Směrnice
Ochrana osobních údajů
pro Obecní úřad Březí u Mikulova

Vypracoval: Ing. Vilém Umlauf

Schválil: JUDr. Jiří navrátil

Dne: 24.5.2018

OBSAH

1	**Účel**	**4**
2	**Rozsah platnosti**	**4**
3	**Pojmy, zkratky a jejich definice**	**4**
4	**Povinnosti OÚ Březí u Mikulova při ochraně osobních údajů**	**7**
4.1	Povinnosti osob při správě a zpracování osobních údajů	7
4.1.1	Povinnosti Starosty obce	7
4.1.2	Povinnosti osob přicházejících do styku s osobními údaji	7
4.2	Dokumentace dokládající implementaci požadavků GDPR	8
4.2.1	Směrnice Ochrana osobních údajů	8
4.2.2	Registr osobních údajů	8
4.2.3	Analýza stávajícího stavu ochrany osobních údajů	8
4.2.4	Informační memoranda	8
4.2.5	Smlouva o zpracování osobních údajů	9
4.3	Technická opatření k zajištění ochrany osobních údajů	10
4.3.1	Zásady ochrany osobních údajů při jejich zpracování	10
4.4	Technická opatření k zajištění ochrany osobních údajů	10
4.4.1	Písemnosti a jiné hmotné nosiče dat	10
4.4.2	Elektronické datové soubory obsahující osobní údaje	11
4.4.3	Kamerové a audio záznamy	11
4.5	Posouzení dopadu činnosti na ochranu osobních údajů	11
4.6	Konzultace s Úřadem pro ochranu osobních údajů	12
4.7	Povinnost vést záznamy o činnostech zpracování osobních údajů	12
4.7.1	Úvod	12
4.7.2	Registr osobních údajů	12
4.7.3	Detailní popis složky OBEC Březí	12
4.8	Povinnost ohlašovat případy narušení bezpečnosti osobních údajů – řízení incidentů	15
4.8.1	Úvod	15
4.8.2	Zdroje potenciálních incidentů	15
4.8.3	Typy incidentů	15
4.8.4	Detailní postup řízení incidentu v oblasti ochrany OÚ	15
4.9	Přenositelnost osobních údajů	16
4.10	Řízení práv subjektů údajů	17
4.10.1	Úvod	17
4.10.2	Rekapitulace práv subjektů OÚ	17
4.10.3	Typy subjektů OÚ s požadavkem na výkon práv	18

4.10.4	Detailní postup vypořádání požadavku subjektu OÚ na aplikaci jeho práv	18
4.11	Pověřenec pro ochranu osobních údajů	19
4.12	Předávání osobních údajů do zahraničí	20
4.13	Internetové obchodování a věrnostní systémy	20
5	**Odpovědnosti**	**20**
6	**Registr souvisejících dokumentů**	**20**
6.1	Obecně závazné předpisy, Související dokumenty občanů a ostatních zainteresovaných stran 20	
6.2	Přímo související dokumenty OÚ	20
7	**Přílohy**	**20**

1 Účel

Tato směrnice ustavuje technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s NAŘÍZENÍM EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tzv. GDPR (dále jen „GDPR") a předpisů souvisících s cílem zajištění správné praxe při přijímání a realizaci opatření k ochraně osobních údajů v rámci Obecního úřadu Březí u Mikulova.

2 Rozsah platnosti

Směrnice je závazná pro:

- Starostu a Zastupitelstvo obce
- zaměstnance bez ohledu na typ uzavřeného pracovně právního vztahu, kteří přicházejí do styku s osobními údaji v rámci úřadu
- všechny další osoby, které přicházejí do styku s osobními údaji v rámci úřadu

Tato směrnice nabývá účinnosti dnem **25. května 2018**.

3 Pojmy, zkratky a jejich definice

Pojem	Zkratka	Stručná definice
Nařízení GDPR	**GDPR**	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Osobní údaj	**OÚ**	Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů");
Zvláštní osobní údaje		Osobní údaje, které zasluhují vyšší stupeň ochrany (údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby)
Zpracování	-	Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů. Jde o : 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;
Správce	-	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
Zpracovatel (OÚ)	-	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
Konzultant pro ochranu osobních údajů	**KOOÚ**	Osoba (interní / externí) odpovědná za řízení systému ochrany osobních údajů, se zvláštní kompetencí pro oblasti řízení incidentů v oblasti ochrany osobních údajů a práv subjektů údajů
Administrátor IS		Osoba odpovědná za správu informačních systémů (IS) úřadu
Subjekt údajů (OÚ)		Identifikovaná nebo identifikovatelná fyzická osoba

Souhlas	-	Jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle subjektu údajů, kterým dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
Genetické údaje	-	Osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;
Biometrické údaje		Osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;
Právo subjektu údajů na přístup k osobním údajům (Článek 15)		Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány
Právo na opravu (Článek 16)		Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné (a/nebo neúplné) osobní údaje, které se ho týkají.
Právo na výmaz („právo být zapomenut“) (Článek 17)		Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat
Právo na omezení zpracování (Článek 18)		Subjekt údajů má právo na to, aby správce omezil zpracování
Právo na přenositelnost údajů (Článek 20)		Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil
Právo vznést námitku (Článek 21)		Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají,
Automatizované individuální rozhodování, včetně profilování (Článek 22)		Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.
Omezení (Článek 23)		Právo subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na újmu účelu omezení.
Výkon práv subjektů		Sled činností Správce, Zpracovatele OÚ a Administrátora IS, vedoucí k aplikaci práv subjektu OÚ
Incident		Jakékoli porušení zabezpečení OÚ, pokud vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění OÚ
Automatizované zpracování (rozhodování)		Forma zpracování osobních údajů bez jakéhokoliv lidského zásahu
Profilování		Jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace,

	zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;

4 Povinnosti OÚ Březí u Mikulova při ochraně osobních údajů

4.1 Povinnosti osob při správě a zpracování osobních údajů

4.1.1 Povinnosti Starosty obce

Starosta obce Březí u Mikulova se zcela ztotožňuje s požadavky GDPR a prohlašuje, že jejich plnění je součástí strategie rozvoje obce.

