



Parmská 390, 109 00 Praha 10

SMĚRNICE

ředitelky

Centra sociální a ošetrovatelské pomoci Prahy 15

č. 01/2018

S účinností od 25.5.2018 vydávám směrnici č. 01/2018 s názvem „Zpracování osobních údajů a jejich ochrana“.

PhDr. Monika Váilková

ředitelka

Obdrží dle rozdělovníku:

- č. 1 - ředitelka
- č. 2 - vedoucí ekonomicko-provozně-technického úseku
- č. 3 - vedoucí sociálně-ošetrovatelského úseku
- č. 4 - vedoucí sociálně-pečovatelského úseku
- č. 5 - ekonom
- č. 6 - účetní
- č. 7 - pokladní
- č. 8 - administrativní pracovnice
- č. 9 - hospodářka
- č. 10 - referentka majetku
- č. 11 - pověřenec GDPR

Tato směrnice upravuje nakládání s osobními údaji v Centru sociální a ošetřovatelské pomoci Praha 15, příspěvková organizace, IČO: 68405162, se sídlem Parnská 390, 109 00 Praha 10 (dále jen „Správce“).

Tato směrnice je jako vnitřní předpis závazná pro všechny zaměstnance Správce. Tato směrnice stanovuje taková opatření a pravidla, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů spravovaných a zpracovávaných Správцем. Tato směrnice se zabývá ochranou všech osobních údajů ve zpracovávaných Správцем, bez ohledu na formu jejich předání nebo uchování.

I. Pojmy

Pro účely této směrnice se rozumí:

„**osobními údaji**“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě; 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;

„**subjektem údajů**“ fyzická osoba, ke které se osobní údaje vztahují;

„**zvláštními kategoriemi osobních údajů**“ osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby, trestních deliktech či pravomocném odsouzení;

„**biometrickými údaji**“ osobní údaje týkající se fyzických či fyziologických znaků chování fyzické osoby, které umožňují jedinečnou identifikaci (např. zobrazení obličeje, otisk prstu);

„**genetickými údaji**“ údaje týkající se zděděných, nebo získaných genetických znaků určité fyzické osoby, které vyplývají z analýzy biologického vzorku dotčené fyzické osoby.

„**zpracováním**“ jakákoliv operace s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, omezení, výmaz nebo zničení;

„**omezením zpracování**“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

„**Nařízením**“ 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;

„**pseudonymizací**“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

„**anonymizací**“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů a subjekt údajů není nebo již přestal být identifikovatelným;

„**evidencí**“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního hlediska;

„**zpracovatelem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

„**příjemcem**“ fyzická nebo právnická osoba, orgán veřejné moci, nebo jiný subjekt, kterým jsou osobní údaje poskytnuty;

„**porušením zabezpečení osobních údajů**“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

„**údaji o zdravotním stavu**“ osobní údaje týkající se tělesného, nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o zdravotním stavu,

„**dozorovým úřadem**“ Úřad pro ochranu osobních údajů.

II.

Zásady zpracování osobních údajů

1. Osobní údaje jsou zpracovávány vždy pouze v tom rozsahu, který je nezbytný pro splnění účelu, pro který jsou zpracovávány.
2. Správce požaduje od subjektu údajů vždy pouze osobní údaje, které jsou relevantní vzhledem k účelu zpracování. Zásadu zpracování pouze relevantních osobních údajů a zásadu zpracování osobních údajů pouze v rozsahu nezbytném pro splnění účelu Správce dodržuje též v případě, že osobní údaje nebyly získány přímo od subjektu údajů.
3. Osobní údaje jsou zpracovávány s dostatečnou pečlivostí, aby nedocházelo k nepřesnostem.
4. Osobní údaje jsou zpracovávány pouze po dobu nezbytnou ke splnění účelu, pro který jsou zpracovány.
5. Při zpracování osobních údajů je dbáno o jejich náležitě zabezpečení a jejich ochranu zabezpečují přiměřená technická zabezpečení ve formě fyzického zabezpečení i ve formě informačních technologií a přiměřená organizační opatření.

III.

