Obec Markvartice

Směrnice č. 1/2018

o zpracování osobních údajů

a postupech jejich zabezpečení

Ze dne: 22. 5. 2018

Vypracoval: Tomáš Renka

Obsah

1. ÚVODNÍ USTANOVENÍ 3
2. DEFINICE POJMŮ 3
3. PRÁVA A ODPOVĚDNOST 4
   - 3.1. *Právo být informován* 4
   - 3.2. *Právo na přístup* 5
   - 3.3. *Právo na opravu* 5
   - 3.4. *Právo na výmaz* 5
   - 3.5. *Právo na omezení zpracování* 5
   - 3.6. *Právo přenositelnosti* 5
   - 3.7. *Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu* 6
   - 3.8. *Porušení povinnosti mlčenlivosti* 6
4. PRINCIPY ZPRACOVÁNÍ 6
   - 4.1. *Zákonnost, korektnost a transparentnost* 6
   - 4.2. *Minimalizace údajů* 7
   - 4.3. *Omezení uložení* 7
5. ORGANIZAČNÍ OPATŘENÍ 7
   - 5.1. *Školení zaměstnanců* 7
   - 5.2. *Záznamy o činnostech zpracování* 7
6. TECHNICKÁ OPATŘENÍ 8
   - 6.1. *Zabezpečení elektronického zpracování* 8
   - 6.2. *Fyzické zabezpečení* 9
7. ZÁVĚREČNÁ USTANOVENÍ 9
8. PŘÍLOHY 9
   - 8.1. *Všeobecné prohlášení o zpracování osobních údajů* 9
   - 8.2. *Seznam aplikací* 9
   - 8.3. *Vzorový dodatek smlouvy o zpracování osobních údajů* 9
   - 8.4. *Vzor souhlasu se zpracováním osobních údajů* 9
   - 8.5. *Vzor odvolání souhlasu* 9
   - 8.6. *Evidence klíčů* 9
   - 8.7. *Záznamy o činnostech zpracování* 9

1. Úvodní ustanovení

Tato směrnice stanovuje závazná pravidla zpracovávání osobních údajů a postupy pro jejich zabezpečení v souladu s nařízením Evropského parlamentu a Rady (EU) č. 2016/679 (dále jen Obecné nařízení EU). Směrnice je aplikaci ustanovení uvedeného nařízení v podmínkách a v rámci působnosti obecního úřadu Markvartice.

2. Definice pojmů

„**Osobní údaje**" 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.

„**Zvláštní kategorie osobních údajů**" jsou osobní údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje, biometrické údaje a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

„**Zpracování** " je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

„**Zákonnost zpracování**" je dodržena, 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 na správce vztahuje;
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;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce 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.

První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

„Správce" je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

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

„Subjekt údajů" je fyzická osoba, jejíž osobní údaje jsou zpracovávané.

3. Práva a odpovědnost

Obec, jako správce osobních údajů, je odpovědná za zpracovávání osobních údajů. Tato odpovědnost nemůže být přenesena na jiný subjekt. Splnění této odpovědnosti je stanoveno touto směrnicí. Obec zpracovává pouze takové osobní údaje, jež jsou pro její činnost nezbytné, za legitimními účely a pouze po nezbytně nutnou dobu. Doba zpracování je stanovena spisovým a skartačním plánem, případně konkrétními závaznými právními normami.

3.1. Právo být informován

Subjekty údajů mají právo být informovány správcem osobních údajů o zpracování před vznikem smluvního vztahu, případně před vydáním souhlasu se zpracováním. Informace obsahuje zejména následující údaje:

- totožnost a kontaktní údaje správce,
- kontaktní údaje pověřence,
- účely zpracování a jejich právní základ,
- oprávněné zájmy správce nebo třetí strany, pokud je zpracování založeno na oprávněném zájmu,
- případné příjemce nebo kategorie příjemců osobních údajů,
- případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci
- dobu zpracování,

- existenci práv subjektu údajů.

3.2. Právo na přístup

Subjekt údajů má právo na potvrzení o zpracování jeho údajů, na přístup ke svým osobním údajům, na informaci o rozsahu zpracovávaných informací, na poskytnutí informací nejdéle do 1 měsíce od podání žádosti, na vysvětlení (při zamítnutí žádosti). Informace jsou poskytovány na základě písemné žádosti. Jsou poskytovány zpravidla bezplatně, kromě případů, kdy správce posoudí žádost jako zbytečně opakovanou, nepřiměřenou, nedůvodnou, nebo pokud nejde o oprávněný zájem žadatele. Pokud je požadována úhrada, její výše se řídí sazebníkem uvedeným ve směrnici o poskytování informací podle zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů.

