Směrnice pro nakládání s osobními údaji

Obec Skalka,
IČ: 00636819
se sídlem Skalka 69, 696 48 Ježov
(dále jen jako „správce“).
vydává tuto směrnici pro nakládání s osobními údaji:

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 také jako „Nařízení GDPR“), případně dalších souvisejících předpisů a k provedení planých právních předpisů České republiky.

Článek 2
Předmět, účel a působnost

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.

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.).

Směrnice je po seznámení s touto směrnicí závazná pro všechny osoby, které se s ní seznámily, pokud z jakéhokoli důvodu nakládají s osobními údaji, které spravuje správce.

Za účelem ochrany osobních údajů je definován tzv. systém řízení ochrany osobních údajů, který je navržen a zpracován v souladu s Nařízením GDPR a dalšími platnými právními předpisy.

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**“ osoba, 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 zejména identifikaci 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 v pracovněprávním vztahu ke správci (zaměstnanci v pracovním poměru, včetně DPP, DPČ, případně a osoby vykonávající pro práci dle smlouvy o veřejné službě), a to i v případě, že již pracovněprávní vztah byl ukončen.

Článek 4
Určení rolí v systému ochrany osobních údajů

Statutární orgán správce

Odpovědnost za zajištění ochrany osobních údajů v souladu s Nařízením GDPR nese statutární orgán správce zejména tím, že:

- Schvaluje směrnici o nakládání s osobními údaji a její aktualizace,
- jmenuje Pověřence pro ochranu osobních údajů po splnění zákonných podmínek,
- dohlíží nad dodržováním této směrnice,
- rozhoduje o přijetí technických a organizačních opatření pro zajištění souladu ochrany osobních údajů s Nařízením GDPR a dalšími platnými právními předpisy na ochranu osobních údajů.

Koordinátor pro práva subjektů údajů a řízení incidentů

Příjem žádostí subjektů údajů, koordinaci a shromáždění potřebných informací zajišťuje Koordinátor pro práva subjektů údajů a řízení incidentů, kterým je zpravidla statutární orgán správce (lze určit i jinou osobu).

Koordinátor pro práva subjektů údajů a řízení incidentů dále zajišťuje koordinaci a součinnost osob v případech podezření na incident nebo při zjištění incidentu při správě nebo zpracování osobních údajů.

Všechny osoby, na něž dopadá tato směrnice, musí poskytnout Koordinátorovi pro práva subjektů údajů a řízení incidentů bezodkladně na požádání potřebnou součinnost.

Pověřenec pro ochranu osobních údajů
Pověřenec je osobou zodpovědnou za plnění těchto úkolů:
- poskytování informací a poradenství správci při provádění zpracování, o povinnostech podle této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany osobních údajů;
- zajištění pravidelného testování, posuzování a hodnocení účinnosti zavedených organizačních a technických opatření pro zajištění bezpečnosti zpracování dle této směrnice;
- zajištění monitoringu legislativních změn v oblasti ochrany osobních údajů a návrh na jejich implementaci;
- 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 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 nedostává žádné pokyny týkající se výkonu svých úkolů (nemůže mu být zadán 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 nijak 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.

Tam, kde není ustanoven Pověřenec, vykonává jeho činnosti Koordinátor pro práva subjektů údajů a řízení incidentů.

Zodpovědná osoba
Zodpovědné osoby jsou uvedeny v příslušných Záznamech o činnosti zpracování osobních údajů. Každá Zodpovědná osoba má povinnost dodržovat platné právní předpisy a tuto směrnici.

Každá Zodpovědná osoba má povinnost vždy vyhotovit Záznam o činnostech zpracování při výkonu činností zpracování osobních údajů.

Každá Zodpovědná osoba má právo podat Pověřenci návrh na změnu této směrnice, Záznamu o činnostech zpracování, Posouzení vlivu nebo zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle Směrnice.

Zodpovědné osoby 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 se zpracováním osobních údajů, není-li zpracování možné bez tohoto souhlasu;
- zajistit, aby každý Zpracovatel, Uživatel, či Externí příjemce před prvním přístupem ke spravovaným osobním údajům byl prokazatelně seznámen se zásadami ochrany osobních údajů, vydanými správcem a jejich změnami;
- zajistit, aby každý Zpracovatel, Uživatel, či Externí příjemce před prvním přístupem ke spravovaným osobním údajům písemně potvrdil, že byl prokazatelně seznámen se zásadami ochrany osobních údajů, vydanými správcem a jejich změnami.

