti identifikovat daného pracovníka, i fotografii tedy obec zveřejnit může.

- A co se týče informací o společenském či hospodářském životě v obci? K užití fotografií reportážních, popisujících např. pro obec významné události, a to ani na webu, obec v rámci zpravodajské licence upravené v § 16 zákona o zpracování osobních údajů souhlas nepotřebuje. Podobná je situace, pokud obec informuje např. o úspěchu žákyně místní školy a popis události doprovází fotografií dotyčné (s uvedením jejího jména) pořízené v průběhu soutěže anebo jejího vyhlášení; ani zde není souhlas zákonných zástupců dítěte nezbytný, neboť na situaci lze uplatnit zpravodajskou licenci. Příklady dobré praxe při řešení modelové situace:

Zveřejnění pracovních kontaktních údajů volených představitelů obce na základě veřejného zájmu

Zveřejnění ilustračních fotografií obsahujících i hromadné fotografie občanů v rámci dokumentace významných událostí obce na základě veřejného zájmu obce

Zveřejnění kontaktních údajů a/nebo fotografií řadových zaměstnanců obecního úřadu na základě veřejného zájmu (tam, kde je umožnění přímého kontaktu veřejnosti s pracovníkem žádoucí)

Příklady špatné praxe při řešení modelové situace:

Zveřejnění individuálních soukromých fotografií jubilantů bez jejich svolení s využitím podobizny uděleného v souladu s § 85 občanského zákoníku nebo zveřejnění fotografií nově narozených dětí bez svolení jejich zákonných zástupců

Zveřejnění jakýchkoli dehonestujících fotografií občanů či zaměstnanců obecního úřadu včetně fotografií i přes výslovné neudělení svolení dle občanského zákoníku (v rámci ochrany jejich osobnosti v souladu s občanským zákoníkem).

14.8.7 Uveřejňování materiálů ze zastupitelstva

Obec má povinnost alespoň 7 dní před zasedáním zastupitelstva zveřejnit na své úřední desce (rovněž dálkově přístupné, na webových stránkách obce) informaci o navrženém programu připravovaného zasedání. O průběhu zasedání pořizuje obec zápis, který musí být uložen na obecním úřadu k nahlédnutí. Žádný právní předpis však nestanoví



povinnost tento zápis nebo jiné materiály (důvodové zprávy, návrhy usnesení apod.) plošně uveřejňovat. Výjimky z tohoto pravidla jsou popsány níže.

Velká část takových materiálů obsahuje osobní údaje fyzických osob, a to někdy i citlivého charakteru. Např. při žádosti o přidělení sociálního bydlení obsahují žádosti často sociální postavení/poměry žadatele, jeho věk, rodinný a zdravotní stav apod. podobné údaje obsahují např. žádosti o prominutí pohledávky. Smyslem uveřejňování je informovat o činnostech obce, nikoliv o osobách, kterých se může zasedání týkat (například v případě projednání jejich žádosti či stížnosti).

Účel zpracování osobních údajů:

Účelem zpracování osobních údajů je zde poskytování informace o činnosti obce, nikoli informování o individuální situaci osob, jejichž osobní údaje jsou předmětem jednání. Tomuto účelu by měl být podřízen způsob zpracování osobních údajů. Zákonnost zpracování osobních údajů pro účely uveřejňování materiálů před a po zasedání zastupitelstva obce je dána ve výjimečných případech (zejména tam, kde je naplňováno právo na svobodný přístup k informacím) tím, že se jedná o zpracování nezbytné pro splnění právní povinnosti svěřené obci (dle čl. 6 odst. 1 písm. c) GDPR) nebo nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci obcí (dle čl. 6 odst. 1 písm. e) GDPR).

Rozsah zpracovávaných osobních údajů:

V rámci přípravy pro jednání zastupitelstva či schůze rady obce jsou osobní údaje zpracovávány v rozsahu potřebném pro toto projednání. Pro účely zveřejnění je však zapotřebí zvážit rozsah anonymizace údajů týkajících se osob, o jejichž právech a povinnostech orgány obce jednají.

Příklady:

- V průběhu samotného zasedání zastupitelstva (které je veřejné) je možné prezentovat veškeré informace (včetně nezbytného rozsahu osobních údajů), obsah jednání zastupitelstva může být zveřejňován i způsoby umožňujícími dálkový přístup (online streamování, zveřejněné zvukové záznamy, zveřejňování dokumentů určených k projednání v zastupitelstvu apod.).



- V rámci dobrovolně zveřejňovaných dokumentů by však měly být anonymizovány osobní údaje osob, o jejichž právech a povinnostech zastupitelstvo rozhoduje, krom údajů týkajících se veřejnoprávních smluv o poskytnutí dotace (viz dále) a nebo rozhodnutí týkajících se nakládání

s majetkem obce. Výjimku tvoří i jiné situace, kdy existuje veřejný zájem na zveřejnění osobních údajů (např. u výsledků výběrových řízení dle zákona o zadávání veřejných zakázek apod.).

- O průběhu zasedání pořizuje obec zápis, který musí být uložen na obecním úřadu k nahlédnutí.

- V případě, že se obec rozhodne zápis uveřejnit (například na internetu nebo v tištěném zpravodaji), je nutné provést jeho anonymizaci. Výjimku opět tvoří případy, kdy je ke zveřejnění informací obsahujících osobní údaje dán veřejný zájem – nejen u výsledků výběrových řízení, uzavřených majetkových transakcí obce, ale např. i v takových případech, kdy určitá osoba vystoupí na jednání zastupitelstva.

