Směrnice
pro nakládání s osobními údaji pro obec

SMĚRNICE PRO NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI PRO OBEC

SMS
SLUŽBY s.r.o.

Směrnice

pro nakládání s osobními údaji pro obec Velehrad

Směrnice pro nakládání s osobními údaji

Obce Velehrad

1. JAK SE SMĚRNICÍ NAKLÁDAT

1.1. Tuto Směrnici mohou starostové či tajemníci zejména malých obcí využít buď tak, jak je, anebo s přihlédnutím k potřebě jednoduchosti a konkrétních instrukcí zaměstnancům a členům orgánů její pasáže včlenit do pracovního nebo organizačního řádu nebo přímo do některých smluv a pracovních náplní. Konkrétní provedení by měli konzultovat s pověřencem pro ochranu osobních údajů.

1.2. Směrnici musí schválit zastupitelstvo, aby byla závazná také pro členy zastupitelstva.

1.3. Touto směrnicí obec Velehrad (dále jen „obec") stanovuje vnitřní pravidla pro zajištění ochrany osobních údajů a plnění povinností podle Obecného nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů jakožto přímo účinného předpisu EU (dále jen „Obecné nařízení") a podle zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon"), zejména při zpracování osobních údajů vykonávaných obcí, zejména jejím obecním úřadem (dále jen „OÚ") a knihovnou zřízenou obcí[1].

1.4. Ustanovení této směrnice jsou závazná pro všechny osoby v rámci obce, zejména pro zaměstnance obce (dále jen „zaměstnanci"). Obdobně jako pro zaměstnance je tato směrnice závazná i pro členy orgánů obce, jako jsou členové zastupitelstva, komisí a výborů (dále jen „členové orgánů"), pokud se v souvislosti s výkonem své funkce seznamují, případně zpracovávají osobní údaje. Dále je závazná pro osoby, které mají s obcí jiný právní vztah (smlouva o dílo, nájemní smlouva) a které se zavázaly postupovat podle této směrnice, především pokud se při své činnosti seznamují, případně zpracovávají osobní údaje obce jako správce údajů.

1.5. Jakékoliv smlouvy, podle kterých osobní údaje zpracovávají anebo se s nimi seznamují při plnění smlouvy uzavřené s obcí další osoby, (dále jen "zpracovatelé a další smluvní osoby"), musejí být písemné (včetně elektronické formy). Pokud smluvní vztah (např. standardní smluvní dokumenty dodavatele) neobsahuje závazek k ochraně osobních údajů alespoň v rozsahu, upraveném touto směrnicí, musí obsahovat závazek k dodržování této směrnice, konkretizaci povinností podle směrnice a potvrzení, že smluvní strana se se směrnicí seznámila.

1.6. Pokud pro obec zajišťuje zpracování osobních údajů v rámci plnění smluvních povinností jiný subjekt (zpracovatel), pak musí být v rámci smluvních vztahů zaručeno plnění povinností podle Obecného nařízení a podle této směrnice a musí být upravena odpovědnost za tyto činnosti vůči správci a vůči kontrolním orgánům. Náležitosti smlouvy o zpracování osobních údajů upravuje Obecné nařízení.

Základní pojmy ochrany osobních údajů stanovuje Obecné nařízení a zákon. V souladu s tím je

1.7. **osobním údajem** jakákoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby (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;

1.8. **citlivým osobním údajem** osobní údaj vypovídající 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. Osobní údaje týkající se rozsudků v trestních věcech a trestných činů se pro účel této směrnice hodnotí obdobně jako citlivé osobní údaje.

[1] Pro situaci, kdy knihovna je organizační složkou obce, tedy její pracovníci jsou zaměstnanci obce.

1.9. **zpracováním osobních údajů** 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; za zpracování osobních údajů se nepovažuje pořízení a použití jednotlivých fotografií nebo časově omezeného obrazového záznamu (schůze, kulturní, společenské, sportovní akce), aniž se vytváří evidence a nejsou kromě běžné identifikace jménem a příjmením systematicky přiřazovány další osobní údaje,

1.10. **subjektem údajů** fyzická osoba, k níž se osobní údaje vztahují,

1.11. **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.

