

SMĚRNICE NA OCHRANU OSOBNÍCH ÚDAJŮ a ICT BEZPEČNOST

Název organizace : Obec Bělkovice – Laštány

Sídlo organizace : Bělkovice – Laštány č. 139, 783 16 Bělkovice - Laštány

Platnost od: 1.12.2022

Účinnost od: 1.12.2022

Počet stran: 18

Číslo směrnice: 4 / 2022

Tato směrnice je v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů a v souladu s Nařízením Evropského parlamentu a rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (dále jen „Nařízení“) tento vnitřní předpis je využíván pro potřeby naší organizace (dále jen „směrnice“):

Čl. 1

Předmět směrnice

- 1) Tato směrnice upravuje postupy a povinnosti obce, jejich zaměstnanců, zastupitelů a dalších osob při nakládání s osobními údaji. Upravuje dále pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchování osobních údajů a ICT bezpečnosti.
- 2) Touto směrnicí jsou dále stanoveny vnitřní pravidla pro:
 - a) užívání výpočetní techniky (hardware) a programového vybavení (software)
 - b) užívání počítačové sítě obce včetně všech počítačů a dalších technických zařízení (tiskárny, modemy, scannery, rozvaděče atd.), které jsou přímo nebo prostřednictvím jiného zařízení funkčně připojeny k počítačové síti obce.
 - c) informační a datovou bezpečnost, včetně ochrany a zálohování elektronických dat a nakládání s hesly
 - d) používání internetu a elektronické pošty
 - e) zpracování osobních údajů v informačních systémech potřebných pro vedení agend obcí v listinné a elektronické podobě.
- 3) Zásadním dokumentem, který stanoví závazné právní vztahy všech stran, jejich součinnost a postavení při ochraně osobních údajů, je tato směrnice. Aktuální verze bude uložena, pro potřebu kontrolních orgánů, u vedení obce, případně u kontaktní osoby, která je pověřena vedením agend GDPR a ICT bezpečnosti.

Čl. 2

Působnost směrnice

- 1) Tato směrnice je závazná pro všechny zaměstnance obce. Směrnice je závazná i pro další osoby, které mají s obcí jiný právní vztah (smlouva o dílo, nájemní smlouva, smlouva o poskytování služeb) a které se zavázaly postupovat podle této směrnice.
- 2) Základní právní normou upravující ochranu osobních údajů v obci je Nařízení Evropského parlamentu a Rady (EU) 2016/679 a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) – GDPR a dále pak Zákon č 262/2006 Sb, Zákon č.133/2000 o evidenci obyvatel a další zákonné normy, dle kterých se vede registr zpracovatelských činností a záznam o činnostech zpracování dle čl 30.
- 3) Zastupitelstvo obce ukládá jednotlivým členům zastupitelstva obce, aby při plnění svých úkolů zajišťovali dodržování těchto pravidel. Starostovi obce ukládá zajistit dodržování těchto pravidel při zpracování osobních údajů obecním úřadem a při plnění smluv, jejichž předmětem je zpracování osobních údajů.

Čl. 3

Základní pojmy

- a) **osobním údajem** je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,
- b) **zvláštní kategorií osobních údajů** (dříve **citlivé údaje**) jsou osobní údaje vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových

organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů, citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,

c) **zpracováním osobních údajů** se rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,

d) **zpracovatelem je fyzická nebo právnická osoba**, nebo subjekt, který zpracovává osobní údaje pro správce (správce si jej najímá - účetní, ICT správce, lékař a jiné),

e) **správce je právnická nebo fyzická osoba**, která určuje účely a prostředky zpracování osobních údajů,

f) **pověřencem je osoba**, která posuzuje činnost správce či zpracovatele, zda je v souladu s platnou právní úpravou, informuje, radí, dává doporučení,

g) **subjektem údajů je fyzická osoba**, k níž se osobní údaje vztahují,

h) **souhlasem subjektu údajů je** svobodný, konkrétní, informovaný, jednoznačný, jasný a prokazatelný vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.

ch) **počítačová síť obce** (dále jen „sít“) – všechna technická zařízení a programové vybavení používané při činnosti orgánů obce v budovách obce k vzájemnému technickému a datovému propojení počítačů. Síť spolu s přímo nebo nepřímo na síť připojenými počítači a jinými technickými zařízeními a programovým vybavením tvoří **počítačový systém obce** (dále jen „systém“)

i) **počítač** (dále jen „PC“) – počítač ve vlastnictví obce nebo oprávněně obcí využívaný a připojený do sítě případně fungující samostatně mimo síť

j) **výpočetní technika obce** (dále jen „výpočetní technika“) – všechny PC, ostatní zařízení informační techniky a všechny technické součásti sítě, které jsou ve vlastnictví nebo v oprávněném užívání obce a jsou využívána při činnosti orgánů obce

k) **programové vybavení** (dále jen „programy“) – programy a aplikace ve vlastnictví nebo v oprávněném užívání obce, které jsou využívány při provozu výpočetní techniky

l) **uživatel** – je zaměstnanec, zastupitel, který je oprávněn užívat výpočetní techniku a programy

m) **uživatelské oprávnění** – je oprávnění uživatele ve vymezeném rozsahu užívat výpočetní techniku a programy; podmínky vzniku uživatelského oprávnění stanoví tato směrnice

n) **uživatelský účet** – fyzické vyjádření uživatelského oprávnění; základními parametry jsou uživatelské jméno (login), heslo (password), definice přístupových práv a e-mailová adresa uživatele

o) **správce sítě** – zabezpečuje podle této směrnice provoz výpočetní techniky, systému, sítě a další úkoly stanovené touto směrnicí

Kategorie A

Ochrana osobních údajů

Čl. 4

Zásady nakládání s osobními údaji

Při nakládání s osobními údaji se obec, její zaměstnanci, zastupitelé a další osoby řídí těmito zásadami:

- postupovat při nakládání s osobními údaji v souladu s právními předpisy,
- s osobními údaji nakládat uvážlivě,
- souhlas se zpracováním osobních údajů nenadužívat,
- zpracovávat osobní údaje ke stanovenému účelu a ve stanoveném rozsahu a dbát na pravdivost a přesnost údajů,
- zpracovávat osobní údaje v souladu se zásadou zákonnosti – na základě právních předpisů, při plnění ze smlouvy, při plnění právní povinnosti správce, při ochraně životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (zejména děti požívají vyšší ochrany), při ochraně oprávněných zájmů obce, při ochraně veřejného zájmu, a zpracování osobních údajů na základě souhlasu,
- respektovat práva člověka, který je subjektem údajů, zejména práva dát a odvolat souhlas se zpracováním, práva na výmaz, práva namítat rozsah zpracování a jiné,
- poskytovat při zpracování osobních údajů zvláštní ochranu dětem,
- poskytovat informace o zpracování osobních údajů, komunikovat,
- při uzavírání smluv a právním jednání postupovat se zřetelem na povinnost chránit osobní údaje před zneužitím,
- spolupracovat s pověřencem pro ochranu osobních údajů.

Čl. 5

Postupy obce, jejich zaměstnanců a dalších osob při nakládání s osobními údaji

- 1) Obec všechny osobní údaje, se kterými nakládá a které zpracovává, chrání vhodnými a dostupnými prostředky před zneužitím. Obec především uchovává osobní údaje v prostorách nebo v systému, do kterého má přístup omezený, předem stanovený a známý okruh osob. Jiné osoby mohou získat přístup k osobním údajům pouze se svolením starosty, místostarosty, popř. tajemníka nebo jím pověřené osoby.
- 2) Obec zavede taková opatření, aby o nakládání s osobními údaji měl přehled starosta, tajemník nebo jimi pověřená osoba a pověřenec pro ochranu osobních údajů. Mezi tato opatření řadíme písemnou komunikaci, stanovení povinností v pracovní smlouvě, ve smlouvě, kterou obec uzavírá s třetí osobou (nájemní smlouva, smlouva o dílo, smlouva o poskytování služeb).
- 3) Obec alespoň jednou za rok provede zhodnocení postupů nakládání s osobními údaji. Zhodnocení může být provedeno dle zvyklostí obce, zpravidla se učiní stručný záznam např. v zápisu z jednání Rady obce, zastupitelstva. Zjistí-li se, že některé postupy obce jsou zastaralé, zbytečné nebo se neosvědčily, učiní obec bezodkladně nápravu.
- 4) Každý zaměstnanec obce při nakládání s osobními údaji respektuje jejich povahu, že jde o součást soukromí člověka jako subjektu údajů, a tomu přizpůsobí úkony s tím spojené.

- 5) Zaměstnanec a zastupitel nezveřejňují osobní údaje bez ověření, že takový postup je možný, nepřístupňují osobní údaje osobám, které neprokáží právo s nimi nakládat.
- 6) Obec při nakládání a zpracovávání osobních údajů aktivně spolupracuje s pověřencem pro ochranu osobních údajů.
- 7) Obec ihned řeší bezpečnostní incidenty týkající se osobních údajů, a to v součinnosti s pověřencem pro ochranu osobních údajů. V případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob, obec tuto osobu vždy informuje a sdělí, jaká opatření k nápravě přijala. O každém incidentu se sepíše záznam do knihy Evidence bezpečnostních incidentů. O každém závažném incidentu obec informuje Úřad pro ochranu osobních údajů.

Čl. 6

Organizační opatření k ochraně osobních údajů

- 1) Agendy, které obsahují osobní údaje občanů a zaměstnanců, jsou trvale uloženy v uzamykatelných skříních v kancelářích vedení obce a příručních spisovných referentů obcí. Zastupitelům a pověřeným osobám jsou zapůjčeny na nezbytně dlouhou dobu k provedení zápisů nebo jako podklady pro jednání zastupitelstva. Je zakázáno předávat cizím osobám dokumenty v listinné a elektronické podobě nebo kopírovat a kopie poskytovat neoprávněným osobám bez anonymizace nebo pseudonymizace osobních údajů, pokud takové úkony nejsou v souladu s právními předpisy EU a ČR.
- 2) V organizaci je stanoven klíčový režim (klíče přidělené zaměstnancům jsou evidovány). Stejně tak v případě pronájmů nebytových prostor v areálu úřadu. Duplikáty klíčů nejsou na veřejně přístupném místě.
- 3) Úklid prostor organizace je prováděn vlastními zaměstnanci. V případě využití externího dodavatele, dbá organizace na to, aby úklid prostor, obsahující písemnosti s osobními údaji, byl realizován pod dohledem pověřené osoby.
- 4) V případě zřízení serverovny je zabráněno vstupu nepovolaným osobám.
- 5) Při práci s elektronickou evidencí v informačních systémech nesmí oprávněné osoby opouštět počítač bez odhlášení, nemohou nechat nahlížet žádnou jinou osobu a musí chránit své přihlašovací heslo. V případě nebezpečí jeho vyžrazení jej ihned změnit. Přístupy nastavuje pověřený zaměstnanec obce – správce počítačové sítě, který nastavuje potřebné zabezpečení dat a počítačové sítě (dle pokynů starosty nebo jiné pověřené osoby).
- 6) Zastupitelé a další pověřené osoby mají zajištěný zabezpečený dálkový přístup k emailové schránce a zodpovídají za bezpečné nastavení hesla a v případě úniku osobních údajů za ohlášení bezpečnostního incidentu. Zastupitelé dodržují bezpečné nakládání s osobními údaji.
- 7) Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních v kanceláři starosty, místostarosty, či tajemníka. Přístup k nim má vedení obce, nebo je-li to nutné, též referent obce nebo mzdová účetní.
- 8) Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu. O tomto právu jsou zaměstnanci poučeni.
- 9) Zaměstnanci obce neposkytují bez právního důvodu osobám a institucím žádnou formou osobních údajů zaměstnanců obce a občanů. Tyto údaje nelze poskytovat telefonicky, emailem ani v rámci osobního jednání, pokud to ovšem nevyžadují kontrolní orgány nebo právní předpisy, kdy je povinnost poskytnout součinnost (Policie ČR, soudy atd.).
- 10) Seznamy občanů se nezveřejňují, nevyplývá-li to ze zákona.