- Schůze rady obce jsou neveřejné a zápis z její schůze je uložen u obecního úřadu k nahlédnutí členům zastupitelstva obce a nikoliv veřejnosti. Obec je povinna zajistit, aby k osobním údajům v zápisu obsaženém byl umožněn přístup pouze oprávněným osobám anebo v případech, zveřejnění osobních údajů osob, jimž byly poskytnuty veřejné prostředky.

- Veřejnoprávní smlouva o poskytnutí dotace nebo návratné finanční pomoci musí být zveřejněna na úřední desce po dobu nejméně 3 let ode dne zveřejnění. Maximální doba zveřejnění není předepsána, měla by však být obcí stanovena právě s ohledem na zásadu omezeného uložení osobních údajů jako co nejkratší (případně je možné po 3 letech veškeré osobní údaje anonymizovat a smlouvu ponechat zveřejněnou i nadále).

Proces zpracování osobních údajů:

Hlavními dotčenými procesy zpracování jsou příprava podkladů pro připravované zasedání orgánů obce a dále pak v případě zveřejnění dokumentů souvisejících s jednáním orgánů obce anonymizace osobních údajů obsažených v dokumentech. Pro účely nahlížení do zápisů ze zasedání zastupitelstva není třeba anonymizaci provádět, stejně tak ani pro účely online streamování jednání anebo pořizování audiozáznamu (není-li určen k následnému zveřejnění) z jednání zastupitelstva, které je zásadně



veřejné. U schůze rady, které je zásadně neveřejné, pak platí opačný přístup – nepočítá se s účastí veřejnosti ani s nahlížením do zápisů ze schůzí, výjimku tvoří pouze postup v rámci svobodného přístupu k informacím. Tam by, v situacích, kdy to není bezpodmínečně nutné z hlediska vyhovění žádosti a zajištění informování veřejnosti o způsobu hospodaření s veřejnými prostředky, měla obec zvážit anonymizaci osobních údajů obsažených v poskytnuté informaci. Pravidla pro zpracování osobních údajů:

Na zpracování osobních údajů v souvislosti se zveřejňováním materiálů před nebo po zasedání zastupitelstva či schůze rady obce je třeba aplikovat všechny zásady GDPR.

Každý subjekt, jehož údaje jsou shromažďovány, má právo být informován o podstatných náležitostech zpracování jeho osobních údajů a může se taktéž obrátit na pověřence pro ochranu osobních údajů (DPO) s dotazy či žádostmi o vysvětlení.

Na obec dopadají v obecné rovině veškeré povinnosti správce osobních údajů, zejména je povinna podrobnosti o zpracování osobních údajů pro účely uveřejňování materiálů v souvislosti se zasedáním zastupitelstva a schůzí rady obce zavést do evidence zpracování (záznamů o činnostech zpracování), zajistit odpovídající zabezpečení a omezení přístupu k osobním údajům pouze pro příslušné osoby a v případě bezpečnostního incidentu na poli ochrany osobních údajů takový incident zdokumentovat, ohlásit Úřadu pro ochranu osobních údajů a v případě vysoké rizikovosti incidentu i oznámit dotčeným subjektům. Kdo má ke zpracovávaným osobním údajům přístup:

Úsek tajemníka úřadu, který povětšinou připravuje podklady pro zasedání zastupitelstva a schůze rady, a současně i všechny ostatní zapojené úseky, jejichž záležitosti zastupitelstvo či rada projednává. K osobním údajům, které jsou součástí jednání obecního zastupitelstva, může mít

v rámci své přítomnosti na jednání, online sledování nebo poslechu či sledování záznamu pořízeného na jednání (za předpokladu, že je zpřístupňován na žádost a v sídle úřadu, nikoli neomezeně a/nebo online) přístup kdokoli, stejně tak i k zápisům a dokumentům k jednání zastupitelstva, které jsou k dispozici v sídle obce nahlédnutí. Zásadně opačná je situace u schůzí rady, které je zásadně neveřejné. Pokud jsou zveřejňovány jednotlivé dokumenty ze zasedání zastupitelstva i schůze rady, osobní údaje v nich obsažené musejí být vždy zásadně anonymizované. Jedinou výjimku tvoří



veřejnoprávní smlouvy o poskytnutí dotace, kde zákon stanoví náležitosti jejího zveřejnění na úřední desce obce včetně obecné povinnosti anonymizace údajů zakotvené v § 10d) odst. 3 zákona č. 250/2000 Sb. Příklady dobré praxe při řešení modelové situace:

Informace o navrženém programu připravovaného zasedání zastupitelstva obce by v obecné rovině až na výjimky explicitně stanovené zákonem neměly obsahovat osobní údaje fyzických osob, o jejichž právech a povinnostech orgán obce jedná (doporučením Úřadu pro ochranu osobních údajů je uvést pouze popis věci bez informací o konkrétní osobě nebo uvést iniciály a označení obce bydliště dané osoby).

Příklady špatné praxe při řešení modelové situace:

Zveřejnění zápisu ze schůze rady obce na internetu bez předchozí anonymizace osobních údajů v něm obsažených.