3.3. Právo na opravu

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. Obec předchází tomu, aby zpracovávané údaje byly neaktuální, údaje o zaměstnancích pravidelně ověřuje.

3.4. Právo na výmaz

Subjekt údajů má právo na výmaz údajů, pokud již nejsou potřebné pro původní účely, při odvolání souhlasu subjektu, při námitkách proti zpracování, při protiprávním zpracování, pokud není poskytnut souhlas se zpracováním, pokud je povinnost výmazu dána právní povinností.

Výmaz se provádí na základě písemné žádosti a provádí se u údajů, k jejichž zpracování byl poskytnut informovaný souhlas, výmaz nelze provést u zákonného zpracování osobních údajů.

3.5. Právo na omezení zpracování

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

- subjekt údajů popírá přesnost osobních údajů,
- zpracování je protiústavní,
- správce již osobní údaje nepotřebuje, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků,
- subjekt údajů vznesl námitku proti zpracování.

3.6. Právo přenositelnosti

Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, a to v případě, že:

- zpracování je založeno na souhlasu nebo na smlouvě
- zpracování se provádí automatizovaně.

Subjekt údajů má právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, 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 pověřen.

3.7. Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

Při zjištění, že bylo porušeno zabezpečení osobních údajů, nebo při podezření, že bylo porušeno toto zabezpečení, je každý subjekt povinen informovat správce a pověřence. Ti ve vzájemné součinnosti posoudí, zda skutečně došlo k porušení zabezpečení, vyhodnotí závažnost a podle závažnosti (bez rizika, nízké riziko, vysoké riziko) o porušení informují dozorový orgán i subjekt údajů. Organizace zajistí provedení nápravných opatření.

3.8. Porušení povinnosti mlčenlivosti

Vědomé porušení povinnosti mlčenlivosti, neoprávněné zveřejnění, sdělení, zpřístupnění a přisvojení osobních údajů zaměstnancem je porušením povinností, které mu vyplývají z pracovního poměru, zvlášť hrubým způsobem.

Při neoprávněném nakládání s osobními údaji může jít o trestný čin podle § 180 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů – jde o neoprávněné zveřejnění, zpracování, sdělení, zpřístupnění, přisvojení osobních údajů, porušení mlčenlivosti.

4. Principy zpracování

4.1. Zákonnost, korektnost a transparentnost

Jakékoli osobní údaje jsou zpracovávány obcí zákonným způsobem, tedy buď na základě zákona (právního předpisu), smluvního vztahu nebo se souhlasem subjektu, jehož údaje se zpracovávají. Obec zajišťuje průběžnou kontrolu, zda nedochází ke zpracování nad rámec zpracovaný zákonem, zda údaje, které obec získává, jsou pro její činnost nezbytné; zda všechny údaje jsou zpracovávány v souladu s právními předpisy. Informace jsou poskytovány stručným, srozumitelným a snadno přístupným způsobem, za použití jednoznačných a jednoduchých jazykových prostředků.

Pokud je pro zpracování osobních údajů nezbytný souhlas, pak musí být informovaný, konkrétní a písemný. Zpracování takových osobních údajů je možné provádět až po získání souhlasu. Písemná podoba souhlasu se uchovává minimálně po celou dobu zpracování údajů.

4.2. Minimalizace údajů

Zpracovávané informace jsou omezeny jen na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány. Nelze požadovat údaje nepřiměřené, nerelevantní a pokud nejsou nezbytné. Údaje nelze uchovávat poté, co pomine právní základ, poté, co je naplněn účel zpracování.

4.3. Omezení uložení

Osobní údaje jsou uloženy pouze po nezbytnou dobu. Ta vychází zejména spisového a skartačního plánu, který je součástí spisového řádu.

Na konci úložné doby jsou data přezkoumána a odstraněna, pokud neexistuje oprávněný důvod pro jejich další uchování.

5. Organizační opatření

5.1. Školení zaměstnanců

Obec zajišťuje:

- vstupní školení všech nových zaměstnanců při vzniku jejich pracovně-právního vztahu;
- periodická školení všech zaměstnanců nejméně jednou za dva roky, případně při změně pravidel pro zabezpečení osobních údajů daných touto směrnicí, nebo právními normami, na které se odkazuje;
- při ukončování pracovněprávního vztahu poučení zaměstnanců o tom, že jejich povinnosti při ochraně osobních údajů trvají i po ukončení pracovněprávního vztahu k organizaci;
- zveřejnění této směrnice pro potřeby zaměstnanců.

