Směrnice 1/2018
o nakládání s osobními údaji

Obec Lužice

(dále také jako „správce“)

Článek 1

Úvodní ustanovení

Tato směrnice o nakládání s osobními údaji (dále jen směrnice) se vydává k provedení 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 (dále jen „Nařízení GDPR“), případně dalších souvisejících předpisů a je závazný pro všechny zaměstnance obce Lužice.

Po schválení směrnice radou obce a zastupitelstvem obce je tato směrnice závazná rovněž pro členy zastupitelstva, rady obce a také pro členy výborů zastupitelstva a členy komisí rady obce.

Článek 2

Předmět, účel a působnost

1) Směrnice stanovuje taková opatření a pravidla, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů spravovaných a zpracovávaných správcem. Ochranou osobních údajů je míněno zajištění důvěrnosti spravovaných a zpracovávaných osobních údajů, jejich integrity, dostupnosti a dalších bezpečnostních aspektů všech osobních údajů v míře potřebné pro činnost správce, a to v souladu s Nařízením GDPR a jinými právními předpisy.

2) Tato směrnice se zabývá ochranou všech osobních údajů ve vlastnictví nebo ve správě správce, bez ohledu na jejich podobu (tištěnou, psanou, uloženou elektronicky, odesílanou poštou, předávanou elektronicky, ústním podáním, telefonem, faxem apod.).

3) Za účelem ochrany osobních údajů je v rámci správce definován tzv. systém řízení ochrany osobních údajů, fungující v souladu s těmito dokumenty:

   - Organizační řád správce,
   - Spisový a skartační řád vydaný u správce,
   - závazných pokynů provozovatelů základních registrů a dalších centrálně provozovaných rejstříků a registrů,

   a s touto směrnicí.

4) Systém ochrany osobních údajů definovaný touto směrnicí je navržen a zpracován v souladu s Nařízením GDPR.

5) Přehled spravovaných datových sad osobních údajů formou Záznamů o činnostech zpracování je k dispozici zde v kanceláři tajemníka. Zpracování Záznamů o činnostech zpracování bylo provedeno dialogem s odpovědnými pracovníky správce. Záznamy o činnostech zpracování jsou pravidelně aktualizovány v návaznosti na změny ve zpracování osobních údajů u správce.

6) Směrnice je závazná pro všechny osoby organizačně zařazené do struktury správce, ať již se jedná o zaměstnance na HPP, DPP či DPČ.

7) Osoby, které osobní údaje zpracovávají v roli zpracovatele na základě smlouvy uzavřené se správcem, jakožto správcem osobních údajů jsou k dodržování ochrany osobních údajů zavázáni uzavřením smlouvy o ochraně osobních údajů podle článku 24 této směrnice.

8) Členové rady a zastupitelstva obce a členové výborů zastupitelstva a komisí rady postupují při nakládání s osobními údaji dle Nařízení GDPR, dle dalších platných právních předpisů na ochranu osobních údajů a obdobně dle této směrnice.

Článek 3

Pojmy a definice

Pro účely této směrnice se rozumí:

1) „**osobními údaji**“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „**subjekt údajů**“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

2) „**zvláštními kategoriemi osobních údajů**“ osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;

3) „**biometrickými údaji**“ 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;

4) „**zpracováním**“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

5) „**omezením zpracování**“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

6) „**pseudonymizací**“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

7) „**anonymizací**“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů a subjekt údajů není nebo již přestal být identifikovatelným;

8) „**evidencí**“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

9) „**správcem**“ obec jako orgán veřejné moci, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;

10) „**zpracovatelem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

11) „**příjemcem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty;

12) „**souhlasem**“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

13) „**porušením zabezpečení osobních údajů**“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

14) „**údaji o zdravotním stavu**“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;

15) „**záznamem o činnostech zpracování**“ záznamy vedené správcem o zpracování osobních údajů. Záznamy obsahují jméno a kontaktní údaje správce, účely zpracování, rozsah zpracovávaných osobních údajů, informace o příjemcích daných osobních údajů, o předávání údajů do třetích zemí, lhůtách pro výmaz jednotlivých kategorií údajů a popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů;

16) „**dozorovým úřadem**“ Úřad pro ochranu osobních údajů;

17) „**Unií**“ Evropská unie;

18) **„Členské státy“** Členské státy Evropské unie;

19) „**Zaměstnancem**“ fyzická osoba, která měla nebo má pracovně-právní vztah se správcem.

Článek 4

Rozsah působnosti

1) Starosta a tajemník odpovídají za to, že jim podřízení zaměstnanci, kteří nakládají s osobními údaji u správce, byli seznámeni s pravidly ochrany osobních údajů, tj. s touto směrnicí. Zaměstnanci obce jsou povinni pravidla pro nakládání s osobními údaji dodržovat.