- 11) Pokud jsou pro vedení dokumentace využívány formuláře a software, je nutné provést kontrolu, zda nepožadují či nenabízejí evidenci nadbytečných údajů a tyto údaje nezpracovávat.

Čl. 7

Pravidla v oblasti ochrany osobních údajů u smluvních vztahů

Uzavírá-li obec jakoukoli smlouvu (nájemní smlouvu, smlouvu o dílo, smlouvu o poskytnutí služeb, nepojmenovanou smlouvu apod.), k jejímuž plnění je zapotřebí druhé smluvní straně poskytnout osobní údaje, obec vždy a bezpodmínečně bude trvat na tom, aby ve smlouvě byla druhé smluvní straně uložena povinnost:

- 1) přijmout všechna bezpečnostní, technická, organizační a jiná opatření s přihlédnutím ke stavu techniky, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování k zabránění jakéhokoli narušení poskytnutých osobních údajů,
- 2) nezapojit do zpracování žádné další osoby bez předchozího písemného souhlasu obce,
- 3) zpracovávat osobní údaje pouze pro plnění účelu smlouvy (vč. předání údajů do třetích zemí, a mezinárodním organizacím); výjimkou jsou pouze případy, kdy jsou určité povinnosti uloženy přímo právním předpisem,
- 4) zajistit, aby osoby oprávněné zpracovávat osobní údaje u dodavatele byly zavázány k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
- 5) zajistit, že dodavatel bude obci bez zbytečného odkladu nápomocen při plnění povinností obce, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 nařízení, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 nařízení, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 nařízení a povinnosti provádět předchozí konzultace dle čl. 36 nařízení, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje obec,
- 6) po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí obci a vymaže existující kopie apod.,
- 7) poskytnout obci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené právními předpisy,
- 8) umožnit kontrolu, audit, který je prováděn obcí nebo příslušným orgánem dle právních předpisů,
- 9) poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví obec, součinnost potřebnou pro plnění zákonných povinností spojených s ochranou osobních údajů, či jejich zpracováním,
- 10) poskytnuté osobní údaje chránit v souladu s právními předpisy,

Čl. 8

Pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů

Obec nakládá a zpracovává pouze osobní údaje, které:

- 1) souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních pracovníků, se sociálním, a zdravotním pojištěním,
- 2) souvisejí s jednoznačnou identifikací občanů v souladu se zákonem (jméno, příjmení, bydliště, email, kontakt, další údaje nezbytné např. pro vydání správního rozhodnutí apod.),

- 3) souvisejí s identifikací občanů ze zákona (datum narození, místo narození, rodné číslo, státní příslušnost, bydliště, údaj o zákonném zástupci, nutný zdravotní údaj apod.),
- 4) jsou nezbytné pro plnění právní povinnosti, ochranu oprávněných zájmů obce nebo ve veřejném zájmu, k jejichž zpracování získala souhlas subjektu údajů.

K osobním údajům mají přístup osoby k tomu oprávněné zákonem nebo na základě zákona. Do jednotlivých dokumentů obce, které obsahují osobní údaje, mohou nahlížet: do osobního spisu zaměstnance vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni. Právo nahlížet do osobního spisu má orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby. Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele (§ 312 zákoníku práce),

Souhlas se zpracováním osobních údajů:

- 5) ke zpracování osobních údajů nad rozsah vyplývající ze zákonů (ze zákona vyplývá i oprávněný zájem, plnění právní povinnosti, plnění smlouvy, veřejný zájem) je nezbytný souhlas osoby, o jejíž osobní údaje se jedná. Souhlas musí být poučený, informovaný a konkrétní, nejlépe v písemné podobě. Souhlas se získává pouze pro konkrétní údaje (určené např. druhově), na konkrétní dobu a pro konkrétní účel.
- 6) souhlas se získává pro zpracování osobních údajů jen tehdy, pokud je jejich zpracování nezbytně nutné a právní předpisy jiný důvod pro toto zpracování nestanoví.
- 7) souhlas se poskytuje podle účelu např. vítání občánků, svatby, blahopřání jubilantům a jiné. Udělený souhlas může být v souladu s právními předpisy odvolán v případě zveřejnění obrazových záznamů a jiných audiovizuálních záznamů, které jsou umístěny na webové stránky, sociální síť obce.

Čl.9

Osobní údaje v listinné podobě

Dokumenty s osobními údaji v listinné podobě podléhají režimu spisového a skartačního řádu. Při práci s nimi musí zaměstnanci obce dbát zvýšené opatrnosti. K dokumentům mají přístup jen ti zaměstnanci, kteří přístup k těmto dokumentům nezbytně potřebují k výkonu svých pracovních činností. Dokumenty musí být zabezpečeny proti odcizení a prohlížení nepovolanými osobami.

Čl. 10

Doba zpracování osobních údajů

Zpracování osobních údajů může být vykonáváno jen po nezbytně nutnou dobu. Pomine-li účel, pro který byly osobní údaje zpracovávány, zpracování musí být ukončeno. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely archivace, vědeckého či historického výzkumu a statistické.