Současně prohlašuje tyto požadavky a jejich plnění za závazné pro všechny zaměstnance úřadu.

Starosta obce Březí u Mikulova v rámci své odpovědnosti za ochranu osobních údajů, samo, nebo prostřednictvím pověřených osob zajišťuje:

- podmínky pro správu implementovaného systému, mj. ustavením role Konzultant ochrany osobních údajů (dále jen KOOÚ) s definovanými právy a povinnostmi
- podmínky pro řádnou ochranu osobních údajů, ve smyslu GDPR a ostatních právních předpisů, včetně příslušné legislativy Evropské unie;
- plnou aplikaci práv subjektů údajů
- průběžné vzdělávání zaměstnanců v oblasti ochrany osobních údajů, a to v první řadě formou jejich samostudia, v případě potřeby formou školení, či konzultací; prioritně je kladen důraz na školení nových nastupujících zaměstnanců
- provádění systematických a pravidelných kontrol / auditů činnosti souvisejících s ochranou osobních údajů;
- realizaci nápravných či preventivních opatření v oblasti ochrany osobních údajů, a to na základě vyhodnocení interních auditů GDPR, hlášení incidentů včetně potenciálních a na základě reportů KOOÚ o realizaci práv subjektů údajů
- provádění tzv. **Posouzení dopadu činnosti na ochranu osobních údajů**, a to pouze v případě, že nastal stav či událost, které tuto potřebu vyvolaly
- provádění předběžných konzultací s Úřadem pro ochranu osobních údajů (dále jen ÚOOÚ), a to prostřednictvím KOOÚ za podmínek, kdy je to nutné a účelné
- prostřednictvím KOOÚ ohlašování případů narušení bezpečnosti osobních údajů do 72 h od doby, kdy se jako správce o narušení dozví, na ÚOOÚ a pokud je to třeba i dotčeným osobám, o jejichž osobní údaje se jednalo;
- vedení záznamů o zpracováních osobních údajů, a to prostřednictvím dokumentu Registr osobních údajů, který je přílohou 1. tohoto dokumentu
- plnění pokynů ÚOOÚ v plném rozsahu

4.1.2 Povinnosti osob přicházejících do styku s osobními údaji

Starosta obce Březí u Mikulova stanovuje tímto povinnosti zaměstnanců přicházejících do styku s OÚ.

Osoby přicházející do styku s osobními údaji jsou povinny:

- zpracovávat osobní údaje v souladu s GDPR a příslušnými zákony ČR, ostatními právními normami, jakož i dalšími předpisy EU, které se na tuto problematiku při jejich práci vztahují;
- zachovávat mlčenlivost o osobních údajích a přijatých opatřeních k jejich ochraně, a to i po skončení svého pracovněprávního nebo smluvního vztahu u úřadu;
- zabránit neoprávněnému čtení, pozměnění, smazání, či znepřístupnění osobních údajů, nevytvářet kopie software nebo listin s osobními údaji pro jinou než pracovní potřebu a nepřipustit takové jednání ani jiným osobám, například tím, že nebude možné z nosičů či úložišť počítačových dat kopírovat na jiné nosiče větší množství osobních údajů bez toho, že by toto kopírování schválilo a zároveň i technicky umožnilo (např. zadáním hesel) současně dvě nebo více osob;
- při používání výpočetní techniky používat pouze bezpečný hardware a software, a to bezpečným způsobem a bezodkladně hlásit veškeré nestandardní projevy používané výpočetní techniky příslušným zaměstnancům v oddělení IT;

- dodržovat zásady bezpečného používání výpočetní techniky zejména používáním vhodných hesel a dbát na jejich ochranu před prozrazením; nenavštěvovat rizikové webové stránky apod., okamžitě hlásit jakékoli důvodné podezření na ohrožení bezpečnosti osobních údajů.

4.2 Dokumentace dokládající implementaci požadavků GDPR

Aby Obec prokázala shodu s požadavky GDPR, byly zpracovány a implementovány následující dokumenty:

4.2.1 Směrnice Ochrana osobních údajů

V tomto dokumentu jsou popsána veškerá pravidla související s požadavky GDPR v podmínkách Obce.

4.2.2 Registr osobních údajů

Výchozí dokument pro identifikaci a správu osobních údajů. Detailní popis je uveden v kapitole 4.7.2 Registr osobních údajů.

4.2.3 Analýza stávajícího stavu ochrany osobních údajů

Dokument popisující výchozí stav zabezpečení ochrany osobních údajů a soupis nápravných a preventivních opatření nutných k dosažení shody s požadavky GDPR.

4.2.4 Informační memoranda

Informační memorandum je dokument, vycházející z povinnosti GDPR v článku 13 Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů.

Informační memorandum musí poskytovat příslušnému subjektu údajů (zaměstnanec, občan, obchodní partner - dodavatel, subjekt nahlížející na internetové stránky Obce a využívající Kontaktní formulář) následující informace:

- totožnost a kontaktní údaje správce a jeho případného zástupce, případně kontaktní údaje případného pověřence pro ochranu osobních údajů
- účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;
- oprávněné zájmy správce
- případné příjemce nebo kategorie příjemců osobních údajů;
- případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci
- dobu, po kterou budou osobní údaje uloženy
- existenci práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů
- existenci práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
- existenci práva podat stížnost u dozorového úřadu;
- skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů
- skutečnost, že dochází / nedochází k automatizovanému rozhodování, včetně profilování

4.2.4.1 Informační memorandum pro zaměstnance

Po zpracování a schválení tohoto informačního memoranda musí organizace zajistit seznámení zaměstnanců s tímto dokumentem.

