Charita Frenštát pod Radhoštěm

Charita Frenštát pod Radhoštěm, Dolní 504, 744 01 Frenštát pod Radhoštěm
Bankovní spojení – **Fio banka, a.s. 2000906119 / 2010**, IČO: 49590588
telefon: 731 141 801, e-mail: info@frenstat.charita.cz; ww.frenstat.charita.cz

CHARITA ČESKÁ REPUBLIKA

SMĚRNICE O ZPRACOVÁNÍ A OCHRANĚ OSOBNÍCH ÚDAJŮ

(ve znění účinném od 25. 5. 2018)

Článek 1.
ÚVODNÍ USTANOVENÍ

1.1. Charita Česká republika, (arci)diecézní Charity Brno, Praha, Olomouc, Ostrava-Opava, České Budějovice, Hradec Králové, Plzeň a Litoměřice a všechny farní, městské a oblastí Charity v nich sdružené se s ohledem na povahu své činnosti, která zahrnuje také zpracování osobních údajů fyzických osob, rozhodly společně přijmout tuto informačně-organizační směrnici o zpracování a ochraně osobních údajů, aby naplňovaly své povinnosti vyplývající z příslušné právní úpravy, včetně obecného nařízení Evropské unie o ochraně osobních údajů (dále také jako „*GDPR*“).

1.2. Účelem této směrnice je deklarace zásad, kterými se řídí jednotlivé Charity při nakládání s osobními údaji, a zakotvení postupů pro řízení situací vzniklých ze zpracování osobních údajů a s nimi souvisejících, včetně odpovídajících opatření pro soulad se zákonnými povinnostmi správců údajů.

1.3. Tato směrnice je vnitřním předpisem Charity Česká republika (dále také jako „*CHČR*“) **s obecnou působností pro CHČR jako celek a pro všechny její organizační součásti**, tj. všechny (arci)diecézní, farní, městské a oblastní Charity, s tím, že specifika u jednotlivých Charit jsou dle potřeby upřesněna a upravena v jejich prováděcí dokumentaci navazující na tuto směrnici. Prováděcí dokumentace jednotlivé Charity má v případě odchylné úpravy od směrnice přednost. Tam, kde se dále v této směrnici mluví o „Charitě“, rozumí se tím CHČR nebo jednotlivá (arci)diecézní, farní, městská či oblastní Charita, která se v konkrétní situaci nachází v roli správce zpracovávaných osobních údajů.

1.4. Tato směrnice je závazná pro všechny zaměstnance, dobrovolníky a jiné osoby činné v rámci Charity; tyto osoby jsou povinné řídit se touto směrnicí a dalšími pokyny Charity v oblasti ochrany osobních údajů. Tam, kde je to možné, Charita zaváže k dodržování této směrnice také své dodavatele v rozsahu, v jakém to nevylučuje povaha a kontext jednotlivých ustanovení směrnice.

1.5. CHČR podrobuje tuto směrnici pravidelné revizi z hlediska její aktuálnosti a dle potřeby přijímá její nová aktualizovaná znění, k čemuž ji všechny v ní sdružené Charity zmocňují.

Článek 2.
ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V RÁMCI CHČR

2.1. Charita chrání osobní údaje, kterými jsou **veškeré údaje o identifikované nebo identifikovatelné fyzické osobě**, tj. údaje určující fyzickou osobu (např. jméno, příjmení, rodné číslo, fotografie) či údaje přiřaditelné ke konkrétní fyzické osobě (je-li u údajů uvedeno jméno osoby nebo jiný identifikátor). Předmětem ochrany jsou osobní údaje *žijících fyzických osob* a takové údaje o zesnulých osobách, které mohou nadále nést informaci rovněž o žijících osobách (např. údaje o dědičných nemocech).

2.2. Předmětem ochrany jsou také případné pseudonymizované údaje. Charita je srozuměna s tím, že osobními údaji ve smyslu příslušné právní úpravy nejsou pouze úplně anonymní či

anonymizované údaje.

2.3. Charita zpracovává osobní údaje **následujících fyzických osob**:

2.3.1. klientů a příjemců Charitou poskytovaných sociálních a zdravotních služeb a další pomoci, zájemců o tyto služby a pomoc a rodinných příslušníků klientů i zájemců;

2.3.2. sponzorů, dárců, členů v Klubu přátel CHČR a dalších spolupracujících osob;

2.3.3. zaměstnanců, dobrovolníků a uchazečů o zaměstnání či dobrovolnickou činnost, případně jejich rodinných příslušníků;

2.3.4. dodavatelů;

2.3.5. zástupců a kontaktních osob výše uvedených kategorií subjektů údajů.

