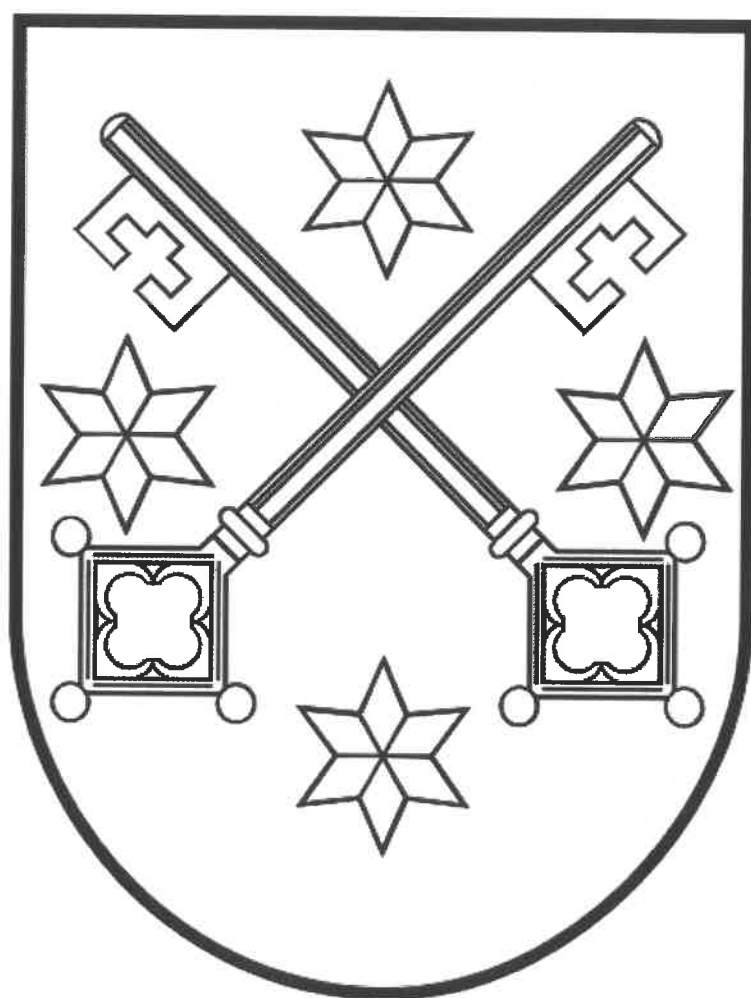


# OBEC PETROVICE U KARVINÉ



## SMĚRNICE ZASTUPITELSTVA OBCE

### PETROVICE U KARVINÉ 1/2018

#### o ochraně osobních údajů

účinnost od 05.06.2018

## Článek 1 ÚVODNÍ USTANOVENÍ

- 1.1 Tuto směrnici o ochraně osobních údajů včetně příloh (dále také jen „směrnice“) schválilo Zastupitelstvo obce Petrovice u Karviné na svém 22. zasedání konaném dne 04.06.2018 usnesením č. 358 s účinností od 05.06.2018.
- 1.2 Touto směrnicí obec Petrovice u Karviné (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 též „Obecné nařízení“) a podle zákona o zpracování osobních údajů (dále též „zákon“), zejména při zpracování osobních údajů vykonávaných obcí, zejména Obecním úřadem obce Petrovice u Karviné (dále jen „OÚPuK“) a organizačními složkami obce.
- 1.3 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 města, jako jsou členové zastupitelstva, komisí a výborů (dále jen „členové orgánů“), pokud se v souvislosti s výkonem své funkce seznamují, případně zpracovávají osobní údaje.
- 1.4 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) a obsahují závazek k dodržování této směrnice, konkretizaci povinností podle směrnice a potvrzení, že smluvní strana se se směrnicí seznámila.
- 1.5 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.

## Článek 2 ZÁKLADNÍ POJMY

- 2.1 Základní pojmy ochrany osobních údajů stanovuje Obecné nařízení a zákon.
- 2.2 **Osobní údaj** je 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;
- 2.3 **Citlivý osobní údaj** je 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;
- 2.4 **Zpracování osobních údajů** je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení; 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;
- 2.5 **Subjekt údajů** je fyzická osoba, k níž se osobní údaj vztahuje,
- 2.6 **Souhlas 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.

### Článek 3 OSOBNÍ ÚDAJE A JEJICH ZPRACOVÁNÍ

- 3.1 Způsob zpracování osobních údajů a pověřené osoby
- 3.1.1 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.
- 3.1.2 Zpracovávat osobní údaje a seznamovat se s nimi mohou v rozsahu podle následujících ustanovení pouze pověřené osoby, kterými jsou:
- zaměstnanec, který v souladu se svým pracovním zařazením vykonává agendu, jejíž nezbytnou součástí je zpracování osobních údajů,
  - člen orgánu, pokud je to nezbytné pro výkon jeho funkce,
  - osoby, které k tomu mají oprávnění na základě uzavřené smlouvy.
- 3.2 Účel zpracování, zákonnost a nově zaváděné účely zpracování
- 3.2.2 Veškerá zpracování osobních údajů probíhají v rámci jednotlivých agend, tzv. „účelech zpracování“. Ten, kdo rozhoduje o činnosti zpracování (dále „odpovědný zaměstnanec“), 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) 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.
- 3.2.3 Právní titul či tituly každého účelu zpracování určí odpovědný zaměstnanec. 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.
- 3.2.4 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.
- 3.2.5 Ke stanovení účelu zpracování, určení právního titulu a případně právního základu si odpovědný zaměstnanec vyžádá posouzení pověřencem.
- 3.2.6 O každém nově zamýšleném účelu zpracování je ten, kdo navrhuje jeho účel, povinen informovat pověřence, a to před jakýmkoliv krokem, který vyvolává závazek nebo náklady obce. Zahájit novou činnost zpracování lze jen na základě doložitelného posouzení pověřencem.
- 3.2.7 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.
- 3.2.8 Ustanovení tohoto článku se přiměřeně vztahuje i na člena orgánu při výkonu jeho funkce, který spolupracuje s odpovědným zaměstnancem a pověřencem.
- 5.2 Zásady zpracování osobních údajů
- 3.3.1 Základní zásady při zpracování osobních údajů jsou:
- zpracovávat osobní údaje korektním a transparentním způsobem,
  - před zavedením každého zpracování osobních údajů stanovit účel, právní titul a případně právní základ či oprávněné důvody správce pro toto zpracování,
  - zpracovávat osobní údaje pouze v nezbytném rozsahu a po dobu nezbytnou k danému účelu,
  - zpracovávat osobní údaje přesně a podle potřeby je aktualizovat,
  - zajišťovat náležité zabezpečení osobních údajů.
- 3.4 Záznamy o zpracování a kontrolní seznam
- 3.4.1 Každý odpovědný zaměstnanec vede ve formuláři, jímž byla provedena implementace Obecného nařízení (dále jen „Kontrolní seznam“)
- záznamy o příslušných účelech zpracování (dále jen „záznam o zpracování“)
  - záznamy o provedených opatřeních k dosažení souladu s Obecným nařízením, jako je šifrování, likvidace či výmaz dat, lhůty pro likvidaci, forma a lhůty zálohování záznamy o bezpečnostních incidentech jako je únik, ztráta, neoprávněný přenos či zveřejnění, další údaje potřebné k vyhodnocení a doložení souladu s Obecným nařízením a k informování subjektů údajů.

- 3.4.2 Ke kontrolnímu seznamu mají přístup odpovědní zaměstnanci a pověřenec. O změnách v kontrolním seznamu musejí odpovědní zaměstnanci vždy informovat pověřence, např. sdílením aktualizované verze.
- 3.4.3 Starosta nebo jím určená osoba zajistí pravidelné zálohování kontrolního seznamu a případných souvisejících dokladů.
- 3.5 Doklady o souladu s Obecným nařízením
- 3.5.1 Každá pověřená osoba, tj. osoba, která vykonává svěřenou agendu dle pracovní náplně nebo ze zákonného zmocnění, dbá na uchování dokladů, opravňujících určité zpracování osobních údajů, jako jsou:
- smlouvy, pro jejichž plnění se zpracovávají osobní údaje,
  - doklady o informování subjektů údajů v případech, kdy nepostačuje zveřejnění na webu,
  - doklady o vyřízení žádostí subjektů údajů,
  - souhlasy se zpracováním osobních údajů,
  - balanční testy v případě zpracování na základě právního titulu oprávněného zájmu správce nebo třetí osoby,
  - evidence klíčů, je-li potřebná
  - evidence přístupů do počítačů a přístupových práv v informačním systému, je-li potřebná
  - údaje o zpřístupnění záznamu kamerového systému či dalších specifických záznamů osobních údajů,
  - další obdobné doklady.
- 3.5.2 Doklady dle bodu 3.5.1 vede odpovědný zaměstnanec v kontrolním seznamu, pokud to jejich povaha umožňuje, jinak se v kontrolním seznamu pouze uvede, kde jsou uloženy.

#### **Článek 4 PRÁVA SUBJEKTŮ ÚDAJŮ**

- 4.1 Informování subjektů údajů
- 4.1.1 Starosta 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.
- 4.1.2 Odpovědný zaměstnanec zajistí také doložitelnost uvedeného informování. Může v rámci své kompetence tento úkol uložit jinému zaměstnanci.
- 4.2 Přístup k osobním údajům
- 4.2.1 Požadavky subjektů údajů vyřizuje odpovědný zaměstnanec. Může v rámci své kompetence tento úkol uložit jinému zaměstnanci. Pro vyřízení se přiměřeně postupuje podle obecného předpisu pro přístup k informacím, neuplatní se správní řád.
- 4.2.2 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“).
- 4.2.3 Běžné provozní dotazy týkající se osobních údajů (zejm. informace o zpracování osobních údajů), vyřídí příslušný zaměstnanec podle okolností co nejdříve. O vyřízení žádosti bezodkladně informuje nadřízeného.
- 4.2.4 K vyřízení ostatních žádostí o přístup k osobním údajům (zejm. export údajů) je příslušný odpovědný zaměstnanec. Žádost se vyřídí do 30 dnů.
- 4.2.5 V případě potřeby a s ohledem na složitost a počet žádostí může odpovědný zaměstnanec 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.
- 4.2.6 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.
- 4.2 Právo na výmaz, opravu a doplnění
- 4.3.1 Pověřené osoby jsou povinny dbát na správnost zpracovávaných osobních údajů.

- 4.3.2 Subjekt údajů má právo žádat výmaz, opravu a doplnění osobních údajů, které se ho týkají. Případy, kdy je požadavek na výmaz oprávněný, stanoví čl. 17 odst. 1 a 3 Obecného nařízení. Žádost vyřídí odpovědný zaměstnanec po ověření totožnosti a po prověření oprávněnosti požadavku ihned, jakmile je to možné, nejdéle do 30 dnů; čl. 4.2.5 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 a informuje o tom žadatele. Ve složitých případech si vyžádá posouzení pověřencem.
- 4.3.3 Oznámi-li subjekt údajů (např. telefonicky nebo emailem), že osobní údaje, které se ho týkají, se změnil, a nelze dostatečně ověřit jeho totožnost s ohledem na závažnost požadované změny (např. na základě osobní znalosti hlasu, znalosti e-mailové adresy), vyzve ho odpovědný zaměstnanec k postupu, umožňujícímu totožnost ověřit.
- 4.3.4 Zjistí-li pověřená osoba při své činnosti, že při zpracování osobních údajů došlo ke zjevné chybě v psaní (např. překlepu), informuje odpovědného zaměstnance a údaj opraví.

## **Článek 5 POVĚRENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ**

- 5.1 Pro obec vykonává úkoly pověřence pro ochranu osobních údajů:  
Jméno, příjmení, titul: Bc. Daniel Stuchlík  
e-mailová adresa: daniel.stuchlik@sms-sluzby.cz  
kontaktní telefon: +420 774 420 750
- 5.2 Starosta zajistí zveřejnění kontaktních údajů pověřence a Úřadu pro ochranu osobních údajů je sdělí včetně jeho identifikace.
- 5.3 Všechny pověřené osoby jsou povinny :
- konzultovat s pověřencem všechny záležitosti, související s ochranou osobních údajů, pokud si nejsou zcela jisty jejich prováděním v souladu s Obecným nařízením,
  - poskytnout pověřenci součinnost při plnění jeho úkolů, zejména mu umožnit plný přístup k osobním údajům a k operacím zpracování,
  - zdržet se jakéhokoli jednání, které by mohlo ohrozit nezávislé posouzení věci pověřencem,
  - neukládat pověřenci úkoly, které by vedly k jeho střetu zájmů.
- 5.4 Povinnosti pověřence jsou stanoveny ve zvláštní smlouvě.

## **Článek 6 BEZPEČNOST INFORMACÍ**

- 6.1 Obecné postupy při zabezpečení osobních údajů
- 6.1.2 Iměněn zabezpečeny musejí být zpracováváné osobní údaje i ty, které nejsou systematicky zpracováváné, například vyskytující se v jednotlivých nezařazených dopisech, sděleních, e-mailech.
- 6.1.3 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
- na základě zákona o svobodném přístupu k informacím,
  - jsou veřejně dostupné (například ve veřejně přístupných registrech),
  - nepředstavují žádné riziko pro subjekty údajů, například malý počet nahodilých nevýznamných informací.
- 6.1.4 V pochybnostech je pověřená osoba vždy povinna konzultovat potřebu zabezpečení s nadřízeným nebo s pověřencem.
- 6.1.5 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 a dále v dodržování pravidel informační bezpečnosti.

- 6.1.6 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:
- sdělovat jakékoliv osobní údaje jiné osobě, než která je subjektem údajů nebo je jejím zákonným zástupcem,
  - hlasitě sdělovat osobní údaje ve veřejně přístupných prostorách
  - umožnit nepovolaným osobám nahlížet do listin, které nesou osobní údaje, nebo na obrazovku monitoru, kde jsou takové údaje zobrazeny,
  - sdělovat komukoliv svá přístupová hesla do počítače, do informačních systémů a hesla k zašifrovaným souborům nebo zařízením.
- 6.3 Zabezpečení písemností a záznamových médií obsahujících osobní údaje
- 6.3.1 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.
- 6.3.2 Za plnění povinností stanovených ve výše uvedených odstavcích tohoto článku jsou odpovědní pověřené osoby podle rozsahu svých oprávnění.
- 6.4 Zabezpečení dat obsahujících osobní údaje v osobních počítačích a na sítích
- 6.4.1 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.
- 6.4.2 Pevné 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.
- 6.4.3 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.
- 6.4.4 Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, uložení souborů mobilního telefonu a podobně, musejí být, i když se nepředpokládá jejich vynášení z objektu alespoň:
- zajištěna šifrováním disku či jiného uložení pomocí šifrovacího programu,
  - zajištěna zabezpečeným přístupem do programového vybavení, které data ukládá šifrovaně,
  - být jako soubor šifrované,
  - je-li to dostatečné s ohledem na riziko pro subjekty osobních údajů, být dostatečně pseudonymizována, nebo pokud přenosné médium sloužilo jen k přenosu, bezodkladně po přenosu bezpečně vymazána,
  - 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.
- 6.4.5 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.
- 6.4.6 Přenos souborů s osobními údaji nezabezpečenou sítí Internet (např. protokol HTTP) a jejich uložení na nezabezpečených uloženištích (běžné e-mailové schránky, přechodná uloženiště jako Úschovna.cz) je přípustný jen se zašifrováním souboru a předáním hesla příjemci jinou cestou, například SMS zprávou na ověřené číslo telefonu či pomocí jiné bezpečné aplikace.
- 6.4.7 Umožňuje-li to programové vybavení, pověřené osoby vždy využijí možnosti záznamu přístupů a činnosti (auditního záznamu, logu) na počítačích nebo v informačním

- systemu. Záznamy pravidelně kontrolují. Tímto úkolem může být pověřen určený zaměstnanec.
- 6.4.8 Za plnění povinností stanovených v tomto článku jsou odpovědní pověřené osoby podle rozsahu svých oprávnění.
- 6.5 Porušení zabezpečení a míra jeho rizika
- 6.5.1 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, starostu a tajemníka.
- 6.5.2 Odpovědný zaměstnanec 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 kontrolním seznamu. 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.
- 6.5.3 Pokud je riziko pro práva a svobody fyzických osob vysoké, odpovědný zaměstnanec vhodným způsobem navíc informuje subjekty údajů. 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.

## Článek 7 ZÁVĚREČNÁ USTANOVENÍ

- 7.1 Starosta zajistí kontrolu plnění povinností vyplývajících z jednotlivých ustanovení Směrnice.
- 7.2 Starosta případně tajemník a vedoucí zaměstnanci zajistí, aby byli se směrnicí seznámeni všechny pověřené osoby, další zaměstnanci a dodavatelé, kteří mohou přijít jakýmkoliv způsobem do styku s osobními kontakty.
- 7.3 Revize Směrnice je provedena v případě potřeby, minimálně však jednou za dva roky.
- 7.4 Za zpracování, údržbu a revize Směrnice odpovídá starosta na základě konzultace s pověřencem pro ochranu osobních údajů.
- 7.5 Tuto směrnici schválilo Zastupitelstvo obce Petrovice u Karviné na svém 22. zasedání konaném dne 04.06.2018 usnesením č. 358. Směrnice nabývá účinnosti a platnosti dnem 05.06.2018.
- 7.6 Směrnice je uložena v souladu se směrnicí pro vydávání interních právních předpisů.



z. pov.  
**doc. Ing. Marian Lebieczik, PhD.**  
starosta

### PŘÍLOHY :

- Příloha č. 1 – Vzor textu mlčenlivosti k zpracování do smluv  
Příloha č. 2 – Vzor textu souhlasu se zpracováním osobních údajů  
Příloha č. 3 – Sazebník úhrad za poskytování informací

## PŘÍLOHA Č. 1 ke směrnici ZO Petrovice u Karviné č. 1/2018 o ochraně osobních údajů

### VZOR TEXTU MLČENLIVOSTI DO SMLUV

#### 1. Pracovní smlouvy:

*„Zaměstnanec se zavazuje pro zajištění náležitého zabezpečení osobních údajů podle čl. 5 odst. 1 písm. f) nařízení EP a Rady (EU) 2016/679 o ochraně osobních údajů zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, o nichž se dozvěděl v souvislosti s výkonem práv a povinností vyplývajících z tohoto pracovního vztahu a jejichž neoprávněné poskytnutí nebo zpřístupnění by mohlo ohrozit toto zabezpečení osobních údajů. Povinnost mlčenlivosti podle tohoto odstavce smlouvy trvá i po případném skončení pracovního poměru.“*

#### 2. Smlouvy s dodavateli:

##### a) S osobami s nahodilým přístupem k osobním údajům (např. IT servis)

*„Dodavatel bere na vědomí, že při plnění této smlouvy se dostává do styku s osobními údaji zpracovávanými objednatelem, aniž by jejím předmětem bylo tyto osobní údaje jakkoliv zpracovávat.*

*Pro zajištění náležitého zabezpečení osobních údajů podle čl. 5 odst. 1 písm. f) nařízení EP a Rady (EU) 2016/679 o ochraně osobních údajů se zavazuje :*

- *tyto údaje nijak nezpracovávat, například je měnit, ukládat, přenášet, komukoliv jinému zpřístupnit nebo vymazat,*
- *zachovávat mlčenlivost o těchto osobních údajích a o bezpečnostních opatřeních, o nichž se v této souvislosti dozvěděl, a jejichž neoprávněné poskytnutí nebo zpřístupnění by mohlo ohrozit toto zabezpečení osobních údajů,*
- *zajistit, že jeho zaměstnanci, které oprávní při plnění této smlouvy se dostávat do styku s osobními údaji zpracovávanými objednatelem, se zaváží ve stejném rozsahu, a na žádost objednatele mu bezodkladně poskytne veškeré informace potřebné k doložení těchto závazků. Totéž zajistí u subdodavatele a jeho zaměstnanců, pokud je se souhlasem objednatele využije.*
- *Povinnost mlčenlivosti podle tohoto odstavce smlouvy trvá i po ukončení smlouvy.“*

##### b) Se zpracovateli (např. externí zpracování mezd, externí správce sítě, externí bezpečnostní správce, poskytovatel datového úložiště – cloudu apod.)

*„Dodavatel bere na vědomí, že předmětem smlouvy je také zpracování osobních údajů a je tedy v postavení jejich zpracovatele. Pro zajištění náležitého zabezpečení osobních údajů podle čl. 5 odst. 1 písm. f) nařízení EP a Rady (EU) 2016/679 o ochraně osobních údajů se zavazuje zajistit, že osoby jím oprávněné zpracovávat osobní údaje se před zpracováním prokazatelně zaváží zachovávat mlčenlivost o těchto osobních údajích a o bezpečnostních opatřeních, o nichž se v této souvislosti dozvedí, a jejichž neoprávněné poskytnutí nebo zpřístupnění by mohlo ohrozit toto zabezpečení osobních údajů. Dodavatel zajistí, že tato povinnost pro něj i pro oprávněné osoby bude platit i po skončení vztahu těchto osob s ním. Dodavatel se zavazuje na žádost objednatele mu bezodkladně poskytnout veškeré informace potřebné k doložení těchto závazků.“*



**Upozornění:** smlouva se zpracovatelem musí obsahovat i další povinné náležitosti a závazky zpracovatele ke správci. Jde rámcově o tyto a některé z nich bude třeba pro konkrétní smlouvy, s ohledem na okolnosti a typ zpracovatele, přesněji formulovat:

- přijmout všechna bezpečnostní, technická, organizační a jiná opatření s přihlédnutím ke stavu techniky, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování k zabránění jakéhokoli narušení poskytnutých osobních údajů,
- nezapojit do zpracování žádnou další osobu bez předchozího písemného souhlasu objednatele,
- zpracovávat osobní údaje pouze pro plnění smlouvy (vč. předání údajů do třetích zemí a mezinárodním organizacím); výjimkou jsou pouze případy, kdy jsou určité povinnosti uloženy přímo právním předpisem,
- zajistit, že dodavatel bude objednateli bez zbytečného odkladu nápomocen při plnění povinností objednatele, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 nařízení, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 nařízení, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 nařízení a povinnosti provádět předchozí konzultace dle čl. 36 nařízení, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje objednatele,
- po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí objednateli a vymaže existující kopie apod.,
- poskytnout objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené objednateli právními předpisy,
- umožnit kontrolu, audit či inspekci prováděné objednatel nebo příslušným orgánem dle právních předpisů,
- poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví objednatel, součinnost potřebnou pro plnění zákonných povinností objednatele spojených s ochranou osobních údajů, jejich zpracováním,
- poskytnuté osobní údaje chránit v souladu s právními předpisy.

## **PŘÍLOHA Č. 3 ke směrnici ZO Petrovice u Karviné č. 1/2018 o ochraně osobních údajů**

### **SAZEBNÍK ÚHRAD ZA POSKYTOVÁNÍ INFORMACÍ**

**pro úhradu nákladů podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, zákona č. 123/1998 Sb. o právu na informace o životním prostředí a podle Obecného nařízení EU o ochraně osobních údajů č. 2016/679**

#### **Obec Petrovice u Karviné stanoví**

v souladu s § 5 odst. 1 písm. f) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění, ve spojení s § 17 tohoto zákona, s nařízením vlády č. 173/2006 Sb., o zásadách stanovení úhrad a licenčních odměn za poskytování informací podle zákona o svobodném přístupu k informacím, s § 10 odst. 3 a 4 zákona č. 123/1998 Sb. o právu na informace o životním prostředí, s článkem 12 odst. 5 Obecného nařízení EU o ochraně osobních údajů č. 2016/679 a na základě § 102 odst. 3 zákona č. 128/2000 Sb., o obcích (obecní zřízení), v platném znění, tento sazebník úhrad za poskytování informací:

#### **Článek I.**

##### **Náklady na pořízení kopíí**

1. Za pořízení jedné černobílé kopie formátu A4:

a) jednostranná ..... 2 Kč

b) oboustranná ..... 4 Kč

2. Za pořízení jedné černobílé kopie formátu A3:

a) jednostranná ..... 4 Kč

b) oboustranná ..... 8 Kč

3. Za tisk na černobílé tiskárně (formát A4, jednostranný) jedna stránka 3 Kč

4. Za pořízení skenu či fotografie do souboru jedné stránky do velikosti A4 při skenování a do velikosti A3 při fotografování včetně úpravy k odeslání ..... 5 Kč

5. Za poskytnutí kopie nebo tisku v jiném formátu nebo barvě bude účtována skutečná cena za pořízení kopie u komerčního poskytovatele kopírovacích služeb, kterou obec za pořízení kopie nebo tisku bude u tohoto poskytovatele povinna uhradit.

6. V případě informací obsažených v publikacích a tiskovinách vydávaných obcí se výše úhrady stanoví ve výši ceny za příslušný výtisk, poskytuje-li se informace formou prodeje tohoto výtisku.

#### **Článek II.**

##### **Náklady na opatření technických nosičů dat**

1. 1 ks CD ..... 10 Kč

2. 1 ks DVD ..... 20 Kč

3. Pokud žadatel poskytne vlastní technický nosič dat, na který bude možné požadované informace zaznamenat, nebude úhrada tohoto nákladu uplatňována.

**Článek III.**  
**Náklady na odeslání informací žadateli**

1. Náklady na poštovní služby budou vyčísleny dle ceníku České pošty s. p., případně jiného poskytovatele poštovní služby. Náklady na balné se stanoví paušální částkou 20,- Kč za jednu poštovní zásilku.
2. V případě osobního odběru požadovaných informací nebude úhrada nákladů na odeslání informací žadateli uplatňována.

**Článek IV.**  
**Náklady na mimořádně rozsáhlé vyhledání informací**

1. V případě mimořádně rozsáhlého vyhledání informací se úhrada požaduje za vyhledávání delší než 1 hodinu. Úhrada za hodinu vyhledávání jedním pracovníkem je 250,- Kč, započítává se každých i započatých 30 minut. Úhrada je odvozena od ročních nákladů na platy zaměstnanců obce, kteří se mohou podílet na vyhledávání informací, podle schváleného rozpočtu pro rok 2018. V případě mimořádně rozsáhlého vyhledání informací více pracovníky bude úhrada dána součtem doby připadající na každého pracovníka.
2. Vzniknou-li při mimořádně rozsáhlém vyhledání informací jiné osobní náklady, nezbytné k vyhledání informace (např. náklady na jízdné na odlehlé pracoviště), budou účtovány na základě individuální kalkulace.
3. Do vyhledávání se zahrne s ohledem na konkrétnost formulace žádosti pouze vyhledání, ve kterém dokumentu se požadovaná informace nachází (např. v evidenci, spisové službě), vyhledání samotného dokumentu (např. ve spisovně, v počítači), vyhledání požadovaných informací v dokumentu, přenesení informací do sdělení žadateli (výpisem nebo kopírováním v počítači). Omezeně lze zahrnout čas nutný na anonymizaci chráněných údajů. Ostatní činnosti spojené s vyřízením žádosti, včetně právního posouzení, se nezapočítávají. Nezapočte se ani čas kopírování listinných dokumentů, který je již vyjádřen jednotkovou sazbou za kopii.

**čl. V.**  
**Ostatní ustanovení**

1. Celková výše úhrady je součtem jednotlivých nákladů spojených s poskytnutím požadovaných informací. Do celkové výše 100,- Kč nebude úhrada požadována, pokud žadatel nepodal po dobu jednoho měsíce od podání předchozí žádosti další žádost.
2. Z důvodu hodných zvláštního zřetele může starosta obce od úhrady nákladů zcela nebo zčásti upustit na základě žádosti žadatele.
3. Žadatel může úhradu provést buď v hotovosti v pokladně obecního úřadu v úředních hodinách nebo převodem na bankovní účet obce
4. Tento sazebník se stanoví na účetní období 2018 - 2020.

## **PŘÍLOHA Č. 2 ke směrnici ZO Petrovice u Karviné č. 1/2018 o ochraně osobních údajů**

### **VZOR TEXTU SOUHLASU SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ**

- 1 Osobní údaje se zpracovávají zejména dle základních zásad, kterými jsou:
  - zákonnost - správce osobních údajů může osobní údaje k určitému účelu zpracovávat pouze tehdy, pokud má k zpracování alespoň jeden právní důvod,
  - korektnost - správce nesmí klamat subjekt údajů o tom, že jejich údaje zpracovává, za jakým účelem je zpracovává a jakým způsobem je zpracovává,
  - transparentnost - informace, které subjekt údajů od správce dostává, musí být srozumitelné a snadno přístupné,
  - omezení účelu - osobní údaje musí být shromážděny pro určité, výslovně vyjádřené legitimní účely a nesmějí být zpracovány způsobem, který je s těmito údaji neslučitelný,
  - minimalizace údajů - představuje povinnost zpracovávat osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ke stanovenému účelu zpracování, Např.: Ptáme se jen na ty údaje, které skutečně potřebujeme.
  - přesnost - musí být přesné (aktuální) a v případě potřeby pak aktualizovány podle skutečného stavu,
  - omezené uložení - osobní údaje by měly být uloženy jen po nezbytně nutnou dobu, respektive po dobu, kdy je to nutné pro splnění účelu jejich zpracování, Např.: Údaje, které jsou staré, a už je v praxi nevyužíváme, tak jsme povinni vymazat.
  - integrita a důvěrnost - osobní údaje by měly být dostatečně zabezpečeny, a to prostřednictvím vhodných opatření. Např.: heslo na počítači, nevynášení notebooku, atd.
- 2 Využívání souhlasu by mělo být omezeno na případy, kdy neexistuje žádný jiný právní titul. Jedná se o nejslabší právní titul a je ho možné vždy odvolat. Dále je třeba si dávat pozor na nadbytečný souhlas (existuje jiný zákonný důvod zpracování a správce i přesto má souhlas), takové jednání je pak deliktem.
- 3 Pro platnost souhlasu musí být splněny následující podmínky, respektive souhlas musí být:
  - svobodný - na základě svobodné volby a souhlas může odvolat nebo odmítnout, aniž by byl poškozen,
  - konkrétní - musí být jasně uvedeno k jakému účelu je souhlas dán,
  - informovaný - subjekt musí znát totožnost správce a účel zpracování,
  - odlišitelný - zřetelně oddělený od jiného textu,
  - jednoznačný - nedává možnost dvojího výkladu.
- 4 Písemné znění musí být vždy odsouhlaseno pověřencem.
- 5 Vzor textu:

*Souhlas je udělen dle nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. 4. 2016 Obecné nařízení o ochraně osobních údajů (dále jen „Nařízení“).*

*Obec Petrovice u Karviné, coby správce osobních údajů, je oprávněna zpracovávat osobní údaje manuálně i automatizovaně rovněž prostřednictvím určených zpracovatelů, jejichž aktuální seznam poskytne na vyžádání. Osobní údaje budou zpřístupněny pouze oprávněným zaměstnancům správce či případně zaměstnancům zpracovatele, a to pouze v míře nezbytné pro účely zpracování. Tento souhlas lze kdykoli písemně odvolat.*

*Osobními údaji se rozumí jméno a příjmení, adresu trvalého bydliště, korespondenční adresu, datum narození, fotografie, audio a videozáznamy, telefonní čísla a e-mailové adresy.*

6 Poskytovatele osobních údajů je nutné dále poučit o právech a povinnostech, zejména o právu:

- na přístup k osobním údajům (čl. 15 Nařízení)
- na opravu nepřesných nebo nepravdivých osobních údajů (čl. 16 Nařízení)
- na výmaz osobních údajů, nejsou-li již osobní údaje potřebné pro účely, pro které byly shromážděny či jinak zpracovány (čl. 17 Nařízení)
- na omezení zpracování osobních údajů (čl. 18 Nařízení)
- na přenositelnost údajů (čl. 20 Nařízení)
- na vznesení námítky je-li zpracování osobních údajů prováděno ve veřejném zájmu či pro účely oprávněných zájmů správce (čl. 21 Nařízení)
- podat proti správci stížnost u dozorového orgánu (čl. 77 Nařízení)