2) Členové rady a zastupitelstva obce a členové výborů zastupitelstva a komisí rady obce postupují při nakládání s osobními údaji dle Nařízení GDPR, dle dalších platných právních předpisů na ochranu osobních údajů a obdobně dle této směrnice.

3) Pravidla ochrany osobních údajů se vztahují rovněž na všechny další subjekty, které pracují s osobními údaji správce. Tyto subjekty musí být k dodržování zásad ochrany osobních údajů zavázány postupem dle článku 24 této směrnice.

Článek 5

Určení rolí v systému ochrany osobních údajů

1) Starosta a tajemník

Odpovědnost za zajištění ochrany osobních údajů v souladu s Nařízením GDPR nesou starosta a tajemník zejména tím, že:

- schvalují/předkládají ke schválení Směrnici o nakládání s osobními údaji města a její aktualizace,

- vyjadřují se k osobě, která má vykonávat funkci Pověřence pro ochranu osobních údajů (dále také „Pověřenec“),
- jmenují Pověřence pro ochranu osobních údajů,
- rozhodují o přijetí technických, fyzických a organizačních opatření pro zajištění souladu ochrany osobních údajů s Nařízením GDPR a dalšími platnými právními předpisy na ochranu osobních údajů,
- zajistit, aby každý zaměstnanec správce před prvním přístupem ke spravovaným osobním údajům byl prokazatelně seznámen a proškolen se zásadami ochrany osobních údajů a touto směrnicí a zajistit min. v roční frekvenci prokazatelné opakování tohoto proškolení;
- zajistit, aby každý zaměstnanec správce před prvním přístupem ke spravovaným osobním údajům písemně potvrdil Prohlášení o ochraně osobních údajů;

2) Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů (dále také jako „Pověřenec“) je osobou odpovědnou za plnění těchto úkolů:

- poskytování informací a poradenství vedoucím pracovníkům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany osobních údajů;
- monitorování souladu s touto směrnicí, Nařízením GDPR a dalšími předpisy Unie nebo členských států v oblasti ochrany osobních údajů a s vnitřními předpisy správce v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
- zajištění pravidelného testování, posuzování a hodnocení účinnosti zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle Směrnice o nakládání s osobními údaji správce;
- zajištění monitoringu legislativních změn v oblasti ochrany osobních údajů a návrh na jejich implementaci v rámci správce;
- poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 Nařízení GDPR;
- spolupráce s dozorovým úřadem;
- působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 Nařízení GDPR, a případně vedení konzultací v jakékoli jiné věci.
- působení jako kontaktní místo pro subjekty údajů. Subjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle Nařízení.

Pověřenec pro ochranu osobních údajů bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.

Pověřenec pro ochranu osobních údajů je přímo podřízen starostovi a tajemníkovi.

Pověřenec pro ochranu osobních údajů nedostává žádné pokyny týkající se výkonu svých úkolů (např. nemůže dostat pokyn, jakého výsledku má dosáhnout nebo jaký názor nebo právní výklad má zastávat, jak prošetřit stížnost a námitku nebo zda kontaktovat dozorový úřad).

Pověřence nelze postihovat za nezávislý způsob výkonu povinností (tzn. za to, že zastává jiný názor než správce osobních údajů, nebo že kontaktoval dozorový úřad atp.).

Pověřenec je v souvislosti s výkonem svých úkolů vázán mlčenlivostí, a to v souladu s právem Unie nebo zákony a právními předpisy České republiky. Pověřenec může plnit i jiné úkoly a povinnosti, které však nesmějí vést ke střetu zájmů jeho činností.

3) Uživatelé osobních údajů

Uživatelem osobních údajů je zaměstnanec správce, člen zastupitelstva, rady obce, výboru zastupitelstva či komise rady obce, používající spravované osobní údaje k plnění svých pracovních povinností nebo k výkonu své funkce. Každý uživatel osobních údajů má právo podat Pověřenci návrh na změnu této směrnice, Záznamu o činnostech zpracování, Posouzení vlivu nebo zavedených organizačních a technických opatření pro zajištění bezpečnosti zpracování osobních údajů.