1.12. **likvidací osobních údajů** fyzické zničení jejich nosiče nebo jejich fyzické vymazání. K fyzickému vymazaní nepostačuje vymazat data ze souboru nebo soubor z adresáře.

1.13. Způsob zpracování osobních údajů a pověřené osoby

1.13.1. Osobní údaje lze zpracovávat pouze za podmínek stanovených Obecným nařízením, případně zvláštními zákony, přičemž je nezbytné dodržovat ustanovení této směrnice. Zpracovávat lze pouze osobní údaje získané zákonným způsobem.

1.13.2. Zpracovávat osobní údaje a seznamovat se s nimi mohou v rozsahu podle následujících ustanovení pouze pověřené osoby, kterými jsou:

1.13.2.1. zaměstnanec, který v souladu se svým pracovním zařazením vykonává agendu, jejíž nezbytnou součástí je zpracování osobních údajů,

1.13.2.2. člen orgánu, pokud je to nezbytné pro výkon jeho funkce,

1.13.2.3. osoby, které k tomu mají oprávnění na základě uzavřené smlouvy.

1.14. Účel zpracování, zákonnost a nově zaváděné účely zpracování[2]

1.14.1. Veškerá zpracování osobních údajů probíhají v rámci jednotlivých agend, tzv. „účelech zpracování". Ten, kdo rozhoduje o činnosti zpracování (dále „odpovědný zaměstnanec (garant)"), pro každé zpracování (agendu, evidenci) stanoví účel zpracování, tedy jeho výstižný a konkrétně vymezující popis v rozsahu několika slov. O účelu drobných zpracování (tj. zpracování s nízkým rizikem[3], např. pomocné a dočasné evidence občanů, zaměstnanců, dodavatelů apod., bez citlivých osobních údajů) rozhoduje osoba, do jejíž kompetence spadá úkol, který zpracování osobních údajů vyžaduje. V případě, kdy lze předpokládat, že účel zpracování zasahuje subjekty osobních údajů ve velkém rozsahu, je povinna předložit stanovení účelu k rozhodnutí svému starostovi, tajemníkovi obce, případně svému nadřízenému.

1.14.2. Právní titul či tituly[4] každého účelu zpracování určí odpovědný zaměstnanec (garant). V případě, kdy agenda obsahuje také citlivé osobní údaje, určí zároveň právní titul pro citlivé údaje. K obojímu určí také právní základ, je-li potřebný.

- plnění právní povinnosti;
- plnění úkolu ve veřejném zájmu;
- plnění smlouvy;

[2] Čl. 5 odst. 1 písm. a) a b) Obecného nařízení

[3] Čl. 33 odst. 1 ON, případy, kdy není pravděpodobné, že by porušení zabezpečení mělo za následek riziko pro práva a svobody fyzických osob

[4] Právním titulem je některé ustanovení čl. 6 odst. 1 písm. a) až f), čl. 9/2 písm. a) až j) , čl. 10 Obecného nařízení

- oprávněný zájem správce;
- výjimečně též souhlas subjektu údajů.

1.14.3. Při potřebě nového zpracování osobních údajů ten, kdo navrhuje jeho účel, posoudí oprávněnost účelu a navrhne nezbytný rozsahu údajů pro dané zpracování, dobu a způsob uchování a způsob informování subjektů údajů.

1.14.4. Ke stanovení účelu zpracování, určení právního titulu a případně právního základu si odpovědný zaměstnanec (garant) vyžádá posouzení pověřencem.

1.14.5. O každém nově zamýšleném účelu zpracování, vyjma drobných zpracování, jak jsou uvedena v bodu 4.2.1, je ten, kdo navrhuje jeho účel, povinen informovat pověřence, a to před jakýmkoliv krokem. Zahájit novou činnost zpracování lze jen na základě doložitelného posouzení pověřencem.

