

SMĚRNICE O OCHRANĚ OSOBNÍCH ÚDAJŮ

ORGANIZACE : Občanská poradna Třebíč, z.s.

ČI 1. ÚČEL SMĚRNICE

- 1.1. Účelem této směrnice je stanovit základní pravidla zpracování osobních údajů ve Společnosti.
- 1.2. Tato směrnice je jedním z organizačních opatření ochrany osobních údajů ve smyslu článku 32 GDPR.
- 1.3. Tato směrnice dále upravuje procesy realizace práva subjektu údajů na přístup k osobním údajům ve smyslu článku 15 GDPR a ohlašování případů porušení zabezpečení osobních údajů ve smyslu článku 33 a 34 GDPR.
- 1.4. Účelem této Směrnice je zároveň stanovit základní pravidla zpracování osobních údajů k ochraně osobních údajů a jejich zabezpečení a řešení porušení zabezpečení zejména v návaznosti na metodický postup a kodex chování, které je součástí Doporučeného postupu č. 02/2018, kterým se v rámci metodického a koncepčního vedení MPSV vypracovává Kodex chování ve smyslu čl. 40 Obecného nařízení o ochraně osobních údajů – GDPR pro potřeby výkonu sociální politiky. Tento doporučený postup je přílohou č. 1 této směrnice. Doporučený postup je přístupný také na internetových stránkách Ministerstva práce a sociálních věcí: www.mpsv.cz.
- 1.5. Konkrétní postupy, procesy a evidence vyplývající z této směrnice jsou řešeny formou příloh, přičemž některé přílohy jsou zveřejňovány spolu se směrnicí, další případně na vyžádání k tomu oprávněnými subjekty po posouzení Organizací.

ČI 2. DEFINICE UŽITÉ VE SMĚRNICI

- 1.1. Za Dozorový úřad je považován Úřad pro ochranu osobních údajů.
- 1.2. Za GDPR se považuje Nařízení Evropského parlamentu a Rady (EU) č. 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).
- 1.3. Za Osobní údaj se považuje jakákoliv 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.
- 1.4. Za Organizaci se považuje Občanská poradna Třebíč, z.s.
- 1.5. Za Pracovníka se považuje každá osoba, včetně právnických osob, která pro Organizaci vykonává jakoukoliv činnost, zejména zaměstnanec, externí spolupracovník, dodavatel apod. Oprávněný pracovník je zaměstnanec Organizace, který zpracovává osobní údaje z pověření Organizace za účelem naplňování hlavního

cíle Organizace, kterým je poskytování odborného sociálního poradenství. Oprávnění pracovníci jsou sociální pracovníci, případně pracovníci v sociálních službách dle definice příslušných zákonů.

- 1.6. Za Subjekt údajů se považuje každá fyzická osoba, včetně osob samostatně výdělečně činných.
- 1.7. Za Zpracování osobních údajů se považuje 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.
- 1.8. Za Příslušnou osobu se považuje zaměstnanec Organizace uvedený v příloze č. 2 této Směrnice, odpovědný za příslušnou agendu v Organizaci.
- 1.9. Další pojmy touto Směrnicí neurčené mají význam ve smyslu GDPR.

ČI 2. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- 2.1. Organizace určuje účel a prostředky zpracování Osobních údajů pro každou evidenci v Organizaci, včetně doby zpracování, nebo kritéria na základě kterých bude tato doba určena, pokud tyto nevyplývají z právního předpisu.
- 2.2. Osobní údaje jsou zpracovávány po dobu určenou v bodu 2.1. v souladu s právními předpisy nebo po dobu trvání důvodu ke zpracovávání osobních údajů správcem.
- 2.3. Evidence o Zpracování osobních údajů je vedena v záznamech o činnostech zpracování vedených dle čl. 30 GDPR, které jsou přílohou č. 4 této směrnice.
- 2.4. Pracovníci jsou povinni zpracovávat Osobní údaje ve vztahu k subjektu údajů korektně a zákonně.
- 2.5. Každý pracovník smí zpracovávat osobní údaje pouze za Organizací určeným účelem, a to pouze Organizací určenými prostředky.
- 2.6. Pracovníci jsou oprávněni zpracovávat Osobní údaje pouze v souladu s pokyny Organizace. Pracovníci smí zpracovávat pouze Osobní údaje nezbytné pro plnění svých povinností vůči Organizaci. Za plnění pokynů Organizace lze považovat také smlouva s doložkou souladu s GDPR. Pokyny Oprávněným pracovníkům organizace jsou vymezeny přílohou č. 5 této směrnice.
- 2.7. Organizace za účelem Zpracování dle bodu 2.6. zřizuje Pracovníkům přístup pouze k nezbytně nutným evidencím osobních údajů.
- 2.8. Má-li Pracovník podezření, nebo dozví-li se, že jsou Osobní údaje jakéhokoliv subjektu údajů nepřesné, neúplné či zastaralé, ohlásí to Příslušné osobě.
- 2.9. Má-li pracovník podezření, nebo dozví-li se, že jsou Osobní údaje zpracovávány déle, než je nezbytné pro účely, pro které jsou zpracovávány, ohlásí to Příslušné osobě.
- 2.10. Tato směrnice se vztahuje na každého Pracovníka organizace, když zpracovává osobní údaje nebo plní jinou činnost, která je upravena v GDPR. Soulad zpracování osobních údajů s GDPR lze nahradit smlouvou, případně doložkou smlouvy o souladu s GDPR.