Zpracovatel
Zpracovatelem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Zpracovatelé jsou vždy uvedeni v příslušných Záznamech o činnosti zpracování osobních údajů.

Každý Zpracovatel má povinnost:
- dodržovat platné právní předpisy a zásady ochrany osobních údajů, vydané správcem a jejich změny;
- hlásit veškeré bezpečnostní incidenty statutárnímu orgánu správce;
- informovat statutární orgán správce o změnách ve způsobu zpracování a nakládání s osobními údaji.

Uživatel osobních údajů
Uživatelem osobních údajů je osoba používající spravované osobní údaje k plnění svých povinností. Uživatelé jsou uvedeni v příslušných Záznamech o činnosti zpracování osobních údajů. Uživatelem je vždy Statutární orgán správce, Koordinátor pro práva subjektů údajů a řízení incidentů a Zodpovědná osoba.

Všichni Uživatelé osobních údajů mají za povinnost:
- dodržovat platné právní předpisy a tuto směrnici;
- hlásit veškeré bezpečnostní incidenty statutárnímu orgánu správce;
- informovat statutární orgán správce o změnách ve způsobu zpracování a nakládání s osobními údaji.

Externí příjemce
Externím příjemce osobních údajů je osoba mající přístup ke spravovaným osobním údajům v souvislosti s plnění svých povinností. Externí příjemci jsou uvedeni v příslušných Záznamech o činnosti zpracování osobních údajů.

Každý Externí příjemce má povinnost dodržovat platné právní předpisy a zásady ochrany osobních údajů, vydané správcem a jejich změny.

Článek 5
Přístup k osobním údajům

K příslušným osobním údajům mají přístup pouze Zodpovědná osoba, Zpracovatel, Uživatel osobních údajů, Koordinátor pro práva subjektů údajů a řízení incidentů, Pověřenec, Externí příjemce.

Rozsah oprávnění přístupu k příslušným osobním údajům vymezuje správce pro jednotlivé osoby v příslušných Záznamech o činnosti zpracování osobních údajů.

Článek 6
Zásady zpracování osobních údajů

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“);
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“).

Zpracovávány mohou být 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.

Záznamy obsahující osobní údaje v jakékoli formě (zejména písemnosti, elektronické záznamy apod.) podléhají procesu fyzické a elektronické skartace v souladu se Spisovým a skartačním řádem správce. V případě ostatních záznamů (zejména dokumentace na vědomí, kopie písemností a dalších záznamů) je za jejich likvidaci v elektronické i fyzické podobě odpovědný uživatel osobních údajů, který takový záznam vytvořil.

Je třeba zamezit neoprávněnému přístupu ke shromážděným osobním údajům.

Článek 7
Zákonnost zpracování osobních údajů

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 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 pověřen správce osobních údajů;
f) zpracování je nezbytné pro účely oprávněných zájmů 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 správcem osobních údajů při plnění jeho úkolů jako orgánu veřejné moci.

Pokud je zpracování osobních údajů podmíněno udělením souhlasu subjektu osobních údajů, musí být Zodpovědná osoba schopna doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů.

a) Souhlas musí být udělen samostatně a musí být jasně odlišitelný od ostatních sdělení (jako samostatný dokument).
b) Subjekt údajů vždy musí obdržet jednu kopii uděleného souhlasu, včetně informace o způsobu odvolání uděleného souhlasu.
c) 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.

d) Uživatel osobních údajů je povinen ve spolupráci Zodpovědnou osobou a Koordinátorem pro práva subjektu údajů a řízení incidentů zajistit výmaz osobních údajů v případě odvolání souhlasu se zpracováním osobních údajů, včetně výmazu v zálohách a kopiích dat.
e) Každá Zodpovědná osoba je povinna vést v rámci výkonu své činnosti evidenci udělených souhlasů subjektů údajů a tuto v kopii předávat Koordinátorovi pro práva subjektů údajů a řízení rizik.