Čl. 11

Práva subjektu údajů

Subjekt údajů má následující práva:

- 1) **právo na informace a přístup k osobním údajům** – správce je povinen subjekt údajů informovat o zpracování osobních údajů nejpozději v okamžiku získání osobních údajů. Informace musí být zajištěna v plné šíři dle Nařízení
- 2) **právo na opravu** – subjekt údajů má právo, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje nebo doplnil neúplné osobní údaje. Subjekt údajů má právo na opravu údajů, pokud jsou nepřesné, nebo neúplné, na provedení opravy nejdéle do jednoho měsíce, na vysvětlení, pokud oprava nebyla provedena
- 3) **právo na výmaz** – subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají. Toto právo svědčí subjektu údajů tehdy, je-li zpracování založeno na souhlasu a dojde-li k jeho odvolání, jestliže zpracování osobních údajů již není potřebné pro vymezené účely, jestliže subjekt údajů vznese námitku proti zpracování osobních údajů založeném na oprávněném či veřejném zájmu a z balančního testu vyplyne, že již neexistují převažující oprávněné zájmy správce a dále pokud je zpracování osobních údajů protiprávní. Výmaz se provádí na základě písemné žádosti
- 4) **právo na omezení zpracování** – subjekt údajů má právo požádat o omezení zpracování osobních údajů, a to tehdy, žádá-li o opravu osobních údajů. Do doby opravy správce pozastaví zpracování osobních údajů. Dalšími důvody omezení zpracování osobních údajů je protiprávní zpracování, správce již osobní údaje pro vymezené účely nepotřebuje, subjekt údajů vznesl námitku proti zpracování a do doby jejího posouzení se osobní údaje nezpracovávají
- 5) **právo na přenositelnost** - svědčí subjektu údajů u osobních údajů zpracovávaných automatizovaně na základě souhlasu nebo smlouvy. V takovém případě správce poskytne subjektu údajů osobní údaje ve strukturovaném běžně používaném a strojově čitelném formátu
- 6) **právo vznést námitku** má subjekt údajů z důvodů týkajících se zpracování osobních údajů založených na veřejném nebo oprávněném zájmu. V takovém případě správce osobních údajů musí doložit, že oprávněný či veřejný zájem převažuje nad ochranou osobních údajů subjektu, a že je tedy jeho zpracování osobních údajů oprávněné. Doložení se provádí zpracováním balančního testu.
- 7) **právo podat stížnost** – každý subjekt údajů má právo podat stížnost u dozorového úřadu, pokud se subjekt údajů domnívá, že zpracováním jeho osobních údajů je porušeno Nařízení.

Čl.12

Přístup subjektu údajů k informacím

- 1) Obec vydává na žádost subjektu údajů informace, zda osobní údaje, které se ho týkají, jsou nebo nejsou zpracovávány. Pokud zpracovávány jsou, má subjekt údajů přístup k následujícím informacím:
 - a) účely zpracování
 - b) kategorie dotčených osobních údajů
 - c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
 - d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby
- 2) Lhůta k vyřízení žádosti subjektu údajů je jeden měsíc od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení.
- 3) Informace se subjektům údajů poskytují písemně a bezplatně.

Čl. 13

Přístup do registru obyvatel

Zaměstnanci obce, kteří disponují právem přístupu do Registru obyvatel, mohou do Registru obyvatel nahlížet jen v odůvodněných případech při plnění svých pracovních povinností např. zjištění adresy nebo ověření místa trvalého pobytu. Vkládání a opravy údajů v Registrech obyvatel mohou pouze pověření pracovníci. Zaměstnanec v žádném případě nesmí pořizovat opisy osobních údajů ani vytvářet seznamy obyvatel, které by osobní údaje obsahovaly. Zaměstnanci jsou rovněž povinni zachovávat mlčenlivost o osobních údajích, k nimž mají tímto způsobem přístup.

Čl.14

Předávání osobních údajů

- 1) Předávání osobních údajů dalším stranám (mimo úřad) je možné jen tehdy, je-li umožněno účinným právním předpisem. Výjimku tvoří předání v rámci přenesené působnosti, kde je předání provedeno průvodním dopisem a doručenkou. V ostatních případech předání osobních údajů platí následující ustanovení.
- 2) O každém takovém předání musí být vyhotoven předávací protokol, který je podepsán osobou předávající, tak osobou přejímající. Obsahem protokolu jsou všechny důležité okolnosti předání – účel, právní titul, popis předávaných dat (rozsah, formát, nosič) a způsob předání.
- 3) Za předávání osobních údajů je zodpovědný Statutární zástupce organizace Ing.Tomáš Němčic, starosta obce. S předávacími protokoly je nakládáno dle spisového a skartačního řádu.
- 4) Předávání spisů s osobními údaji v případě déletrvajících nepřítomností zaměstnance je v rámci běžného zastupování. Při předávání agendy je třeba brát na vědomí ustanovení článku 9 této směrnice.

Čl.15

Nahlížení a zveřejňování zápisů a usnesení z jednání zastupitelstva obce a rady obce

- 1) Nahlížení a pořizování výpisů ze zápisů ze zasedání zastupitelstva obce a usnesení zastupitelstva obce a rady obce probíhá tak, že nahlížení do plného textu a pořizovat si z něj výpisy mohou:
 - a) občané obce od 18 let věku s trvalým pobytem na území obce
 - b) vlastníci nemovitostí na území obce
 - c) cizí státní příslušníci, kteří mají trvalý pobyt na území obce
- 2) Ostatním fyzickým a právnickým osobám je umožněno získat informace na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Osobní údaje se při poskytnutí informace redukuje nebo anonymizují.
- 3) Zveřejňování zápisů a usnesení ze zasedání zastupitelstva obce a usnesení ze schůzí rady obce na úřední desce a na webových stránkách podléhá ochraně osobních údajů, tzn. osobní údaje se minimalizují nebo anonymizují, avšak tak, aby konkrétní sdělení ještě plnilo svůj účel. Zveřejnění musí obsahovat informaci, že se jedná o upravenou verzi dokumentů z důvodu ochrany osobních údajů.