U zaměstnanců stávajících lze toto provést formou seznámení v rámci porad příslušných organizačních jednotek s tím, že v zápisu bude tato skutečnost uvedena.

V rámci přijímacího řízení s novým zaměstnancem je nutno ho s tímto informačním memorandem seznámit a vložit do Osobního spisu.

Platí zásada informovanosti, tzn. každý zaměstnanec, a to s jakoukoli formou pracovněprávního vztahu musí být s tímto memorandem seznámen.

4.2.4.2 Informační memorandum pro smluvní partnery (Dodavatele)

Informační memorandum pro smluvní partnery je vhodné a účelné přikládat jako přílohu SoD, a to u tzv. „nových smluv", tedy smluv uzavřených po 25.5.2018, data nabytí účinnosti GDPR.

U stávajících smluv, především se to týká rámcových smluv, je vhodné a účelné smluvního partnera pouze informovat. Není bezpodmínečně nutné v rámci rámcových smluv s dodavateli provádět dodatek SoD, jedině na jeho přímý požadavek.

Není vhodné vkládat obsah informačního memoranda přímo do textu SoD. Při případně změně GDPR a především v souvislosti se změnami legislativy ČR by bylo následně nutné doplnit Dodatek k SoD.

4.2.4.3 Informační memorandum pro občany Obce

Forem, jak občany obce informovat o zpracování jejich osobních údajů je více:

- Umístění textu memoranda na Úřední desce
- Vložení textu memoranda na internetových stránkách obce
- Dát k dispozici občanovi při návštěvě obecního úřadu v tištěné formě

4.2.5 Smlouva o zpracování osobních údajů

V případě, že je dodavatel současně Zpracovatelem osobních údajů Správce (Obec) není možné využít pouze Informační memorandum – dodavatel, jak je popsáno v kapitole 4.2.5 ale je nutno uzavřít s tímto dodavatelem Smlouvu o zpracování osobních údajů.

Obsah takové smlouvy je definován v článku 28 odstavec 3 GDPR. Tato smlouva zejména stanoví, že zpracovatel:

- zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;
- zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
- přijme všechna opatření požadovaná podle článku 32 (Zabezpečení zpracování);
- dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 (Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky) a 4 (Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě mezi správcem a zpracovatelem podle odstavce 3, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto nařízení. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel)
- zohledňuje povahu zpracování, je Správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů (stanovených v kapitole III – Práva subjektu údajů)
- je Správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 (Zabezpečení zpracování); 33 (Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu), 34 (Oznamování případů porušení zabezpečení osobních údajů subjektu údajů), 35 (Posouzení vlivu na ochranu osobních údajů) a 36 (Předchozí konzultace), a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;
- v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí Správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;

- poskytne Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.

Tuto smlouvu je bezpodmínečně nutné uzavírat s dodavateli v následujících případech, kdy dodavatel zabezpečuje:

- zpracování personálních osobních údajů – personální agentury
- zpracování finančních a mzdových podkladů – účetní firmy
- provozování informačního systému

Není potřeba uzavírat tuto smlouvu v oblastech, kde je mlčenlivost daná přímo zákonem, tj. u služeb advokátů, smluvních lékařů (pokud nejde o firmu s více lékaři poskytující službu apod.

4.3 Technická opatření k zajištění ochrany osobních údajů

Zajištění ochrany osobních údajů v rámci jejich zpracování se věcně dotýká celé řady činností ve Obce. Je nezbytné nastavit některé procesy pro řízení práv subjektů nebo pro řešení incidentů. Nicméně implementace požadavků GDPR nemá po nastavení principů do každodenního života Obce žádný vliv na realizaci procesů nebo agend tak, jak byly doposud v souladu se stávajícími interními dokumenty každodenně vykonávány.

4.3.1 Zásady ochrany osobních údajů při jejich zpracování

- zákonnost (tzn. i předvídatelnost) – předpokládá plnění smlouvy se subjektem údajů (zaměstnanec, zákazník, dodavatel), splnění právní povinnosti Obce, ochrana životně důležitých zájmů Obce
- transparentnost - všechny informace a sdělení ke zpracování a ochraně osobních údajů jsou jednoduše přístupné, srozumitelné a vyhotovené v jasné a jednoduché řeči
- korektnost (tzn. nikoli lstivé jednání) - zohledňovat zájmy a očekávání dotčených osob, nelze je bezdůvodně přehlížet, nelze zneužívat mylných představ osob o tom, jak bude s jejich osobními údaji pracováno,
- účelové omezení - účel zpracování osobních údajů musí být znám již při sběru dat
- minimalizace údajů – používat jen nezbytně nutné minimum osobních údajů, dbát na jejich přesnost
- časové omezení uložení – pracovat s osobními údaji jen po nezbytně nutnou dobu, čím méně osobních údajů spravuji, tím více snižuji riziko potenciálního incidentu
- integrita, důvěrnost, mlčenlivost (ochrana osobních údajů)

Následující zásady je povinen dodržovat každý zaměstnanec Obce:

- jakékoli osobní údaje, a to obzvláště citlivé, sděluji jen tomu, pro koho jsou určeny,
- dávat pozor, aby e-mail s citlivými údaji nebyl odeslán jinému příjemci než tomu, komu byl určen.
- vytištěné materiály s osobními údaji vždy zabezpečím tak, aby nemohly být zneužity
- když se vzdálím od pracovního stolu, uschovám tištěné materiály do stolu, který zamknu a vypnu počítač
- svůj firemní notebook, tablet a telefon, který obsahuje citlivé a osobní údaje, ochráním i mimo firmu proti krádeži a zneužití.
- nesmím vynášet a sdělovat jakékoli informace o organizaci, kde pracuji
- data, která potřebuji předat na externím nosiči, šifruji
- všechna svá hesla chráním jako oko v hlavě
- při každé manipulaci s osobními údaji se snažím předvídat a zabránit rizikům jejich úniku, ztráty či zneužití.

