



INTERNÍ SMĚRNICE GDPR - O ZÁSADÁCH ZPRACOVÁNÍ OSOBNÍCH A CITLIVÝCH ÚDAJŮ

Cílem tohoto dokumentu je shrnutí základních informací o zásadách zpracování osobních údajů, kterými se organizace řídí a které přijala za účelem zajištění souladu s **nařízením parlamentu a Rady EU 2016/679 (dále jen „GDPR“)**, které je na území ČR účinné od 25. 5. 2018. Toto nařízení se dnem nabytí účinnosti 25. května 2018 stává přímo aplikovatelným právním předpisem na území všech členských států Evropské unie.

Charita Neratovice podnikla veškeré nezbytné kroky k posílení bezpečnosti a důvěrnosti zpracovávaných údajů a ke splnění všech předepsaných povinností.

V souladu s GDPR zpracovává organizace osobní údaje dle těchto zásad:

1. **Zákonnost, korektnost a transparentnost** – Provádíme zpracování jen v případě, kdy k tomu existuje legitimní důvod (např. zákonná povinnost, plnění smlouvy, ochrana našich zájmů, ochrana zájmů třetích osob nebo udělený souhlas subjektu údajů).
2. **Účelové omezení** – Shromažďujeme osobní údaje jen pro konkrétní, výslovně vyjádřené a legitimní účely.
3. **Minimalizace údajů** – Zpracování osobních údajů provádíme pouze v míře a rozsahu, který je nezbytný ve vztahu k danému účelu.
4. **Přesnost** – Zpracováváme pouze aktuální osobních údajů, které odrážejí skutečný stav věci.
5. **Omezení uložení** – Držíme osobní údaje po dobu ne delší, než je nezbytné a zákonné.
6. **Integrita, důvěrnost** – Zavedli jsme dostatečné technické a organizační opatření k ochraně osobních údajů před náhodným nebo protiprávním zničením, ztrátou, změnou nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.
7. **Odpovědnost** – Jsme kdykoli schopni doložit soulad dodržování zásad dle bodů 1. – 6.

Většinu osobních údajů zpracováváme za účelem splnění zákonem předepsaných povinností. V případě, že provádíme zpracování, jehož účelem není splnění zákonem předepsaných povinností, plnění smlouvy nebo oprávněného zájmu, jedná se o zpracování osobních údajů, ke kterému potřebujeme výslovný, svobodný konkrétní a informovaný souhlas subjektů údajů (zaměstnanců, uživatelů, opatrovníků apod.). V takovém případě se jedná zejména o zpracování osobních údajů o podobě těchto osob (fotografie). Poskytnutí takového souhlasu je zcela dobrovolné a souhlas lze kdykoli odvolat či využít další práva, která jsou přesně v písemném souhlasu popsána.

Zájemcům o naše služby sdělujeme, že požadované údaje o nich, o opatrovnících či zákonných zástupcích, bydlišti a další identifikační údaje jsou uloženy zákonem. Pokud má Charita rozhodnout o přijetí nebo nepřijetí zájemce, musí nám být sděleny základní identifikační údaje a jeho osobní údaje.

Organizace přijala nezbytná opatření k zajištění bezpečnosti zpracovávaných osobních údajů jak v jejich fyzické, tak elektronické podobě. Mezi tato opatření patří zejména stanovení interních pravidel pro práci s danými informačními systémy, zajištění, aby tyto osoby měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, pořizování záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány a zamezení neoprávněnému přístupu k datovým nosičům, zejména prostřednictvím nastavení hesel, přístupových práv, šifrování, vypracování dokumentace k přijatým technicko-organizačním opatřením, zvýšení bezpečnosti instalací zámků, nákupem zamykacích skříní apod.

Všichni zaměstnanci a osoby, které mají v rámci činnosti naší organizace přístup k osobním údajům, jsou řádně proškoleni a jsou seznámeni s pravidly bezpečnosti a důvěrnosti při nakládání s osobními údaji.

Osobní údaje předáváme třetím osobám pouze v zákonem předepsaných případech (povinná hlášení orgánům státní správy, samosprávy apod.) nebo v nezbytném rozsahu vybraným dodavatelům, kteří pro nás zajišťují některé služby, jako například vedení účetnictví nebo správu informačních technologií (IT). Se všemi takovými osobami máme jasně nastavené smluvní vztahy a všichni dodavatelé splňují nezbytná pravidla pro zpracování osobních údajů v rozsahu a parametrech vyžadovaných nařízením GDPR.

Doba zpracování a uchování osobních údajů je stanovena zpravidla legislativními požadavky nebo v případě souhlasů je po dobu uvedenou v souhlasech (po dobu uzavření smlouvy, do ukončení pracovního poměru apod.) nebo do jeho odvolání.

V rámci GDPR rozlišujeme mezi osobními a citlivými údaji. Za osobní údaje jsou považovány veškeré informace, které se vztahují k identifikované osobě, pomocí nichž lze danou osobu identifikovat. Přesto, že není definován kompletní výčet osobních údajů, rozlišujeme několik kategorií:

- Obecné - jméno, datum narození, pohlaví, osobní stav, občanství, fotografie, IP adresa
- Organizační - osobní nebo pracovní adresa, telefonní číslo, e-mailová adresa, identifikační čísla vydaná státem

Zvláštní kategorie jsou:

- Citlivé údaje - zdravotní stav, sexuální orientace, rasový a etnický původ, politické názory a angažovanost, náboženství a víra, členství v odborech
- Genetické údaje - analýzy biologických vzorků, zděděné nebo získané genetické charakteristiky
- Biometrické údaje - fyzické, fyziologické nebo behaviorální charakteristiky (např. otisky prstů, fotografie obličeje, podpis...)