Důvody zpracování osobních údajů

1. Zpracování osobních údajů Správcem je možné pouze ze zákonných důvodů vymezených v ustanovení čl. 6 odst. 1 písm. a) až f) Nařízení. V největším rozsahu budou osobní údaje zpracovávány Správcem za účelem splnění smlouvy, za účelem splnění právní povinnosti, která se na správce vztahuje, a dále za účelem splnění smlouvy a na základě souhlasu subjektu údajů a oprávněného zájmu Správce.
2. Správce získává osobní údaje jak od subjektu údajů, tak od jiného subjektu (např. z veřejných rejstříků).
3. V případě, že bude zpracování osobních údajů probíhat na základě souhlasu, musí být žádost o udělení souhlasu předložena Správcem subjektu údajů jednoznačná a snadno jazykově srozumitelná tak, aby subjektu údajů bylo zřejmé, pro jaký účel je zpracování osobních údajů vyžadováno.
4. Správce musí subjektu údajů připravit takové podmínky, aby při udělení souhlasu mohl jednat zcela svobodně. Správce nesmí žádat o udělení souhlasu ke zpracování osobních údajů ve větším rozsahu, než který je nezbytný pro splnění účelu, pro který mají být osobní údaje zpracovány.
5. Pozvánky na akce pořádané Správcem a jiné aktuality o aktivitách Správce mohou být subjektu údajů zasílány vždy pouze na základě jeho souhlasu. Subjekt údajů má právo souhlas kdykoliv odvolat.

6. Při pořizování jakýchkoliv záznamů z akcí pořádaných v prostorách Správce, Správce zajistí informování účastníků o pořizování této dokumentace a uvedení účelu tohoto pořízení a vyžádá si souhlas dotčených subjektů údajů. Zveřejňování fotografií z akcí pořádaných Správcem na webových stránkách Správce a v Hlasateli Prahy 15 apod. je možné jen na základě písemného souhlasu subjektu údajů.

IV.

Záznamy o činnostech zpracování osobních údajů

1. Správce vede záznamy o činnostech zpracování osobních údajů. Tyto záznamy o činnostech vede písemně. Za písemnou formu se považuje i forma elektronická.
2. Správce na požádání poskytne tyto záznamy o činnostech dozorovému orgánu.
3. Záznamy o činnostech obsahují tyto informace:
 - a) identifikační a kontaktní údaje Správce a případného společného správce, či zástupce správce a pověřence pro ochranu osobních údajů je-li jmenován;
 - b) účely zpracování;
 - c) popis kategorií subjektů údajů a kategorií osobních údajů;
 - d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
 - e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a příp. doložení vhodných záruk;
 - f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
 - g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření k zabezpečení osobních údajů.
4. Správce aktualizuje záznamy o činnostech zpracování osobních údajů dle potřeby, nejméně 1x ročně.

V.

Zabezpečení osobních údajů a porušení tohoto zabezpečení

1. Ochrana osobních údajů je zaručena na základě přiměřených technických a organizačních opatření k zabezpečení zpracování osobních údajů. Při výběru vhodných technických a organizačních opatření Správce přihledne ke stavu techniky, nákladům na provedení opatření, povaze, rozsahu, kontextu a účelům zpracování osobních údajů, a také k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.
2. Za účelem ochrany osobních údajů má Správce definován tzv. systém řízení ochrany osobních údajů, fungující v souladu s těmito interními předpisy:
 - a) organizační řád
 - b) spisový řád a skartační plán,
 - c) tato směrnice.
3. K předání osobních údajů do zahraničí nedochází, zpracování probíhá výlučně na území ČR.
4. Osobní údaje zaměstnanců, které jsou zaznamenány na dokumentech v listinné podobě zařazené v personálních složkách, jsou uchovávány v registrační skříni v kanceláři ředitele Správce. Ředitel Správce umožní přístup k těmto osobním údajům jen pověřeným osobou vykonávajícím personální a účetní agendu. V době nepřítomnosti ředitele Správce je kancelář uzamčena. Osobní údaje zaměstnanců, které jsou zaznamenány na dokumentech v listinné podobě nezbytné pro výkon mzdové agendy, jsou uchovávány v trezoru. Klíč k trezoru má pouze účetní, v době nepřítomnosti účetní a po skončení pracovní doby je klíč uložen u ředitele Správce v uzamčené kanceláři.
5. Osobní údaje obsažené ve složkách týkajících se účetnictví jsou uloženy v uzamykatelné skříni, do které má přístup účetní.