14.8.8 Zveřejňování na úředních deskách

Pro účely sledování povinností obcí jako správců při zpracování osobních údajů je zapotřebí rozlišovat, zda se jedná o povinné uveřejňování informací na úředních deskách, ke kterému může principiálně docházet:

- v případě povinně zveřejňovaných informací dle zákona o obcích, správního řádu, zákona o rozpočtových pravidlech územních rozpočtů (např. informace o konání zastupitelstva obce, která obsahuje i návrh programu, veřejnoprávní smlouvy o poskytnutí dotace nebo návratné finanční výpomoci, obecně závazné vyhlášky apod.) nebo
- při doručování veřejnou vyhláškou dle správního řádu, a nebo zda jde o zveřejňování nepovinné, a jde tedy o publikaci dalších informací zveřejňovaných v rámci snahy o transparentnost jednání obce. V návaznosti na toto rozdělení lze pak hovořit o plnění zákonné povinnosti zahrnující i zveřejnění osobních údajů u zveřejňování povinného, anebo o zveřejňování nepovinném.

Dle správního řádu se osobám, kterým se prokazatelně nedaří doručovat (rovněž tak osobám neznámého pobytu) a v dalších zákonem stanovených případech, doručuje veřejnou vyhláškou. Zvláštními zákony, na jejichž základě může být obecnímu úřadu



uloženo doručení veřejnou vyhláškou, jsou například daňový řád nebo občanský soudní řád.

Na úřední desce mohou být nepovinně zveřejňovány např. i zápisy z jednání zastupitelstva (blíže viz situace č. 14.). Dále obec obvykle zveřejňuje i nepovinné informace jako údaje o společenském, kulturním a sportovním životě obce, oznámení o ztrátách a nálezích apod. Při zveřejňování je vždy třeba důsledně rozlišovat, jaké typy osobních údajů jsou ve zveřejňovaném dokumentu obsaženy, kterým dotčeným subjektům tyto údaje náleží a zejména zda je dán příslušný právní titul pro zveřejnění údajů. V tomto ohledu je zapotřebí upozornit, že zveřejňování osobních údajů vyvěšováním na úřední desce je jejich zpracováním pouze za podmínky, že se uskutečňuje jako operace prováděná s osobními údaji z jiného (zdrojového) zpracování. Režim obecného nařízení se nepoužije na správu úřední desky jako celek.

Účel zpracování osobních údajů:

Účelem zpracování osobních údajů je zde jejich zveřejnění na úřední desce. Zákonnost zpracování osobních údajů pro účely doručování veřejnou vyhláškou je dána tím, že se jedná o zpracování nezbytné pro splnění právní povinnosti uložené obci (dle čl. 6 odst. 1 písm. c) GDPR) případně o zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci obcí (dle čl. 6 odst. 1 písm. e) GDPR).

Rozsah zpracovávaných/zveřejňovaných osobních údajů:

K účelu zveřejnění mohou být osobní údaje využity buď v plném rozsahu (tam, kde je dána zákonná povinnost obce zveřejnit tyto údaje – např. při doručování veřejnou vyhláškou), v rozsahu částečně anonymizovaném (zejm. u povinného zveřejňování veřejnoprávních smluv o poskytnutí dotace nebo návratné finanční výpomoci) anebo v podobě zcela anonymizované (tam, kde se jedná o nepovinné zveřejňování informací o přijatých rozhodnutích nebo smlouvách uzavřených obcí). Samostatnou kapitolu pak tvoří nepovinně zveřejňované informace o dění v obci, které mohou obsahovat i přesné osobní údaje určitých osob, které hrají v tomto dění důležitou roli a na jejich zveřejnění existuje veřejný zájem.

Proces zpracování osobních údajů:

Na zpracování osobních údajů v souvislosti se zveřejňováním informací na úřední desce je třeba aplikovat všechny zásady GDPR, tedy zejména:



- Obec musí mít pro zpracování osobních údajů právní titul (viz níže) a zpracovávat osobní údaje adresátů zveřejňovaných informací korektně a zákonným a transparentním způsobem (zásada zákonnosti, korektnosti a transparentnosti).
- Písemnosti doručované veřejnou vyhláškou a osobní údaje v nich obsažené mohou být zpracovávány obcí pouze pro účely doručování veřejnou vyhláškou (zásada účelového omezení zpracování osobních údajů).
- Je nezbytné, aby rozsah zveřejňovaných osobních údajů byl přiměřený a omezený na nezbytné minimum (zásada minimalizace údajů).

Poznámka:

- V případě dokumentů jiných orgánů veřejné správy nebo orgánů veřejné moci nezkoumá obecní úřad obsah dané písemnosti, nemůže ji měnit ani jakkoli do ní zasahovat.

- Odpovědnost za dodržování nařízení či jiných předpisů na ochranu osobních údajů, a případné sankce za jeho porušení a odpovědnost k náhradě způsobené škody, nese orgán, který obecnímu úřadu danou písemnost k vyvěšení zaslal.

- Při doručování veřejnou vyhláškou podle správního řádu jsou přípustné jak publikace úplného znění písemnosti samotné, tak i publikace oznámení o možnosti převzít písemnost na úřední desce správního orgánu, který písemnost doručuje. Správní řád neupravuje kritéria pro volbu daného způsobu, obec jako správní orgán by měla tedy zvážit okolnosti konkrétního případu, resp. obsah doručované písemnosti v jednotlivém případě. Vyvěšení písemnosti by mělo být primárním způsobem, pro vyvěšení pouhého oznámení by měly existovat důvody bránící vyvěšení samotné písemnosti (typicky její velký rozsah) a nebo důvody dané ochranou osobních údajů tedy například případy, kdy písemnost samotná obsahuje rovněž osobní údaje jiných osob než adresáta, osobní údaje zvláštních kategorií apod.

- Zpracování osobních údajů jen po dobu nezbytně nutnou pro dané zpracování, která je dána příslušnými právními předpisy (zásada omezení uložení).