4.4 Technická opatření k zajištění ochrany osobních údajů

4.4.1 Písemnosti a jiné hmotné nosiče dat

Řízení písemností je v rámci úřadu OÚ Březí u Mikulova upraveno dokumentem Spisový řád (v platném aktuálním znění).

Tento dokument obsahuje veškerá pravidla a postupy zacházení s dokumenty, které obsahují mj. i OÚ, a to včetně tzv. citlivých OÚ.

4.4.2 Elektronické datové soubory obsahující osobní údaje

Pro správu a využívání elektronických datových souborů platí následující pravidla:

- Každý počítač OÚ Březí u Mikulova je součástí domény, chráněn doménovým uživatelským jménem a heslem
- Zálohování probíhá pouze na serverech, lokální stanice se automaticky nezálohují. Uživatelé mají možnost kopírovat data do přiděleného síťového úložiště, které se pak zálohuje
- Práva pro přístup k datům na síti přiděluje správce IT na základě požadavku vedoucího zaměstnance (ne nutně od Starosty obce),

4.4.3 Kamerové a audio záznamy

Veškeré kamerové, či audio záznamy, musí být pořizovány jen v souladu s příslušnými právními předpisy. Veškeré kamery a ukládání záznamů z těchto kamer, musí být posuzovány i z hlediska jejich dopadu na ochranu osobních údajů. Záznamy z těchto kamer musí být kódovány a ve formě tzv. černé skříňky musí být uloženy mimo dosah nepovolaných osob, nebo musí být přijata jiná vhodná opatření, která by zabránila jejich ztrátě, zničení nebo zneužití. Z důvodu bezpečnosti a ochrany zdraví při práci, včetně využití pro náhradu škody zaměstnanci, se považuje **lhůta pro vymazání kamerových záznamů** za přiměřenou, pokud jsou kamerové záznamy vymazány nejpozději do **21 dnů od jejich pořízení**, a to vzhledem ke lhůtám, ve kterých jsou zaměstnanci povinni hlásit zaměstnavateli vznik škody podle zákoníku práce, **jinak platí lhůta 7 dnů** od jejich pořízení.

Žádné kamerové, či audio záznamy, nesmí být pořizovány tam, kde by mohly urážet lidskou důstojnost nebo zvyšovat nebezpečí úrazu či vzniku škody.

O umístění kamer nebo pořizování audiozáznamů musí být všechny osoby řádně informovány informačními tabulkami, či jiným vhodným způsobem, včetně informace, kde mohou získat o takových záznamech podrobnější informace.

4.5 Posouzení dopadu činnosti na ochranu osobních údajů

Pokud je pravděpodobné, že určitý druh zpracování osobních údajů v rámci úřadu, nebo u jejího zpracovatele, zejména při využití nových (počítačových) technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, vypracuje KOOÚ dokument **Posouzení dopadu své činnosti na ochranu osobních údajů**, který musí obsahovat:

- systematický popis zamýšleného zpracování,
- posouzení rizik,
- provedení testu proporcionality, je-li to vhodné a účelné
- přijatá opatření ke snížení nebo eliminace rizika iniciace incidentu, a to včetně potenciálního

Starosta a zaměstnanci úřadu jsou povinni zkoumat, zda:

- v rámci úřadu není prováděno systematické a rozsáhlé 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 nebo mají na fyzické osoby podobně závažný dopad.
- nejsou podle úrovně výpočetní techniky, zvláště pak v případě využití umělé inteligence, zaměstnanci, zákazníci, či jiné osoby, tříděny do určitých skupin a v důsledku takového roztřídění do skupin, zda pak nejsou bez konečného rozhodnutí člověka určována jejich práva, či povinnosti (např. rozhodování o změně pracovního zařazení, o výši mzdy, či benefitů, o skončení pracovního poměru a podobně).
- v rámci úřadu není prováděno rozsáhlé zpracování zvláštních kategorií údajů (citlivých údajů, včetně biometrických),

Vzhledem k tomu, že podle znalostí procesů a agend v rámci úřadu OÚ Březí u Mikulova není prováděno rozsáhlé zpracování zvláštních kategorií údajů (citlivých údajů, včetně biometrických), není v rámci úřadu v tomto směru vysoké riziko pro práva a svobody fyzických osob.

Pokud se jedná o rozsáhlé systematické monitorování veřejně přístupných prostorů kamerovými systémy, tím, že Obec dodržuje zásady uvedené v kapitole 4.4.3 není ani toto zpracování osobních údajů vysokým rizikem pro práva a svobody fyzických osob.

4.6 Konzultace s Úřadem pro ochranu osobních údajů

Vzhledem k tomu, že v rámci analýzy stavu ochrany osobních údajů a posouzení dopadu činnosti úřadu na ochranu osobních údajů nebylo zjištěno, že by určitý druh zpracování osobních údajů v rámci úřadu, nebo u jejího zpracovatele, zejména při využití nových (počítačových) technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování osobních údajů, mohl mít za následek vysoké riziko pro práva a svobody fyzických osob, v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika, jsou vedoucí zaměstnanci úřadu povinni sledovat, zda nedošlo ke změně těchto poměrů v rámci úřadu.

Pokud by v souvislosti se změnami zpracování osobních údajů v rámci úřadu došlo k situaci, že by vzniklo vysoké riziko pro práva a svobody fyzických osob a nebylo by známo, jaká přijmout opatření ke zmírnění tohoto rizika, jsou vedoucí zaměstnanci úřadu povinni informovat KOOÚ a nastalou situaci s ním konzultovat.

KOOÚ zpracuje stanovisko, které předloží Starostovi ke schválení. Veškeré následné aktivity jsou již plně v kompetenci KOOÚ, který:

- projedná stanovisko s ÚOOÚ
- Informuje Starostu o výsledku jednání s ÚOOÚ
- Ve spolupráci se Starostou a původcem podnětu dále řeší situaci až do konečné fáze implementace nápravných či preventivních opatření

4.7 Povinnost vést záznamy o činnostech zpracování osobních údajů

4.7.1 Úvod

Starosta je povinen zajistit, aby byly o veškerém zpracování osobních údajů vedeny záznamy.