Od 25. 5. 2018 proto v organizaci Charita Neratovic. platí v návaznosti na GDPR tato nová pravidla a opatření:

- Všechny počítače jsou chráněny heslem. Na počítačích v jednotlivých službách je vždy jeden zaheslovaný účet pro pracovníky, jeden pro uživatele (bez hesla). Na tomto účtu se nikdy nepracuje s žádnými dokumenty organizace s osobními údaji, neukládají se žádné fotografie, slouží opravdu jen pro uživatele v případě, že chtějí využít internet, nebo využívají počítač pro plnění cílů z individuálního plánování (kognitivní cvičení, nácvik psaní životopisu apod.).
- Všichni pracovníci, kteří při práci využívají flash disky je mají chráněné heslem.
- Je zakázáno používat soukromé flash disky, na služební servery se nelze připojovat ze soukromých počítačů mimo pracovní dobu.
- Dokumentace obsahující osobní nebo citlivé údaje musí být v uzamčeném prostoru.
- Mlčenlivost mají podepsanou všichni zaměstnanci v rámci nového vzoru pracovních smluv (i neoborové profese – držba, úklid). Ostatní osoby, které vstupují do služeb (praxe, stáže, dobrovolníci) musí vždy podepsat závazek mlčenlivosti.
- Pořizování fotografií klientů a zaměstnanců je možné pouze na základě písemného souhlasu.
- Aktualizovaný souhlas s poskytnutím osobních a citlivých údajů nově k 25. 5. 2018 bude předložen všem uživatelům. Pro ostatní osoby, které vstupují do služeb (praktikanti, stážisti, dobrovolníci) je také vytvořený Souhlas s poskytnutím osobních a citlivých údajů, který je nutné podepsat při podpisu smlouvy.
- Zasílání e-mailů se řídí novými pravidly GDPR. U e-mailů zasílaných více adresátům, nikdy neuvádíme adresy viditelně, ale využíváme možnosti tzv. skryté kopie. Osobní a citlivé údaje o osobách nikdy nezasiíláme volně v textu e-mailu nebo příloze (př. data narození a jména stážistů, vysílající organizace zašle pouze jména, my vytvoříme potvrzení o stáži a pracovník si sám po absolvování stáže doplní své datum narození). V e-mailu již údaje nebudou přeposílány. V případě, že bude pracovník pouze přeposílat e-mail, který obsahuje osobní data, ale nebude autorem e-mailu, ani nikdo z naší organizace není jeho autorem, neneseme za obsah odpovědnost.
- Přílohy e-mailů – všechny přílohy, ve kterých se vyskytnou osobní a citlivé údaje musí být chráněné heslem.
- Zasílání pozvánek – při zasílání pozvánek, je nutné na konec e-mailu vždy uvést větu: Pokud si nepřejete, aby vám byly informace o akcích a činnosti Charity Neratovice nadále zasílány, odpovězte na tento e-mail a v předmětu uveďte „NEZASÍLAT“. Seznam lidí, kteří nechtějí dostávat pozvánky, povede vedoucí kanceláře. Pracovníci ji vždy budou hlásit aktuálně osoby, které si nepřejí nadále zasílat pozvánky a informace o organizaci.

- Akce pro širokou veřejnost – pokud bude organizací organizace pořád veřejnou akci, na které se bude fotografovat, je nutné na pozvánku či plakát uvést: Na akci se bude pořizovat fotodokumentace, která může být použita pro zveřejnění a následnou propagaci organizace. Svou účastí na akci se zveřejněním souhlasíte.
- Nadbytečné údaje – jsou získávány pouze údaje nezbytné k základní identifikaci, př. v Žádosti o zařazení do evidence vedoucí získává od zájemce pouze jméno, datum narození - rok, bydliště – město nebo obec. Trvalé bydliště s celou adresou nebo celé datum narození už je nadbytečný údaj, pro zařazení do evidence stačí pouze město nebo obec a rok narození k tomu, abychom zjistili, zda splňuje cílovou skupinu.
- Jednání vedoucích – každý vedoucí je zodpovědný za zajištění informovanosti jak pracovníků, tak uživatelů. Každý vedoucí má povinnost vždy sdělit proč a za jakým účelem osobní údaje požadujeme, na jak dlouho, kdo k nim bude mít přístup, seznámí s možností odvolatelnosti souhlasu. Musí mít přehled o GDPR, musí řádně proškolit pracovníky.

Související dokumenty :

ŘF-ZS-CH-001 Záznam o souhlasu pacienta s poskytováním informací

ŘF-ZS-CH-001 Záznam o souhlasu pacienta s domácí péčí

ŘF-SS-CH-008 Souhlasy klienta

ŘF-CH-035 Souhlas pro zaměstnance Charity Neratovice

ŘF-CH-048 Souhlas se zpracováním osobních údajů

Přílohy :

Katalog rizik - elektronická verze

Katalog osobních údajů - elektronická verze

Doporučený postup č.02/2018 MPSV

Ochrana dokumentů

Neratovice dne 25.5.2018

.....

Miloslava Machovcová
statutární zástupce organizace