Příklad:

Príslušné právní předpisy, např. zákon o rozpočtových pravidlech územních rozpočtů, správní řád aj. stanoví minimální lhůtu pro vyvěšení na úřední desce. Po uplynutí této lhůty (nebyla-li dříve písemnost vyzvednuta jejím adresátem) obecní úřad veřejnou vyhlášku z úřední desky sejme.

- Zajistit náležitě zabezpečení osobních údajů včetně ochrany před neoprávněným zpracováním (zásada integrity a důvěrnosti), a to zejména tím, že do kontaktu s osobními údaji obsaženými v plném textu dokumentů před jejich eventuální anonymizací nebo pseudonymizací by měl přijít pouze přesně vymezený okruh osob, které jsou v rámci obce pověřeny výkonem předmětné agendy.

Obec odpovídá za soulad zpracování s uvedenými zásadami a musí být schopna dodržení souladu doložit (zásada odpovědnosti). Pravidla pro zpracování osobních údajů:

Každý subjekt, jehož údaje jsou zpracovávány, má právo být informován o podstatných náležitostech zpracování jeho osobních údajů již v okamžiku získání osobních údajů, přičemž samozřejmě není již nutné informovat subjekt údajů o skutečnostech, které již ví anebo má možnost se s nimi seznámit. Informace mohou být taktéž publikovány na úřední desce anebo jinými prostředky umožňujícími dálkový přístup (např. webu obce) a není tedy nutné o nich informovat každý dotčený subjekt údajů individuálně. Pokud je osoba neznámého pobytu, přirozeně vždy postačí jí informace poskytnout v obecné podobě na úřední desce nebo na webu obce.

Každý subjekt údajů se taktéž může obrátit na pověřence pro ochranu osobních údajů (DPO) s dotazy či žádostmi o vysvětlení.

V úvahu zde přichází zejména právo podat námitku proti zpracování osobních údajů i jejich zveřejnění, pokud obec údaje zpracovává z důvodu plnění úkolu prováděného ve veřejného zájmu.

Na obec dopadají v obecné rovině veškeré povinnosti správce osobních údajů, zejména je povinna související operace zpracování osobních údajů zavést do své evidence zpracování osobních údajů (záznamů o činnostech zpracování).

Kdo má ke zpracovávaným osobním údajům přístup:



Ve všech popsanych případech dochází k zpřístupnění osobních údajů těchto osob na úřední desce neurčitému okruhu osob.

Příklady dobré praxe při řešení modelové situace:

V případě písemnosti obce, kterou chce obec doručovat veřejnou vyhláškou a která obsahuje osobní údaje, lze zejména v případech, kdy obsahuje písemnost samotná rovněž osobní údaje jiných osob než adresáta nebo osobní údaje zvláštních kategorií, namísto vyvěšení samotné písemnosti zvolit možnost vyvěšení oznámení o možnosti převzít písemnost, ve kterém budou uvedeny pouze nezbytné identifikační údaje dotčené osoby (jméno, příjmení, adresa, případně i datum narození).

Příklady špatné praxe při řešení modelové situace:

Vyvěšení obsahu jiné, než veřejnou vyhláškou doručované písemnosti

Uvedení osobních údajů, které nejsou nezbytně nutné k identifikaci adresáta, v rámci zveřejnění veřejnoprávní smlouvy o poskytnutí dotace na úřední desce

14.8.9 Kyberbezpečnost

Používání informačních systémů orgány veřejné moci je právně regulováno zákonem o informačních systémech veřejné správy. Jako informační systém veřejné správy se označuje informační systém, který slouží pro výkon veřejné správy. Obce v rámci tohoto zákona jsou povinny uplatňovat opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy. Obce provozují svoje informační systémy i v rámci ochrany dat v souladu s bezpečnostními principy, které jsou regulovány v zákoně o informačních systémech veřejné správy. Povinnosti vyplývající z GDPR na tyto principy navazují.

Posouzení z pohledu ochrany osobních údajů:

Povinnost zabezpečit zpracování osobních údajů je přímo stanovena v článku 32 GDPR. V praxi to znamená, že obec musí provést (s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob) vhodná technická a organizační opatření k zajištění zabezpečení odpovídající danému riziku.



Popis povinnosti zajistit zabezpečení osobních údajů:

Povinnost zajistit zabezpečení zpracování osobních údajů je přímým požadavkem vyplývajícím z článku 32 GDPR a zahrnuje povinnosti:

- Zajistit odpovídající technická a organizační opatření pro zabezpečení osobních údajů.
- Přihlédnout přitom ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování.
- Vyhodnotit pravděpodobnost a závažnost bezpečnostních rizik a jejich existenci zohlednit při provádění opatření.

V rámci této povinnosti se tedy projevuje jak princip proporcionality bezpečnostního řešení ve vztahu k situaci správce, tak i přístup založený na riziku, který se prolíná celým obecným nařízením.

Příklady:

- Vstup do budovy organizace je pouze proti autentizaci pomocí vstupní identifikační karty, která je založena na zabezpečené technologii. Karty jsou současně využívány i pro dvoufaktorovou autentizaci osob pohybujících se v budově.
- Wifi síť, kterou obec na svých pobočkách zdarma poskytuje, je odděleným síťovým segmentem a není součástí intranetu organizace.
- Celé prostředí organizace je sledováno řešením SIEM zajišťujícím bezpečnostní monitoring.
- Personální složky jsou uloženy v kovových uzamykatelných skříních.