Při školeních či poučení jsou předávány informace zejména o povinnostech obce a zaměstnanců vyplývajících z Obecného nařízení EU, nebezpečí plynoucích ze záměrných pokusů narušit ochranu osobních údajů (falešné identity, pokusy získat údaje způsobem, kdy nelze spolehlivě ověřit identitu žadatele) a níže uvedených technických opatřeních.

5.2. Záznamy o činnostech zpracování

O činnostech při zpracování (jak v listinné, tak elektronické podobě) vede obec písemné záznamy, které jsou přílohou této směrnice.

6. Technická opatření

Osobní data jsou zpracovávána způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí technických a organizačních opatření před neoprávněným přístupem k údajům, náhodnou ztrátou, zničením, nebo poškozením.

6.1. Zabezpečení elektronického zpracování

Pro zabezpečení počítačů jsou stanovena následujícími opatřeními:

- instalace antivirového programu;
- vhodné nastavení firewallu;
- každý zaměstnanec musí mít vlastní uživatelský účet;
- používání dostatečně silných hesel (heslo o délce minimálně sedmi znaků, vždy musí jít o kombinaci malých a velkých písmen a čísel, případně zvláštních znaků);
- zákaz sdělování hesel jiné osobě;
- „uzamykání" obrazovky při odchodu od počítače (klávesy Win+L);
- pravidelné zálohování dat počítače tak, aby nedošlo k jejich ztrátě při případném odcizení či poruše počítače a byla zajištěna schopnost obnovy dat v případě fyzických či technických incidentů;
- šifrování disku počítače, pokud to umožňuje operační systém;
- zajištění automatických bezpečnostních aktualizací používaného softwaru;
- při jakékoli likvidaci hardwaru musí být znemožněno získání uložených osobních údajů (např. provedením fyzické destrukce pevného disku);
- neotvírání a mazání nevyžádané pošty;
- pravidelné testování přijatých technických opatření nejméně jednou ročně;
- pravidelná školení zaměstnanců v této oblasti nejméně jednou za dva roky;
- používání pouze agendových informačních systémů a aplikací, jejichž seznam a způsob technického zabezpečení je uveden v příloze této směrnice;
- aplikace umístěné v hostovaném prostředí nebo webových aplikací musí komunikovat šifrovaně;
- pokud jsou využívány cloudové služby, musí jít o cloud umístěný v legislativním prostoru Evropské unie;
- používání počítače výhradně k pracovním účelům;
- v případě posílání dokumentů obsahujících větší množství osobních údajů e-mailem, tyto dokumenty opatřit heslem a heslo sdělit adresátovi jiným způsobem (např. telefonicky).

V případě mobilních telefonů a tabletů je povinností zaměstnance mít přístup do zařízení zabezpečen heslem, pinem nebo prostřednictvím otisku prstu. Pokud to zařízení umožňuje, mít zapnuté jeho šifrování.

6.2. Fyzické zabezpečení

Pro zabezpečení listinných dokumentů jsou stanovena následující opatření:

- veškeré dokumenty jsou vedeny v souladu s platným spisovým řádem;
- listinné dokumenty se zvláštními osobními údaji jsou ukládány do uzamykatelných skříní;
- při odchodu z pracoviště je zaměstnanec povinen uzamknout, případně jinak zabezpečit prostor před vstupem neoprávněných osob;
- pracoviště je vybaveno elektronickým zabezpečovacím systémem;
- do budovy a na jednotlivá pracoviště mají přístup jen oprávněné osoby na základě evidence klíčů, která je přílohou této směrnice.

7. Závěrečná ustanovení

Za správnost, aktualizaci a kontrolu provádění ustanovení této směrnice je odpovědný starosta obce.

Tato směrnice byla schválena zastupitelstvem obce dne 24.5.2018 usnesením č. ZO 18 03 22.

Směrnice nabývá účinnosti dne 25.5.2018.

8. Přílohy

8.1. Všeobecné prohlášení o zpracování osobních údajů

8.2. Seznam aplikací

8.3. Vzorový dodatek smlouvy o zpracování osobních údajů

8.4. Vzor souhlasu se zpracováním osobních údajů

8.5. Vzor odvolání souhlasu

8.6. Evidence klíčů

8.7. Záznamy o činnostech zpracování