4.7.2 Registr osobních údajů

Základním dokumentem o veškerém zpracování osobních údajů a jejich záznamů je v rámci úřadu **OÚ Březí u Mikulova** dokument **Registr osobních údajů**. Tento dokument obsahuje veškeré požadavky GDPR uvedené v kapitole 4.7.1Úvod, a to v kontextu všech procesů, které jsou v rámci úřadu OÚ Březí u Mikulova realizovány. Registr osobních údajů je řízený dokument, tzn. podléhá změnovému řízení dokumentů.

Registr OÚ je dokument ve formátu .xls a obsahuje několik následujících záložek":

- Obec Březí – obsahem záložky je kompletní seznam osobních údajů zpracovávaných v rámci Obce
- Zákony ČR – ve složce jsou uvedeny zákony a související legislativa, použitá v Registru OÚ vzhledem k definování tzv. Právního statusu osobních údajů v jednotlivých dokumentech
- Skartační znaky – tabulka skartačních znaků jednotlivých dokumentů
- ZOZOÚ_Správce – zjednodušený schematický přehled tzv. Záznamů o zpracování osobních údajů z pohledu Správce - tento přehled nemá praktický dopad, jde jen o formální naplnění požadavku nařízení GDPR
- ZOZOÚ_Zpracovatel – zjednodušený schematický přehled tzv. Záznamů o zpracování osobních údajů z pohledu Zpracovatele- tento přehled nemá praktický dopad, jde jen o formální naplnění požadavku nařízení GDPR

4.7.3 Detailní popis složky OBEC Březí

- Oblast procesů/proces/subproces – hierarchická struktura procesů a agend Obce
- Dokument – název konkrétního dokumentu, který obsahuje osobní údaje – dokument může nabývat více forem, viz sloupec Způsob zpracování
- Status dokumentu
  - Interní – interní dokument, sloužící jak pro interní potřebu Obce při realizaci procesů nebo v některých případech jako výstup předávaný orgánům veřejné a státní moci
  - Externí – dokument, který vychází ze zákonné či jiné předlohy a v Obci je zpracováván, například formulář Přiznání k dani silniční za kalendářní rok XXXX podle zákona č. 16/1993 Sb., o dani silniční, apod.
- Archivační/skartační znak – příslušný znak podle Spisového řádu
- Zpracovatel – název pracovní funkce či role zaměstnance, který osobní údaje v daném dokumentu zpracovává, kontroluje a / nebo schvaluje, tj. dostane se tzv. do kontaktu s osobními údaji v dokumentu.
- Umístění dokumentu – znamená definovat možnosti umístění dokumentu v rámci jeho životního cyklu. Detailní popis je uveden v dokumentu Spisový řád. Z důvodů přehledu je tedy u každého dokumentu uvedeno, kde je možný jeho výskyt.
  - Příruční registratura – stoly či skříně umístěné v kanceláři – k dokumentům má přístup jen příslušný zpracovatel, který je současně odpovědný za jejich ochranu před zneužitím. V případě skříní na chodbách, je bezpodmínečně nutné zabránit přístupu k dokumentům nepovolaným osobám.
  - Spisovna – zpravidla uzavřený uzamykatelný prostor, kam jsou ukládány dokumenty a popřípadě i data v době, kdy již dokumenty nejsou potřebné, ale podle příslušného archivačního znaku je organizace povinna je mít ještě uložené
- Způsob zpracování – nastávají v zásadě tři „stavy" dokumentů
  - PP – dokument je a navždy bude jen v tzv. papírové formě
  - DD – dokument je digitalizován, původní předloha je založena jako papírový dokument a dále je využívaná pouze jeho digitální forma, v případě dokumentu došlého např. formou e-maulu se již s dokumentem pracuje jako s plně digitalizovaným
  - DIS – data, a to včetně osobních údajů jsou zpracovávána pouze v informačních systémech Obce
- Účel zpracování - nařízení GDPR v článku 30 Záznamy o činnostech zpracování předepisuje povinnost Správce přesně definovat tzv. účel zpracování. Registr osobních údajů je v Obci vytvořen na principu využití struktury procesů a agend, realizovaných v rámci Obce. V Registru osobních údajů je tedy jako účel zpracování uvedeno Realizace procesů.
- Právní titul – informace o tom, na jakém právním základě jsou osobní údaje zpracovávány. Mohou nastat následující varianty:
  - Zpracování na základě požadavků zákona – osobní údaje jsou zpracovávány na základě konkrétního zákona ČR (Vyhlášky, Nařízení vlády ČR, Rozhodnutí Ústavního soudu ČR či Nařízení EU. Seznam zákonů využitých v Obci je uveden v následujícím sloupci Registru osobních údajů s názvem „ID zákona".
  - Zpracování na základě požadavků smlouvy – osobní údaje jsou zpracovávány na základě smlouvy a to i ty osobní údaje, které jsou zpracovávány v rámci jednání před jejím uzavřením, pokud je toto jednání prokazatelně vedeno s úmyslem smlouvu uzavřít – to se týká prakticky jakýchkoliv smluv
  - Zpracování na základě oprávněného zájmu Obce – oprávněný zájem Obce je dle nařízení GDPR článku 6 Zákonnost zpracování definováno jako nezbytné pro účely zájmů Správce (Obec) kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů (např. děti). Z toho vyplývá, že i v Obci je využit tento typ zpracování, i když v malém rozsahu.
  - Zpracování na základě získaného souhlasu – tento způsob zpracování je využíván jen tehdy, není-li možné využít některý z výše uvedených právních titulů. Vzhledem k administrativní náročnosti získávání souhlasů je vhodné tento způsob zpracování minimalizovat. V žádném případě ale nesmí být porušena základní práva a svobody subjektu údajů.
    POZNÁMKA: V rámci implementace požadavků GDPR nebyla v Obci definována potřeba zpracování osobních údajů na základě souhlasu.
- ID zákona – číselné označení zákona ze seznamu v záložce Zákony ČR
- Osobní údaje – identifikační údaje