Rozsah povinnosti zajistit zabezpečení údajů:

Subjekty údajů mají právo, aby bylo zpracování jejich osobních údajů bylo prováděno zabezpečenou formou. Tomu odpovídají i povinnosti správce a nutná opatření na jeho straně.

Pravidla pro naplňování povinnosti:



Bezpečnost osobních údajů má několik základních oblastí, na které by se měla každá organizace zaměřit:

- Zajištění fyzické bezpečnosti: Tato zásada mluví primárně o materiální (listinné) podobě zpracování a jejím obsahem je kontrola a zajištění bezpečnosti přístupu do prostor, kde je možné dostat se k datům, resp. k osobním údajům. Jde například o zajištění uzamykatelnosti skladovacích prostor včetně pečlivého vymezení okruhu osob, které mají k dispozici klíč, kontrolu přístupů do budovy, politiku čisté pracovní plochy a další.
- Autorizace a autentizace: Každý uživatel s přístupem k osobním údajům by měl mít přístup pouze k údajům, které nezbytně potřebuje pro výkon své agendy. Tyto přístupy a úrovně oprávnění by měly být jasně organizačně i technicky zajištěny. Mohou se prakticky promítnout například jako různé úrovně přístupových práv v aplikacích nebo adresářích, případně jako restrikce přístupů do některých částí budovy (personální archiv). Z pohledu autentizace (zajištění identifikace uživatele) je zásadní politika hesel a udržení auditní stopy o přístupu k osobním údajům.
- Ochrana proti kybernetickým incidentům a jejich detekce: V této oblasti jde převážně o ochranu pro kybernetickými hrozbami pomocí bezpečnostních nástrojů jako je například firewall, IPS, IDS nebo DLP systémy. U detekce kybernetických bezpečnostních incidentů lze pak především doporučit napojení na dohledové centrum eGovernmentu nebo na externí firmu, která bude dodatečně provádět monitoring provozních a bezpečnostních logů.
- Zavedení systému řízení informační bezpečnosti: Tato část je hlavně organizačním opatřením. Jde o vytvoření systému politik zajišťující výkon a dokumentaci agendy informační bezpečnosti v organizaci (politika hesel, politika ochrany bezpečnostního perimetru ad.)

Příklady dobré praxe při řešení modelové situace:

Organizace má zavedený systém řízení informační bezpečnosti včetně jeho dokumentace.

Nasazení odpovídajících technických opatření kybernetické bezpečnosti.



Rozdělení odpovědností za zabezpečení zpracování osobních údajů.

Příklady špatné praxe při řešení modelové situace:

Informační bezpečnost není řízená a řeší se ad hoc na základě proběhlých bezpečnostních incidentů.

Neexistuje dokumentace, která by zajišťovala přenositelnost informací na další pracovníky a doložitelnost bezpečnostních procesů u případné kontroly.

Zaměstnanci nejsou pravidelně vzděláváni v oblasti informační bezpečnosti a ochrany osobních údajů a zvyšuje se tak riziko chyby lidského faktoru a ním spojeného porušení zabezpečení zpracování osobních údajů.

14.8.10 Personální praxe a výběrová řízení

Popis Životní situace 1:

Obec, která má v úmyslu provést výběrové řízení na pozice úředníků nebo ostatních zaměstnanců shromažďuje, zpracovává a uchovává osobní údaje předem neurčitého počtu osob (zájemců). Jak dopadá nová právní úprava na výběrová řízení?

Posouzení z pohledu ochrany osobních údajů:

V rámci výběrových řízení na pozice úředníků i ostatních zaměstnanců obecních úřadů či organizačních složek obce může obec za účelem výběru vhodného uchazeče vyžadovat a shromažďovat určité informace o zájemcích, a to i bez jejich souhlasu.

V případě zaměstnanců obcí je odlišný režim u úředníků – tam vzniku pracovního poměru na dobu neurčitou povinně předchází výběrové řízení nebo veřejná výzva – a u ostatních zaměstnanců obce – kde výběrové řízení může, ale nemusí proběhnout a pokud proběhne, není upraveno zákonem. V případě výběrového řízení a veřejné výzvy v režimu zákona č. 312/2002 Sb. je přímo zákonem dán rozsah údajů, které zájemce, resp. uchazeč musí obci poskytnout (v přihlášce). Ze zákona č. 312/2002 Sb. pak také vyplývají některá specifika, pokud jde o přístup k údajům z výběrového řízení (např. úprava postupu výběrové komise, nahlížení do zprávy o posouzení uchazečů).

Účel zpracování osobních údajů:

Základním účelem zpracování osobních údajů je zde provedení výběrového řízení na obsazení volných míst zaměstnanců obecního úřadu, zaměstnanců do obecního úřadu



nezařazených, zaměstnanců organizačních složek a nebo osob vykonávajících práci pro obecní úřad mimo pracovní poměr. Konkrétními operacemi zpracování pak budou zpracování životopisů a dalších podkladů (např. doklad o vzdělání, doklady o dosavadní praxi, výpis z Rejstříku trestů aj.), vedení evidence uchazečů, vypracování zprávy vedoucího úřadu/výběrové komise o posouzení a hodnocení uchazečů.

Zákonnost zpracování osobních údajů pro účely výběrového řízení je dána na základě nezbytnosti pro plnění smlouvy, resp. pro provedení opatření před uzavřením této smlouvy (jde tedy o právní titul dle čl. 6 odst. 1 písm. b) GDPR). Po skončení výběrového řízení si může obec ponechat osobní údaje za účelem svého oprávněného zájmu pro obhajobu svých práv v případném sporu (dle čl. 6 odst. 1 písm. f) GDPR) a nebo eventuálně pro účely využití v budoucím výběrovém řízení. Další použití shromážděných osobních údajů pro účely dalších výběrových řízení je možné jen se souhlasem subjektu (dle čl. 6 odst. 1 písm. a) GDPR).