Uživatelé osobních údajů mají právo a zároveň povinnost:

- pro případy vzniku nových druhů osobních údajů tuto skutečnost co nejdříve nahlásit Pověřenci, který provede aktualizaci Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
- informovat bezodkladně Pověřence o všech skutečnostech, které mají vliv na aktuálnost Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
- zabezpečit získání souhlasu subjektu údajů, a to v souladu s Nařízením GDPR, není-li zpracování možné bez tohoto souhlasu;
- při uzavírání smluv s třetími stranami dbát na to, aby obsahovaly zásady zajištění ochrany osobních údajů, pokud je to vzhledem k povaze obsahu smlouvy relevantní.
- dodržovat zásady vyplývající z této směrnice a související dokumentace;
- hlásit veškeré bezpečnostní incidenty svému nadřízenému, případně přímo Pověřenci;
- informovat Pověřence o zjištěných bezpečnostních slabinách;
- informovat Pověřence o změnách ve způsobu zpracování a nakládání s osobními údaji;
- vykonávat další činnosti vyplývající z platných vnitřních předpisů správce, především zajistit průběh skartačního řízení v souladu se spisovým a skartačním řádem správce.

4) Administrátor[1]

Administrátor je zaměstnancem správce, který má na starost provoz a údržbu systémů a aplikací, zálohování a zabezpečení (elektronických) dat. Tento zaměstnanec má obvykle přístup ke všem datům uloženým v informačním systému správce nebo přístup k zařízením, pomocí nichž jsou tato data zpracovávána.

Administrátor zabezpečuje spolupráci s jednotlivými uživateli osobních údajů při ochraně osobních údajů uložených v osobních počítačích, včetně těch přenosných.

5) Koordinace pro práva subjektů údajů a pro řízení incidentů

Koordinaci vyřizování žádostí subjektů údajů, shromáždění potřebných informací, jakož i řízení vyřizování bezpečnostních incidentů zajišťuje tajemník.

Článek 6

Přístup k osobním údajům

K osobním údajům u správce mají přístup pouze starosta, místostarosta, tajemník, uživatelé osobních údajů, Pověřenec a administrátor.

Článek 7

Zásady zpracování osobních údajů

1) Osobní údaje musí být:

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 Nařízení GDPR nepovažuje za neslučitelné s původními účely („účelové omezení“);

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);

d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“);

[1] platí v případě, že je administrátor zaměstnancem správce; pokud se jedná o třetí osobu, pak se jedná o zpracovatele osobních údajů

e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 Nařízení GDPR, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných Nařízením GDPR s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);

f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“).

2) Standardně jsou zpracovávány pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Spis vedený Uživatelem osobních údajů obsahuje pouze informace relevantní pro průběh řízení a agendu s ohledem na minimalizaci údajů k dosažení účelu zpracování.

3) Písemnosti obsahující osobní údaje podléhají procesu fyzické a elektronické skartace v souladu se spisovým a skartačním řádem správce. V případě neevidovaných dokumentů (dokumentace na vědomí, kopie písemností a dalších dokumentů bez čísla jednacího) je za jejich likvidaci v elektronické i fyzické podobě odpovědný uživatel osobních údajů.

4) Pro statistické účely je nutné osobní údaje anonymizovat.

5) Je třeba zamezit neoprávněnému přístupu ke shromážděným údajům.

Článek 8

Zákonnost zpracování osobních údajů

1) Obec jako správce osobních údajů zpracovává pouze takové osobní údaje, jejichž zpracování je zákonné. Zpracování osobních údajů je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se vztahuje na obec jako správce osobních údajů;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřena obec jako správce osobních údajů;

f) zpracování je nezbytné pro účely oprávněných zájmů obce jako správce osobních údajů či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě. Toto se netýká zpracování prováděného obcí jako správcem osobních údajů při plnění jeho úkolů jako orgánu veřejné moci.

2) Účel zpracování osobních údajů musí vycházet z výše uvedených právních základů. Osobní údaje nesmějí být použity k jinému účelu, než ke kterému byly pořízeny nebo musí být takové zpracování nutné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřena obec jako správce osobních údajů.

3) Pokud je zpracování založeno pouze na souhlasu, musí být správce schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů. Tuto odpovědnost za doložení souhlasu nese u správce konkrétní uživatel osobních údajů, tj. konkrétní osoba, která v rámci své agendy u správce osobní údaje zpracovává.

a) Souhlas musí být udělen samostatně a musí být jasně odlišitelný od ostatních sdělení (jako samostatný dokument). Vzor souhlasu se zpracováním osobních údajů je zaměstnancům obce k dispozici u tajemníka.

b) Subjekt údajů vždy musí obdržet jednu kopii uděleného souhlasu, včetně informace o způsobu odvolání uděleného souhlasu.

c) Pro zpracování zvláštních kategorií osobních údajů (biometrické údaje, fotografie, audio, video, zdravotní stav, sociální postavení a další) je nutné vždy udělit samostatný souhlas, oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji).