- Jméno -
- Příjmení
- Rodné příjmení
- Podpis
- Elektronický podpis
- Datum narození
- Rodné číslo
- Osobní číslo (zaměstnanec)
- Funkce
- Útvar
- Identifikační údaje zákazníka / dodavatele

- Osobní údaje – kontaktní údaje
  - Adresa trvalého bydliště/sídla
  - Adresa přechodného bydliště
  - Adresa doručovací
  - e-mail
  - Kód datové schránky
  - Telefonní číslo
  - IČO
  - DIČ
  - Kontaktní údaje na sociálních sítích
- Osobní údaje – bankovní spojení
  - Číslo účtu
  - Číslo SIPO
- Osobní údaje - doklady ke ztotožnění
  - Cestovní pas č.
  - Občanský průkaz č.
  - Řidičský průkaz č.
- Zdravotní a sociální pojištění - veřejné
  - Zdravotní pojišťovna
  - Číslo průkazu pojištěnce
- Zdravotní a sociální pojištění – komerční
  - Druh pojistky
  - Pojistná smlouva
- Sociální/demografické informace
  - Věk
  - Pohlaví
  - Titul
  - Rodinný stav
  - Údaje o rodině (děti, manželka, atd.)
- IT identifikátory (nepovinné)
  - Uživatelské jméno
  - Heslo
  - IP adresa

- Typ koncového zařízení
- GPS

- Citlivé osobní údaje
  - Lékařské zprávy
  - Zdravotní stav
  - Účast v odborech
  - Náboženství
  - Trestní věci
- Informační systémy
  - Název IS
  - Server
  - Součást reportů

4.8 Povinnost ohlašovat případy narušení bezpečnosti osobních údajů – řízení incidentů

4.8.1 Úvod

Řízení incidentů v oblasti ochrany OÚ je jedním ze stěžejních interních procesů úřadu. Aby nedošlo ke škodám v důsledku pokut od ÚOOÚ, je bezpodmínečně nastavit proces přesně podle požadavků GDPR, dále ho implementovat a vyhodnocovat rizika tak, aby byla minimalizována hrozba incidentů s možnými rozsáhlými dopady.

4.8.2 Zdroje potenciálních incidentů

Incidenty mohou pocházet z těchto zdrojů

- Zaměstnanci – zpravidla bývalí nebo i současní
- Politická konkurence – s cílem poškození OÚ Březí u Mikulova
- Nespokojený občan
- Subjekt, který se domnívá, že nebylo učiněno zadost při uplatňování jeho práv
- Kdokoli – s možným potenciálem pro vydírání apod.

4.8.3 Typy incidentů

V zásadě mohou nastat následující situace:

- Zaměstnanec upozorní na možnost hrozby incidentu – toto je pozitivní případ a v rámci implementace GDPR je potřeba všem zaměstnancům OÚ Březí u Mikulova sdělit informaci o takové možnosti. Nahlášení, byť jen potenciální hrozby musí být řízeno jako jakýkoli incident.
- Zaměstnanec upozorní na incident – řízení přímo podle pravidel pro řízení incidentů
- Incident ohlášen „z venku" – jakékoli hlášení incidentu tzv. „z venku" musí být prověřeno a řízeno
- Incident ohlášen přímo z ÚOOÚ – bezpodmínečně nutno řídit podle pravidel

4.8.4 Detailní postup řízení incidentu v oblasti ochrany OÚ

V následujících kapitolách jsou popsány procesy řízení incidentů v oblasti OÚ.

Nástrojem pro řízením požadavků je tabulka **„Registr incidentů"**, uvedená v příloze tohoto dokumentu.

4.8.4.1 Převzetí a evidence nahlášení incidentu

Mezi základní povinnosti každého zaměstnance úřadu patří převzetí podnětu o incidentu a následné předání informace KOOÚ.

Oznámení o incidentu však může být doručeno i z jiných zdrojů, následující postup je však zcela jednotný.

KOOÚ zaeviduje následující údaje o incidentu:

- Subjekt hlášení incidentu
- Datum převzetí hlášení, přesný čas
- Předmět incidentu

KOOÚ následně provede ověření / ztotožnění odesílatele informace o incidentu. Ztotožnění však není podmínku pro realizaci následných kroků, pouze je prováděna z hlediska usnadnění komunikace. Řídit je bezpodmínečně nutno, a to se stejnou mírou odpovědnosti i **anonymní oznámení**.

Závěrečnou aktivitou je předání informace subjektu hlášení o incidentu o zahájení aktivit v souvislosti s jeho podnětem.

4.8.4.2 Zpracování interního stanoviska k incidentu

KOOÚ dále projedná s příslušnými zainteresovanými interními stranami následující:

- Oprávněnost hlášení o incidentu
- Návrh na možné řešení incidentu

KOOÚ následně stanoví další postup řešení. Možné varianty jsou:

- Bude muset být informován subjekt OÚ, vůči kterému došlo k incidentu
- Bude muset být informován Úřad pro ochranu osobních údajů, a to v časovém limitu 72 hodin
- Incident není takové povahy, aby bylo nutno informovat jakoukoli z výše uvedených stran, bude projednáván pouze interně

KOOÚ zpracuje návrh stanoviska a:

- Provede záznam do „Registru incidentů"
- Bezodkladně informuje Starostu obce Březí u Mikulova o incidentu
- Ve spolupráci se zaměstnanci OÚ Březí u Mikulova zpracuje konečné stanovisko
- Zašle závazné stanovisko oznamovateli incidentu

POZNÁMKA: v případě potřeby projedná Starosta incident se Zastupitelstvem obce.