1.14.6. Pověřené osoby jsou povinny zpracovávat osobní údaje pouze ke stanovenému účelu, v rozsahu pracovní náplně a úkolů, které jim byly stanoveny jejich nadřízenými anebo vyplývajícím z jejich funkce, a na místech k tomu určených. Jsou povinny dodržovat základní zásady při zpracování osobních údajů.

1.14.7. Ustanovení tohoto článku se při výkonu jeho funkce přiměřeně vztahuje i na člena školské rady, který spolupracuje s odpovědným zaměstnancem (garant) a pověřencem, a to za podmínky, že není zaměstnancem.

1.15. Zásady zpracování osobních údajů

Pověřené osoby jsou povinny dodržovat tyto základní zásady při zpracování osobních údajů:

1.15.1. zpracovávat osobní údaje korektním a transparentním způsobem;

1.15.2. před zavedením každého zpracování osobních údajů stanovit účel, právní titul a případně právní základ či oprávněné důvody správce pro toto zpracování;

1.15.3. zpracovávat osobní údaje pouze v nezbytném rozsahu a po dobu nezbytnou k danému účelu, včetně archivace v případech stanovených skartačním plánem, poté je likvidovat;

1.15.4. zpracovávat osobní údaje přesně a podle potřeby je aktualizovat; přesnost údajů je zajištěna: ověřováním údajů poskytnutých subjektem, například porovnáním s osobními doklady, doklady o vzdělání; pravidelnými opakovanými kontrolami; aktivním dotazováním;

1.15.5. zajišťovat náležité zabezpečení osobních údajů (viz bod 8).

1.16. Záznamy o zpracování a kontrolní seznam

1.16.1. Každý odpovědný zaměstnanec (garant) vede v excelové tabulce jímž byla provedena implementace Obecného nařízení (dále jen „Komplexní kontrolní záznamy"):

1.16.1.1. záznamy o příslušných účelech zpracování (dále jen „záznam o zpracování")[5];

1.16.1.2. záznamy o provedených opatřeních k dosažení souladu s Obecným nařízením jako je likvidace či výmaz dat, lhůty pro likvidaci, forma a lhůty zálohování, šifrování přenosných médií;

1.16.1.3. záznamy o bezpečnostních incidentech jako je únik, ztráta, neoprávněný přenos či zveřejnění;

1.16.1.4. další údaje potřebné k vyhodnocení a doložení souladu s Obecným nařízením a k informování subjektů údajů.

1.16.2. Ke komplexním kontrolním záznamům mají přístup odpovědní zaměstnanci (garanti) a pověřenec. O změnách v komplexních kontrolních záznamech musejí odpovědní zaměstnanci (garanti) vždy informovat pověřence, např. sdílením aktualizované verze.

1.16.3. Starosta nebo jím určená osoba zajistí pravidelné zálohování komplexních kontrolních záznamů a případných souvisejících dokladů.

[5] Čl. 30 Obecného nařízení

1.17. Každá pověřená osoba, pokud to plyne z náplně její práce, dbá na uchování dokladů, opravňujících určité zpracování osobních údajů, jako jsou

1.17.1. smlouvy, pro jejichž plnění se zpracovávají osobní údaje;

1.17.2. doklady o informování subjektů údajů v případech, kdy nepostačuje zveřejnění na webu;

1.17.3. doklady o vyřízení žádostí subjektů údajů;

1.17.4. souhlasy se zpracováním osobních údajů;

1.17.5. balanční testy v případě zpracování na základě právního titulu oprávněného zájmu správce nebo třetí osoby;

1.17.6. evidence klíčů, je-li potřebná;

1.17.7. evidence přístupů do počítačů a přístupových práv v informačním systému, je-li potřebná;

1.17.8. údaje o zpřístupnění záznamu kamerového systému či dalších specifických záznamů osobních údajů;

1.17.9. další obdobné doklady.

1.18. Tyto doklady vede odpovědný zaměstnanec (garant) v kontrolním seznamu, pokud to jejich povaha umožňuje, jinak se v komplexním kontrolním záznamu pouze uvede, kde jsou uloženy.