d) Pro zpracování souhlasů s vytvořením kopie občanského průkazu (souhlas podle ust. § 15a zákona č. 328/1999 Sb., o občanských průkazech, v platném znění) je nutné vždy udělit samostatný souhlas, oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji).

e) Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně dostupné jako jej poskytnout.

f) V případě využití konkludentního souhlasu[2] je nutné zajistit informování subjektu údajů (např. na webových stránkách správce, informační tabule u vstupu na akce, informace na pozvánce a dalších místech sběru osobních údajů).

g) Uživatel osobních údajů je povinen ve spolupráci s tajemníkem zajistit výmaz osobních údajů v případě odvolání souhlasu se zpracováním osobních údajů, včetně výmazu v zálohách a kopiích dat. V případě technických problémů uživatel zkonzultuje postup s Administrátorem.

[2] Konkludentní právní jednání je projev vůle učiněný jiným způsobem než slovně , přičemž právně jednající takovým způsobem, jako je např. kývnutí hlavou, potřesení rukou, nevyjádření protestu, mlčky, vyjádří svou vůli se právně vázat.

h) Uživatel osobních údajů je povinen vést evidenci datových sad, jejichž zpracování je podloženo uděleným souhlasem subjektu údajů a vést evidenci udělených souhlasů subjektu údajů.

4) Zpracování údajů na základě uděleného souhlasu subjektu údajů je využíváno pouze v krajních případech, kdy je zpracování nezbytné a neexistuje jiné oprávnění pro nakládání s osobními údaji.

Článek 9

Opatření pro ochranu a zabezpečení osobních údajů

1) Uživatel osobních údajů je povinen dodržovat tzv. pravidlo čistého stolu (neponechávat volně položené písemnosti obsahující osobní údaje bez dozoru na svém pracovním stole, po ukončení pracovního dne je každý zaměstnanec povinen takové listinné písemnosti uložit do uzamykatelných úložných prostor a klíče zajistit tak, aby k nim neměly přístup osoby bez oprávnění).

2) Uživatel osobních údajů je povinen v případě odchodu z kanceláře, kde se již nenachází žádný další zaměstnanec města, zavřít okna a tuto místnost zamknout.

3) Uživatel osobních údajů je povinen v případě přítomnosti cizí osoby v kanceláři a nutnosti odchodu zaměstnance z kanceláře, kde se již nenachází žádný další zaměstnanec obce, vyprovodit cizí osobu na chodbu, kancelář zamknout a opětovný vstup cizí osoby do kanceláře umožnit až při vlastním návratu zaměstnance města do kanceláře (neponechávat cizí osoby bez dozoru v kanceláři).

4) Uživatel osobních údajů je povinen aktivovat spořič obrazovky chráněný heslem kdykoli se vzdálí od pracovní stanice.

5) Uživatel osobních údajů je povinen využívat pro elektronické zpracování osobních údajů k tomu určené informační systémy správce. Uživatel osobních údajů je povinen písemnostem obsahujícím osobní údaje přiřazovat skartační znaky dle platného spisového a skartačního řádu správce. Užívání pevných disků pro ukládání písemností obsahujících osobní údaje je povoleno v případě, že není možné tuto dokumentaci ukládat do informačních systémů správce.

6) Uživatel osobních údajů je povinen udržovat písemnosti obsahující osobní údaje uložené na pevných discích a ve svých emailových schránkách v souladu s lhůtami stanovenými pro zpracování dle spisového a skartačního řádu správce a v minimálním rozsahu umožňujícím dosažení účelu zpracování.

7) Uživatel osobních údajů není oprávněn ukládat písemnosti obsahující osobní údaje na sdílené disky správce, pokud to nevyžaduje spolupráce více Uživatelů a přístup na sdílené disky je omezen pouze na skupinu spolupracujících oprávněných Uživatelů osobních údajů správce.

8) Uživatel osobních údajů je povinen využívat pro ukládání fyzické dokumentace obsahující osobní údaje (včetně fyzických nosičů elektronické dokumentace) k tomu určené zabezpečené úložné prostory a tyto úložné prostory při opuštění kanceláře uzamknout. Uživatel osobních údajů je povinen písemnostem obsahujícím osobní údaje přiřazovat skartační znaky dle platného spisového a skartačního řádu správce. To platí i pro písemnosti na vědomí, kopie písemností a další dokumenty bez čísla jednacího.

9) Pokud není fyzická dokumentace obsahující osobní údaje uchovávána v uzamykatelných úložných prostorech, musí být zajištěn přístup pouze pro oprávněné zaměstnance (např. úklid pouze s doprovodem oprávněného zaměstnance).