6. V případě služby Sociálně ošetřovatelské jednotky a Domu zvláštního režimu Správce zpracovává též osobní údaje obsažené ve zdravotní dokumentaci, ke které mají přístup pouze sestry. Pouze sestry mají přístup k jednotlivým kartám klientů, kterým je poskytována služba Sociálně ošetřovatelské jednotky nebo Domu zvláštního režimu. Zdravotní dokumentace a karty klientů jsou uzamčeny a je k dispozici pouze jeden klíč, který je uložen v trezoru. V případě poskytování pečovatelské služby Správce vede karty klientů, ke kterým mají přístup sestry a ošetřovatelé, k dispozici je 1 klíč, uložen v trezoru. Přístupy ke klíči -číselný kód sester, nebo pečovatelů. V nepřítomnosti je kancelář uzamčena.
7. Dále Smlouvy a karty všech klientů v písemné formě jsou umístěny v kanceláři sociální pracovnice v uzamykatelné skříni, ke které náleží jeden klíč. V době její nepřítomnosti je kancelář uzamčena.
8. Interní počítačová síť Správce a další IT systémy jsou chráněny přiměřenými technickými opatřeními proti útokům zvenčí. Tato technická opatření vychází z bezpečnostní strategie stanovené správcem sítě a schválené Správcem. Správce sítě má na starosti provoz a údržbu systémů a aplikací, archivaci a zabezpečení (elektronických) dat uživatelů počítačové sítě. Správce sítě má přístup ke všem datům uloženým v počítačové síti Správce nebo na elektronických zařízeních, pomocí nichž jsou tato data zpracovávána. Správce sítě spolupracuje s jednotlivými uživateli osobních údajů při ochraně osobních údajů uložených v osobních počítačích, včetně těch přenosných. V případě, že je správcem sítě poskytovatel externích služeb, musí být se Správcem sítě uzavřena zpracovatelská smlouva ve smyslu čl. 28 odst. 3 Nařízení.
9. Interní počítačová síť je nastavena tak, aby každý konkrétní uživatel měl přístup pouze k těm osobním údajům, které se vztahují k jeho činnosti pro Správce. Počítače musí být zabezpečeny heslem. Každý uživatel má přiděleno vlastní heslo, které uchovává v tajnosti a v návaznosti na výzvy Správce sítě provádí jeho úpravu.
10. Interní počítačovou síť mohou využívat pouze Správcem autorizovaní uživatelé, přistupující do sítě na základě přihlašovacích údajů přidělených správcem sítě. Přihlašovací údaje jsou vázány na konkrétní osobu a jsou nepřenosné.
11. Uživatel je oprávněn užívat síť, svěřenou výpočetní techniku a programové vybavení výlučně k plnění pracovních úkolů, výkonu státní služby nebo k plnění smlouvy sjednané se Správcem, a to v rozsahu svého uživatelského oprávnění a přístupových práv.
12. Vzdálený přístup je možný pouze na základě souhlasu správce sítě a Správce a uživatel musí dodržovat přiměřená bezpečnostní opatření, aby nedošlo k útokům zvenčí a aby přístup do sítě nedostaly osoby, které k tomu nejsou oprávněné. Zejména se uživatel nebude připojovat přes nezabezpečené připojení, vyloučí funkci před vyplňování hesla atd. Elektronická zařízení, přes které je uživateli umožněn vzdálený přístup, uživatel neopouští bez dozoru nebo nezabezpečená heslem.
13. Při zjištění porušení pravidel provozu sítě má správce sítě právo omezit uživatelská práva nebo i zabránit uživateli v přístupu do sítě nebo v používání konkrétního zařízení.
14. Po ukončení zaměstnaneckého poměru nebo jiného právního vztahu, na jehož základě uživatel obdržel přístupová hesla do sítě a pracovní emailovou adresu, jsou jeho přístupy zneplatněny, a jeho uživatelský účet a pracovní emailová adresa jsou smazány, a to nejpozději do 3 dnů od ukončení zaměstnaneckého poměru nebo jiného právního vztahu.
15. Zaměstnanci a další osoby, kterým jsou zpřístupněny osobní údaje zpracováváné Správcem, nejsou oprávněni si vytvářet vlastní databáze bez souhlasu Správce a bez souhlasu Správce vynášet osobní údaje v listinné podobě nebo na datových nosičích mimo pracoviště. Zaměstnanec je povinen při tisku písemností obsahujících osobní údaje neopouštět vytištěné dokumenty bez dozoru u tiskárny.
16. Zaměstnanci nejsou oprávněni přeposílat písemnosti obsahující osobní údaje do své nebo cizí soukromé emailové schránky.
17. Data obsahující osobní údaje zaměstnanci nesmí ukládat na sdílené disky v síti.
18. Zaměstnanci jsou povinni neopouštět volně položené písemnosti obsahující osobní údaje bez dozoru na svém pracovním stole a náležitě je zabezpečit proti neoprávněnému přístupu jiných osob.