1.19. Informování subjektů údajů[6]

1.19.1. Odpovědný zaměstnanec (garant) zajistí informování subjektů údajů, jejichž údaje obec zpracovává, zejména na webu obce, případně při uzavření smlouvy nebo získání souhlasu se zpracováním. Zajistí též stručný, transparentní, srozumitelný a snadno přístupný způsob těchto sdělení[7].

1.19.2. Odpovědný zaměstnanec (garant) zajistí také doložitelnost uvedeného informování. Může v rámci své kompetence tento úkol uložit jinému zaměstnanci.

1.20. Přístup k osobním údajům[8]

1.20.1. Požadavky subjektů údajů vyřizuje odpovědný zaměstnanec (garant), který může v rámci své kompetence tento úkol uložit jinému zaměstnanci. Pro vyřízení se přiměřeně postupuje podle obecného předpisu pro přístup k informacím (zákon č. 106/1999 Sb.), neuplatní se správní řád.

1.20.2. Požádá-li subjekt údajů o sdělení svých osobních údajů, ověří se totožnost žadatele a potvrdí na žádosti, případně se ověření totožnosti k žádosti přiloží, např. číslo průkazu, podle kterého byla ověřena, ověření uznávaného elektronického podpisu, datové schránky (dále jen „ověření totožnosti").

1.20.3. Běžné provozní dotazy týkající se osobních údajů (zejm. informace o zpracování osobních údajů), vyřídí zaměstnanec podle okolností co nejdříve.

1.20.4. K vyřízení ostatních žádostí o přístup k osobním údajům (zejm. export údajů) je příslušný odpovědný zaměstnanec (garant). Žádost se vyřídí do 30 dnů.

Odesílané informace obsahují pouze odpovědi na kladené dotazy, jen v nezbytném rozsahu, uvádějí se pouze oficiálně zpracovávané informace (nikoli neoficiální, byť známé, např. o rodinném zázemí). Jakýkoli odesílaný text musí být schválen vedením obce či odeslán přímo vedením obce (například z oficiálního e-mailu obce).

1.20.5. V případě potřeby a s ohledem na složitost a počet žádostí může odpovědný zaměstnanec (garant) prodloužit lhůtu vyřízení žádosti o další dva měsíce, přičemž o tom informuje subjekt údajů do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

1.20.6. Jestliže subjekt údajů podává žádost v elektronické formě a je-li to možné, poskytnou se informace v elektronické formě, pokud subjekt údajů nepožádá o jiný způsob.

---

[6] Čl. 13 a 14 Obecného nařízení

[7] Čl. 12 Obecného nařízení

[8] Čl. 15 Obecného nařízení

1.21. Právo na výmaz, opravu a doplnění

1.21.1. Pověřené osoby jsou povinny dbát na správnost zpracovávaných osobních údajů.

1.21.2. Subjekt údajů má právo žádat výmaz, opravu a doplnění osobních údajů, které se ho týkají.[9] Případy, kdy je požadavek na výmaz oprávněný, stanoví čl. 17 odst. 1 a 3 Obecného nařízení. Žádost vyřídí odpovědný zaměstnanec (garant) po ověření totožnosti a po prověření oprávněnosti požadavku ihned, jakmile je to možné, nejdéle do 30 dnů; čl. 6.2.5. Směrnice se použije obdobně. Pokud má ověření oprávněnosti požadavku trvat delší dobu, zejména by se osobní údaje dotčené žádostí měly zpracovávat ke stanovenému účelu zpracování (např. zaslat pravidelné vyúčtování s chybným údajem), zajistí jejich vyřazení ze zpracování [10] a informuje o tom žadatele. Ve složitých případech si vyžádá posouzení pověřencem.

1.21.3. Oznámí-li subjekt údajů (např. telefonicky nebo e-mailem), že osobní údaje, které se ho týkají, se změnily, a nelze dostatečně ověřit jeho totožnost s ohledem na závažnost požadované změny (např. na základě znalosti e-mailové adresy), vyzve ho odpovědný zaměstnanec (garant) k postupu, jenž umožní totožnost ověřit.