2.4. Charita zpracovává osobní údaje zejména **v následujícím rozsahu**:

2.4.1. identifikační a kontaktní údaje: jméno, příjmení, rodné číslo, datum narození, trvalý/přechodný pobyt, kontaktní adresa, telefonní číslo;

2.4.2. „klientské“ údaje: o poptávaných službách a pomoci, o poskytnutých službách a pomoci a jejich průběhu, včetně informací o věku, rasovém či etnickém původu, zdravotním stavu, rodinné situaci;

2.4.3. „sponzorské“ údaje: výše příspěvků a darů, čísla bankovních účtů, podporované projekty;

2.4.4. „zaměstnanecké“ údaje: výše mzdy a dalších plnění, číslo bankovních účtů, odpracované hodiny, pracovní výsledky, další údaje o zaměstnaneckém vztahu a jeho průběhu, údaje o rodinném stavu a vyživovaných osobách, evidence odvodů do sociálního a zdravotního pojištění a daňová evidence;

2.4.5. fotografie z akcí pořádaných Charitou (umožňující identifikaci konkrétních osob);

2.4.6. video a záznamy z kamerového systému.

2.5. Charita zpracovává výše uvedené údaje **zejména z právního titulu (a za účelem)**:

2.5.1. plnění zákonných povinností poskytovatele sociálních a zdravotních služeb, a u citlivých „klientských“ údajů z titulu a za účelem poskytování sociální nebo zdravotní péče či z titulu ochrany životně důležitých zájmů subjektů údajů nebo jiných fyzických osob (předejití vzniku újmy na životě, humanitární účely);

2.5.2. plnění zákonných povinností daňového subjektu – za účelem evidence darů, zasílání potvrzení o darech;

2.5.3. plnění zákonných povinností zaměstnavatele – za účelem zpracování mezd a provádění příslušných daňových odvodů a odvodů do systémů sociálního a zdravotního pojištění, za účelem vedení osobních spisů;

2.5.4. oprávněných zájmů Charity – za účelem vedení interní statistiky dárců, propagace činnosti Charity (včetně adresného informování dárců o dalších možnostech podpory a pořádaných akcích), za účelem ochrany majetku a osob v prostorech Charity (např. kamerový systém);

2.5.5. souhlasu subjektu údajů se zpracováním – zejména u používání fotografií klientů a dárců za účelem propagace činnosti Charity.

Charita provádí všechny úkony zpracování osobních údajů uvědoměle za jasně definovaným účelem a na základě některého z právních titulů vyjmenovaných v čl. 6 odst. 1 nařízení GDPR, a jde-li o citlivé údaje (zvláštní kategorie osobních údajů), v čl. 9 odst. 2 nařízení GDPR.

2.6. V případě vedení listinné (papírové) kartotéky je **ochrana osobních údajů zabezpečena** minimálně vhodným umístěním kartotéky v prostorech Charity, uzamčením kartotéky a poskytnutím přístupového klíče pouze nezbytnému okruhu zaměstnanců s příslušnou působností. V případě elektronicky vedených evidencí jsou příslušné složky chráněny minimálně přístupovými hesly a umožněním přístupu pouze zaměstnancům s příslušnou působností; koncová uživatelská zařízení jsou chráněná antivirovým a antispamovým softwarem. Ke každé evidenci s osobními údaji, ať už listinné nebo elektronické, vede Charita bezpečnostní zálohu. Úplný a konkretizovaný popis bezpečnostních opatření u jednotlivé Charity je předmětem její prováděcí dokumentace k této směrnici.

2.7. Využívá-li Charita externího **zpracovatele osobních údajů**, tj. subjektu, který zpracovává osobní údaje pro Charitu a na její pokyn (např. externí mzdová účtárna, účetní či daňový poradce), jedná se pouze o subjekt, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření pro splnění požadavků GDPR a zajištění ochrany práv subjektů údajů. Se zpracovatelem je uzavírána smlouva, která obsahuje náležitosti dle čl. 28 nařízení GDPR. Zpracovatel je povinen zpracovávat osobní údaje získané od Charity pouze k účelu, pro který mu byly svěřeny, a pouze v souladu s doloženými pokyny Charity.

2.8. Všichni zaměstnanci, dobrovolníci a další osoby uvnitř Charity s přístupem k osobním údajům jsou zavázáni **povinností mlčenlivosti**, a tato povinnost trvá i po ukončení jejich činnosti pro Charitu. Může-li mít externí poskytovatel služeb pro Charitu, který není zpracovatelem, i jen nahodilý přístup k osobním údajům zpracovávaným Charitou (např. správce IT systému), Charita jej smluvně zaváže povinností mlčenlivosti a zajištěním mlčenlivosti u jeho zaměstnanců a dalších osob pro něj činných.