19. Dokumentaci obsahující osobní údaje v elektronické podobě je povoleno předávat příjemcům mimo Správce pouze prostřednictvím datových schránek. V případech, kdy není možné dokumentaci předat prostřednictvím datové schránky nebo ve fyzické podobě, lze dokumentaci předat v podobě šifrovaného zaheslovaného souboru (např. zip).
20. V případě, že zaměstnanec nebo osoba, které byl přidělen uživatelský přístup pro účely plnění smlouvy, zjistí, že došlo k porušení zabezpečení osobních údajů, neprodleně, nejpozději pak do 48 hodin, tuto skutečnost oznámí svému nadřízenému nebo jeho zástupci v případě nepřítomnosti nadřízeného, který informuje vedení.
21. Správce ohlašuje jakékoliv porušení zabezpečení osobních údajů dozorovému úřadu, a to bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o tomto porušení zabezpečení dozvěděl. Ohlášení nemusí být provedeno, je-li nepravděpodobné, že by toto porušení mělo na za následek riziko pro práva a svobody fyzických osob. Pokud Správce provede ohlášení později, uvede spolu s ohlášením dozorovému úřadu i důvody pozdního ohlášení.
22. V ohlášení porušení zabezpečení osobních údajů dozorovému úřadu Správce uvede:
 - a) povahu porušení zabezpečení osobních údajů, a pokud je to možné, i kategorie a přibližný počet dotčených subjektů údajů a přibližné množství dotčených záznamů osobních údajů;
 - b) jméno a kontaktní údaje kontaktního místa, které může poskytnout bližší informace o porušení (např. příslušného zpracovatele) a pověřence pro ochranu osobních údajů, je-li jmenován;
 - c) pravděpodobné důsledky daného porušení;
 - d) opatření, která Správce přijal k nápravě, případně ke zmírnění možných nepříznivých dopadů.
23. Každé porušení zabezpečení osobních údajů musí být Správce řádně zdokumentováno, včetně informací o přijatých nápravných opatřeních.
24. Jakmile se Správce o porušení zabezpečení osobních údajů dozví, provede posouzení rizika, které toto porušení představuje pro práva a svobody fyzických osob. Pokud z výsledku posouzení vyplývá, že porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí dané porušení i subjektu údajů. Oznámení učiní jasně, srozumitelně a s použitím jednoduchých jazykových prostředků.
25. Správce není povinen oznámení subjektu údajů učinit, pokud zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením, která je činí nesrozumitelnými pro osoby neoprávněné k nakládání s nimi (např. šifrování). Dále není Správce povinen oznámení subjektu údajů učinit v případě, že přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se pravděpodobně již neprojeví, a dále pokud by to představovalo nepřiměřené úsilí.

VI.

Posouzení vlivu na ochranu osobních údajů

V případě, že Správce vyhodnotí, že je pravděpodobné, že určitý druh zpracování osobních údajů (zejména při využití nových technologií) bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů v souladu s ustanovením čl. 35 Nařízení.

VII.

Povinnosti Správce ve vztahu k subjektům údajů a práva subjektů údajů

1. Správce poskytuje subjektům údajů informace a sdělení stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků. Informace a sdělení může Správce subjektům údajů poskytovat písemně, ve vhodných případech i elektronicky nebo ústně, pokud si ověří totožnost příslušného subjektu údajů.

