

Směrnice
pro nakládání s osobními údaji pro obec



SMĚRNICE PRO NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI PRO OBEC

Směrnice

pro nakládání s osobními údaji pro obec

OBSAH

| | |
|----------------------------------------------------------------------------------------|-----------|
| 1. JAK SE SMĚRNICÍ NAKLÁDAT | 4 |
| 2. PŘEDMĚT SMĚRNICE A ZÁKLADNÍ USTANOVENÍ | 4 |
| 3. ZÁKLADNÍ POJMY | 5 |
| 4. OSOBNÍ ÚDAJE A JEJICH ZPRACOVÁNÍ..... | 7 |
| 4.1. Způsob zpracování osobních údajů a pověřené osoby | 7 |
| 4.2. Účel zpracování, zákonnost a nově zaváděné účely zpracování | 7 |
| 4.3. Zásady zpracování osobních údajů | 9 |
| 4.4. Záznamy o zpracování a kontrolní seznam | 10 |
| 5. DOKLADY SOULADU S OBECNÝM NAŘÍZENÍM | 10 |
| 6. PRÁVA SUBJEKTŮ ÚDAJŮ..... | 11 |
| 6.1. Informování subjektů údajů..... | 11 |
| 6.2. Přístup k osobním údajům..... | 11 |
| 6.3. Právo na výmaz, opravu a doplnění..... | 12 |
| 7. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ | 13 |
| 8. BEZPEČNOST INFORMACÍ | 14 |
| 8.1. Obecné postupy při zabezpečení osobních údajů | 14 |
| 8.2. Zabezpečení písemností a záznamových médií obsahujících osobní údaje..... | 15 |
| 8.3. Zabezpečení dat obsahujících osobní údaje v osobních počítačích a na sítích | 16 |
| 9. PORUŠENÍ ZABEZPEČENÍ A MÍRA JEHO RIZIKA..... | 19 |
| 10. ZÁVĚREČNÁ USTANOVENÍ..... | 20 |
| 10.1. Kontrola dodržování směrnice | 20 |
| 10.2. Revize směrnice..... | 20 |
| 10.3. Účinnost směrnice | 21 |
| PŘÍLOHA Č. 1: SLOVNÍČEK POJMŮ | 22 |

1. JAK SE SMĚRNICÍ NAKLÁDAT

Poznámky a příklady

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>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.</p> | <p>Směrnice se řadí mezi další interní směrnice obce. Levý sloupec obsahuje normativní text směrnice, pravý sloupec uvádí příklady, nebo podrobněji popisuje jednotlivá ustanovení směrnice.</p> |
| <p>1.2. Směrnici musí schválit zastupitelstvo, aby byla závazná také pro členy zastupitelstva.</p> | <p>Je doporučeno směrnici přijímat zastupitelstvem obce.</p> <p>Zaměstnanci obce, včetně zaměstnanců na dohody o provedení práce či pracovní činnosti se musí se směrnici prokazatelně seznámit.</p> |

2. PŘEDMĚT SMĚRNICE A ZÁKLADNÍ USTANOVENÍ

Poznámky a příklady

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>2.1. Touto směrnici obec (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 obcí¹.</p> | <p>Upozorňujeme, že dřívější zákon č. 101/2000 Sb., o ochraně osobních údajů byl zrušen. Pokud na něj máte ve svých formulářích odkaz, nahraďte ho odkazem na Obecné nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (GDPR) a na zákon č. 110/2019 Sb., o zpracování osobních údajů.</p> |
| <p>2.2. 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.</p> | <p>K zaměstnancům obce se řadí i zaměstnanci na dohody o provedení práce či pracovní činnosti.</p> <p>Mezi další osoby se řadí např. dodavatele služeb – pravidelný IT servis softwaru; školitel bezpečnosti a ochrany zdraví při práci; externí účetní a další.</p> |

Poznámky a příklady

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>2.3. 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.</p> | <p>KEO, Gordic, Triada, Galileo, Antee a další poskytovatelé softwaru a on-line služeb s cloudovými službami; externí účetní; poskytovatelé cloudových služeb a další.</p> |
| <p>2.4. 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.</p> | <p>KEO, Gordic, Triada, Galileo, Antee a další poskytovatelé softwaru a on-line služeb s cloudovými službami; externí účetní; poskytovatelé cloudových služeb a další.</p> <p>Smlouva o zpracování osobních údajů obsahuje zejména: popis povahy zpracování a jednotlivé činnosti zpracování; prohlášení zpracovatele o schopnosti dostát souladu s Obecným nařízením; závazek mlčenlivosti, a to i po ukončení smlouvy či pracovního vztahu; povinnost zpracovávat údaje pouze na pokyn správce; bez souhlasu správce nevyužívat služby jiného zpracovatele; popis zabezpečení osobních údajů při zpracování.</p> |