Článek 8
Opatření pro ochranu a zabezpečení osobních údajů

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

Uživatel osobních údajů je povinen v případě odchodu z prostor, kde se již nenachází žádný další Uživatel, zavřít okna a tuto místnost zamknout, pokud je to možné.

Uživatel osobních údajů je povinen neponechávat cizí osoby bez dozoru v prostorách, kde se nachází osobní údaje.

Uživatel osobních údajů je povinen aktivovat spořič obrazovky chráněný heslem kdykoli se vzdálí od svého elektronického zařízení, které obsahuje záznamy obsahující osobní údaje (PC, notebook, tablet, mobilní telefon).

Uživatel osobních údajů je povinen využívat pro elektronické zpracování osobních údajů k tomu určené informační systémy správce.

Užívání pevných disků pro ukládání záznamů obsahujících osobní údaje je povoleno pouze v případě, že není možné tyto záznamy ukládat do informačních systémů správce.

Uživatel osobních údajů není oprávněn ukládat záznamy, obsahující osobní údaje na sdílené disky správce, pokud to nevyžaduje spolupráce více Uživatelů a je zabezpečeno, že přístup k takovým záznamům na sdílených discích je omezen pouze na skupinu spolupracujících oprávněných Uživatelů.

Uživatel osobních údajů je povinen využívat pro ukládání fyzické záznamy, obsahující osobní údaje (včetně fyzických nosičů elektronické dokumentace) k tomu určené zabezpečené úložné prostory a tyto úložné prostory při opuštění prostor, kde se nachází osobní údaje uzamknout.

Pokud nejsou fyzické záznamy, obsahující osobní údaje uchovávány v uzamykatelných úložných prostorech, musí být zajištěn přístup pouze pro oprávněné osoby dle této Směrnice (např. úklid provádění montážních, či stavebních prací pouze pod dohledem oprávněné osoby dle této Směrnice).

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

Každý Uživatel je povinen při tisku záznamů, obsahujících osobní údaje tyto nikdy neponechávat bez dozoru na tiskárně.

Žádný Uživatel není oprávněn přeposílat záznamy, obsahující osobní údaje na své nebo cizí soukromé e-mailové schránky nezabezpečeným způsobem, pokud jiný právní předpis nestanoví jinak.

Žádný Uživatel není oprávněn ukládat nezabezpečeným způsobem na veřejné servery Internetu (např. www.uloz.to, www.uschovna.cz apod.) jakékoli záznamy, obsahující osobní údaje.

Žádný Uživatel 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.

Každý Uživatel je oprávněn využívat mobilní zařízení správce (mobilní telefon, notebook apod.) pouze při dodržení pravidel pro jejich zabezpečení stanovených samostatnou směrnicí.

Uživateli osobních údajů je umožněno využívat k přístupu k informačním systémům a záznamům správce soukromá mobilní zařízení (mobilní telefon, notebook apod.) pouze při dodržení pravidel pro jejich zabezpečení stanovených samostatnou směrnicí.

Žádný Uživatel není oprávněn jakkoliv měnit nastavení, případně vypínat ochranu proti škodlivému kódu (antivirový program, antispyware apod.) na svěřených technických zařízeních (PC, mobilní telefon, notebook apod.).

Žádný Uživatel není oprávněn ukládat na vyměnitelná média (CD/DVD disky, přepisovatelné CD/DVD, pevné počítačové disky externí, flash disky apod.) jakékoliv záznamy, obsahující osobní údaje.

Článek 9
Předávání osobních údajů

Záznamy, obsahující osobní údaje ve fyzické podobě je povoleno předávat třetím osobám pouze tak, aby nedošlo k porušení platných právních předpisů a zásad ochrany osobních údajů stanovených správcem. V případech, kdy není možné takové záznamy předat prostřednictvím datové schránky, lze záznamy předat zabezpečeným způsobem (tj. např. v podobě šifrovaného souboru ve formátu .zip a heslo k odšifrování předat adresátovi nezávislým kanálem, např. zasláním na mobilní telefon).