Čl. 16

Pověřenec pro ochranu osobních údajů

- 1) Činnost pověřence pro ochranu osobních údajů je vykonávána prostřednictvím externí společnosti 2K CONSULTING s.r.o, tato osoba je nahlášena u dozorového úřadu ÚOOÚ.
- 2) Pověřenec pro ochranu osobních údajů si plní povinnosti dle uzavřeného smluvního vztahu:

- a) poskytuje poradenskou a informační činnost
- b) monitoruje dodržování ochrany osobních údajů
- c) provádí kontrolní činnost
- d) zajišťuje školení zaměstnanců prezenční formou nebo on-line (e-learning)
- e) poskytuje součinnost při ohlášení bezpečnostních incidentů dozorovému úřadu (ÚOOÚ), případně subjektům údajů a plní další povinnosti dle legislativy

Čl. 17

Kontrolní činnost

- 1) Správce i pověřenec pro ochranu osobních údajů provádí namátkovou kontrolu, zda zaměstnanci obce mají v rámci IS přístup jen k takovým agendám s osobními údaji, ke kterým mají oprávnění. Pověřenec pro ochranu osobních údajů dále monitoruje soulad s obecným nařízením o ochraně osobních údajů, za tímto účelem sbírá informace o zpracování a identifikuje procesy zpracování, analyzuje je a ověřuje jejich soulad. Pověřenec pro ochranu osobních údajů je kontaktním místem pro styk s dozorovým úřadem.
- 2) O průběhu a výsledku kontroly je proveden zápis. Za odstranění zjištěných nedostatků zodpovídá správce.

Čl. 18

Mlčenlivost

Zaměstnanci, kteří zpracovávají osobní údaje nebo k nim mají přístup, jsou povinni zachovávat mlčenlivost jak o těchto osobních údajích, tak o všech technicko-organizačních opatřeních na jejich ochranu. Tato povinnost trvá i po skončení pracovního poměru zaměstnance.

Čl. 19

Likvidace osobních údajů

- 1) Pomine-li účel, pro který byly osobní údaje zpracovávány, je nutné provést jejich likvidaci. Zvláštní zákon stanoví výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském řízení soudním, trestním řízení a správním řízení.
- 2) Data uchovávaná na datových nosičích jsou po uplynutí archivační doby likvidována.
- 3) Data z přepisovatelných datových nosičů jsou vymazána, nosiče, u kterých tuto operaci nelze provést jsou zlikvidovány fyzicky tak, aby nebyla možná jejich rekonstrukce.
- 4) Likvidaci provádí pověřený referent obce. O každé likvidaci osobních údajů je proveden zápis, který je podepsán. Zápisy o provedené likvidaci jsou ukládány.

Čl. 20

Ohlášení bezpečnostních incidentů

- 1) Organizace je bez zbytečného odkladu, a pokud je to možné do 72 hodin od okamžiku, kdy bylo porušení zabezpečení zjištěno, povinna ohlásit ÚOOÚ porušení zabezpečení osobních údajů, v případě nejvyššího rizika a velkého množství osobních údajů.
- 2) Organizace dokumentuje veškeré případy porušení zabezpečení osobních údajů, a to tak, aby tato dokumentace umožnila ÚOOÚ ověření souladu s článkem 33 Nařízení GDPR.
- 3) Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob (a nejsou splněny vylučující podmínky

uvedené v článku 34 Nařízení GDPR) oznámí organizace toto porušení bez zbytečného odkladu subjektům údajů

Kategorie B

Informační a datová bezpečnost/ICT Bezpečnost

Čl. 21

Základní povinnosti a oprávnění ICT Bezpečnost

- 1) Uživatel je oprávněn užívat výpočetní techniku, síť a programy v rozsahu svého uživatelského oprávnění a přístupových práv. Uživatel je povinen respektovat pokyny správce sítě, které vydá v souladu se svými oprávněními a povinnostmi.
- 2) Uživatel s uživatelským oprávněním je zaměstnanec nebo zastupitel, k jehož výkonu práce je nezbytné používání výpočetní techniky a programů.
- 3) Výpočetní techniku a programy jsou oprávněni používat pouze zaměstnanci s uživatelským účtem, a to v rozsahu svého uživatelského oprávnění
- 4) Zaměstnancům je zakázáno:
 - a) poškozovat výpočetní techniku, programy nebo data nesprávným nebo neoprávněným užíváním
 - b) používat výpočetní techniku, programy nebo data protiprávním způsobem nebo k protiprávní činnosti
 - c) používat výpočetní techniku, programy nebo data k činnostem namířeným proti obci či proti jakémukoliv jinému subjektu, jehož počítačové prostředky jsou dostupné prostřednictvím sítě nebo prostřednictvím internetu
 - d) umožnit přístup k výpočetní technice, programům nebo datům osobám, které nejsou oprávněny uživateli podle této směrnice,
 - e) používat elektronické informace a data, k nimž nemají oprávněný přístup,
 - f) používat elektronické informace a data, k nimž mají oprávněný přístup způsobem, který je v rozporu s platnými právními předpisy nebo v rozporu s vnitřními předpisy obce,
 - g) kopírovat neoprávněně programy nebo jejich části,
 - h) modifikovat neoprávněně programy a data,
 - i) odposlouchávat neoprávněně provoz (komunikaci) v síti a vytvářet kopie elektronických informací či dat procházejících jednotlivými uzly sítě,
- 5) Zaměstnanec je však povinen respektovat, že soukromé záležitosti lze v pracovní době a na pracovišti vyřizovat pouze výjimečně v přiměřené a nezbytné míře a nesmí tím být dotčeno plnění povinností zaměstnance podle právních předpisů a podle vnitřních předpisů obce.
- 6) Zaměstnavatel je oprávněn v případě vážného důvodu nebo úniku osobních údajů nebo řešení jiného bezpečnostního incidentu, kontrolovat elektronickou poštu.