1.21.4. Zjistí-li pověřená osoba při své činnosti, že při zpracování osobních údajů došlo ke zjevné chybě v psaní (např. překlepu), informuje odpovědného zaměstnance (garanta) a údaj opraví.

1.22. Pro obec zajišťuje pověřence společnost SMS-služby s.r.o. prostřednictvím svého zaměstnance, který je hlavní odpovědnou osobou ve vztahu ke škole pro výkon úkolů pověřence.

1.23. Starosta zajistí zveřejnění kontaktních údajů pověřence a Úřadu pro ochranu osobních údajů je sdělí včetně jeho identifikace.

1.24. Všechny pověřené osoby jsou povinny [11]:

1.24.1. konzultovat s pověřencem všechny záležitosti, související s ochranou osobních údajů, pokud si nejsou zcela jisty jejich prováděním v souladu s Obecným nařízením;

1.24.2. poskytnout pověřenci součinnost při plnění jeho úkolů, zejména mu umožnit plný přístup k osobním údajům a k operacím zpracování;

1.24.3. zdržet se jakéhokoli jednání, které by mohlo ohrozit nezávislé posouzení věci pověřencem;

1.24.4. neukládat pověřenci úkoly, které by vedly k jeho střetu zájmů.

1.25. V případě řešení otázek o zpracování osobních údajů se zaměstnanci, fyzickými a dalšími osobami, jejichž osobní údaje obec zpracovává, obrací na pověřence s žádostí o radu, týkající se jejich osobních údajů.

1.26. Povinnosti pověřence jsou stanoveny ve zvláštní smlouvě.

1.27. Obecné postupy při zabezpečení osobních údajů

1.27.1. Přiměřeně zabezpečeny musejí být zpracovávané osobní údaje i ty, které nejsou systematicky zpracovávané, například vyskytující se v jednotlivých nezařazených dopisech, sděleních, e-mailech.

1.27.2. Úroveň zabezpečení lze přiměřeně snížit u osobních údajů, u nichž je riziko pro subjekty údajů nepatrné nebo jsou běžně dostupné veřejnosti, zejména o zaměstnancích a členech orgánů, dalších osobách

1.27.2.1. na základě zákona o svobodném přístupu k informacím;

1.27.2.2. jsou veřejně dostupné (například ve veřejně přístupných registrech),

[9] Čl. 16, 17 Obecného nařízení

[10] „omezení zpracování"

[11] Čl. 38 Obecného nařízení

1.27.2.3. nepředstavují žádné riziko pro subjekty údajů, například malý počet nahodilých nevýznamných informací.

1.27.3. V pochybnostech je pověřená osoba vždy povinna konzultovat potřebu zabezpečení s nadřízeným nebo s pověřencem.

1.27.4. Osobní údaje musí být zabezpečeny před neoprávněným nebo nahodilým přístupem k nim, proti jejich změně, zničení či ztrátě (zejména dostatečné zálohování), neoprávněným a nezabezpečeným přenosům, proti jejich jinému neoprávněnému zpracování, jakož i proti jinému zneužití osobních údajů. Zabezpečení spočívá při nepřítomnosti pověřených osob zejména v uchovávání záznamových médií (písemných i elektronických), obsahujících osobní údaje, v uzamčených skříních, v uzamykání kanceláří a jiných míst.

1.27.5. Pověřené osoby jsou povinny dodržovat pravidla informační bezpečnosti, zejména nesmějí bez souhlasu správce informačního systému instalovat nedůvěryhodné programy (zejm. „zdarma"). Je zakázáno otevírat podezřelé odkazy nebo přílohy e-mailů. V případě nejasností je pověřená osoba povinna kontaktovat nadřízeného anebo správce informačního systému.