Speciální případ tvoří výběrová řízení na obsazení volných míst úředníků územně samosprávných celků realizovaná v režimu zákona č. 312/2002 Sb., o úřednících územně samosprávných celků.

Základním právním titulem v případě takového výběrového řízení, resp. veřejné výzvy v režimu zákona o úřednících územně samosprávných celků, je plnění právní povinnosti a tedy právní titul dle čl. 6 odst. 1 písm. c) GDPR. Územní samosprávný celek má totiž zákonem uloženu povinnost výběrové řízení, resp. veřejnou výzvu, provést, a to za přesně zákonem upravených podmínek.

Rozsah zpracovávaných osobních údajů:

Je zapotřebí posoudit vždy především ve vztahu k danému účelu – tj. provedení výběrového řízení na obsazení volných pozic na obecním úřadě. Tomu je třeba, jde-li o výběrové řízení v režimu zákoníku práce, přizpůsobit rozsah údajů, které jsou vyžadovány od uchazečů a současně i nastavit odpovídající oprávnění ke zpracování údajů uvnitř obecního úřadu (tj. stanovit okruh pracovních pozic, které přicházejí s danými osobními údaji do kontaktu). Jde-li o výběrové řízení realizované v režimu zákona č. 312/2002 Sb., je třeba mít na paměti, že rozsah vyžadovaných údajů je v případě těchto výběrových řízení (veřejných výzev) stanoven zákonem (konkrétně v



jeho § 6) a obec by tedy neměla jít nad rámec zákonných požadavků např. v rámci postupu výběrové komise, nahlížení do zprávy o posouzení uchazečů aj.

Proces zpracování osobních údajů:

Osobní údaje by měly být zpracovány v následujících krocích:

1. Vypsání výběrového řízení, sběr nabídek uchazečů, založení evidence jejich životopisů, resp. v případě výběrového řízení v režimu zákona čl. 312/2002 Sb., i přihlášek do výběrového řízení včetně jejich příloh
2. Realizace výběrového řízení (pohovory, testy, assessmenty uchazečů) a vybrání vhodného uchazeče
3. Informování úspěšných i neúspěšných uchazečů. Zahájení jednání o uzavření pracovní smlouvy s úspěšným uchazečem a informování neúspěšných uchazečů o tom, zda a případně k jakému účelu a po jakou dobu budou jejich osobní údaje dále uchovávány a zpracovávány.
4. Pro případ, že budou uchované životopisy neúspěšných uchazečů využity pro účely jiného budoucího výběrového řízení, je nutné pamatovat na to, že je zapotřebí si k tomu vyžádat jejich souhlas.

Pravidla pro zpracování osobních údajů:

- Obec musí mít pro zpracování osobních údajů právní titul (viz níže) a zpracovávat osobní údaje uchazečů o zaměstnání korektně a zákonným a transparentním způsobem (zásada zákonnosti, korektnosti a transparentnosti).
- Osobní údaje mohou být zpracovávány pouze pro účely konkrétního výběrového řízení, po jeho skončení dále mohou být uchovány jen po nezbytně dlouhou dobu pro účely ochrany právních zájmů obce v případě případných sporů ohledně průběhu výběrového řízení. Pro účely dalších výběrových řízení lze osobní údaje využít pouze se souhlasem subjektu údajů (zásada účelového omezení zpracování osobních údajů).
- Je nezbytné, aby byly zpracovávány jen osobní údaje nezbytné pro výběrové řízení (zásada minimalizace údajů).



- Zpracovávané osobní údaje musí být přesné a v případě potřeby aktualizované. Osobní údaje, které jsou nepřesné, mají být opraveny nebo vymazány (zásada přesnosti).
- Zpracování osobních údajů je možné jen po dobu nezbytně nutnou pro daný účel, tj. po dobu trvání a vyhodnocení výběrového řízení (dále jen pro dobu nezbytně nutnou k ochraně zájmů obce, dle spisového a skartačního řádu). V případě souhlasu se zpracováním pro účely dalších výběrových řízení po dobu trvání uděleného souhlasu (zásada omezení uložení).
- Zajistit náležité zabezpečení osobních údajů včetně ochrany před neoprávněným zpracováním (zásada integrity a důvěrnosti).

Obec odpovídá za soulad zpracování s uvedenými zásadami a musí být schopna dodržení souladu doložit (zásada odpovědnosti). Každý subjekt, jehož údaje jsou shromažďovány, má právo být informován o podstatných náležitostech zpracování jeho osobních údajů. Většinu osobních údajů získá obec přímo od uchazeče (z jeho přihlášky), v takovém případě je dána povinnost informovat uchazeče o zpracování již v okamžiku přijetí přihlášky, přičemž samozřejmě není již nutné informovat uchazeče o skutečnostech, které již ví anebo má možnost se s nimi seznámit. Informace o zpracování osobních údajů uchazečů mohou být uvedeny u veřejné výzvy nebo v oznámení o vyhlášení výběrového řízení a není tedy nutné o nich informovat každého uchazeče individuálně.

Obec je rovněž povinna poskytnout informace o zpracování a případně kopii zpracovávaných osobních údajů uchazeče na jeho žádost. Subjekt osobních údajů se také může obrátit na pověřence pro ochranu osobních údajů (DPO) s dotazy či žádostmi o vysvětlení.