Čl. 22

Bezpečnostní pravidla uživatelů

Zaměstnanci jsou povinni dodržovat následující bezpečnostní pravidla při zpracovávání osobních údajů:

- 1) svěřenou výpočetní techniku využívají pouze pro plnění pracovních povinností
- 2) dodržují zásady pro tvorbu přístupového hesla k operačním systémům nebo aplikacím
- 3) zachovávají jedinečnost a důvěrnost přístupového hesla, tj. nikomu heslo nesdělují a nikde a nijak si jej nezaznamenávají
- 4) při přihlašování k operačním systémům nebo aplikacím dbají na to, aby nebylo možné heslo odpozorovat další osobou
- 5) v případě jakéhokoliv podezření na kompromitaci hesla nebo dokonce jeho zneužití heslo okamžitě změní
- 6) před opuštěním pracoviště zabezpečují výpočetní techniku uzamčením pracovní plochy nebo odhlášením (např. pomocí kláves +L nebo ctrl+alt+del)
- 7) dodržují pravidlo „prázdného stolu“, to znamená, že všechny dokumenty obsahující osobní údaje, které v danou chvíli nezpracovávají, jsou uloženy v uzamykatelných skříních
- 8) Při používání přenosné výpočetní techniky a datových nosičů (notebooků, flash disků, externích HDD, DVD apod.) mimo prostory organizace:
 - nepředávají tuto techniku a nosiče třetím osobám,
 - učiní všechna dostupná opatření, která mohou zabránit ztrátě či odcizení výpočetní techniky (neponechávají je bez dohledu nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.),
 - nepoužívají výpočetní techniku na veřejných místech pro práci s daty organizace,
 - ztrátu či odcizení okamžitě nahlásí svému nadřízenému.
- 9) neinstalují software na výpočetní techniku organizace
- 10) nepoužívají soukromé datové nosiče (např. CD, flash disky, externí HDD)
- 11) nenavštěvují rizikové internetové stránky
- 12) důsledně ověřují doručenou elektronickou poštu a v případě podezření, že se jedná o závadný e-mail (spam, podvodný e-mail apod.), takovou zprávu neotvírají, nereagují na ní a tuto skutečnost neprodleně ohlásí správci ICT
- 13) nezasahují do výpočetní techniky a její konfigurace, vyjma situací, kdy toto bude vyžadováno přímo správcem ICT
- 14) odpovídají za zálohování dat na přidělené výpočetní technice
- 15) nekopírují, neukládají, nepřenáší osobní údaje a data z aplikací organizace na pevných discích počítačů, jiných datových nosičích či cloudu, vyjma stanovených úkolů a povinností či po schválení ředitelem organizace
- 16) soubory, obsahující osobní údaje, adresované mimo doménu obce, zasílat pouze chráněné (prostřednictvím datových schránek, nebo prostřednictvím elektronické pošty minimálně v archivním souboru (např. ve formátu „zip“, „rar“ atd.) opatřeného heslem, přičemž heslo zaslat adresátovi jiným komunikačním kanálem, např. prostřednictvím SMS).
- 17) soubory, obsahující zvláštní kategorie osobních údajů, zasílat pouze prostřednictvím datové schránky
- 18) netisknou data z aplikací organizace pro jiné než pracovní účely
- 19) pokud dojde k úniku, kompromitaci nebo ztrátě dat obsahujících osobní údaje je každý zaměstnanec povinen neprodleně hlásit tento incident nadřízenému vedoucímu zaměstnanci, který tuto skutečnost hlásí neprodleně pověřenci pro ochranu osobních údajů.

Zaměstnanci mají vysloveně zakázáno:

- 1) sdělovat někomu své uživatelské jméno a heslo do PC, do počítačové sítě, a pracovní emailové adresy, jiných informačních systémů obce. Dále je zakázáno sdělovat přístupové údaje do administrace webových stránek a sociálních sítí, pokud jej k tomu nevyzve starosta nebo tajemník, tj. zaměstnanec nemůže udělovat přístupové údaje oprávnění k administraci nebo editaci komukoliv bez povolení vedení obce.
- 2) zasahovat do instalace počítačových programů, měnit konfiguraci, příkazové soubory nebo adresáře potřebné pro chod systému
- 3) jakkoliv šířit počítačový program a používat či poskytnout jakékoliv neoprávněně získané prostředky (licenční kódy, hardwarové klíče), které slouží k ochraně počítačových programů
- 4) provádět nezodpovědnou nebo dokonce zlomyslnou činnost na internetu (rozesílání spamu, šíření virů)
- 5) komunikovat se subjekty údajů ze soukromých emailových adres.

Čl. 23

Práce z domova (home office)

- 1) Při práci z domova je místem výkonu práce pro zaměstnance jejich bydliště či jiné zvolené místo. Změna místa výkonu práce se provádí písemnou dohodou výkonu práce z domova obou smluvních stran nebo dodatkem obsahu pracovní smlouvy.
- 2) Doba trvání práce z domova je vykonávána dle § 317 zákoníku práce.
- 3) Dohoda o práci z domova je vždy stanovena mezi zaměstnavatelem a zaměstnancem.
- 4) Při práci z domova je na dohodě zaměstnavatele se zaměstnancem, jaké IT zařízení bude pro plnění pracovních úkolů využívat. V případě využití svého soukromého IT zařízení je nutné, aby výpočetní a telekomunikační technika měla odpovídající software, který bude mít prvky technického zabezpečení. Náklady na pořízení takového software jsou však v režii zaměstnance, nikoliv zaměstnavatele. V případě zapůjčení IT techniky ze strany zaměstnavatele dochází k uzavření dohody o odpovědnosti za ztrátu svěřených předmětů ve smyslu § 255 zákoníku práce a písemného potvrzení o převzetí techniky.