1.27.6. Dále jsou pověřené osoby povinny vyvarovat se jakéhokoliv jednání, které by mohlo být chápáno jako neoprávněné zveřejňování osobních údajů nebo vést k neoprávněnému přístupu třetích osob k osobním údajům. Zejména, ale nikoliv pouze:

1.27.6.1. sdělovat jakékoliv osobní údaje jiné osobě, než která je subjektem údajů nebo je jejím zákonným zástupcem;

1.27.6.2. hlasitě sdělovat osobní údaje ve veřejně přístupných prostorách úřadu;

1.27.6.3. umožnit nepovolaným osobám nahlížet do dokumentů s osobními údaji nebo na obrazovku monitoru, kde jsou takové údaje zobrazeny, nechávat třetí osoby samotné v kanceláři;

1.27.6.4. sdělovat komukoliv svá přístupová hesla do počítače, do informačních systémů a hesla k zašifrovaným souborům nebo zařízením, v případě jeho vyzrazení ihned zajistit jeho změnu.

1.28. Zabezpečení písemností a záznamových médií obsahujících osobní údaje

1.28.1. Písemnosti a digitální záznamová média, které obsahují osobní údaje, musí být mimo dobu, kdy jsou pod dohledem zaměstnanců, zabezpečeny v uzamčených skříních, popř. na jiných místech, zajišťujících jejich ochranu. To platí i pro kopie písemností a digitální zálohy, obsahující osobní údaje.

1.28.2. Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních v kanceláři, přístup k nim má pověřená osoba. Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu[12].

1.28.3. Likvidace osobních údajů se provádí podle spisového řádu a skartačního plánu obce. Pokud skartace určitého typu osobních údajů není skartačním plánem upravena, likvidují se po uplynutí doby nezbytné k danému účelu. Osobní údaje se likvidují zároveň v listinné i elektronické formě, pokud jejich účely zpracování nejsou odlišné.

Dokumenty uložené v elektronické podobě jsou zničeny fyzickou destrukcí nosičů, pokud jde o CD, DVD nebo použitím software zabezpečující vymazání.

1.28.4. Za plnění povinností stanovených ve výše uvedených odstavcích tohoto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění.

1.29. Zabezpečení dat obsahujících osobní údaje v osobních počítačích a na sítích

1.29.1. Data obsahující osobní údaje, která jsou uložena v osobních počítačích, musí být zabezpečena před volným přístupem neoprávněných osob, před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů. To platí i pro služební telefony, pokud obsahují osobní údaje zpracovávané v agendách obce podle článku 4.2.1. nebo k nim mají dálkový přístup.

[12] § 312 zákoníku práce

1.29.2. Počítače s přístupem k osobním údajům musejí mít alespoň zabezpečený přístup do počítače (přihlášení pod heslem) a nastaveno uzamčení obrazovky po době nečinnosti nejvýše 5 minut. Při odchodu z pracoviště (např. pauza na oběd) se oprávněná osoba odhlásí (např. klávesová zkratka Win+L).

1.29.3. Významné evidence osobních údajů (například mzdová, personální agenda, rozsáhlá evidence obyvatel s dalšími, zejména kontaktními údaji typu evidence svozu komunálního odpadu) musejí být zabezpečeny také zvláštním přístupem do programového vybavení anebo být jako soubor šifrované.

1.29.4. Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, uložiště souborů mobilního telefonu a podobně, musejí být, i když není určen k vynášení z objektu alespoň:

1.29.4.1. zajištěna šifrováním disku či jiného uložiště pomocí šifrovacího programu;

1.29.4.2. zajištěna zabezpečeným přístupem do programového vybavení, které data ukládá šifrovaně;

1.29.4.3. být jako soubor šifrované, nebo

1.29.4.4. je-li to dostatečné s ohledem na riziko pro subjekty osobních údajů, být dostatečně pseudonymizována.

1.29.5. Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, úložiště souborů mobilního telefonu a podobně, které jsou vynášeny mimo pracoviště, zaměstnanec:

1.29.5.1. nesmí tuto techniku předávat třetím osobám;

1.29.5.2. musí učinit všechna dostupná opatření, která mohou zabránit ztrátě či odcizení výpočetní techniky (neponechávat ji bez dohledu a/nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.);

1.29.5.3. nesmí používat výpočetní techniku pro práci s daty obce na veřejných místech;

1.29.5.4. musí ztrátu či odcizení okamžitě nahlásit svému nadřízenému.