10) Uživatel osobních údajů je povinen udržovat v tajnosti svá přístupová oprávnění (přihlašovací jméno a heslo) k informačním systémům města, tato přístupová oprávnění si nezapisovat (na papír, do volně přístupného nezabezpečeného souboru apod.) ani je neprozrazovat žádné další osobě.

11) Uživatel osobních údajů je povinen při tisku písemností obsahujících osobní údaje tyto nikdy neponechávat bez dozoru, tj. volně přístupné.

12) Uživatel osobních údajů není oprávněn přeposílat písemnosti obsahující osobní údaje na své nebo cizí soukromé e-mailové schránky nezabezpečeným způsobem, pokud zákon neukládá jinak[3].

13) Uživatel osobních údajů není oprávněn ukládat na veřejné servery Internetu (např. www.uloz.to, www.uschovna.cz apod.) jakékoli písemnosti obsahující osobní údaje.

14) Uživatel osobních údajů není oprávněn provádět na svěřených prostředcích jakékoliv hardwarové zásahy (např. měnit komponenty počítače, připojovat vlastní externí zařízení apod.) a spouštět či instalovat jakýkoliv nepovolený software.

15) Uživatel osobních údajů je oprávněn využívat mobilní zařízení správce (mobilní telefon, notebook apod.) pouze při dodržení pravidel pro jejich zabezpečení definovaných Administrátorem.

[3] např. zákon 106/1999 Sb., o svobodném přístupu k informacím

16) Uživateli osobních údajů je umožněno využívat k přístupu k informačním systémům a datům obce soukromá mobilní zařízení (mobilní telefon, notebook apod.) pouze při dodržení pravidel pro jejich zabezpečení definovaných Administrátorem.

17) Uživatel osobních údajů není oprávněn jakkoliv měnit nastavení, případně vypínat ochranu proti škodlivému kódu (antivirový program, antispyware apod.) na svěřených prostředcích.

18) Uživatel osobních údajů není oprávněn ukládat na vyměnitelná média jakékoliv písemnosti obsahující osobní údaje (mimo jednorázově schválených výjimek[4]). Vyměnitelnými médii rozumíme CD/DVD disky, přepisovatelné CD/DVD, pevné počítačové disky externí, flash disky apod.

19) Každý zaměstnanec, který přichází do styku s písemnostmi obsahujícími osobní údaje uloženými na médiích (CD, DVD, papírové dokumenty, flash paměťové moduly) je povinen zajistit jejich bezpečnou likvidaci (skartování, neobnovitelné vymazání, fyzické zničení) v souladu se spisovým a skartačním řádem správce.

20) Klíče od kanceláří jsou zaměstnancům správce vydávány prokazatelným způsobem a je vedena evidence vydaných klíčů. Je zajištěno ukládání a zabezpečení náhradních klíčů od kanceláří a úložných prostor.

Článek 10

Předávání osobních údajů

Dokumentaci obsahující osobní údaje v elektronické podobě je povoleno předávat příjemcům mimo správce pouze prostřednictvím datových schránek. V případech, kdy není možné dokumentaci předat prostřednictvím datové schránky nebo ve fyzické podobě, lze dokumentaci předat zabezpečeným způsobem (tj. např. v podobě šifrovaného souboru ve formátu .zip a heslo k odšifrování předat příjemcům nezávislým kanálem, např. zasláním na mobilní telefon).

[4] výjimky schvaluje tajemník

Článek 11

Zveřejňování osobních údajů

1) Při zveřejňování osobních údajů musí dojít k opatřením, kdy veškerá zveřejňovaná dokumentace (text, audio, video) bude anonymizována v rozsahu zajišťujícím minimalizaci rozsahu zveřejňovaných osobních údajů při dosažení účelu zveřejnění uloženého legislativou (dokumentaci anonymizovat vždy, pokud zákon neukládá jinak).
2) Musí dojít k zajištění anonymizace osobních údajů uvedených v uzavřených smlouvách, které jsou zveřejněny[5].
3) Při pořizování jakýchkoliv záznamů z akcí pořádaných v prostorách správce zajistit informování účastníků o pořizování, zveřejňování a uchovávání této dokumentace a uvedení účelu tohoto pořízení.
4) V případě pořizování fotografické nebo video dokumentace z veřejných akcí správce, musí správce zajistit informování účastníků o pořizování této dokumentace za účelem informování veřejnosti o činnosti správce a možném uložení do odvolání uděleného souhlasu. Pracovníci pořizující tuto dokumentaci musí být viditelně výrazně označeni.
5) Fotografie zaměstnanců města se mohou zveřejňovat na webových stránkách města apod., pouze po výslovném souhlasu zaměstnance města s tímto zveřejněním (souhlas není vynutitelný) s výjimkou případů uvedených v předchozím odstavci.