V rámci plnění pracovních povinností je zaměstnanec povinen:

- a) účastnit se on-line způsobem školení v oblasti GDPR
- b) účastnit se online pracovních porad, webinářů a jiných aktivit pro plnění pracovních povinností
- c) zabezpečit důvěrnost veškerých osobních údajů a jiných informací zpracovaných v souvislosti s výkonem práce z domova
- d) zamezit přístupu neoprávněným osobám k užívaným pracovním prostředkům a zpracovávaným údajům
- e) se svěřenými prostředky ze strany obce, v případě zápůjčky, řádně hospodařit, ochraňovat před ztrátou, poškozením, zničením a zneužitím
- f) předávat zaměstnavateli údaje pro evidenci pracovní doby
- g) v případě úniku osobních údajů informovat vedení obce

Čl. 24

Práva a povinnosti Správce ICT

Správce ICT

Správce ICT je zodpovědný za dodržování bezpečnostních pravidel při zpracovávání a ochraně osobních údajů v rámci počítačové sítě a na výpočetní technice organizace. Je povinen dodržovat následující bezpečnostní pravidla při plnění pracovních úkolů správce ICT:

- 1) spolupracuje s organizací na tvorbě a aktualizaci analýzy rizik
- 2) spravuje antivirový systém na všech výpočetních prostředcích organizace a to především:
 - provádí jeho instalaci,
 - kontroluje funkčnost aktualizací,
 - kontroluje výstupy programu.
- 3) pro zaměstnance organizace připravuje a instaluje výpočetní techniku, kterou nastaví dle definovaných bezpečnostních požadavků (např. způsoby přihlášení, oprávnění uživatelského účtu, uzamykání počítače při neaktivitě apod.) a následně ji předává určeným zaměstnancům k použití
- 4) vytváří a nastavuje zaměstnancům uživatelská oprávnění do počítačové sítě a aplikací v rozsahu schválení vedení obce
- 5) na základě požadavku vedení obce zřizuje nebo ruší přístupy do operačních systémů organizace
- 6) na základě požadavku garanta aplikace zřizuje nebo ruší přístupy do aplikace organizace
- 7) zajišťuje fyzickou bezpečnost datových úložišť, nosičů a dat organizace
- 8) poskytuje zaměstnancům organizace technickou podporu při využívání výpočetní techniky
- 9) provádí kontrolní činnost k zajištění bezpečnosti osobních údajů zpracovávaných ve výpočetní technice organizace
- 10) provádí bezpečnou likvidaci datových nosičů organizace, zejména pak pevných disků, flash disků, paměťových karet, CD a DVD disků apod
- 11) v případě nutnosti odeslat výpočetní techniku či jejich komponenty obsahující osobní údaje mimo organizaci (oprava u servisní organizace, výpůjčka, pronájem, vyřazení). V případě nutnosti odeslat výpočetní techniku či jejich komponenty obsahující osobní údaje mimo organizaci (oprava u servisní organizace, výpůjčka, pronájem, vyřazení, likvidace apod.), musí před odesláním vymazat z pevného disku veškeré osobní údaje nebo musí vyjmout paměťová média
- 12) provádí zálohování zpracovávaných dat a klíčových síťových prostředků organizace tak, aby při selhání např. hlavního datového úložiště, bylo možné provést obnovu dat s minimální ztrátou uložených dat

Bezpečnost sítě

- 1) V případě, že organizace provozuje WIFI síť, je potřeba dodržovat určitá bezpečnostní pravidla. Wi-Fi síť organizace je používána jen pro přístup do sítě Internet. Je chráněna standardními prostředky včetně přístupového hesla. Heslo pro přístup do sítě Wi-Fi je pravidelně měněno 1x za 12 měsíců.
- 2) V nastavení přístupových údajů k administraci routerů musí odpovědná osoba změnit továrně nastavené přístupové údaje. Kvalita nového hesla splňuje požadavky pro heslo správce ICT.

- 3) Mobilní zařízení organizace (smartphony, tablety) s vlastním operačním systémem jsou vybavena antivirovou aplikací.
- 4) Zaměstnanci mohou využívat soukromá mobilní zařízení pouze pro práci s obsahem pracovní emailové schránky. Jiné využití soukromých mobilních zařízení pro pracovní účely (např. připojení do vnitřní sítě organizace, administrace aplikací apod.) je zakázáno.
- 5) Pokud je Wi-Fi síť používána pro přístup k interní síti, a tedy i aplikacím organizace, je identita zaměstnance před zpřístupněním této sítě ověřena prostřednictvím zadání přístupových údajů. Bez ověření identity zaměstnance nejsou interní síť, aplikace nebo síťové disky zpřístupněny.
- 6) Přístup k zálohám síťových prostředků a síťovým aplikacím je striktně omezen jak na logické, tak i fyzické úrovni pouze na odpovědné osoby.
- 7) Všechny vzdálené přístupy k síti organizace (pomocí např. vzdálené plochy nebo VPN) povoluje starosta, tajemník.

Všechny způsoby vzdáleného přístupu k síti organizace splňují následující:

- a) vytvořené spojení v rámci vzdáleného přístupu je šifrované (bez ohledu na povahu přenášených dat) a předchází mu autentizace (minimálně heslem, lépe uživatelským certifikátem),
- b) každý vzdálený přístup je jednoznačně identifikovatelný (uživatel) a je zaznamenán,
- c) uživatelé nesmí „propůjčovat“ své oprávnění vzdáleného přístupu třetím osobám, byť zaměstnancům organizace, připojení probíhá prostřednictvím bezpečného kanálu (HTTPS, VPN, pomocí VPN mimo veřejnou síť poskytovatele apod.).
- d) správce ICT vede evidenci zaměstnanců a výpočetní techniky s povoleným vzdáleným přístupem. Tyto seznamy jsou v pravidelných intervalech (alespoň jedenkrát za rok) přezkoumávány vedoucím organizace, nebo jím pověřenou osobou.