- 2.11. Každý Pracovník, jehož se tato směrnice dotýká, bude informován o existenci směrnice v organizaci. Každý Oprávněný pracovník bude proškolen o ochraně osobních údajů dle této směrnice ve znění příloh připojených ke dni proškolení a proškolení své osoby stvrdí podpisem v příloze č. 5.
- 2.12. Ukládá-li tato směrnice povinnost osobě oznámit jakoukoliv informaci druhé osobě, provede první osoba oznámení v písemné podobě. Za tuto písemnou podobu se považuje listinný dopis nebo e-mail.

ČI 3. ZÁSADY BEZPEČNOSTI

- 3.1. Pracovník, případně další spolupracující osoby jsou povinny nakládat s Osobními údaji s řádnou péčí, tak aby nedocházelo k únikům Osobních údajů nebo ke zpřístupnění Osobních údajů osobám, které nemají oprávnění. Konkrétní povinnosti a omezení zpracovávají další body směrnice.
- 3.2. Ochrana elektronických dokumentů (evidence) a ochrana před neoprávněným přístupem do sítě je zabezpečena přístupovým heslem, data jsou šifrována, organizace má HW firewall. Spisová služba, e-mailová schránka, elektronický diář a webové stránky organizace jsou chráněny taktéž šifrováním údajů a přístupovými hesly, přičemž do spisové služby Oprávnění pracovníci přistupují pod individuálními přístupovými údaji. Uvedené způsoby práce s elektronickými daty vykonávají pro organizaci Pracovníci na základě smluvních ujednání, přičemž tato ujednání jsou v souladu s nařízením GDPR. Přístupová hesla v organizaci jsou měněna každý 6. měsíc. Osobní údaje jsou ukládány v počítačích Oprávněných pracovníků, přičemž každý pracovník odpovídá za jemu přidělený počítač. Přístupy do počítačů jsou chráněny heslem. V uzamykatelných prostorách Organizace se nachází také úložiště dat, které je proti neoprávněnému přístupu chráněno heslem, přičemž pro každého Oprávněného pracovníka je určen individuální přístup. Organizace pro přenos dat využívá datovou schránku. Přístup do datové schránky má pouze statutární zástupce organizace jako Oprávněný pracovník. Oprávnění pracovníci jsou povinni dodržovat zásady bezpečnosti. Přístupová hesla Oprávnění pracovníci nesdělují třetím osobám ani je neevidují tak, aby mohlo dojít k opatření hesla neoprávněnou osobou. Oprávnění pracovníci odpovídají v pracovní době za přístupy do evidencí, případně dalších systémů, stejně tak v případě přenosu zařízení za jejich bezpečnost a ochranu před neoprávněnými osobami, aktivně zamezují situacím, kdy zařízení může být zcizeno nebo neoprávněné využíváno.
- 3.3. Ochrana před neoprávněným přístupem do prostor Společnosti je zabezpečena uzamykáním vchodových dveří a elektronickým zabezpečovacím systémem. V organizaci jsou prostory vymezené pro pracovníky, které jsou taktéž uzamykatelné. Pro uživatele služeb jsou v organizaci vymezeny prostory, ve kterých nemůže dojít ke kontaktu s osobními údaji třetích osob, nad to v době přítomnosti uživatelů služeb nebo jiných návštěv je v těchto prostorách, ale i prostorách určených pro pracovníky, držena stálá služba z řad Oprávněných pracovníků organizace. Klíče k uzamykatelným prostorám v organizaci mají v dispozici po jednom kusu Oprávnění pracovníci

organizace, klíče od uzamykatelných prostor pro ukládání dokumentů jsou v dispozici Příslušné osoby, která na vyžádání Oprávněných pracovníků do těchto prostor umožní přístup. Po jednom klíči k uzamykatelným prostorům organizace mají také pracovníci úklidové služby, kteří mají do těchto prostor přístup mimo pracovní dobu Oprávněných pracovníků organizace, tedy v době, kdy se v prostorách mimo uzamčené skříně nenacházejí dokumenty obsahující osobní údaje a přístupy do počítačů uložených v těchto prostorách jsou chráněny heslem.