3. ZÁKLADNÍ POJMY

Poznámky a příklady

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <p>Základní pojmy ochrany osobních údajů stanovuje Obecné nařízení a zákon. V souladu s tím je</p> | |
| <p>3.1. 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;</p> | |

Poznámky a příklady

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>3.2. 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.</p> | <p>Členství v odborech; zdravotnická dokumentace při nástupu do zaměstnání; osobní údaje týkající se rozsudků v trestních věcech a trestných činů; údaje o národnosti; víře (někdy uvedené nadbytečně v životopise); otisk prstu, portrét použitý pro identifikaci osoby kamerou.</p> <p>Citlivým osobním údajem není rodné číslo, to však neznamená, že ho lze volně používat!</p> |
| <p>3.3. 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,</p> | <p>Zpracováním v praxi není vytváření a zveřejňování momentek z běžných činností v obci, video a fotografie z veřejné akce, fotografie vítězů. Předpokládá se pak umístění fotek na webu obce nebo v obecním a zpravodaji, někdy také na veřejně dostupné nástěnce.</p> <p>Pokud nejde o zpracování osobních údajů, nepodléhá práce s nimi pravidlům Obecného nařízení.</p> |
| <p>3.4. subjektem údajů fyzická osoba, k níž se osobní údaje vztahují,</p> | <p>Občan; zaměstnanec; podnikající fyzická osoba; smluvní partner.</p> |
| <p>3.5. 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.</p> | |
| <p>3.6. likvidací osobních údajů fyzické zničení jejich nosiče nebo jejich fyzické vymazání. K fyzickému vymazání nepostačuje vymazat data ze souboru nebo soubor z adresáře.</p> | <p>Skartování dokumentů včetně mazání dokumentů z počítače.</p> <p>Dokumenty uložené v elektronické podobě jsou fakticky zničeny: fyzickou destrukcí nosičů (pokud jde o CD, DVD); použitím software zabezpečující vymazání. V tomto případě nesmí jít o pouhé smazání dokumentů z adresáře, protože i poté by byla možná obnova smazaných souborů. Musí jít o opakované přepsání původních souborů novými údaji.</p> |

4. OSOBNÍ ÚDAJE A JEJICH ZPRACOVÁNÍ

Poznámky a příklady

| 4.1. Způsob zpracování osobních údajů a pověřené osoby | | |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.1.1. | 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. | Konkrétně se pak jedná o čl. 6 Obecného nařízení. Nezákonný způsob zpracování je např. uchovávání kopií rodných listů dětí zaměstnanců; kopírování občanských průkazů; využívání e-mailových adres k zasílání marketingových sdělení, pokud k tomu nebyl dán souhlas. |
| 4.1.2. | Zpracovávat osobní údaje a seznamovat se s nimi mohou v rozsahu podle následujících ustanovení pouze pověřené osoby, kterými jsou: | |
| 4.1.2.1. | zaměstnanec, který v souladu se svým pracovním zařazením vykonává agendu, jejíž nezbytnou součástí je zpracování osobních údajů, | Účetní; mzdová účetní; referent; vedoucí odboru; asistent; knihovnik; pokladní atd. |
| 4.1.2.2. | člen orgánu, pokud je to nezbytné pro výkon jeho funkce, | Zastupitelé, členové komisí a výborů. |
| 4.1.2.3. | osoby, které k tomu mají oprávnění na základě uzavřené smlouvy. | Jedná se o zpracovatele (viz bod 2.3) - např. externí účetní; IT; poskytovatel cloudového úložiště a další. |
| 4.2. Účel zpracování, zákonnost a nově zaváděné účely zpracování ² | | |
| 4.2.1. | 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. | Účelem je často název agendy – mzdová a personální agenda; místní poplatky, nájemní a kupní smlouvy; vidimace a legalizace a další. |
| 4.2.2. | 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. | Citlivé osobní údaje viz bod 3.2 - např. složka opatrovance. |