V případě, že Správce ICT nastavuje samostatné segmenty sítě, jako jsou např. servery, síťové tiskárny, zasedací místnosti apod, síťové zásuvky organizace jsou připojeny dle jejich využití. Nepoužívané zásuvky jsou správcem ICT v rozvaděči odpojeny. Správce ICT přezkoumává v pravidelných intervalech (alespoň 1x za měsíc) důležité bezpečnostní logy firewallu. Například využití sítě (jednotlivých portů), neúspěšné pokusy o vzdálené přihlášení, pokusy o skenování sítě apod.

Používání výpočetní techniky

- 1) Uživatel je oprávněn užívat pouze výpočetní techniku, která mu byla řádně předána, nebo jejíž užívání má zpřístupněno prostřednictvím výpočetní techniky, která mu byla řádně předána (např. sdílené notebooky, tiskárny).
- 2) Výpočetní techniku je zaměstnanec oprávněn užívat pouze k činnostem souvisejícím s jeho prací a pouze v souladu s příslušným návodem k danému zařízení výpočetní techniky.
- 3) Pokud jde o technickou manipulaci s výpočetní technikou, je uživatel oprávněn pouze k běžným uživatelským činnostem jako např. výměna toneru, cartridge, doplnění papíru v tiskárně, připojení k síti a odpojení od sítě. Uživateli je zakázáno rozpojovat nebo přerušovat počítačovou síť, připojovat poprvé k síti nové PC nebo jiná technická zařízení. Manipulace s výpočetní technikou, které nesmí provádět uživatel, zabezpečuje správce sítě.
- 4) Závadu ve funkčnosti výpočetní techniky je uživatel povinen neprodleně oznámit správci sítě. Veškeré opravy výpočetní techniky zabezpečuje pouze správce sítě.
- 5) Uživatel nesmí provádět změny konfigurace PC, jiných zařízení nebo zásahy do systému, které by mohly vést k jeho zhroutilí, poruše nebo nežádoucímu chování. Jakékoliv nestandardní zásahy do konfigurace nebo systému je nutné předem projednat se správcem sítě.

- 6) Do sítě je zakázáno bez souhlasu správce nebo nadřízeného pracovníka, přímo nebo nepřímo připojovat jakákoliv technická zařízení, která uživatel nemá schválená k užívání.
- 7) Do PC je zakázáno připojovat přenosné a externí diskové jednotky včetně USB flash disků kromě zařízení schválených správcem sítě nebo nadřízeného pracovníka.
- 8) Obdrží-li uživatel (na přenosném médiu, elektronickou poštou či jiným způsobem) jakýkoliv soubor z neznámé adresy, nebo o jehož původu lze důvodně pochybovat, je zakázáno soubor otevírat či ukládat na disk. Rovněž je zakázáno spouštět bez předchozí konzultace se správcem sítě spustitelné soubory došlé na přenosném médiu nebo elektronickou poštou, zejména pak soubory s koncovkami *.exe, *.com, *.bat, *.pif, *.vbs, *.vbe.
- 9) Má-li uživatel podezření na napadení PC virem, neprodleně informuje správce sítě.
- 10) Uživatel je oprávněn využívat pouze ta přístupová práva, která mu byla řádně přidělena. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu nebyla řádně přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci sítě a takto neoprávněně získaná přístupová práva náležející jinému uživateli; na pracovištích s výpočetní technikou užívanou společně více uživateli, je možné společné užívání je možné společné užívání přístupových práv, pokud byla takto stanovena.
- 11) Elektronické informace a data přístupná prostřednictvím výpočetní techniky a sítě může uživatel využívat pouze, je-li k tomu oprávněn v rámci výkonu své práce a je-li to pro výkon jeho práce nezbytné. Uživatel je povinen při nakládání s daty dodržovat všechny související právní předpisy.
- 12) Obec si vyhrazuje právo v odůvodněných případech v souladu s právními předpisy monitorovat dobu přístupu jednotlivých zaměstnanců na internetové stránky, včetně adres těchto stránek a dále právo monitorovat u jednotlivých zaměstnanců počty došlých a odeslaných e-mailů, včetně adres odkud nebo kam je e-mail směrován. Se zjištěnými údaji musí být nakládáno v souladu s ochranou soukromí a ochranou osobních údajů.
- 13) Zaměstnanec musí v případě využití IT techniky, které není v majetku obce, zabezpečit toto zařízení při používání internetu neb jiných aplikací, využívání neautorizovaných internetových portálů a neoriginálních software tak, aby nedocházelo k úniku osobních údajů nebo jiných bezpečnostních incidentů.

Čl. 25

Závěrečná ustanovení

- 1) Vnitřní předpis je zaměstnancům a zastupitelům k dispozici u vedení obce, popřípadě pověřené osoby.
- 2) Všichni vedoucí zaměstnanci obce jsou povinni seznámit s ním své podřízené zaměstnance, včetně osob pracujících pro obec na základě DPP nebo DPČ, mimo dělnických profesí a pomocných prací.
- 3) Tato směrnice nahrazuje Směrnici o ochraně osobně údajů ze dne: 25.5.2018
- 4) Schváleno Radou obce dne: 21.11.2022 - bod č. 6

.....
Podpis statutárního zástupce obce

Přílohy:

Příloha č. 1

Záznamy o činnostech zpracování dle čl. 30 a splnění informační povinnosti dle čl. 13 a 14 Nařízení Evropského parlamentu a rady EU O ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.