Článek 12

Získávání informací od subjektu údajů

1) Odpovědný zaměstnanec správce (Uživatel osobních údajů) v okamžiku získání osobních údajů poskytne subjektu údajů tyto informace:
   a) totožnost a kontaktní údaje správce a jeho odpovědného zaměstnance (Uživatele osobních údajů);
   b) kontaktní údaje Pověřence;
   c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro jejich zpracování;
   d) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na oprávněném zájmu obce jako správce osobních údajů;
   e) případné příjemce nebo kategorie příjemců osobních údajů;

[5] např. smlouvy o poskytnutí dotace

f) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

g) existence práva požadovat od obce jako správce osobních údajů přístup k osobním údajům týkajících se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

h) existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním (pokud je zpracování založeno na uděleném souhlasu se zpracováním osobních údajů);

i) existence práva podat stížnost u dozorového úřadu;

j) 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 poučení ohledně možných důsledků neposkytnutí těchto údajů.

2) Naplnění informační povinnosti podle bodu 1) může být zajištěno zveřejněním Informačního memoranda (informace o zpracování osobních údajů) na webových stránkách obce.

3) Pokud obec jako správce osobních údajů hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace v rozsahu dle tohoto článku. Nemohou být zpracovány osobní údaje subjektů osobních údajů, pokud ke zpracování osobních údajů správci nesvědčí žádný právní důvod ke zpracování.

Článek 13

Práva subjektu údajů

1) Subjekt údajů může uplatnit tato práva:

a) přístup k osobním údajům,

b) opravu a výmaz osobních údajů,

c) omezení zpracování osobních údajů,

d) přenositelnost osobních údajů,

e) vznesení námitky.

2) Naplnění práv subjektů údajů zajišťuje věcně příslušný Uživatel osobních údajů.

3) Pokud je pro zajištění práv subjektů údajů nutné zapojení více zaměstnanců správce, zajišťuje jejich koordinaci a shromáždění potřebných informací tajemník.

4) Subjektu údajů jsou poskytovány informace v souladu se zásadami zpracování osobních údajů dle čl. 7 této směrnice, a to především stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, zejména pokud se jedná o informace určené dítěti.

5) Informace jsou subjektu údajů poskytovány výhradně na základě prokazatelného jednoznačného ověření totožnosti subjektu údajů (občanský průkaz, datová schránka).

Článek 14

Právo subjektu údajů na přístup k osobním údajům

1) Subjekt údajů má právo získat od obce jako správce osobních údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a 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;
   e) existence práva požadovat od obce jako správce osobních údajů opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování, anebo vznést námitku proti tomuto zpracování;
   f) právo podat stížnost u dozorového úřadu;
   g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

2) Právem získat přístup k osobním údajům nesmějí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

Článek 15

Oprava a výmaz osobních údajů

1) Subjekt údajů má právo na to, aby obec jako správce osobních údajů bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

2) Subjekt údajů má právo na to, aby obec jako správce osobních údajů bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a obec má povinnost osobní údaje bez zbytečného odkladu vymazat (tzv. „právo být zapomenut“), pokud je dán jeden z těchto důvodů:
   a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
   b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování a jejich uchovávání;
   c) subjekt údajů vznese námitky proti zpracování s ohledem na uplynutí lhůty pro zpracování nebo s ohledem na prokazatelnou nedostatečnost zabezpečení osobních údajů;
   d) osobní údaje byly zpracovány protiprávně;
   e) osobní údaje musí být skartovány ke splnění právní povinnosti stanovené právem Unie nebo zákony a platnými právními předpisy České republiky, které se na obec jako správce osobních údajů vztahují.

3) Jestliže obec jako správce osobních údajů osobní údaje zveřejnilo a je povinno je podle odstavce 2 vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně všech technických opatření, aby informovalo zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

4) Odstavce 2 a 3 se neuplatní, pokud je zpracování nezbytné:

a) pro výkon práva na svobodu projevu a informace;
b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo ČR, které se na obec jako správce osobních údajů vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je obec pověřena;
c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3 Nařízení GDPR;
d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely podle zvláštních právních předpisů;
e) pro určení, výkon nebo obhajobu právních nároků.

Požadavek subjektu údajů na výmaz tedy nelze splnit, pokud je zpracování nezbytné pro splnění právní povinnosti.

Článek 16

Právo na omezení zpracování

1) Subjekt údajů má právo na to, aby obec jako správce osobních údajů omezil zpracování, v kterémkoli z těchto případů:

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

2) Pokud bylo zpracování omezeno, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Unie nebo některého členského státu.