- 3.4. Ochrana analogových dokumentů (evidence) před neoprávněným kopírováním a užitím je zabezpečena uložením v uzamčených prostorách poradny. Během pracovní doby odpovídá každý Oprávněný pracovník za dokumenty obsahující osobní údaje, má-li je z důvodu rozpracovanosti ve své dispozici. V době nepřítomnosti nebo po skončení pracovní doby má Oprávněný pracovník povinnost dokumenty obsahující osobní údaje uložit do uzamykatelné skříně. Dokumenty zaměstnanecké, organizační a dodavatelské agendy jsou v dispozici statutárního zástupce Organizace, chráněny v uzamykatelných prostorách a uzamykatelné skříně. Za ochranu těchto dokumentů zodpovídá statutární zástupce Organizace. Jsou-li písemné dokumenty předávány smluvním Pracovníkům organizace za účelem plnění zákonných povinností, zodpovídá za ochranu těchto údajů Pracovník.
- 3.5. Data předávaná příjemcům dat dle terminologie GDPR jsou předávána v režimu vyžadovaném příjemci.
- 3.6. Osobní mobilní zařízení a osobní počítače mohou být využívány k přístupu do systémů Organizace pouze se souhlasem Příslušné osoby. Za ochranu přístupu k takovému zařízení odpovídá každý Oprávněný pracovník sám.
- 3.7. Tato směrnice se vztahuje na každého Pracovníka Organizace, když zpracovává osobní údaje nebo plní jinou činnost, která je upravena v GDPR.
- 3.8. Každý Pracovník, jehož se tato směrnice dotýká, bude proškolen na ochranu osobních údajů dle této směrnice a proškolení své osoby stvrdí podpisem.

ČI 4. PŘÍSLUŠNÉ OSOBY, OPRAVNĚNÍ PRACOVNÍCI, PRACOVNÍCI ORGANIZACE

- 4.1. Agenda Příslušných osob se skládá zejména z prevence incidentů, zabezpečením zpracování osobních údajů, řešením stížností a žádostí, správou systémů a dalšími činnostmi.
- 4.2. Příslušné osoby jsou uvedeny v příloze č. 1 této Směrnice a obsahuje seznam osob s uvedením rolí.
- 4.3. Oprávnění pracovníci vykonávají agendu služby sociální práce, přičemž při zpracování osobních údajů se řídí touto směrnicí a doporučeným postupem uvedeným v čl. 1 této směrnice. Oprávnění pracovníci jsou uvedeni v příloze č. 2 této směrnice.
- 4.4. Pracovníci vykonávají pro organizaci zejména servisní, případně konzultační činnost, přičemž pravidla ochrany osobních údajů jsou upraveny zejména ve smluvních ujednáních s těmito subjekty a jsou v souladu s nařízením GDPR. V termínech zmíněného zákona pracovníci vystupují k Organizaci jako zpracovatelé osobních

údajů, přičemž Organizace je jejich správcem. Pracovníci jsou uvedeni v příloze č. 3 této směrnice.

ČI 5. ZPRÁVA O POSOUZENÍ VLIVŮ

- 5.1. Pokud bude pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody subjektů údajů, provede Organizace před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.
- 5.2. Zpráva o posouzení vlivů se zpracovává dle čl. 35 a násl. GDPR. Pro soubor podobných operací zpracování, které představují podobné riziko stačí jedno posouzení.
- 5.3. Pokud ze zprávy o posouzení vlivů vyplývá, že by předmětné zpracování osobních údajů mělo za následek vysoké riziko pro práva a svobody subjektů údajů v případě, že by Správce nepřijal opatření ke zmírnění tohoto rizika, Organizace konzultuje zprávu o posouzení vlivů s Dozorovým úřadem.