1.29.6. Pokud přenosné médium sloužilo jen k přenosu, bezodkladně po přenosu bezpečně fyzicky vymazána podle článku 3.6.

1.29.7. Před vyřazením jakéhokoliv elektronického nosiče dat (likvidace, prodej, výpůjčka, darování) musí být nosič zkontrolován a všechny osobní údaje bezpečně fyzicky vymazány podle článku 3.6.

1.29.8. Pověřené osoby pravidelně posuzují úroveň zabezpečení informačních systémů včetně přenosu dat s ohledem na rizika pro subjekty osobních údajů, a v případě potřeby přijímají vhodná technická a organizační opatření, aby rizika zmírnily.[13]

1.29.9. Pověřené osoby zejména dbají na dostatečnou kvalitu hesel (nejméně 8 znaků, obsahuje minimálně 3 ze 4 položek: Velká písmena, malá písmena, čísla, symboly jako pomlčka či lomítko), pravidelné obměny hesel a je-li to možné vzhledem k nutné zastupitelnosti, důvěrnosti pouze pro jednoho uživatele. V případě potřeby ukládají hesla zabezpečeně a zcela odděleně od počítačů a médií, na nichž jsou použita.

1.29.10. Přenos souborů s osobními údaji nezabezpečenou sítí Internet (např. protokol http://) prostřednictvím běžné elektronické pošty a jejich uložení na nezabezpečených uložištích (běžné e-mailové schránky, přechodná úložiště jako Úschovna.cz) je přípustný jen v šifrované podobě minimálně v archivním souboru (např. ve formátu „zip", „rar", atd.) se zaheslováním souboru a předáním hesla příjemci jinou cestou, například SMS zprávou na ověřené číslo telefonu či pomocí jiné bezpečné aplikace. Šifrování však není nutné při předání datovou schránkou nebo zabezpečeným cloudem.

1.29.11. Umožňuje-li to programové vybavení, pověřené osoby (garanti) vždy využijí možnosti záznamu přístupů a činnosti (auditního záznamu, logu) na počítačích nebo v informačním systému. Záznamy pravidelně kontrolují. Tímto úkolem může být pověřen určený zaměstnanec.

1.29.12. Počítačová (kybernetická) bezpečnost v organizaci je zajištěna na všech počítačích organizace:

1.29.12.1. instalací antivirových programů;

[13] Čl. 32 Nařízení

1.29.12.2. stanovením přístupových práv, hesel, zákazu sdílení hesel několika osobami;

1.29.12.3. zajištěním automatických bezpečnostních aktualizací používaného software;

1.29.12.4. při jakékoliv likvidaci hardware musí být znemožněna možnost získání osobních údajů;

1.29.12.5. pravidelný servis výpočetní techniky je zaměřen i na kontrolu oblasti bezpečnosti dat;

1.29.12.6. je prováděno pravidelné testování přijatých technických a organizačních opatření;

1.29.12.7. pravidelným školením zaměstnanců;

1.29.12.8. vhodnou pracovní náplní metodika ICT (pokud v organizaci působí).

1.29.13. Za plnění povinností stanovených v článku 8.3.12. jsou odpovědny odpovědné osoby (garanti) podle rozsahu svých oprávnění.

1.29.14. Zaměstnanec pomáhá zajišťovat kybernetickou bezpečnost na počítačích tím, že

1.29.14.1. provádí pravidelné zálohování dat, tak aby nedošlo k jejich ztrátě při případném odcizení či poruše počítače a byla zajištěna schopnost obnovy dat v případě fyzických či technických incidentů, ledaže je to uloženo jiné pověřené osobě;

1.29.14.2. používá pouze silná hesla;

1.29.14.3. maže a neotvírá nevyžádanou poštu, odmazává SPAM v emailové schránce i v počítačích.

1.30. Vědomé porušení povinnosti mlčenlivosti, neoprávněné zveřejnění, sdělení, zpřístupnění a přisvojení osobních údajů zaměstnancem je porušení 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.