2. Správce musí na žádost subjektu údajů o informace a sdělení reagovat bez zbytečného odkladu, nejpozději však do 30 dnů od obdržení takové žádosti. V odůvodněných případech může Správce tuto lhůtu prodloužit, nejdéle však o 30 dnů. Správce o prodloužení lhůty informuje subjekt údajů, a to 30 dnů od obdržení žádosti subjektu údajů a sdělí subjektu údajů důvody tohoto prodloužení. V případě, že subjekt údajů podá žádost o informace a sdělení elektronicky, Správce mu je poskytne elektronicky, ledaže subjekt údajů nepožádá o jiný způsob poskytnutí informací a sdělení, např. písemně.
3. Pokud subjekt údajů žádá Správce o přijetí určitých opatření (opravu jeho osobních údajů, jejich výmaz apod.) a Správce takové opatření nepřijme, informuje o tom subjekt údajů neprodleně, nejpozději do 30 dnů od obdržení žádosti o přijetí příslušného opatření, a to včetně důvodů neprovedení těchto opatření a také informace o možnosti subjektu údajů podat stížnost u dozorového úřadu, příp. se obrátit na soud.
4. V případě, že Správce získá osobní údaje přímo od subjektu údajů, sdělí při jejich získání subjektu údajů následující informace:
 - a) identifikační a kontaktní údaje Správce a případného zástupce Správce;
 - b) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;
 - c) oprávněné zájmy Správce nebo třetí strany v případě, že je zpracování nezbytné pro účely oprávněných zájmů Správce, či třetí osoby;
 - d) případné příjemce nebo kategorie příjemců osobních údajů;
 - e) případný úmysl Správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Evropské komise, že tato třetí země nebo mezinárodní organizace poskytuje odpovídající ochranu osobním údajům, dále pak odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.
5. Pokud je to nezbytné pro zajištění spravedlivého a transparentního zpracování, Správce poskytne subjektu údajů i další informace, zejména dobu zpracování osobních údajů, příp. kritéria pro její stanovení, dále pak informace o právu subjektu údajů na opravu osobních údajů, jejich výmaz apod.
6. V případě, že Správce nezíská osobní údaje přímo od subjektu údajů, sdělí při jejich získání subjektu údajů informace uvedené v odst. 4 písm. a), b), d) a e) tohoto článku.
7. Správce informuje subjekt údajů o změně účelu zpracování osobních údajů, kdykoliv k ní dojde.
8. Správce je povinen dát subjektu údajů na požádání potvrzení o tom, zda Správce osobní údaje, které se ho týkají, zpracovává, a pokud ano, zajistit subjektu údajů přístup k těmto údajům a poskytnout následující informace:
 - a) účely zpracování;
 - b) kategorie dotčených osobních údajů;
 - c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;
 - d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
 - e) existence práva požadovat opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;
 - f) právo podat stížnost u dozorového úřadu;
 - g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů.
9. Správce je povinen poskytnout subjektu údajů kopii zpracovávaných osobních údajů. Za poskytnutí dalších kopií dle předchozí věty může Správce požadovat po subjektu údajů úhradu přiměřeného administrativního poplatku.
10. Správce je povinen bez zbytečného odkladu opravit nepřesné osobní údaje a doplnit neúplné osobní údaje, jsou-li mu známy.
11. Správce je povinen bez zbytečného odkladu vymazat osobní údaje, týkající se subjektu údajů, pokud je naplněn jeden z následujících důvodů:

- a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
 - b) subjekt údajů odvolá souhlas, pokud byly osobní údaje zpracovávány na základě tohoto souhlasu, a neexistuje žádný další právní důvod pro zpracování;
 - c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
 - d) osobní údaje byly zpracovány protiprávně;
 - e) osobní údaje musí být vymazány za účelem splnění právní povinnosti stanovené právem Evropské unie nebo právním řádem České republiky.
12. V případě, že Správce osobní údaje subjektu údajů zveřejnil a je povinen je vymazat, musí Správce přijmout (s ohledem na dostupnou technologii a náklady) přiměřené kroky k tomu, aby informoval jiné správce osobních údajů, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje a jejich kopie.
13. Správce však není povinen splnit povinnosti dle odst. 11 a 12 tohoto článku, pokud je zpracování osobních údajů pro něj nezbytné, např. pro splnění právní povinnosti, jež vyžaduje zpracování osobních údajů právem Evropské unie nebo právním řádem České republiky, které se na Správce vztahuje, nebo pro určení, výkon nebo obhajobu svých právních nároků apod.
14. Správce je povinen omezit zpracování osobních údajů subjektu údajů, pokud:
- a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby mohla být ověřena přesnost osobních údajů;
 - b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
 - c) Správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
 - d) subjekt údajů vznesl námitku proti zpracování, a to do doby, dokud nebude ověřeno, zda oprávněné důvody Správce pro zpracování převažují nad oprávněnými důvody subjektu údajů.
15. V případě, že Správce přistoupil k omezení zpracování osobních údajů dle předchozího odstavce, mohou být tyto osobní údaje zpracovávány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Evropské unie nebo některého členského státu Evropské unie.
16. O zrušení omezení zpracování Správce informuje subjekt údajů předem.
17. Správce je povinen oznámit jednotlivým příjemcům osobních údajů informace o všech opravách nebo výmazech osobních údajů, o omezení zpracování osobních údajů, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce rovněž informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.
18. V případě, že subjekt údajů vznese námitku proti zpracování osobních údajů, které Správce zpracovává na základě oprávněných zájmů, Správce přestane tyto osobní údaje zpracovávat, pokud neprokáže oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů.