Kdo má ke zpracovávaným osobním údajům přístup:

K obsahu dokumentace zahrnující osobní údaje uchazečů by měli mít přístup výlučně pracovníci obecních úřadů, s jejichž pracovní náplní realizace předmětného výběrového řízení nedílně souvisí: samozřejmě tedy pracovníci personálních oddělení nebo úseku tajemníka úřadu (a eventuálně i externí personální agentury, s kterou má obec smlouvu na poskytování služeb zahrnujících realizaci výběrových řízení), starosta a místostarosta a rovněž tak i vedoucí pracovníci úseků, v kterých jsou obsazovány volné pozice,



eventuálně orgány obce, které si vyhradily rozhodnutí o přijetí konkrétního zaměstnance. V případě realizace výběrového řízení v režimu zákona č. 312/2002 Sb., by k obsahu dokumentace musejí mít přístup i členové výběrové komise, kteří mohou být jak úředníky obce, tak i externisty. Spisy (ať už v papírové, nebo i v elektronické podobě) by v žádném případě neměly být k dispozici neomezenému okruhu pracovníků obecního úřadu, externím členům výběrové komise, kteří participují na realizaci více výběrových řízení nebo osobám na pracovních pozicích, které nemají souvislost s realizací výběrového řízení.

Příklady dobré praxe při řešení modelové situace:

Získání souhlasu uchazeče ke zpracování jeho osobních údajů pro účely případných dalších výběrových řízení

Informování uchazečů o tom, po jak dlouhou dobu si obec ponechá jejich osobní údaje z důvodu případných kontrol či sporů ohledně průběhu a výsledků výběrového řízení (tedy obvykle po dobu běhu promlčecí doby – tedy po dobu dvou let od ukončení výběrového řízení) anebo pro účely využití pro eventuální budoucí jiné výběrové řízení.

Příklady špatné praxe při řešení modelové situace:

Využití osobních údajů nepřijatých uchazečů výběrového řízení pro účely jiného výběrového řízení, aniž by k tomu subjekty údajů poskytly souhlas

Vyžadování osobních údajů, které nejsou potřebné pro výběrové řízení, například plošný požadavek na dodání výpisu z Rejstříku trestů (v případě výběrových řízení realizovaných dle zákoníku práce) nebo jakýkoli požadavek jdoucí nad rámec § 6 zákona o úřednících územně samosprávných celků (v případě výběrového řízení dle tohoto zákona).

Životní situace 2:

V rámci personální praxe obcí je zapotřebí věnovat obzvláštní pozornost ochraně osobních údajů zaměstnanců. Jak tuto ochranu zajistit tak, aby obec při své činnosti vyhověla GDPR?

Popis Životní situace 2:

V personální praxi přichází někteří představitelé a zaměstnanci obce, a případně i externí zpracovatelé (např. mzdové agentury) do styku s řadou osobních údajů



zaměstnanců a zastupitelů obce, včetně osobních údajů zvláštní kategorie (dříve označované jako citlivé osobní údaje). Jak se v této praxi projeví nová právní úprava ochrany osobních údajů?

Posouzení z pohledu ochrany osobních údajů:

Úředníci, další zaměstnanci a členové zastupitelstev a dalších volených orgánů kteří se podílejí na činnosti obce, jsou další kategorií subjektů údajů, jejichž osobní údaje obec zpracovává. I na tato zpracování plně dopadají povinnosti stanovené GDPR a dalšími předpisy na ochranu osobních údajů.

Účel zpracování osobních údajů:

Základním účelem zpracování údajů je zde vedení personálně-mzdové agendy zaměstnanců a právním titulem pro zpracování osobních údajů je tedy buď plnění zákonných povinností obce jako správce údajů, nebo plnění (pracovní či jiné) smlouvy obce jako správce s příslušným zaměstnancem jako subjektem údajů. Pokud by šlo o zpracování údajů nad rámec základní personálně-mzdové agendy (např. zaměstnanecké soutěže nebo publikace informací o zaměstnancích a jejich fotografií v obecním časopisu), je zapotřebí hledat jiný právní titul pro zpracování údajů. Tím může být buď oprávněný zájem obce jako správce údajů, naplňování veřejného zájmu nebo v méně častých případech i souhlas se zpracováním osobních údajů.

Rozsah zpracovávaných osobních údajů:

V souladu se zásadou minimalizace osobních údajů by údaje neměly být zpracovávány v rozsahu větším, než je nutné pro dosažení daného účelu – tj. pro splnění zákonných povinností obce ve vztahu k zaměstnancům anebo pro splnění pracovní či jiné smlouvy. Obec by se měla rozhodně vyvarovat zpracovávání osobních údajů v rozsahu širším než vzhledem k danému účelu nutné.

Proces zpracování osobních údajů:

V souvislosti s personální a mzdovou agendou dochází zejména k následujícím typům a procesům zpracování: vedení spisu zaměstnance, zpracování osobních údajů v základní mzdové evidenci a vedlejších evidencích – například evidence cestovních náhrad, pracovních úrazů. Dále dochází k předávání osobních údajů zaměstnancům oprávněným příjemcům (zdravotní pojišťovny, správa sociálního zabezpečení, finanční úřady, banky,



závodní lékaři atd.). V rámci procesu zpracování je třeba zohlednit i proces vzdělávání úředníků v souladu s obsahem zákona č. 312/2002 Sb., o úřednících samosprávných celků; povinné i nepovinné vzdělávání úředníků bude specifickou součástí základní personálně-mzdové agendy úředníků všech samosprávných celků včetně obcí.