4.8.4.3 Vypořádání incidentu

KOOÚ ve spolupráci se všemi zainteresovanými stranami zahájí okamžité řešení incidentu. O postupu řešení a následně o výsledcích informuje Starostu, a to bezodkladně tak, aby v případě potřeby mohlo být realizováno takové nápravné nebo preventivní opatření, které je pouze a jedině v jeho kompetenci.

O vypořádání incidentu vede KOOÚ záznam v „**Registru incidentů**" a dále podrobně informuje Starostu obce.

Následným krokem je podle závažnosti incidentu jeho projednání buď 1x měsíčně nebo ihned podle okolností v rámci jednání Zastupitelstva obce.

V zápisu z jednání Zastupitelstva obce musí být ve věci incidentu uvedeno minimálně:

- Okolnosti, příčina a dopady incidentu
- Míra operativnosti vyřešení incidentu
- Nutnost definovat nápravná / preventivní opatření
- Nutnost mitigace, aktualizace rizik

Úkoly spojenými s incidenty v oblasti OÚ je přímo pověřen KOOÚ, průběhem jejich plnění a výsledky informuje přímo Starostu obce.

4.9 Přenositelnost osobních údajů

Starosta obce je povinen zajistit, aby byly veškeré osobní údaje, jejichž zpracování je založeno na souhlasu nebo na smlouvě a jejichž zpracování se provádí automatizovaně, přenositelné k jinému správci.

Starosta obce je povinen s právem přenositelnosti počítat již dopředu a zpracování osobních údajů musí být pro správce prováděno takovým způsobem, aby při přenosu osobních údajů na nového zpracovatele bylo v maximální možné míře eliminováno:

- rozkrytí systému práce úřadu,
- prozrazení obchodních tajemství a/nebo obchodní strategie.

Starosta obce je povinen také zajistit, aby při přenosu osobních údajů konkrétní osoby k jinému správci nebyla nepříznivě dotčena práva a svobody jiných osob, nebo práva duševního vlastnictví.

Dále je Starosta obce povinen zajistit, že na přenositelnost osobních údajů musí být subjekt údajů výslovně upozorněn a toto právo musí být uvedeno zřetelně a odděleně od jakýchkoli jiných informací již v okamžiku první komunikace se subjektem údajů, tedy s osobami, jejichž osobní údaje mají být zpracovávány.

4.10 Řízení práv subjektů údajů

4.10.1 Úvod

Aplikace práv subjektů údajů je jedním z nejvýznamnějších přínosů GDPR. Na jedné straně přináší občanům rovnovážný stav vůči zpracovatelům OÚ, na straně druhé musí každá organizace, tedy i obec, která OÚ zpracovává vytvořit interní systém, definovat procesy, jak tato práva subjektů OÚ aplikovat.

4.10.2 Rekapitulace práv subjektů OÚ

Práva subjektů OÚ jsou uvedena v následujícím stručném přehledu.

Právo subjektu údajů na přístup k osobním údajům (Článek 15)	Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány
Právo na opravu (Článek 16)	Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné (a/nebo neúplné) osobní údaje, které se ho týkají.
Právo na výmaz („právo být zapomenut“) (Článek 17)	Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat
Právo na omezení zpracování (Článek 18)	Subjekt údajů má právo na to, aby správce omezil zpracování
Právo na přenositelnost údajů (Článek 20)	Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil
Právo vznést námitku (Článek 21)	Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají,
Automatizované individuální rozhodování, včetně profilování (Článek 22)	Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.
Omezení (Článek 23)	Právo subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na újmu účelu omezení.

4.10.3 Typy subjektů OÚ s požadavkem na výkon práv

Subjekty, které mohou požadovat na úřadu výkon svých práv v oblasti OÚ jsou následující:

- Občané – každý občan ČR je subjektem osobních údajů
- Zaměstnanci – osoba, která byla, je nebo bude ve vztahu k úřadu v jakémkoli typu smluvního vztahu – zaměstnanecký poměr, DPO, DPČ
- Obchodní partneři – dodavatelé
- Externí osoby – jde o osoby, které se v rámci nabídky na internetových stránkách úřadu přihlásili např. za účelem získání informací a kteří si chtějí ověřit, zda jsou či nejsou jejich OÚ Obcí zpracovávány
- Osoby s nepřátelským postojem k úřadu – osoby, jejich jedinou motivací bude jakýmkoli způsobem škodit (politická konkurence, nespokojený občan)

Jak je z výše uvedeného patrné, subjektů, které se mohou ať už právem nebo s jasným cílem poškodit Obec je mnoho. Z tohoto důvodu musí být procesy nastaveny a dodržovány s maximální mírou odpovědnosti.

4.10.4 Detailní postup vypořádání požadavku subjektu OÚ na aplikaci jeho práv

V následujících kapitolách jsou popsány procesy vypořádání práv subjektů OÚ.

Nástrojem pro řízením požadavků je tabulka **„Registr aplikace práv subjektu údajů“,** uvedená v příloze tohoto dokumentu.

4.10.4.1 Převzetí a evidence požadavků subjektu OÚ

Mezi základní povinnosti každého zaměstnance úřadu patří převzetí podnětu k aplikaci práv subjektů OÚ a následné předání informace KOOÚ.

KOOÚ zaeviduje následující atributy požadavku:

- Subjekt OÚ
- Datum převzetí požadavku
- Předmět požadavku

KOOÚ následně provede ověření / ztotožnění Subjektu OÚ. Závěrečnou aktivitou je předání informace Subjektu OÚ o zahájení aktivit v souvislosti s jeho požadavkem.