Záznamy, obsahující osobní údaje v elektronické podobě je povoleno předávat třetím osobám pouze tak, aby nedošlo k porušení platných právních předpisů a zásad ochrany osobních údajů stanovených správcem, především prostřednictvím datových schránek. V případech, kdy není možné takové záznamy předat prostřednictvím datové schránky, lze záznamy předat zabezpečeným způsobem (tj. např. v podobě šifrovaného souboru ve formátu .zip a heslo k odšifrování předat adresátovi nezávislým kanálem, např. zasláním na mobilní telefon).

Článek 10
Zveřejňování osobních údajů

Při zveřejňování osobních údajů musí dojít k opatřením, aby záznamy, obsahující osobní údaje (text, audio, video) byly anonymizovány v rozsahu, zajišťujícím minimalizaci rozsahu zveřejňovaných osobních údajů při dosažení účelu zveřejnění.

Při zveřejňování smluv v souladu s platnými právními předpisy (zejm. na profilu zadavatele, v registru smluv) musí dojít k zajištění anonymizace osobních údajů, uvedených v uzavřených smlouvách, které jsou zveřejňovány.

Článek 11
Získávání informací od subjektu údajů

Každý Uživatel osobních údajů v okamžiku získání osobních údajů poskytne subjektu údajů na písemné vyžádání tyto informace:

a) totožnost a kontaktní údaje správce;
b) totožnost a kontaktní údaje Pověřence;
c) účely zpracování, pro které jsou osobní údaje určeny, a zdůvodnění zákonnosti jejich zpracování;
d) případné příjemce nebo kategorie příjemců osobních údajů;
e) doba, po kterou budou osobní údaje zpracovány, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

f) existence práva požadovat od 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;
g) existence práva odvolat kdykoli souhlas se zpracováním osobních údajů;
h) existence práva podat stížnost u dozorového úřadu;

Naplnění informační povinnosti může být zajištěno zveřejněním těchto informací na webových stránkách správce.

Článek 12
Práva subjektu údajů

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.

Naplnění práv subjektů údajů zajišťuje příslušný Uživatel osobních údajů.

Pokud je pro zajištění práv subjektů údajů nutné zapojení více osob, zajišťuje jejich koordinaci a shromáždění potřebných informací Koordinátor pro práva subjektů údajů a řízení rizik.

Subjektu údajů jsou poskytovány informace o jejich právech především stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, zejména pokud se jedná o informace určené dítěti.

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

Článek 13
Právo subjektu údajů na přístup k osobním údajům

Subjekt údajů má právo získat od 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) totožnost a kontaktní údaje správce;
b) totožnost a kontaktní údaje Pověřence;
c) účely zpracování, pro které jsou osobní údaje určeny, a zdůvodnění zákonnosti jejich zpracování;
d) případné příjemce nebo kategorie příjemců osobních údajů;
e) doba, po kterou budou osobní údaje zpracovány, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
f) existence práva požadovat od 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;
g) existence práva odvolat kdykoli souhlas se zpracováním osobních údajů;
h) existence práva podat stížnost u dozorového úřadu;

Článek 14
Oprava a výmaz osobních údajů

Subjekt údajů má právo na to, aby 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.

Subjekt údajů má právo na to, aby správce osobních údajů bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce osobních údajů má povinnost osobní údaje bez zbytečného

odkladu vymazat (tzv. „právo být zapomenut“), pokud není splněna podmínka zákonnosti zpracování osobních údajů.

Jestliže správce osobních údajů osobní údaje zveřejnil a je povinen je vymazat z důvodu, že není splněna podmínka zákonnosti zpracování osobních údajů, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně všech technických opatření, aby informoval zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

Článek 15
Právo na omezení zpracování

Subjekt údajů má právo na to, aby správce osobních údajů omezil zpracování osobních důvodů tak, aby byla dodržena podmínka zákonnosti zpracování osobních údajů.

Subjekt údajů, který dosáhl omezení zpracování, musí být předem upozorněn na to, že bude omezení zpracování zrušeno, pokud bude po zrušení omezení dodržena podmínka zákonnosti zpracování osobních údajů.

Článek 16
Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

Koordinátor pro práva subjektů údajů a řízení incidentů je povinen za správce osobních údajů 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.