VIII.

Doba uložení osobních údajů

1. Doba uložení osobních údajů se řídí právními předpisy, které stanovují povinnost archivace, a interními předpisy Správce, zejména archivačním a skartačním řádem. Pokud nestanoví právní předpisy a interní předpisy zvláštní dobu archivace, činí nejdelší přípustná délka doby archivace 5 let. Tato doba je dostatečná pro to, aby se Správce dozvěděl, zda v souvislosti předmětným případem zpracování osobních údajů nebyl zahájen soudní spor nebo správní řízení, ve kterém vůči Správci subjekt údajů uplatňuje svá práva.

2. Doba archivace může být prodloužena v případě, že na tom má Správce oprávněný zájem. Doba archivace se prodlouží vždy v případě, že osobní údaje se vztahují k případu zpracování, v souvislosti s nímž byl zahájen soudní spor, správní, daňové nebo jiné řízení a prodloužení doby archivace je nezbytné pro ochranu práv Správce nebo plnění jeho zákonných povinností.
3. V případě, že jsou na internetových stránkách Správce zveřejněny osobní údaje zaměstnance nebo externího spolupracovníka, budou tyto osobní údaje z internetových stránek smazány do 1 měsíce ode dne, kdy tato osoba svou činnost pro Správce ukončila.
4. Osobní údaje uchazečů o práci jsou archivovány pouze po dobu, kdy probíhá výběrové řízení. Po skončení výběrového řízení Správce přistoupí k výmazu a skartaci, a to ve lhůtě 1 roku.

IX.

Pověřenec pro ochranu osobních údajů

1. Správce jmenuje pověřence pro ochranu osobních údajů. Při jmenování konkrétní osoby jako pověřence pro ochranu osobních údajů Správce přihledne k jeho profesním kvalitám, odborným znalostem práva a praxe v oblasti ochrany osobních údajů a schopnosti plnit úkoly pověřence pro ochranu osobních údajů.
2. Pověřenec pro ochranu osobních údajů:
 - a) poskytuje informace a poradenství Správci, zejména zaměstnancům a státním zaměstnancům, kteří v rámci své činnosti pro Správce vykonávají jednotlivé úkony zpracování, a informuje je o jejich povinnostech podle Nařízení a dalších právních a interních předpisů z oblasti ochrany údajů, a též poskytuje poradenství zpracovatelům Správce, co se týče zpracovávání osobních údajů pro Správce,
 - b) monitoruje soulad koncepcí Správce s Nařízením a dalšími právními a interními předpisy z oblasti ochrany údajů, a to též se zaměřením na rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy osob zapojených do operací zpracování osobních údajů a souvisejících auditů,
 - c) na požádání poskytuje poradenství a vyjadřuje se k posouzení vlivu na ochranu osobních údajů
 - d) spolupracuje s dozorovým úřadem,
 - e) působí jako kontaktní místo pro dozorový úřad v záležitostech týkající se zpracování, včetně předchozí konzultace podle ustanovení článku 36 Nařízení a případně konzultace v jakékoliv jiné věci.
3. Pověřenec pro ochranu osobních údajů bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.
4. Správce zveřejní kontaktní údaje pověřence pro ochranu osobních údajů a sdělí je dozorovému úřadu bez zbytečného odkladu.
5. Správce a zpracovatel zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.
6. Správce podporuje pověřence pro ochranu osobních údajů při plnění jeho úkolů tak, že mu poskytuje zdroje nezbytné k plnění těchto úkolů, poskytuje mu přístup k osobním údajům a operacím zpracování a též zdroje a příležitosti k udržování jeho odborných znalostí.
7. Správce zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů nesmí být pověřenec pro ochranu osobních údajů Správcem propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídicím pracovníkům Správce.
8. Subjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle tohoto nařízení.