4.10.4.2 Zpracování interního stanoviska

KOOÚ dále projedná s příslušným Zpracovatelem OÚ následující:

- Je nutno ověřit, zda je předmět požadavku relevantní – tedy zda OÚ existují či ne
- V případě potvrzení jejich existence je nutno vyhodnotit oprávněnost požadavku

Oprávněnost požadavku bude vyhodnocena následujícím způsobem. KOOÚ ve spolupráci se Zpracovatelem zkontrolují v Registru OÚ tzv. Právní titul OÚ, který může být:

- Zpracování OÚ na základě souhlasu Subjektu OÚ
- Zpracování OÚ na základě zákonného požadavku
- Zpracování OÚ na základě Smlouvy
- Zpracování OÚ na základě oprávněného zájmu úřadu

Následujícím krokem následujícím krokem je posouzení příslušného archivačních /skartačního znaku ve vztahu k osobním údajům.

V případě, že v Registru OÚ je uvedeno, že se OÚ nacházejí v IS, projedná KOOÚ s Administrátorem IS možnosti výkonu práv subjektu.

Závěrem této etapy zpracuje KOOÚ závazné stanovisko a provede záznam do „**Registru aplikace práv subjektu údajů“.**

4.10.4.3 Vypořádání stanoviska k požadavku Subjektu OÚ

KOOÚ odešle vyjádření Subjektu OÚ.

V případě pozitivního stanoviska oznámí Subjektu OÚ termín, ke kterému bude jeho požadavek naplněn.

V případě, že by vyhovění požadavku Subjektu OÚ vyžadovalo nepřiměřené úsilí či náklady, informuje KOOÚ daný subjekt. Současně může požádat o prodloužení data na vypořádání požadavku.

V případě negativního stanoviska na požadavek Subjektu OÚ je KOOÚ povinen předat Subjektu OÚ exaktní zdůvodnění negativního stanoviska, jako například:

- Archivační lhůta OÚ neumožňuje naplnění daného požadavku
- OÚ jsou zpracovávány v souladu se zákonem nebo na základě smlouvy, a tedy neexistuje jakákoli možnost vyhovět požadavku
- OÚ jsou zpracovávány na základě tzv. oprávněného zájmu úřadu a vyhověním požadavku Subjektu OÚ by došlo k porušení GDPR.

O veškeré komunikaci se subjektem OÚ vede řádnou dokumentaci a současně vše zaznamenává v **Registru aplikace práv subjektu údajů.**

4.10.4.4 Realizace požadavku Subjektu OÚ

V případě dohody se subjektem OÚ provedou příslušný Zpracovatel OÚ a Administrátor IS technické kroky, které vedou ke splnění požadavku Subjektu OÚ. O provedení těchto kroků je proveden záznam v **Registru aplikace práv subjektu údajů.**

4.10.4.5 Záznamy o realizaci aplikace práv Subjektů OÚ

KOOÚ má povinnost minimálně 1 x měsíčně informovat Starostu obce o stavu řízení práv Subjektů OÚ. Ve zprávě bude uvedeno minimálně:

- Počet a způsoby vypořádání požadavků Subjektů OÚ
- Problémy, nápravná / preventivní opatření
- Nutnost mitigace rizik (změna hodnocení míry rizika – snížení či naopak zvýšení)
- Návrh systémových změn

V případě potřeby seznámí Starosta obce Zastupitelstvo, obsah jednání musí být součástí zápisu z jednání Zastupitelstva obce.

4.11 Pověřenec pro ochranu osobních údajů

Z nařízení GDPR nevyplývá povinnost Starosty obce Březí u Mikulova jmenovat pověřence pro ochranu osobních údajů – DPO.

S vědomím společenské odpovědnosti při ochraně osobních údajů však Starosta obce Březí u Mikulova zajistilo osobu, vykonávající roli tzv. Konzultanta pro ochran osobních údajů (KOOÚ), který bude odpovědný přímo Starostovi obce Březí u Mikulova a který bude odpovědný za následující aktivity:

- Dohled nad řádnou a úplnou implementací požadavků GDPR do OÚ Březí u Mikulova
- Poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;
- Monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
- Poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování
- Řízení procesů aplikace práv subjektů OÚ
- Řízení incidentů v oblasti OÚ
- Komunikaci s Úřadem pro ochranu osobních údajů v nezbytných případech

Starosta obce Březí u Mikulova se zavázal ve vztahu k působnosti role Konzultanta pro ochranu osobních údajů k zajištění:

- náležitého a včasného zapojení do veškerých záležitostí souvisejících s ochranou osobních údajů

- podpory Konzultanta pro ochranu osobních údajů při plnění úkolů tím, že mu poskytují zdroje nezbytné k plnění těchto úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí
- aby konzultant pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován.
- že konzultant pro ochranu osobních údajů je přímo podřízen Starostovi obce Březí u Mikulova
- že konzultant pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností, v souladu s právem Unie nebo členského státu.
- Že konzultant pro ochranu osobních údajů může plnit i jiné úkoly a povinnosti. Správce nebo zpracovatel zajistí, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.

4.12 Předávání osobních údajů do zahraničí

OÚ Březí u Mikulova nepředává osobní údaje zaměstnanců do zahraničí.

4.13 Internetové obchodování a věrnostní systémy

OÚ Březí u Mikulova nerealizuje internetový obchod.

OÚ Březí u Mikulova využívá prostředí internetu k prezentaci svých činností. Na stránkách http://www.breziumikulova.cz/kontaktni-formular je prezentována možnost získat formou dotazu informace.

5 Odpovědnosti

Odpovědnosti jednotlivých rolí jsou definovány přímo v textu.

6 Registr souvisejících dokumentů

6.1 Obecně závazné předpisy, Související dokumenty občanů a ostatních zainteresovaných stran

Přehled identifikovaných Nařízení EU, Zákonů a Vyhlášek ČR je uveden v dokumentu Registr osobních údajů, záložka Obec Březí.

6.2 Přímo související dokumenty OÚ

Řád	Organizační řád
Řád	Spisový řád

7 Přílohy

Příloha 1: Registr osobních údajů

Příloha 2: Registr aplikace práv subjektu údajů

Příloha 3: Registr incidentů