3) Subjekt údajů, který dosáhl omezení zpracování, musí být předem upozorněn na to, že bude omezení zpracování zrušeno.

Článek 17

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

Tajemník za obec jako správce osobních údajů je povinen oznámit jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré provedené opravy nebo výmazy osobních údajů nebo omezení zpracování, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.

Naplnění informační povinnosti podle bodu 1) může být zajištěno zveřejněním Informačního memoranda (Informace o zpracování osobních údajů) na webových stránkách obce.

Článek 18

Právo na přenositelnost údajů

1) Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl obci jako správci osobních údajů, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu město jako správce osobních údajů bránilo, a to v případě, že:
   a) zpracování je založeno na uděleném souhlasu se zpracováním osobních údajů nebo na uzavřené smlouvě; a
   b) zpracování se provádí v elektronické podobě.
2) Subjekt údajů má právo na to, aby osobní údaje předalo přímo obec jako správce osobních údajů druhému správci, je-li to technicky proveditelné.
3) Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je obec jako správce osobních údajů pověřeno.
4) Uplatněním práva na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

Článek 19

Právo vznést námitku

1) Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají. Obec jako správce osobních údajů

osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

2) Subjekt údajů je na právo vznést námitku výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.

Článek 20

Řešení případů porušení zabezpečení osobních údajů

1) Zjištění případu porušení zabezpečení osobních údajů ohlásí zaměstnanec neprodleně svému nadřízenému nebo přímo Pověřenci pro ochranu osobních údajů. Ostatní uživatelé osobních údajů (členové rady, zastupitelstva, výborů zastupitelstva a komisí rady) ohlásí zjištění případu porušení zabezpečení osobních údajů starostovi, tajemníkovi nebo přímo Pověřenci pro ochranu osobních údajů.

2) Okamžité hlášení bude obsahovat minimálně tyto informace:
   a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
   b) popis pravděpodobných důsledků porušení zabezpečení osobních údajů pro město jako správce osobních údajů a pro subjekty údajů;
   c) návrh okamžitých opatření k zastavení porušení zabezpečení osobních údajů a případně návrh okamžitých nápravných opatření.

3) Pověřenec pro ochranu osobních údajů ve spolupráci s Uživateli osobních údajů, Administrátorem, relevantními zpracovateli osobních údajů, případně dalšími relevantními zaměstnanci města, rozhodne o dalším postupu.

4) Pověřenec pro ochranu osobních údajů neprodleně informuje starostu a tajemníka a předloží jim ke schválení návrh na řešení případu porušení zabezpečení osobních údajů a případně doporučení ohlášení porušení zabezpečení osobních údajů dozorovému úřadu.

5) Pověřenec pro ochranu osobních údajů neprodleně předloží starostovi a tajemníkovi ke schválení návrh nápravných opatření pro zamezení opakování obdobného porušení zabezpečení osobních údajů. Nápravné opatření obsahuje kroky obnovy a postup, jak zamezit opakování stejného porušení zabezpečení, termíny realizace opatření, jména zaměstnanců odpovědných za jejich splnění. Realizace nápravných opatření podléhá schválení starostou obce.

6) Pověřenec pro ochranu osobních údajů provádí kontrolu plnění nápravných opatření a výsledky předkládá tajemníkovi v termínech k tomu dohodnutých.

Článek 21

Činnost při zjištění porušení zabezpečení osobních údajů

1) Jakékoli porušení zabezpečení osobních údajů nebo ztrátu dostupnosti osobních údajů (dále jen incident) nebo podezření na takové porušení je každý povinen oznámit tajemníkovi. Podezření na incident se posuzuje pro potřeby postupu podle této směrnice stejně jako incident, dokud není zjištěno, že incident nevznikl.

2) V případě incidentu, spočívajícího ve ztrátě dostupnosti osobních údajů se ustanovení článku 21 použijí přiměřeně.

3) Tajemník oznámí neprodleně incident nebo podezření na incident Pověřenci pro ochranu osobních údajů a projedná s ním případnou součinnost, komunikaci a postup.

4) Tajemník vede dokumentaci činností a komunikace při reakci na incident tak, aby byla úplná a průkazná.

5) Úkony v reakci na incident se provádějí bez zbytečného odkladu, a pokud je to možné, ihned.