9. Pověřenec pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů vázán mlčenlivostí. Pověřenec může povinnost mlčenlivosti prolomit, stanoví-li tak právní předpis, je-li to nezbytné pro plnění jeho povinností vůči dozorovému úřadu nebo s tím souhlasí Správce.
10. Pověřenec pro ochranu osobních údajů může být Správcem pověřen též jinými úkoly či povinnostmi, pokud nepovedou ke střetu zájmů.

X.

Požadavky na zpracovatele

1. Správce využívá ke zpracování osobních údajů pouze ty zpracovatele, kteří poskytují dostatečné záruky ochrany osobních údajů, zejména zavedením vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení a aby byla zajištěna ochrana práv subjektů údajů.
2. Se zpracovatelem je uzavírána dohoda o mlčenlivosti, pokud smlouva se zpracovatelem neobsahuje odpovídající ujednání o mlčenlivost. Tato dohoda uzavřena být nemusí v případě, že je zpracovatel vázán profesní mlčenlivostí zakotvenou právními předpisy.
3. Správce může zpracovatelem umožnit zapojení dalšího zpracovatele, a to pouze písemně. Tento požadavek bude zakotven ve smlouvě se zpracovatelem.
4. Smlouva se zpracovatelem musí zohlednit:
 - a) typy osobních údajů, které bude zpracovatel zpracovávat, a kategorie subjektů údajů, ke kterým se vztahují;
 - b) dobu trvání zpracování osobních údajů;
 - c) povahu a účel zpracování osobních údajů;
 - d) práva a povinnosti Správce a zpracovatele.
5. V smlouvě se zpracovatelem se zpracovatel zaváže, že:
 - a) zpracovává osobní údaje pouze na základě doložených pokynů Správce a informuje Správce o případných požadavcích na předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud právní předpisy nestanoví, že toto informování z důležitých důvodů veřejného zájmu není možné;
 - b) zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
 - c) přijme všechna technická a organizační opatření k zabezpečení osobních údajů, tak aby vyhověl požadavkům Nařízení, a zohledňuje povahu zpracování;
 - d) dodrží podmínky pro zapojení dalšího zpracovatele, zejména bude vybírat dalšího zpracovatele se zvláštní pečlivostí a bude od něj požadovat takové záruky, které zabezpečí ochranu osobních údajů aspoň v rozsahu odpovídající úrovni zabezpečení zpracovatele a požadavkům Nařízení;
 - e) poskytne součinnost Správci pro splnění jeho povinnosti vyřídit žádost subjektu údajů vztahující se k výkonu jeho práv a k jednáním s dozorovým orgánem;
 - f) bude se Správcem spolupracovat při posuzování vlivu na ochranu osobních údajů a v otázkách zabezpečení osobních údajů a ohlašování porušení tohoto zabezpečení;
 - g) po ukončení smlouvy podle pokynu Správce buď osobní údaje smaže, nebo je všechny předá Správci, tato povinnost se nevztahuje na osobní údaje, u kterých má zpracovatel povinnost archivace stanovenou právními předpisy;
 - h) poskytne Správci veškeré informace nutné k doložení plnění všech povinností zpracovatele při zpracování osobních údajů a umožní Správci provádění kontroly;
 - i) v případě, že má za to, že určitý pokyn Správce je v rozporu s Nařízením nebo jinými právními předpisy týkajícími se ochrany osobních údajů, neprodleně na to Správce upozorní.

XI.
Kontrolování

1. Správce provádí namátkové kontroly dodržování této směrnice a dalších interních předpisů patřících do systému ochrany řízení ochrany osobních údajů.
2. Zaměstnanci Správce jsou řádně proškolení, co se týče systému ochrany řízení ochrany osobních údajů Správce.
3. Správce bude pravidelně provádět revizi interních předpisů a aktualizovat je.

XII.

Závěrečná ustanovení

Tato směrnice nabývá účinnosti dnem 25. 5. 2018 a v plném rozsahu nahrazuje Směrnicí č. 14/2009.