Poznámky a příklady

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ■ plnění právní povinnosti; | Agendy, jednoznačně vyplývající ze zákona – evidence obyvatel; personální a mzdová agenda; osobní spisy zaměstnanců podle zákoníku práce; dokumentace v oblasti BOZP; vedení účetnictví; spisová služba; evidence projektů a další. |
| ■ plnění úkolu ve veřejném zájmu; | Agendy, které nejsou v zákoně jednoznačně uloženy, ale vyplývají z obecných úkolů, stanovených zákonem nebo jiným obecně závazným předpisem. Jedná se např. o vedení pomocných evidencí k místním poplatkům apod. |
| ■ plnění smlouvy; | Osobní údaje nutné k uzavření pracovní smlouvy; osobní údaje nájemců obecních prostor apod. |
| ■ oprávněný zájem správce; | Nainstalovaná kamera pouze za účelem ochrany majetku, např. na zadní, nepoužívaný vchod do budovy. |
| ■ výjimečně též souhlas subjektu údajů. | <p>Pokud je pro zpracování osobních údajů nezbytný souhlas (např. uvedení datumu narození jubilanta) pak musí být informovaný, konkrétní a písemný (viz bod 4.5.3). Zpracování osobních údajů je možné provádět až po získání souhlasu. Písemná podoba souhlasu se uchovává po celou dobu zpracování údajů.</p> <p>V praxi se jedná o zveřejnění významného výročí jubilanta, u které se uvede nejen jméno a příjmení, ale i datum narození, případně č. p. domu, ve kterém žije.</p> |
| 4.2.3. Při potřebě nového zpracování osobních údajů ten, kdo navrhuje jeho účel, posoudí oprávněnost účelu a navrhne nezbytný rozsah údajů pro dané zpracování, dobu a způsob uchování a způsob informování subjektů údajů. | Obec začne poskytovat pronájem tělocvičny a k tomu účelu zřídí evidenci pravidelných nájemců. |
| 4.2.4. Ke stanovení účelu zpracování, určení právního titulu a případně právního základu si odpovědný zaměstnanec (garant) vyžádá posouzení pověřencem. | |
| 4.2.5. 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. | Tato povinnost jednoznačně vyplývá z čl. 38 odst. 1 Obecného nařízení. |

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>4.2.6. Pověřené osoby jsou povinny zpracovávat osobní údaje pouze ke stanovenému účelu, v rozsahu pracovní náplně a úkolů, které jim byly stanoveny jejich nadřízenými anebo vyplývajícími z jejich funkce, a na místech k tomu určených. Jsou povinny dodržovat základní zásady při zpracování osobních údajů.</p> | <p>Např. mzdová účetní má přístup pouze k personalistice a podkladům pro mzdy; pouze vybraný úředník má přístup k evidenci obyvatel apod. Náplně práce zaměstnanců by měly mít co nejpřesněji formulovány jednotlivé činnosti zaměstnanců.</p> |
| <p>4.2.7. 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.</p> | |
| <p>4.3. Zásady zpracování osobních údajů</p> | |
| <p>Pověřené osoby jsou povinny dodržovat tyto základní zásady při zpracování osobních údajů:</p> | |
| <p>4.3.1. zpracovávat osobní údaje korektním a transparentním způsobem;</p> | <p>Na webu jsou zveřejněny informace o zpracování, s podrobnými informacemi o jednotlivých agendách. Každý správce má toto v části „Informace o zpracování osobních údajů“, často (nesprávně) záložka „GDPR“⁵.</p> |
| <p>4.3.2. před zavedením každého zpracování osobních údajů stanovit účel, právní titul a případně právní základ či oprávněné důvody správce pro toto zpracování;</p> | <p>Uvedeno v komplexních kontrolních záznamech, které pomáhal vytvořit pověřenec (excel tabulka), viz bod 4.4.</p> |
| <p>4.3.3. zpracovávat osobní údaje pouze v nezbytném rozsahu a po dobu nezbytnou k danému účelu, včetně archivace v případech stanovených skartačním plánem, poté je likvidovat;</p> | <p>Jako příklad lze uvést výběrové řízení na nové zaměstnance: Po uchazečích jsou vyžadovány pouze údaje nezbytné pro posouzení vhodnosti uchazečů v rámci výběrového řízení. Další rozšiřující informace jsou požadovány až po případném rozhodnutí o uzavření pracovního vztahu. Osobní údaje neúspěšných uchazečů jsou skartovány a vymazány. V případě, že jsou uchovány pro využití při dalším výběrovém řízení, je subjekt údajů požádán o souhlas.</p> <p>Obec má aktualizovaný a platný spisový řád a skartační plán.</p> |
| <p>4.3.4. 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;</p> | <p>Zaměstnancům je v rámci školení připomínána jejich zákonná povinnost informovat zaměstnavatele o změnách v jejich osobních údajích a také jejich právo nahlížet do svého osobního spisu.</p> <p>Zaměstnanci jsou při získávání údajů od občanů a případně i jiných osob povinni používat výhradně obcí schválené formuláře, dotazníky a jiné texty.</p> |

Poznámky a příklady

| | |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.3.5. zajišťovat náležitě zabezpečení osobních údajů (viz bod 8). | Využití alespoň free antivirového programu; silná hesla; zamčené kanceláře či skříně; vymezené přístupy; organizační řád; aktualizované náplně práce zaměstnanců. |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|

4.4. Záznamy o zpracování a kontrolní seznam

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.4.1. Každý odpovědný zaměstnanec (garant) vede v excelové tabulce jímž byla provedena implementace Obecného nařízení (dále jen „Komplexní kontrolní záznamy“): | Vedeno ve spolupráci s pověřencem, který pravidelně aktualizuje záznamy zpracování i komplexní kontrolní záznamy (excel tabulku). |
| 4.4.1.1. záznamy o příslušných účelech zpracování (dále jen „záznam o zpracování“); | Stručný výtah z excelové tabulky, tj. z komplexních kontrolních záznamů – dvanáct povinných údajů ke každé agendě |
| 4.4.1.2. 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; | Každý výmaz, oprava či vyřízení požadavku subjektu údajů je vhodné poznamenat do komplexních kontrolních záznamů (excel. tabulka) k příslušné agendě do poznámek. |
| 4.4.1.3. záznamy o bezpečnostních incidentech jako je únik, ztráta, neoprávněný přenos či zveřejnění; | Každý bezpečnostní incident je nutno poznamenat do komplexních kontrolních záznamů (excelová tabulka) k příslušné agendě dole do poznámek, a to i tehdy, když se nehlásil Úřadu. |
| 4.4.1.4. další údaje potřebné k vyhodnocení a doložení souladu s Obecným nařízením a k informování subjektů údajů. | Do komplexních kontrolních záznamů (excelová tabulka) k příslušné agendě dole do poznámek je vhodné poznamenat i další aspekty, například o důvodu určitého postupu, aby bylo možné jej doložit. |
| 4.4.2. 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. | Starosta, účetní – obvykle osoba určená ke komunikaci s pověřencem. |
| 4.4.3. Starosta nebo jím určená osoba zajistí pravidelné zálohování komplexních kontrolních záznamů a případných souvisejících dokladů. | Lze požádat i pověřence. |

5. DOKLADY SOULADU S OBECNÝM NAŘÍZENÍM

Poznámky a příklady

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 5.1. Každá pověřená osoba, pokud to plyne z náplně její práce, dbá na uchování dokladů, opravňujících určité zpracování osobních údajů, jako jsou | |
| 5.1.1. smlouvy, pro jejichž plnění se zpracovávají osobní údaje; | |

Poznámky a příklady

| | | |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.1.2. | doklady o informování subjektů údajů v případech, kdy nepostačuje zveřejnění na webu; | V praxi se jedná např. o zpracování osobních údajů pro plnění smlouvy, nebo o zpracování osobních údajů na základě souhlasu. |
| 5.1.3. | doklady o vyřízení žádostí subjektů údajů; | |
| 5.1.4. | souhlasy se zpracováním osobních údajů; | |
| 5.1.5. | balanční testy v případě zpracování na základě právního titulu oprávněného zájmu správce nebo třetí osoby; | V praxi při instalaci kamer se záznamem, nebo při instalaci zařízení při vstupu pomocí čipu. (<i>Upozorňujeme, že vstupní systémy fungující na principu biometrických údajů, např. otisk prstu nejsou přípustné!</i>) |
| 5.1.6. | evidence klíčů, je-li potřebná; | |
| 5.1.7. | evidence přístupů do počítačů a přístupových práv v informačním systému, je-li potřebná; | |
| 5.1.8. | údaje o zpřístupnění záznamu kamerového systému či dalších specifických záznamů osobních údajů; | |
| 5.1.9. | další obdobné doklady. | |
| 5.2. | 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. | |

6. PRÁVA SUBJEKTŮ ÚDAJŮ

Poznámky a příklady

| | | |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 6.1. Informování subjektů údajů⁷ | | |
| 6.1.1. | 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 ⁸ . | Informace o zpracování na webu obce (výťah z komplexních kontrolních záznamů – excelové tabulky). |
| 6.1.2. | Odpovědný zaměstnanec (garant) zajistí také důležitost uvedeného informování. Může v rámci své kompetence tento úkol uložit jinému zaměstnanci. | Informování probíhá nejčastěji v písemné podobě. |
| 6.2. Přístup k osobním údajům⁹ | | |
| 6.2.1. | 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. | Využití dokumentu <i>“Postupy správce při splnění požadavků, plynoucích z práv subjektů údajů. Manuál pro obce”</i> . |

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>6.2.2. 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“).</p> | <p>Žádost může subjekt údajů podat jakkoliv, včetně obyčejného e-mailu. Podle způsobu podání se následně přistoupí k potřebnému ověření totožnosti (ve formě výzvy).</p> |
| <p>6.2.3. Běžné provozní dotazy týkající se osobních údajů (zejm. informace o zpracování osobních údajů), vyřídí zaměstnanec podle okolností co nejdříve.</p> | |
| <p>6.2.4. 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).</p> | <p>Zpravidla jsou informace poskytovány 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 o poskytování informací podle zákona č. 106/1999 Sb. o svobodném přístupu k informacím.</p> <p>Lhůta začíná běžet až od okamžiku, kdy – pokud to bylo nutné – žadatel vyhověl výzvě k ověření totožnosti nebo doplnil upřesnění žádosti.</p> |
| <p>6.2.5. 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.</p> | |
| <p>6.2.6. 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.</p> | |
| <p>6.3. Právo na výmaz, opravu a doplnění</p> | |
| <p>6.3.1. Pověřené osoby jsou povinny dbát na správnost zpracovávaných osobních údajů.</p> | |

Poznámky a příklady

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>6.3.2. Subjekt údajů má právo žádat výmaz, opravu a doplnění osobních údajů, které se ho týkají.¹⁰ 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 zpracování¹¹ a informuje o tom žadatele. Ve složitých případech si vyžádá posouzení pověřencem.</p> | <p>Podle čl. 17 Obecného nařízení má subjekt údajů právo na výmaz údajů, pokud již údaje 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 nelze ho provést u zpracování osobních údajů na základě právní povinnosti (pokud je dodržena skartační lhůta).</p> <p>Subjekt údajů má právo na opravu údajů, pokud jsou nepřesné nebo neúplné. Na provedení opravy má obec nejdéle jeden měsíc, případně na vysvětlení, pokud oprava nebyla provedena.</p> |
| <p>6.3.3. 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.</p> | <p>Změna údajů o zaměstnanci, smluvním partnerovi, občanovi – změna příjmení; trvalé adresy apod.</p> |
| <p>6.3.4. 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.</p> | <p>Chyba, která má za následek, že subjekt osobních údajů může být zaměnitelný s jinou osobou. Chyba se stane v přepisu rodného čísla apod.</p> |

7. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

Poznámky a příklady

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>7.1. Pro obec zajišťuje pověřence společnost SMS-slужby s.r.o. prostřednictvím svého zaměstnance, který je hlavní odpovědnou osobou ve vztahu k obci pro výkon úkolů pověřence.</p> | |
| <p>7.2. Starosta zajistí zveřejnění kontaktních údajů pověřence a Úřadu pro ochranu osobních údajů je sdělí včetně jeho identifikace.</p> | <p>Informace o pověřenci musí být na webových stránkách obce – stačí e-mail a telefon, není nutné jméno a příjmení (je doporučované). Informace by měly být jednoduše dostupné, max. na 1–2 kliky. Část s informacemi o zpracování osobních údajů a s informacemi o pověřenci doporučujeme nazvat jako “Informace o zpracování osobních údajů”, viz bod 4.3.1.</p> |
| <p>7.3. Všechny pověřené osoby jsou povinny¹²:</p> | |

Poznámky a příklady

| | | |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.3.1. | konzultovat s pověřencem všechny záležitosti, související s ochranou osobních údajů, pokud si nejsou zcela jisty jejich prováděním v souladu s Obecným nařízením; | Zejména jakékoliv rozhodnutí vytvořit nové zpracování osobních údajů (novou agendu); použít na zpracování nové technické prostředky apod. |
| 7.3.2. | poskytnout pověřenci součinnost při plnění jeho úkolů, zejména mu umožnit plný přístup k osobním údajům a k operacím zpracování; | |
| 7.3.3. | zdržet se jakéhokoli jednání, které by mohlo ohrozit nezávislé posouzení věci pověřencem; | |
| 7.3.4. | neukládat pověřenci úkoly, které by vedly k jeho střetu zájmů. | Například aby pro ně sám udělal ty činnosti, u kterých by zároveň měl nezávisle posuzovat jejich soulad s Obecným nařízením. Pověřenec může toliko poskytnout doporučení. |
| 7.4. | 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. | |
| 7.5. | Povinnosti pověřence jsou stanoveny ve zvláštní smlouvě. | |

8. BEZPEČNOST INFORMACÍ

Poznámky a příklady

| | | |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.1. Obecné postupy při zabezpečení osobních údajů | | |
| 8.1.1. | Přiměřeně zabezpečeny musejí být zpracováváné osobní údaje i ty, které nejsou systematicky zpracováváné, například vyskytující se v jednotlivých nezařazených dopisech, sděleních, e-mailech. | E-maily v e-mailové schránce; využití silných hesel; uspávání počítače po určité době neaktivity; šanonny v uzavřených skříních; přehled o přístupech a klíčích do jednotlivých kanceláří apod. |
| 8.1.2. | 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 | |
| 8.1.2.1. | na základě zákona o svobodném přístupu k informacím; | |
| 8.1.2.2. | jsou veřejně dostupné (například ve veřejně přístupných registrech), | IČ; adresy firem; jména jednatelů; registr ekonomických subjektů; katastr nemovitostí; evidence využití půdy LPIS; seznam zastupitelů. |
| 8.1.2.3. | nepředstavují žádné riziko pro subjekty údajů, například malý počet nahodilých nevýznamných informací. | např. zaslání e-mailu členům zastupitelstva s kontakty na zpracovatele územního plánu |
| 8.1.3. | V pochybnostech je pověřená osoba vždy povinna konzultovat potřebu zabezpečení s nadřízeným nebo s pověřencem. | |

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.1.4. 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.</p> | <p>Uzamčení zálohy, případně právní ošetření cloudu; zabezpečení el. zařízení (počítač, externí disk, flash disk atd.), antivirové programy; zabezpečené přístupy; přístup omezeného počtu osob a další.</p> |
| <p>8.1.5. 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.</p> | |
| <p>8.1.6. 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:</p> | |
| <p>8.1.6.1. sdělovat jakékoliv osobní údaje jiné osobě, než která je subjektem údajů nebo je jejím zákonným zástupcem;</p> | <p>Telefonický požadavek na sdělení kontaktních údajů na občana.</p> |
| <p>8.1.6.2. hlasitě sdělovat osobní údaje ve veřejně přístupných prostorách úřadu;</p> | <p>Rozhovor zaměstnance úřadu o sociální situaci občana v místnosti OÚ, kde je rozhovor v doslechu jiných (neoprávněných) osob.</p> |
| <p>8.1.6.3. umožnit nepovolaným osobám nahlížet do dokumentů s osobními údaji nebo na obrazovku monitoru, kde jsou takové údaje zobrazeny, nechávat třetí osoby samotné v kanceláři;</p> | <p>Ponechat sestavu osobních údajů v dosahu cizích osob.</p> |
| <p>8.1.6.4. sdělovat komukoliv svá přístupová hesla do počítače, do informačních systémů a hesla k zašifrovaným souborům nebo zařízením, v případě jeho vyžádání ihned zajistit jeho změnu.</p> | <p>Vyvarovat se např. zaznamenání si hesel na zadní stranu kalendáře nebo na monitor počítače; nalepení si hesla přímo na stůl nebo na spodní stranu police nad stolem.</p> |
| <p>8.2. Zabezpečení písemností a záznamových médií obsahujících osobní údaje</p> | |

- | | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.2.1. 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.</p> | <p>Uzamčení zálohy dat, případně právní ošetření cloudu; zabezpečení el. zařízení (počítač, externí disk, flash disk atd.); antivirové programy; zabezpečené přístupy; přístup omezeného počtu osob a další.</p> |
| | <p>Záznamy obsahující citlivé osobní údaje (například o zdravotním stavu osob), jsou uloženy bezpečně v uzamčené skříni ke které mají přístup pouze oprávněné osoby. Je také zajištěno jejich předávání pouze oprávněným orgánům.</p> |
| <p>8.2.2. Osobní spisy zaměstnanců jsou uloženy v uzamčených skříních v kanceláři, přístup k nim má pověřená osoba. Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu¹³.</p> | <p>Pracovní smlouvy, dohody o provedení práce i dohody o pracovní činnosti a pracovní náplně všech zaměstnanců obsahují povinnosti zaměstnanců v oblasti GDPR. O zaměstnancích jsou shromažďovány pouze nezbytné údaje. Pokud jsou výjimečně pořizovány kopie dokumentů, kterými zaměstnanec dokládá určité skutečnosti (např. doklady o vzdělání), pak bez nadbytečných údajů. Pokud to není nezbytné, kopie dokumentů se nepořizují, údaje se jen ověří porovnáním s originálem (osobní doklady, rodné listy, rozsudky).</p> |
| <p>8.2.3. 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.</p> | <p>Nesmí jít o pouhé smazání dokumentů, protože i poté by byla možná obnova smazaných souborů, musí jít o opakovaně přepsání původních souborů novými údaji.</p> |
| <p>8.2.4. Za plnění povinností stanovených ve výše uvedených odstavcích tohoto článku jsou odpovědní pověřené osoby podle rozsahu svých oprávnění.</p> | <p>Hesla, většinou softwaru s přístupem pouze pro jednoho zaměstnance, pravidelné změny hesel, hesla do mobilů, Řešeno serverem a často přenosný disk – dávají do trezoru</p> |

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

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.3.1. 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.</p> | <p>Využití antivirových programů; silných hesel; heslování přístupu do externích disků; v případě notebooků šifrování disků; pravidelná obměna hesel. Prioritně využívání pracovních zařízení.</p> |
| <p>8.3.2. 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).</p> | <p>Každý má u svého počítače (mobilního telefonu) přihlašovací heslo, které je dostatečně silné. Počítač se uspává v případě delší neaktivity.</p> |
| <p>8.3.3. 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.</p> | |
| <p>8.3.4. Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, uložení souborů mobilního telefonu a podobně, musejí být, i když není určen k vynášení z objektu alespoň:</p> | |
| <p>8.3.4.1. zajištěna šifrováním disku či jiného uložení pomocí šifrovacího programu;</p> | |
| <p>8.3.4.2. zajištěna zabezpečeným přístupem do programového vybavení, které data ukládá šifrovaně;</p> | |
| <p>8.3.4.3. být jako soubor šifrované, nebo</p> | |
| <p>8.3.4.4. je-li to dostatečné s ohledem na riziko pro subjekty osobních údajů, být dostatečně pseudonymizována.</p> | |
| <p>8.3.5. Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, uložení souborů mobilního telefonu a podobně, které jsou vynášeny mimo pracoviště, zaměstnanec:</p> | |
| <p>8.3.5.1. nesmí tuto techniku předávat třetím osobám;</p> | |
| <p>8.3.5.2. 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.);</p> | |
| <p>8.3.5.3. nesmí používat výpočetní techniku pro práci s daty obce na veřejných místech;</p> | |

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.3.5.4. musí ztrátu či odcizení okamžitě nahlásit svému nadřízenému.</p> | |
| <p>8.3.6. Pokud přenosné médium sloužilo jen k přenosu, bezodkladně po přenosu bezpečně fyzicky vymazána podle článku 3.6.</p> | |
| <p>8.3.7. 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.</p> | |
| <p>8.3.8. 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.¹⁴</p> | |
| <p>8.3.9. 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.</p> | <p>Dobré je se vyvarovat např. jménům rodinných příslušníků a datům jejich narození. Nepřípustná jsou hesla jako 1234 nebo 77777.</p> |
| <p>8.3.10. Přenos souborů s osobními údaji nezabezpečenou sítí Internet (např. protokol http://) prostřednictvím běžné elektronické pošty a jejich uložení na nezabezpečených úložištích (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.</p> | |
| <p>8.3.11. 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.</p> | |
| <p>8.3.12. Počítačová (kybernetická) bezpečnost v organizaci je zajištěna na všech počítačích organizace:</p> | |
| <p>8.3.12.1. instalací antivirových programů;</p> | |
| <p>8.3.12.2. stanovením přístupových práv, hesel, záka- zu sdílení hesel několika osobami;</p> | |
| <p>8.3.12.3. zajištěním automatických bezpečnostních aktualizací používaného software;</p> | |
| <p>8.3.12.4. při jakékoliv likvidaci hardware musí být znemožněna možnost získání osobních údajů;</p> | |

| |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.3.12.5. pravidelný servis výpočetní techniky je zaměřen i na kontrolu oblasti bezpečnosti dat; |
| 8.3.12.6. je prováděno pravidelné testování přijatých technických a organizačních opatření; |
| 8.3.12.7. pravidelným školením zaměstnanců; |
| 8.3.12.8. vhodnou pracovní náplní metodika ICT (pokud v organizaci působí). |
| 8.3.13. Za plnění povinností stanovených v článku 8.3.12. jsou odpovědní odpovědné osoby (garanti) podle rozsahu svých oprávnění. |
| 8.3.14. Zaměstnanec pomáhá zajišťovat kybernetickou bezpečnost na počítačích tím, že |
| 8.3.14.1. 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; |
| 8.3.14.2. používá pouze silná hesla; |
| 8.3.14.3. maže a neotvírá nevyžádanou poštu, odmažává SPAM v emailové schránce i v počítačích. |

9. PORUŠENÍ ZABEZPEČENÍ A MÍRA JEHO RIZIKA

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.1. Vědomé porušení povinnosti mlčenlivosti, neoprávněné zveřejnění, sdělení, zpřístupnění a přisvojení osobních údajů zaměstnancem je porušení povinností, které mu vyplývají z pracovního poměru zvláště 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. | |
| 9.2. 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. | Zavirování počítače; odeslání e-mailu s více osobními údaji jinému adresátovi; smazání souborů s osobními údaji; otevření e-mailu, který má v sobě vir; jakýkoliv i situační příznak, že někdo neoprávněně získal osobní údaje - např. spam všem žákům a zákonným zástupcům ve třídě a další. |

Poznámky a příklady

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>9.3. Odpovědný zaměstnanec (garant), je-li to možné, bezodkladně zabrání dalšímu neoprávněnému nakládání, zejména zajistí zneprístupnění, 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 zaměstnanec¹⁵ (garant).</p> | <p>Okamžitá změna hesel; zablokování bankovního účtu; sim karty; kontaktování správce systémů k zálohování dat (např. matrika, účetnictví...).</p> |
| <p>9.4. Pokud je riziko pro práva a svobody fyzických osob vysoké, odpovědný zaměstnanec (garant) vhodným způsobem navíc informuje subjekty údajů.¹⁶ 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.</p> | <p>Např. emailem, zveřejněním na webových stránkách.</p> |

10. ZÁVĚREČNÁ USTANOVENÍ

Poznámky a příklady

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 10.1. Kontrola dodržování směrnice | |
| <p>10.1.1. Starosta, případně tajemník zajistí kontrolu plnění povinností vyplývajících z ustanovení Směrnice pro nakládání s osobními údaji.</p> | <p>Starosta pravidelně kontroluje zabezpečení a nakládání s osobními údaji a dbá na pravidelné zálohování.</p> |
| <p>10.1.2. Starosta, případně tajemník zajistí, aby byli s dokumentem Směrnice pro nakládání s osobními údaji seznámeni všechny pověřené osoby.</p> | <p>Seznámení na poradě – podpisy či zápis jako doložení seznámení.</p> |
| 10.2. Revize směrnice | |
| <p>10.2.1. Revize Směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky.</p> | |

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

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

10.3. Účinnost směrnice

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

Přijato usnesením zastupitelstva č. ze dne

PŘÍLOHA Č. 1: SLOVNÍČEK POJMŮ

BALANČNÍ TEST – vyhodnocení oprávněného zájmu správce (obec) 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 činnosti 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 neseťkává 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.

-
- 1 - Pro situaci, kdy knihovna je organizační složkou obce, tedy její pracovníci jsou zaměstnanci obce.
 - 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
 - 5 - Označit informace o zpracování osobních údajů jen zkratkou „GDPR“ nelze. Povinností správce je mimo jiné komunikovat srozumitelné a vyvarovat se používání zkratk a odborných výrazů. Zkratka „GDPR“ může být použita jen jako doplnění srozumitelného označení dané sekce jako je např. „Informace o zpracování osobních údajů“.
 - 6 - Čl. 30 Obecného nařízení
 - 7 - Čl. 13 a 14 Obecného nařízení
 - 8 - Čl. 12 Obecného nařízení
 - 9 - Čl. 15 Obecného nařízení
 - 10 - Čl. 16, 17 Obecného nařízení
 - 11 - „omezení zpracování“
 - 12 - Čl. 38 Obecného nařízení
 - 13 - § 312 zákoníku práce
 - 14 - Čl. 32 Nařízení
 - 15 - Čl. 33 Obecného nařízení
 - 16 - Čl. 34 Nařízení