6) Hlavními cíli řízení reakce na incident jsou:
   a) Ověřit, zda skutečně došlo k porušení zabezpečení osobních údajů.
   b) Zjistit, zda došlo k neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů, případně jinému nežádoucímu stavu nebo dopadu.
   c) Zamezit možnosti neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů.
   d) Zjistit rozsah incidentu.
   e) Zjistit, které osoby se mohly neoprávněně s osobními údaji seznámit.
   f) Zjistit, kde se osobní údaje a informační systémy nacházejí v rozporu s předpisy obce a obecně závaznými právními normami.
   g) Opatřit důkazy pro řízení, vyšetřování nebo dokazování. Pokud je to třeba, použijí se forenzní metody a standardy.
   h) Zjistit, zda je potřebné oznamovat incident třetím stranám.
   i) Navrhnout a přijmout taková opatření, aby incident pominul, je-li to možné.
   j) Navrhnout a přijmout taková opatření, aby se incident neopakoval, je-li to možné.
   k) Sdílet nebo předat varování třetím osobám, zejména dozorovému úřadu tak, aby se předešlo incidentům u dalších správců.

7) Činnost podle tohoto článku se ukončí, jestliže o tom rozhodne starosta na základě předložené zprávy a zabezpečených podkladů a informací, nebo pokud se prokáže, že k incidentu

nedošlo. Pokud se prokáže, že k incidentu nedošlo, vypracuje tajemník zprávu v obdobném rozsahu.

Článek 22

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1) Jakékoli porušení zabezpečení osobních údajů Pověřenec za obec jako správce osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

2) Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu Pověřenci.

3) Ohlášení případů porušení zabezpečení osobních údajů musí přinejmenším obsahovat:
   a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
   b) jméno a kontaktní údaje Pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
   c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
   d) popis opatření, která obec jako správce přijalo nebo navrhlo k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

4) Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. Pověřenec pro ochranu osobních údajů dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

Článek 23

Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

1) Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí obec jako správce osobních údajů toto porušení bez zbytečného odkladu subjektu údajů.

2) V oznámení určeném subjektu údajů se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a opatření uvedené v čl. 22 této Směrnice.

3) Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:
   a) obec jako správce osobních údajů zavedlo náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
   b) obec jako správce osobních údajů přijalo následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;
   c) oznámení by vyžadovalo nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

4) Jestliže obec jako správce osobních údajů dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámilo, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinilo.

Článek 24

Zpracovatel

1) Pokud má být zpracování provedeno pro obec jako správce osobních údajů, využije obec pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení GDPR a této směrnice a aby byla zajištěna ochrana práv subjektu údajů.

2) Zpracovatel není oprávněn zapojit do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení obce jako správce osobních údajů. V případě obecného písemného povolení zpracovatel informuje obec jako správce osobních údajů o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak obci jako správci osobních údajů příležitost vyslovit vůči těmto změnám námitky.

3) Zpracování zpracovatelem se řídí smlouvou. Tajemník je povinen zajistit, aby s každým zpracovatelem byla před zahájením zpracování uzavřena Smlouva o zpracování osobních údajů, která zavazuje zpracovatele vůči obci jako správci osobních údajů a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce.

4) Seznam zpracovatelů vede tajemník.

Článek 25

Kontrola dodržování ustanovení směrnice

1) Tajemník zajistí kontrolu plnění povinností vyplývajících z ustanovení této Směrnice pro nakládání s osobními údaji.
2) Tajemník zajistí, aby byli s dokumentem Směrnice pro nakládání s osobními údaji seznámeni všichni zaměstnanci obce.
3) Všichni zaměstnanci obce jsou povinni poskytovat Pověřenci přiměřenou součinnost při plnění jeho úkolů. O provedených zjištěních vede Pověřenec pro ochranu osobních údajů prokazatelnou dokumentaci.
4) V případě doporučení ke změnám organizačních a technických opatření pro zajištění bezpečnosti zpracování osobních údajů předkládá Pověřenec pro ochranu osobních údajů tato doporučení starostovi a tajemníkovi ke schválení.

Článek 26

Platnost a účinnost směrnice

1) Směrnice pro nakládání s osobními údaji nabývá pro zaměstnance obce účinnosti dnem jejího vydání tajemníkem. Pro členy zastupitelstva a výborů zastupitelstva nabývá účinnosti okamžikem schválení zastupitelstvem obce. Pro členy rady a komisí rady nabývá účinnosti okamžikem schválení radou obce.

Článek 27

Závěrečná ustanovení

1) Tato směrnice byla schválena zastupitelstvem obce dne 24.5.2018, usnesením č. 24/6.
2) Tato směrnice byla schválena radou obce dne 14.5.2018, usnesením č. 96/2.
3) Tato směrnice byla vydána pro zaměstnance obce tajemníkem s účinností ode dne 25.5.2018.

V Lužicích dne 24.5.2018

……..

starosta obce Lužice