Článek 17
Právo na přenositelnost údajů

Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci osobních údajů, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce osobních údajů bránil, a to v případě, že zpracování je založeno na uděleném souhlasu se zpracováním osobních údajů nebo na uzavřené smlouvě; a zpracování se provádí automatizovaně.

Subjekt údajů má právo na to, aby osobní údaje předal přímo správce osobních údajů druhému správci, je-li to technicky proveditelné.

Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce osobních údajů pověřen.

Uplatněním práva na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

Článek 18
Právo vznést námitku

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají.
Správce osobních údajů osobní údaje dále nezpracovává, pokud neprokáže zákonnost zpracování.

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 19
Řešení případů porušení zabezpečení osobních údajů

Zjištění případu porušení zabezpečení osobních údajů ohlásí každý Uživatel osobních údajů neprodleně Pověřenci pro ochranu osobních údajů a Koordinátorovi pro práva subjektů údajů a řízení incidentů.

Okamžité hlášení bude obsahovat minimálně 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;

Pověřenec pro ochranu osobních údajů ve spolupráci s Koordinátorem pro práva subjektů údajů a řízení incidentů, příslušnými Uživateli osobních údajů (zejména pak statutárním orgánem správce) a příslušnými zpracovateli osobních údajů, případně dalšími osobami rozhodne o dalším postupu v reakci na případ porušení zabezpečení osobních údajů (dále jen „incident“).

Úkony v reakci na incident se provádějí bez zbytečného odkladu nejméně v tomto rozsahu:

a) ověření, zda skutečně došlo k porušení zabezpečení osobních údajů,
b) ověření, zda došlo k neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů, případně jinému nežádoucímu stavu nebo dopadu,
c) zamezení možnosti neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů,
d) zjištění rozsahu incidentu,
e) zjištění, které osoby se mohly neoprávněně s osobními údaji seznámit,
f) zjištění, kde se nacházejí záznamy, obsahující osobní údaje v rozporu s platnými právní předpisy a zásadami ochrany osobních údajů, vydanými správcem,
g) opatřené důkazy pro řízení, vyšetřování nebo dokazování,
h) zjištění, zda je potřebné oznamovat incident třetím stranám,
i) předání varování třetím osobám, tak aby se předešlo incidentům u dalších správců.

Pověřenec pro ochranu osobních údajů ve spolupráci s Koordinátorem pro práva subjektů údajů a řízení incidentů, příslušnými Uživateli osobních údajů (zejména pak statutárním orgánem správce) a příslušnými zpracovateli osobních údajů, případně dalšími osobami, předloží správci ke schválení návrh na řešení případu porušení zabezpečení osobních údajů a případně doporučení ohlášení porušení zabezpečení osobních údajů dozorovému úřadu.

Pověřenec pro ochranu osobních údajů ve spolupráci s Koordinátorem pro práva subjektů údajů a řízení incidentů, příslušnými Uživateli osobních údajů (zejména pak statutárním orgánem správce) a příslušnými zpracovateli osobních údajů, případně dalšími osobami, předloží správci 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, označení osob odpovědných za jejich splnění. Návrh nápravných opatření musí být konzultován s příslušnými Uživateli osobních údajů (zejména pak statutárním orgánem správce), které ho svým podpisem odsouhlasí. Realizace nápravných opatření podléhá schválení statutárním orgánem správce.

Pověřenec pro ochranu osobních údajů provádí kontrolu plnění nápravných opatření a výsledky předkládá statutárnímu orgánu správce v termínech k tomu dohodnutých.

Článek 20
Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

Jakékoli porušení zabezpečení osobních údajů ohlásí správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl 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.

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 město jako správce přijalo nebo navrhlo k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

Za správce plní ohlašovací povinnost Pověřenec pro ochranu osobních údajů.

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 21
Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

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

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 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) 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 město jako správce přijalo nebo navrhlo k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:
a) správce osobních údajů zavedl 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) správce osobních údajů přijal 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.

Jestliže správce osobních údajů dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak správce učinil.

Za správce plní ohlašovací povinnost Pověřenec pro ochranu osobních údajů.

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 22
Závěrečná ustanovení

Revize směrnice je provedena v případě potřeby.
Tato směrnice byla schválena ZO dne 11. 9. 2018 a nabývá účinnosti dnem schválení.

Josef Novák, starosta obce