ČI 6. KOMUNIKACE SE SUBJEKTY ÚDAJŮ

- 6.1. Oprávněný pracovník, který obdržel v jakékoliv formě jakoukoliv žádost či stížnost fyzické osoby, která se týká nebo by se mohla týkat ochrany osobních údajů, zejména žádosti ve smyslu čl. 15–22 GDPR, oznámí tuto skutečnost Příslušné osobě.
- 6.2. Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytnete pověřená osoba v okamžiku získání osobních údajů subjektu údajů informace dle čl. 13 GDPR, v případě, že osobní údaje nebyly získány od subjektu údajů, poskytnete pověřená osoba tyto informace v souladu s čl. 14 odst. 3 GDPR.
- 6.3. Povinnost poskytnout uvedené informace lze splnit odkazem na zásady ochrany osobních údajů Organizace dostupné na internetové adrese Organizace www.optrebic.cz.
- 6.4. Příslušná osoba vyřizuje požadavky subjektů údajů v souladu s obecnými pokyny Organizace, bez zbytečného odkladu, nejdéle však do 1 měsíce, a aby mu byly k vyřízení jeho žádosti poskytnuty veškeré informace a v případě, že žádosti nebylo vyhověno, aby byly sděleny důvody tohoto rozhodnutí.
- 6.5. Pokud není možné dodržet lhůtu, Příslušná osoba tuto skutečnost okamžitě oznámí nadřízenému zaměstnanci, včetně uvedení důvodu, proč není možné lhůtu dodržet, a vyžádá si konzultace, jak správně postupovat dále.
- 6.6. Ověřování identity subjektu údajů bude prováděno vždy přiměřeným způsobem, který zaručí dostatečnou identifikaci subjektu údajů s ohledem na formu podání, využitý komunikační prostředek a obsah žádosti subjektu údajů.
- 6.7. V případě žádosti subjektu údajů o přístup k osobním údajům poskytne příslušná pověřená osoba subjektu údajů nejméně informaci, zda osobní údaje, které se subjektu údajů týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, poskytne mu osobní údaje subjektu údajů a informace o:
 - a) účelu jejich zpracování;

- b) kategoriích dotčených osobních údajů;
 - c) příjemcích nebo kategoriích příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemcích ve třetích zemích nebo v mezinárodních organizacích;
 - d) plánované době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritériích použitých ke stanovení této doby;
 - e) existenci práva požadovat od společnosti opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;
 - f) právu podat stížnost u dozorového úřadu;
 - g) veškerých dostupných informací o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
 - h) skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.
- 6.8. Informace podle tohoto článku poskytuje Organizace subjektu údajů ve stejné formě, v jaké o informace subjekt údajů požádal.
- 6.9. V případě opakovaných žádostí subjektu údajů je subjektu údajů účtováno 100,- Kč za každou opakovanou žádost.

ČI 7. OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ A POSTUP PRO ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ

- 7.1. Jakékoli porušení zabezpečení osobních údajů dle ustanovení čl. 4 odst. 12 GDPR společnost bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděla, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.
- 7.2. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.
- 7.3. Ohlášení dozorovému úřadu se děje prostřednictvím aplikace datové schránky.
- 7.4. Veškeré případy porušení zabezpečení osobních údajů společnost oznámí a konzultuje s DPO.
- 7.5. Ohlášení dozorovému úřadu podle tohoto článku musí přinejmenším obsahovat:
- a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
 - b) jméno a kontaktní údaje místa, které může poskytnout bližší informace;
 - c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
 - d) popis opatření, která Organizace přijala nebo navrhla k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

- 7.6. Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí Organizace toto porušení bez zbytečného odkladu subjektu údajů.
- 7.7. Pracovníci hlásí případy porušení zabezpečení Příslušným osobám.
- 7.8. Organizace přijme opatření k zabránění opakovaného porušení zabezpečení osobních údajů obdobného charakteru.

ČI 8. KONTROLA DODRŽOVÁNÍ SMĚRNICE

- 8.1. Dohled nad dodržováním této směrnice a závazných právních předpisů vykonává Organizace prostřednictvím Příslušných osob.
- 8.2. V případě jakýchkoli pochybností o výkladu této Směrnice či rozsahu a obsahu zákonných povinností poskytuje Organizace závazný výklad, kterým jsou Pracovníci povinni se řídit.

ČI 9. PŘÍLOHY

Součástí směrnice jsou přílohy. Přílohy, na které se odkazuje v textu směrnice jsou číslovány dle označení ve směrnici, další přílohy jsou zařazovány a číslovány dle pořadí vzniku.

V Třebíči dne 2.5.2022

.....
Organizace