Pravidla pro zpracování osobních údajů:

Každý subjekt, jehož údaje jsou shromažďovány, má právo být informován o podstatných náležitostech zpracování jeho osobních údajů. Tato informace mu může být doručena buď individuálně (osobně, e-mailem) nebo i v obecné rovině (způsobem umožňujícím dálkový přístup – např. na webu obce apod.). Obec je rovněž povinna poskytnout mu informace o zpracování a případně kopii zpracovávaných osobních údajů, toto právo koresponduje s právem zaměstnance na nahlížení do svého osobního spisu (podle §312 zákoníku práce). Zaměstnanec se taktéž může obrátit na pověřence pro ochranu osobních údajů (DPO) s dotazy či žádostmi o vysvětlení. Zaměstnanec má právo na opravu nepřesných nebo doplnění neúplných údajů. Vzhledem k tomu, že zpracování osobních údajů je nezbytné pro plnění právních povinností obce jakožto zaměstnavatele, neuplatní se v tomto případě právo na výmaz (čl. 17 odst. 3 písm. e) a b) GDPR).

Kdo má ke zpracovávaným osobním údajům přístup:

Ke zpracování osobních údajů v rámci personální a mzdové agendy (včetně evidence dovolených, zákonného pojištění apod.) by měl mít, stejně jako je tomu i v jiných oblastech, přístup pouze okruh zaměstnanců, resp. volených zástupců obce, pro jejichž výkon povinností je práce s informacemi o zaměstnancích obce nezbytná. personálních oddělení (tam kde je zřízeno). Souvisejícími oblastmi zpracování je agenda a odměňování uvolněných a neuvolněných členů zastupitelstva a členů výborů

a komisí, povinné i nepovinné vzdělávání zaměstnanců, poskytování cestovních náhrad, evidence dovolených, evidence sociálního zabezpečení a zdravotního a nemocenského pojištění, agenda střetu zájmů Do, případně jiné související agendy. V souladu s naplňováním zásady důvěrnosti zpracování osobních údajů by tedy do kontaktu s osobními údaji zaměstnanců by neměl v rámci obecního úřadu přijít širší okruh osob, než je nutné pro naplnění základního účelu zpracování údajů daného těmito okruhy. Samozřejmě, v souladu se svými zákonnými povinnostmi, je obec povinna umožnit



získání osobních údajů veřejnoprávním příjemcům, kterými zde budou zejména orgány daňové a finanční správy, orgány správy sociálního zabezpečení, inspekce práce a úřad práce apod.

Příklady dobré praxe při řešení modelové situace:

Postupná likvidace osobních údajů bývalých zaměstnanců v souladu s právními předpisy.

Zdokumentování každého incidentu, který by mohl (i potencionálně) ohrozit bezpečnost osobních údajů zaměstnanců. V návaznosti na vyhodnocení rizikovosti takových incidentů, která může mít podstatně jinou míru u incidentu, který se stane uvnitř úřadu oproti incidentu, který proběhne ve veřejně přístupných prostorách nebo na veřejném prostranství pak ohlášení předmětného incidentu dozorovému úřadu nebo v případě vysokého rizika i oznámení dotčeným subjektům údajů.

Příklady špatné praxe při řešení modelové situace:

Uchovávání již nepotřebných osobních údajů zaměstnanců i po skončení pracovního poměru.

Umožnění přístupu k veškerým osobním údajům zaměstnanců každému pracovníku z personálního oddělení.

15. Závěr

Hlavním cílem tohoto dokumentu byla analýza implementace GDPR na jednotlivých obcích, což se podařilo zejména zpracováním aktualizovaných analýz rizik, pro každou jednotlivou obci.

V úvodní části práce nesmělo chybět zevrubné teoretické pojednání o ochraně osobních údajů, jelikož bez znalosti této problematiky nemá smysl dále se zabývat přímou implementací nařízení GDPR resp. přímo se zabývat implementací postupů, které vedou k ochraně osobních údajů. Dále bylo pokračováno teoretickým výkladem, avšak vždy s důrazem pouze na problematiku zpracovávaných obcí. Po zpracování analýz rizik pak byla prověřena činnost pověřence a nastíněny praktické doporučení pro další činnosti



obcí v oblasti ochrany osobních údajů. Dále byly řešeny praktické otázky týkající se běžné činnosti obcí v postavení správců osobních údajů.

Po všech úkonech, které byly provedeny, lze konstatovat, že pro dotčené obce nepřineslo nařízení GDPR žádnou převratnou „revoluci“ jelikož tyto zpracovávají osobní údaje pečlivě a svědomitě, tak jak to stanovovala minulá právní úprava (zákon o ochraně osobních údajů), která byla v mnohém podobná znění článků nařízení GDPR. Nařízení GDPR však přineslo celou řadu změn, které se obcím podařilo vhodně implementovat, či budou vhodně implementovány, jak věřím, v brzké době.

Jak již bylo nastíněno dříve, provedením analýzy implementace GDPR nebyly nalezeny žádné závažné nedostatky, vyžadující bezodkladné řešení. Lze však doporučit pokračovat ve správně nastaveném směru, více se věnovat vzdělávání zaměstnanců a více zapojit pověřence pro ochranu osobních údajů. Těmito kroky lze vybudovat komplexní systém, který trvale udrží implementaci GDPR na všech obcích na vysoké úrovni, bez vzniku zbytečných nákladů.

Implementace obecného nařízení o ochraně osobních údajů byla na všech dotčených obcích úspěšná.



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost