



Směrnice pro nakládání s osobními údaji

Správce osobních údajů: Nadace pro rozvoj města Pardubic

23. května 2018

Copyright © 2018 by VIAVIS a.s.			
ID Dokumentu	GDPR_Smernice_NOU_NpRMP	Verze	V01
Zodpovídá	Martin Dušek	Stav	Final
Klasifikace	Pro vnitřní potřebu	Určeno pro	Správce
Počet výtisků	-	Výtisk číslo	-

Obsah

1	Úvodní ustanovení	4
1.1	Základní pojmy	4
1.2	Definice rolí	4
2	Zpracování osobních údajů	6
3	Bezpečnost informací	7
3.1	Zabezpečení písemností a záznamových médií obsahujících osobní údaje	7
3.2	Zabezpečení dat obsahujících osobní údaje v počítačích	7
3.3	Likvidace dokumentů v listinné podobě, záznamových médií a dat obsahujících osobní údaje	7
4	Povinnosti specifických rolí	8
4.1	Garant ochrany osobních údajů	8
4.2	Vedoucí zaměstnanec	9
4.3	Odpovědná osoba	9
4.4	Správce informačních technologií	10
4.5	Pověřené osoby	10
4.6	Ostatní zaměstnanci	11
5	Pravidla pro uživatele při automatizovaném zpracování osobních údajů	12
5.1	Zákaz	12
5.2	Zodpovědnost	13
5.3	Postupy	13
6	Výkon práv subjektu údajů	15
7	Závěrečná ustanovení	17
7.1	Kontrola dodržování ustanovení směrnice	17
7.2	Revize směrnice	17
7.3	Audit směrnice	17
7.4	Účinnost směrnice	17
8	Příloha č. 1	18

1 Úvodní ustanovení

Tyto zásady upravují postup při zpracování a ochraně osobních údajů dle NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a příslušného právního předpisu o ochraně osobních údajů¹.

Tyto zásady se vztahují na zpracování osobních údajů Nadace pro rozvoj města Pardubic, IČO 46495801 (dále jen „Správce“).

1.1 Základní pojmy

Pojmy osobní údaj, zpracování osobních údajů, správce, zpracovatel a další jsou použity dle definice, či ve smyslu Obecného nařízení o ochraně osobních údajů.

Pro účely této Směrnice pro nakládání s osobními údaji se rozumí:

"Směrnici" tato Směrnice pro nakládání s osobními údaji.

"Organizační jednotkou" příslušný úsek Správce.

"Zaměstnancem" osoba vykonávající závislou práci v pracovněprávním vztahu ke Správci (ve smyslu zákoníku práce).

"Úřadem" Úřad pro ochranu osobních údajů.

„Počítačem“ osobní počítač nebo obdobná zařízení (notebook, tablet, smartphone apod.).

„Úschovným objektem“ uzamykatelná skříň, trezor, stůl nebo jiný uzamykatelný nábytek určený správcem pro ukládání písemností obsahujících osobní údaje.

1.2 Definice rolí

Pro účely této směrnice se rozumí:

„Garantem ochrany osobních údajů“ je správce nadace, který u Správce zodpovídá za oblast ochrany osobních údajů a plní úkoly v rozsahu touto směrnicí uvedené. V otázkách ochrany osobních údajů jsou garantovi ochrany osobních údajů podřízeni všechny pověřené osoby uvedené v této směrnici a ostatní zaměstnanci Správce. Při tom jsou povinni plnit jeho pokyny, pokud nejsou v rozporu s obecně závaznými právními předpisy nebo vnitřními předpisy Správce.

¹ zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

„Vedoucím zaměstnancem“ zaměstnanec zodpovědný za zpracování osobních údajů v rozsahu vyplývajícím z jeho pracovní náplně, obecně závazného právního předpisu, vnitřního předpisu nebo jiného aktu, který určuje odpovědné osoby ke stanovení identifikace zpracování. Vedoucí zaměstnanec je v otázkách ochrany osobních údajů podřízen garantovi ochrany osobních údajů a nadřízen odpovědným osobám a pověřeným osobám, pokud jsou na pozicích jím řízených.

„Odpovědnou osobou“ osoba určená k vyhotovení identifikace zpracování osobních údajů a její aktualizaci. Odpovědná osoba je v otázkách ochrany osobních údajů podřízena vedoucímu zaměstnanci a garantovi ochrany osobních údajů. Ostatní zaměstnanci náležející pod řízení vedoucího zaměstnance jsou povinny poskytnout jí součinnost při plnění úkolů odpovědné osoby.

„Pověřenou osobou“ osoba, která je oprávněna zpracovávat osobní údaje. Pověřenými osobami jsou:

- zaměstnanci provádějící zpracování osobních údajů na základě povinností vyplývajících z uzavřeného pracovněprávního vztahu, obecně závazných právních předpisů, vnitřních předpisů Správce nebo na základě zvláštního pověření,
- zaměstnanci, kteří zabezpečují informační systémy pro zpracování osobních údajů,
- osoby, které k tomu mají oprávnění na základě uzavřené smlouvy,
- zaměstnanci zpracovatelů osobních údajů v rozsahu pokynů vydaných Správcem zpracovateli.

„Ostatními zaměstnanci“ zaměstnanci, kteří nejsou osobami uvedenými v předchozích bodech tohoto článku této směrnice a nejsou oprávněni jakýmkoliv způsobem zpracovávat osobní údaje.

„Uživatelem“ zaměstnanec nebo jiná osoba pověřená Správcem, která od Správce získá oprávnění k užívání informačního systému.

2 Zpracování osobních údajů

Zpracování osobních údajů je přípustné pouze pro Správcem stanovené účely zpracování. Pokud hodlá pověřená osoba zpracovávat osobní údaje pro jiné účely, musí o tom před zahájením zpracování vyrozumět garanta osobních údajů a vyčkat jeho pokynů.

Pověřené osoby mohou zpracovávat zvláštní kategorie osobních údajů (tzv. „citlivé osobní údaje“), tedy osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuální životě nebo sexuální orientaci fyzické osoby jen, pokud subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů zpracování, nebo je splněn, některý z dalších případů uvedených v čl. 9 odst. 2 Obecného nařízení o ochraně osobních údajů.

V případě ostatních osobních údajů musí být naplněn alespoň jeden z požadavků uvedených v čl. 6 odst. 1 Obecného nařízení o ochraně osobních údajů.

Rozsah zpracování a další významné skutečnosti o zpracování jsou uvedeny v identifikaci jednotlivých zpracování, za kterou odpovídají určení vedoucí zaměstnanci.

3 Bezpečnost informací

3.1 Zabezpečení písemností a záznamových médií obsahujících osobní údaje

Dokumenty v listinné podobě a digitální záznamová média, které obsahují osobní údaje, musí být ukládány v úschovných objektech, na místech stanovených Správcem, kde je možno zajistit jejich ochranu.

Za plnění povinností stanovených ve výše uvedeném odstavci tohoto článku jsou odpovědný pověřené osoby podle rozsahu svých práv a povinností. Spolupracují při tom s garantem ochrany osobních údajů.

3.2 Zabezpečení dat obsahujících osobní údaje v počítačích

Data obsahující osobní údaje, která jsou uložena v počítačích, musí být zabezpečena před volným přístupem neoprávněných osob (vč. nahlížení do monitoru počítače při práci pověřené osoby), před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů.

Za plnění povinností stanovených v prvním odstavci tohoto článku jsou odpovědný pověřené osoby podle rozsahu svých práv a povinností. Spolupracují při tom se Správcem informačních technologií.

3.3 Likvidace dokumentů v listinné podobě, záznamových médií a dat obsahujících osobní údaje

Za likvidaci dokumentů v listinné podobě a záznamových médií v rámci příslušné organizační jednotky odpovídají pověřené osoby, pokud vnitřní předpis Správce nestanoví jinak. Za likvidaci dat v rámci informačních systémů pro zpracování osobních údajů zodpovídá Správce informačních technologií.

4 Povinnosti specifických rolí

4.1 Garant ochrany osobních údajů

Garant ochrany osobních údajů:

1. zabezpečuje metodickou a kontrolní činnost v oblasti ochrany osobních údajů,
2. vede centrální evidenci zpracování osobních údajů a ve spolupráci s vedoucími zaměstnanci podle potřeb a konkrétní situace její aktualizaci a alespoň 1x ročně její revizi,
3. vede evidenci udělených souhlasů se zpracováním osobních údajů,
4. vede dokumentaci případů porušení zabezpečení osobních údajů podle čl. 33 odst. 5 Obecného nařízení o ochraně osobních údajů a zodpovídá za vyhodnocení, zda porušení představuje riziko, příp., vysoké riziko pro subjekty údajů a podle toho přijímá příslušná opatření v souladu s Obecným nařízením o ochraně osobních údajů, zejména čl. 33 a 34 Obecného nařízení o ochraně osobních údajů,
5. spolupracuje při ochraně osobních údajů zaznamenaných v dokumentech v listinné podobě a na technických nosičích informací,
6. průběžně provádí kontrolu dodržování této směrnice,
7. zabezpečuje poskytnutí subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 12 až 14 Obecného nařízení o ochraně osobních údajů a učiní veškerá sdělení podle článků 15 až 22 a 34 Obecného nařízení o ochraně osobních údajů,
8. zastřešuje komunikaci týkající se ochrany osobních údajů u Správce vůči externím subjektům (subjektům údajů, Úřadu, příjemcům osobních údajů a ostatním oprávněným subjektům),
9. se podílí a návrhu způsobu získání souhlasu subjektu údajů se zpracováním osobních údajů, specifikací požadavků na úpravu vzorů smluv, specifikací požadavků na formulaci všeobecných obchodních podmínek ad. dokumentů souvisejících s ochranou osobních údajů,
10. se podílí na přípravě návrhů smluv o zpracování osobních údajů mezi Správcem a zpracovateli osobních údajů dle specifikace uvedené v čl. 28 odst. 3 Obecného nařízení o ochraně osobních údajů; to platí i v případech, kdy Správce provádí zpracování osobních údajů pro jiného správce,
11. se podílí na specifikaci požadavků na jednotlivé IS – systémy pro automatizované zpracování OÚ,
12. se podílí na rozvojových projektech v oblasti zpracování informací a na projektech v oblastech informačních a komunikačních technologií, které mají dopad na zpracovávané osobní údaje; metodická role v této oblasti je vykonávána zejména oponenturou projektových návrhů ve smyslu prosazení zákonných požadavků, kdy v rámci této činnosti je nezbytné zohlednit zejména zásady zpracování osobních údajů dle specifikace uvedené v čl. 5 Obecného nařízení o ochraně osobních údajů:
 - a. zákonnost, korektnost a transparentnost,
 - b. účelové omezení,

- c. minimalizace údajů,
- d. přesnost,
- e. omezení uložení,
- f. integrita a důvěrnost,
- g. odpovědnost.

4.2 Vedoucí zaměstnanec

Vedoucí zaměstnanec:

1. oznamuje garantovi ochrany osobních údajů nové zpracování osobních údajů na formuláři,
2. informuje bezodkladně garanta ochrany osobních údajů o všech skutečnostech, které mají vliv na aktuálnost evidence zpracování osobních údajů,
3. pověřuje podřízené zaměstnance zpracováním osobních údajů a stanoví jeho podmínky a rozsah, a to písemně s uvedením zaměstnance, zpracování, pro které se pověření vztahuje, účelu a rozsahu oprávnění, pokud tyto skutečnosti nevyplývají z pracovní náplně zaměstnance, obecně závazného právního předpisu, vnitřního předpisu Správce nebo jiných skutečností,
4. vede evidenci pověření zpracováním osobních údajů,
5. neprodleně oznamuje garantovi ochrany osobních údajů případy porušení zabezpečení osobních údajů,
6. zajišťuje kontrolu plnění povinností vyplývajících z ustanovení z této směrnice v mezích své působnosti,
7. zabezpečuje získání souhlasu subjektu údajů, není-li, zpracování možné bez tohoto souhlasu,
8. zabezpečuje splnění povinností ve vztahu ke zpracovatelům OÚ,
9. v souladu s vnitřními předpisy zabezpečuje likvidaci písemností a záznamových médií, použít spisový a skartační řád,
10. zabezpečuje podmínky pro řádné plnění povinností uložených touto směrnicí.

4.3 Odpovědná osoba

Odpovědná osoba:

1. zabezpečuje popis zpracování osobních údajů na Správcem předepsaném formuláři (dále jen „formulář“), jehož rozsah je uveden v Příloze č. 1 této směrnice,
2. zabezpečuje aktualizaci popisu zpracování osobních údajů na formuláři v případě, že dojde ke změně zpracování, vnitřních či vnějších podmínek (např. při změně právních předpisů) a alespoň 1x ročně její revizi.

4.4 Správce informačních technologií

Správce informačních technologií:

1. spolupracuje s garantem ochrany osobních údajů, vedoucími zaměstnanci a odpovědnými osobami při ochraně osobních údajů uložených v datové podobě,
2. zabezpečuje zřizování přístupů k systémům pro automatizované zpracování osobních údajů,
3. zabezpečuje likvidaci dat v rámci informačních systémů pro zpracování osobních údajů, včetně stanovení zálohovacích cyklů a životnosti médií,
4. neprodleně oznamuje garantovi ochrany osobních údajů případy porušení zabezpečení osobních údajů.

4.5 Pověřené osoby

Pověřené osoby jsou povinny v rámci plnění svých povinností vyplývajících z jejich vztahu ke Správci plnit i opatření k ochraně osobních údajů stanovená Obecným nařízením o ochraně osobních údajů, dalšími obecně závaznými právními předpisy a vnitřními předpisy Správce, zejména:

1. zachovávat mlčenlivost o osobních údajích a přijatých technických a organizačních opatřeních k jejich ochraně, o nichž se v souvislosti se svým zaměstnáním, postavením nebo funkcí dozvěděly, a to i po skončení svého pracovněprávního vztahu nebo zániku funkce,
2. zpracovávat osobní údaje za podmínek a v rozsahu jim stanoveném (např. v souladu s platnými přístupy do systémů pro automatizované zpracování osobních údajů),
3. osobní údaje shromažďovat a dále zpracovávat přiměřené, relevantně a s omezením na nezbytný rozsah a po nezbytnou dobu ve vztahu k účelu, pro který jsou zpracovávány,
4. při shromažďování osobních údajů od subjektů údajů:
 - a. vyžadovat jejich předchozí souhlas se zpracováním osobních údajů, není-li zpracování možné bez tohoto souhlasu,
 - b. poskytnout subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků v okamžiku získání osobních údajů veškeré Obecným nařízením o ochraně osobních údajů požadované informace a sdělení,
5. při zpracování osobních údajů:
 - a. zpracovávat pouze přesné osobní údaje; v případě zjištění, že zpracováváné osobní údaje nejsou přesné, zpracování zablokovat do doby jejich opravy nebo doplnění,
 - b. nesdružovat osobní údaje získané k rozdílným účelům,
 - c. ukládat dokumenty v listinné podobě a nosiče informací v elektronické podobě obsahující osobní údaje do určených úschovných objektů a na určená místa; při práci s nosiči informací postupovat tak, aby jiná osoba nemohla zneužít tyto nosiče informací jako zdroj informace (dle zásad „čistého stolu“ a „prázdné obrazovky“),

6. nepořizovat kopie dokumentů v listinné podobě nebo nosičů informací s osobními údaji či osobních údajů samých pro jinou, než pracovní potřebu nebo výkon funkce a ani to umožňovat jiným; s takovými kopiemi nakládat stejně jako s originálem,
7. neumožnit zpracování osobních údajů jiné osobě, která není pro konkrétní účel zpracování pověřenou osobou,
8. osobní údaje v listinné i elektronické formě předávat nebo poskytovat:
 - a. pouze pověřeným nebo oprávněným příjemcům osobních údajů,
 - b. stanoví-li tak zvláštní právní předpis nebo v souladu s platnou smlouvou,
 - c. pouze předepsaným způsobem,
9. neprodleně oznamují vedoucímu zaměstnanci, v jeho nepřítomnosti garantovi ochrany osobních údajů, případy porušení zabezpečení osobních údajů, násilné vniknutí do objektu s osobními údaji nebo výskyt nepovolané osoby a podle svých možností a schopností zajistí ochranu osobních údajů.

4.6 Ostatní zaměstnanci

Ostatní zaměstnanci, kteří nejsou osobami uvedenými v předchozích částech čl. 4 této směrnice nejsou oprávněni jakýmkoliv způsobem zpracovávat osobní údaje.

Ostatní zaměstnanci jsou v případě náhodného seznámení se s osobními údaji povinni zachovávat mlčenlivost ve stejném rozsahu jako pověřené osoby.

V případě nálezu dokumentu v listinné podobě nebo nosiče informací jsou ostatní zaměstnanci povinni neseznamovat se s jejich obsahem (pokud to okolnost nálezu dovoluje) a předat je neprodleně vedoucímu zaměstnanci. Do jejich předání zajistit jejich ochranu.

V případě bezpečnostního incidentu (např. při porušení zabezpečení osobních údajů, násilné vniknutí do objektu s osobními údaji nebo výskytu nepovolané osoby) jsou povinni neprodleně informovat vedoucího zaměstnance, v jeho nepřítomnosti garanta ochrany osobních údajů a podle svých možností a schopností zajistit ochranu osobních údajů.

Pokud z jednotlivých ustanovení této směrnice nevyplývá něco jiného, platí povinnosti uvedené v tomto článku i pro osoby uvedené v předchozích částech čl. 4 této směrnice.

5 Pravidla pro uživatele při automatizovaném zpracování osobních údajů

Pokud nejsou obecně závaznými právními předpisy nebo vnitřními předpisy Správce upravena pravidla pro automatizované zpracování osobních údajů, použijí se pravidla uvedená v čl. 5.1 až 5.3 této směrnice. Pokud tato směrnice stanoví přísnější pravidla než pravidla uvedená v ostatních vnitřních předpisech Správce, platí pravidla uvedená v této směrnici.

5.1 Zákaz

Všechny komponenty počítačové sítě jsou vlastnictvím Správce, případně k nim Správce vlastní či vykonává práva užívání. Zákaz krádeže a vandalismu (poškození) se pak vztahuje na elektronickou podobu dat a informací, stejně jako na vlastní fyzické prostředky.

Uživatelům je zakázáno:

- Používat k provozu v síti Správce nepovolené zařízení, nebo zařízení nedostatečně zabezpečené (bez aktualizací operačního systému nebo antivirového programu apod.).
- Svévolně instalovat a používat nevidované programové vybavení, nebo instalační soubory nevidovaných programů ukládat na pevném disku.
- Šířit, nebo se snažit získat nelegální software.
- Pracovat s uživatelským jménem a heslem, které jim nebylo přiděleno.
- Obcházet bezpečnostní funkce. Bránit operačnímu systému nebo antivirovému programu v provádění automatických aktualizací.
- Provádět neautorizované a neschválené kopírování i částí programového vybavení nebo dat, k nimž Správce vykonává vlastnická práva, resp. práva k užívání.
- Provádět neautorizované modifikace programů, dat nebo technického vybavení v majetku či užívání Správce. Zvláště přísně jsou pak zakázány neautorizované změny konfigurace počítačů či jiných prostředků, které by mohly mít vliv na provoz celé sítě.
- Poškozovat nebo ničit počítačové prostředky (počítače, programové vybavení i komunikační linky).
- Odposlouchávat provoz a vytvářet kopie zpráv či dat procházejících jednotlivými uzly sítě.
- Instalovat programy nebo technická zařízení, která monitorují činnost jiných uživatelů nebo serverů, případně jinak zasahovat do oblasti sítě.
- Využívat síť Správce ke komerčním účelům, nebo rozesílat nevyžádanou poštu (SPAM).
- Používat počítačových prostředků Správce k činnostem namířeným proti jakékoliv další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím počítačové sítě nebo sítě Internet.

5.2 Zodpovědnost

Pověřené osoby zodpovídají za:

1. Uchování v tajnosti všech neveřejných informací Správce.
2. Úplnost přiděleného zařízení a jeho správné používání.
3. Používání legálního a řádně evidovaného software.
4. Zálohování lokálně uložených uživatelských dat.
5. Škody způsobené úmyslně či z nedbalosti.

Uživatelé jsou povinni:

1. Pro přístup do sítě Správce používat pouze povolená zařízení a přidělené přihlašovací údaje.
2. Dodržovat zejména tato pravidla provozu v síti:
 - a. Antivirovým programem testovat stahované soubory, pravidelně spouštět testy pevných disků a kontrolovat používané nosiče při jejich vkládání a vyjímání.
 - b. Při virové nákaze nebo neobvyklém chování zařízení jej okamžitě odpojit od sítě, a tuto skutečnost neprodleně nahlásit vedoucímu zaměstnanci.
 - c. Při zjištění porušení zásad stanovených touto směrnicí, jinými vnitřními předpisy Správce, obecně závaznými právními předpisy nebo při podezření na zneužívání sítě Správce okamžitě informovat vedoucího pracovníka.

5.3 Postupy

Oprávnění k užívání informačního systému.

1. Pověřená osoba se stává uživatelem získáním oprávnění k užívání informačního systému. Uživatel, kterému je účet zřízen, získá heslo, které je povinen udržovat v tajnosti.
2. V případě prozrazení hesla (či sebemenší domněnce, že jeho heslo bylo prozrazeno) uživatel neprodleně informuje vedoucího zaměstnance, změní heslo nebo zažádá o změnu hesla.

Pro používání hesel platí tato pravidla:

1. Heslo musí být uchováno v tajnosti a zodpovědnost za všechny činnosti, související s použitím identifikátoru a hesla, má jeho vlastník.
2. Heslo k vlastnímu účtu uživatel nesmí sdělit druhé osobě.
3. Heslo musí být zvoleno tak, aby nebylo snadné je odhalit. Nepoužívají se běžná slova, jména nebo čísla spojená s uživatelem, a to ani jejich kombinace.
4. Heslo musí být změněno, když existuje možnost, že mohlo být vyzrazeno.
5. Nepoužívá se stejný login a heslo v aplikaci Správce a v aplikaci na internetu.
6. Nepoužívá se stejné heslo do několika aplikací.
7. Heslo se nezapisuje na papír. Pokud je heslo zapsáno, musí být bezpečně uschováno, např. v zalepené obálce v trezoru.
8. Nepoužívají se funkce a programy pro zapamatování hesel, použití kombinace kláves pro vyvolání hesla apod.
9. V případě, kdy jsou dodávány technické nebo programové prostředky s heslem nastaveným výrobcem, musí být toto heslo okamžitě po převzetí (instalaci) změněno.
10. V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je povinností uživatele změnit toto heslo při prvním přihlášení.

6 Výkon práv subjektu údajů

Subjekty údajů se mohou obracet na Správce a požadovat:

1. přístup k osobním údajům,
2. opravu osobních údajů,
3. výmaz osobních údajů,
4. omezení zpracování,
5. přenositelnost údajů,
6. uplatnění námitky proti zpracování,
7. nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, příp.
8. jiné, výše neuvedené požadavky.

Veškeré žádosti subjektu údajů je oprávněn přijímat a rozhodovat o nich garant ochrany osobních údajů a v jeho nepřítomnosti je žádosti oprávněn přijímat příslušný vedoucí zaměstnanec, s výjimkou dále uvedených případů:

1. Žádá-li subjekt údajů o přístup k osobním údajům vedoucího zaměstnance, žádost přijme, ověří totožnost žadatele, oprávněnost jeho žádosti, které případně sám ve stanovené lhůtě vyhoví. O této skutečnosti vyrozumí garanta ochrany osobních údajů.
2. Pokud subjekt údajů požádá o opravu osobních údajů pověřenou osobu, pověřená osoba žádost přijme, ověří totožnost žadatele a pokud je to možné, provede opravu osobních údajů nebo jejich opravu zajistí. O této skutečnosti vyrozumí vedoucího zaměstnance a garanta ochrany osobních údajů, který zajistí vyrozumění subjektu údajů.