1.31. Zjistí-li kdokoliv, že došlo k fyzickému nebo elektronickému porušení zabezpečení osobních údajů, například úniku, ztrátě, zničení, neoprávněnému zveřejnění osobních údajů (dále jen „incident"), neprodleně o tom informuje pověřence, odpovědného zaměstnance (garanta), starostu a tajemníka.

1.32. Odpovědný zaměstnanec (garant), je-li to možné, bezodkladně zabrání dalšímu neoprávněnému nakládání, zejména zajistí znepřístupnění, dále vyhodnotí riziko pro práva a svobody fyzických osob, a konzultuje s pověřencem. Pokud ve shodě s pověřencem posoudí jako nepravděpodobné, že by incident měl za následek riziko pro práva a svobody fyzických osob (dále jen „nízké riziko"), provede o incidentu záznam k příslušnému účelu zpracování v komplexním kontrolním záznamu. Pokud vyhodnotí, že nejde jen o nízké riziko, ohlásí tuto skutečnost Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl některý odpovědný zaměstnanec[14] (garant).

1.33. Pokud je riziko pro práva a svobody fyzických osob vysoké, odpovědný zaměstnanec (garant) vhodným způsobem navíc informuje subjekty údajů.[15] Pokud v konzultaci s pověřencem však vyhodnotí, že již existuje či lze přijmout opatření, díky němuž se vysoké riziko pro subjekty údajů neprojeví, anebo by informování vyžadovalo nepřiměřené úsilí, pouze zveřejní informaci o incidentu na webu obce na výrazném místě.

1.34. Kontrola dodržování směrnice

1.34.1. Starosta, případně tajemník zajistí kontrolu plnění povinností vyplývajících z ustanovení Směrnice pro nakládání s osobními údaji.

1.34.2. Starosta, případně tajemník zajistí, aby byli s dokumentem Směrnice pro nakládání s osobními údaji seznámeni všechny pověřené osoby.

[14] Čl. 33 Obecného nařízení

[15] Čl. 34 Nařízení

1.35. Revize směrnice

1.35.1. Revize Směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky.

1.35.2. Za zpracování, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá starosta nebo jím pověřená osoba.

1.35.3. Revize směrnice se provádí na základě konzultace s pověřencem pro ochranu osobních údajů.

1.36. Účinnost směrnice

Směrnice pro nakládání s osobními údaji nabývá účinnosti a platnosti dnem vydání.

Velehrad, dne18.6.2021

PŘÍLOHA Č. 1: SLOVNÍČEK POJMŮ

- BALANČNÍ TEST – vyhodnocení oprávněného zájmu správce (obce) na zpracování osobních údajů subjektu údajů. Využívá se např. při instalaci kamerového systému ve škole na ochranu majetku. Provádí ho pověřenec, který poměřuje, zda zájem správce na zpracování převažuje nad právem ochrany osobních údajů subjektu údajů.
- ODPOVĚDNÝ ZAMĚSTNANEC (GARANT) – garant zpracování osobních údajů, určuje účel, právní titul a základ zpracování, pověřeným osobám stanovuje rozsah činností s osobními údaji (náplň práce); v případě obce, kde není tajemník vykonává činnost odpovědného zaměstnance starosta.
- POVĚŘENÁ OSOBA – každý, kdo na základě náplně práce pracuje s osobními údaji, zpravidla zaměstnanci, též členové školské rady nebo smluvní partneři.
- PSEUDONYMIZACE – skrytí identit. Například náhodné přiřazení číselného kódu, kde jeho přiřazení není možné dešifrovat bez dodatečných informací a přiřadit tak k určité osobě. Tímto způsobem je možné sbírat určitá data, bez potřeby znát totožnost jednotlivců. Užívá se také ke zvýšení zabezpečení údajů pro případ úniku.
- ZAMĚSTNANEC – každý zaměstnanec, ať se setkává či nesetkává s osobními údaji. Někteří zaměstnanci mají ve své náplni práce též nakládání s osobními údaji, ti pak jsou "pověřenými osobami". Někteří z pověřených zaměstnanců jsou odpovědní za určité zpracování – jsou jejich garanty.