V ostatních případech jsou zaměstnanci povinni:

1. Při osobním podání zajistit, aby žádost osobně převzali v následujícím pořadí:
 - a. garant ochrany osobních údajů, nebo
 - b. vedoucí zaměstnanec, nebo
 - c. pověřená osoba.
2. Nelze-li uplatnit předchozí pravidlo, přijme zaměstnanec žádost sám za splnění následujících podmínek:
 - a. ověří totožnost žadatele,
 - b. pokud žadatel žádá o potvrzení převzetí, potvrdí jej svým podpisem spolu s uvedením data a hodiny převzetí na výtisku, který zůstává žadateli a stejné údaje uvede na převzaté žádosti,
 - c. žádost ihned předá vedoucímu zaměstnanci, v jeho nepřítomnosti garantovi pro ochranu osobních údajů.

3. V případě přijetí podání bez osobní účasti žadatele, zajistí zaměstnanec, kterému byla žádost doručena, její neprodlené předání vedoucímu zaměstnanci nebo garantovi pro ochranu osobních údajů.

7 Závěrečná ustanovení

7.1 Kontrola dodržování ustanovení směrnice

Vedoucí zaměstnanci Správce zajistí kontrolu plnění povinností vyplývajících z ustanovení této směrnice v mezích své působnosti.

7.2 Revize směrnice

Revize této směrnice musí být provedena:

- a. při změně právního předpisu s dopadem na oblast ochrany osobních údajů,
- b. při změně vnitřního předpisu Správce s dopadem na oblast ochrany osobních údajů nebo v případě jiných organizačních opatření (např. změna rozsahu osob s přístupem k osobním údajům, změna místa zpracování, ...),
- c. v případě bezpečnostního incidentu, kterým byla napadena ochrana osobních údajů, ať už přímo nebo nepřímo, a to bez ohledu na skutečnost, zda došlo k zpřístupnění nebo předání osobních údajů neoprávněné osobě,
- d. nejméně jedenkrát ročně, pokud nenastala okolnost uvedená v písm. a) až c).

Za zpracování, prosazení, údržbu a revize této směrnice odpovídá garant ochrany osobních údajů.

7.3 Audit směrnice

K prověření shody ustanovení této směrnice s reálným stavem v rámci Správce se provede audit.

Provádění interních i externích auditů se řídí vnitřními předpisy Správce.

7.4 Účinnost směrnice

Tato směrnice nabývá platnosti dnem jejího vydání a účinnosti ke dni 23. května 2018.

8 Příloha č. 1

Popis zpracování osobních údajů obsahuje minimálně tyto údaje:

- Název zpracování
- Vedoucí zaměstnanec
- Odpovědná osoba
- Osoby s oprávněným přístupem k osobním údajům, příp. rozsah oprávnění ke zpracování
- Účel zpracování
- Kategorie subjektu údajů
- Příjemci osobních údajů
- Zpracovatelé, příp. společní správci
- Zda a za jakých podmínek dochází k předávání osobních údajů do třetích zemí nebo mezinárodní organizaci
- Druh a kategorie osobních údajů
- Právní základ zpracování podle čl. 6 odst. 1, 9 odst. 2 nebo 10 Obecného nařízení o ochraně osobních údajů
- V případě zpracování podle čl. 6 odst. 1 písm. f) Obecného nařízení o ochraně osobních údajů oprávněné zájmy správce nebo třetí osoby
- Zdroje osobních údajů
- Způsob zpracování
- Využívání profilování nebo automatizovaného rozhodování, vč. použitého postupu, významu a příp. důsledků pro subjekty údajů
- Doba uložení osobních údajů nebo kritéria pro její určení