2.9. Osobní údaje zpracovávané Charitou nejsou až na drobné výjimky předávány do třetích zemí, tj. mimo země Evropské unie a Evropského hospodářského prostoru, ani mezinárodním organizacím. Při využívání služeb cloudového úložiště Charita vyžaduje od poskytovatele těchto služeb umístění serverů, na nichž jsou uloženy osobní údaje zpracovávané Charitou, v rámci Evropské unie a Evropského hospodářského prostoru. Dochází-li výjimečně k předání osobních údajů Charitou do třetí země nebo mezinárodní organizaci, děje se tak, s cílem zajistit, aby zůstala zaručena úroveň ochrany fyzických osob dle nařízení GDPR, pouze za splnění podmínek stanovených v kapitole V nařízení GDPR, tj. pokud:

2.9.1. existuje rozhodnutí Evropské komise, že cílová třetí země, území nebo mezinárodní organizace zajišťuje odpovídající úroveň ochrany (např. Andora, Argentina, Švýcarsko, Izrael, Nový Zéland, Uruguay); nebo

2.9.2. v cílové zemi nebo mezinárodní organizaci jsou k dispozici vymahatelná práva subjektů údajů a účinná právní ochrana subjektů údajů a Charita poskytuje vhodné záruky, tj. bez potřeby povolení Úřadu pro ochranu osobních údajů (dále také jako

„*ÚOOÚ*“) zejména pomocí uzavření standardních smluvních doložek s příjemcem, buď přijatých Evropskou komisí nebo dozorovým úřadem, a s výhradou povolení od ÚOOÚ zejména pomocí uzavření vlastních smluvních doložek s příjemcem; nebo

2.9.3. nelze-li postupovat dle předchozích článků 2.9.1. a 2.9.2., pokud je splněna některá z výjimek dle čl. 49 GDPR – např. výslovný a informovaný souhlas subjektu údajů; nezbytnost plnění smlouvy uzavřené se subjektem údajů nebo v jeho zájmu; důležité důvody veřejného zájmu; nezbytnost pro výkon právních nároků; nebo

2.9.4. není-li splněna ani jedna z výjimek dle čl. 49 GDPR, pokud převod osobních údajů není opakovaný, vztahuje se pouze k omezenému počtu subjektů údajů a je nezbytný s ohledem na závažné oprávněné zájmy Charity, které převažují nad zájmy a právy subjektů údajů. V tomto případě Charita posoudí všechny okolnosti a poskytne vhodné záruky ochrany osobních údajů; o předání následně informuje ÚOOÚ a zaznamená posouzení i vhodné záruky v záznamech i činnostech zpracování.

Článek 3.
SOULAD S PRÁVNÍ ÚPRAVOU (GDPR)

3.1. Charita dokládá soulad s právní úpravou ochrany osobních údajů především **dokumentací** této oblasti, která obsahuje informace o situaci zpracování osobních údajů u Charity, zejména o systému přijatých technických a organizačních opatření zavedených k zajištění souladu. Součástí této dokumentace jsou mj. „záznamy o činnostech zpracování“, tato směrnice a její prováděcí dokumentace, záznamy o školeních zaměstnanců v oblasti ochrany osobních údajů a vzory případných souhlasů subjektů údajů se zpracováním či smluvní dokumentace se zpracovateli a příjemci osobních údajů.

3.2. Charita se může rozhodnout, že vedle nebo namísto postupu dle předchozího čl. 3.1 směrnice:

3.2.1. se **přihlásí ke Kodexu chování** (čl. 40 GDPR), který je schválen Úřadem pro ochranu osobních údajů, jím zaregistrován a zveřejněn, nebo který má dle rozhodnutí Evropské komise všeobecnou platnost v rámci Evropské unie, a je zveřejněn, pokud takový kodex pro oblast činnosti Charity vznikne; anebo

3.2.2. **získá osvědčení** o souladu od akreditovaného subjektu (čl. 42 GDPR).

Článek 4.
ZÁKLADNÍ ZÁSADY ZPRACOVÁNÍ OÚ

4.1. Charita se řídí zákonnými zásadami zpracování osobních údajů.

4.2. **Zákonnost.**

4.2.1. Charita postupuje v souladu s právní úpravou ochrany osobních údajů.

4.2.2. Každý úkon zpracování osobních údajů ze strany Charity je založen na jednom z právních titulů zpracování. Existuje-li pro zpracování osobních údajů jiný právní titul, než je souhlas subjektu údajů, Charita nezískává od dotčeného subjektu údajů tento souhlas.

4.2.3. Je-li pro zpracování osobních údajů nezbytný souhlas subjektu údajů, text souhlasu je formulován jednoznačně pro konkrétní účely zpracování, je formulován srozumitelně a je uveden na samostatném dokumentu, anebo je aspoň dostatečně graficky oddělený od zbytku dokumentu. Souhlas se zpracováním osobních údajů musí být subjektem údajů udělen aktivně (tzv. opt-in) a svobodně; Charita nesmí vyžadovat souhlas jako podmínku poskytování služby nebo jiné její činnosti, není-li dotčené zpracování osobních údajů pro to nezbytné. Subjektu údajů je umožněno souhlas snadno odvolat.

4.2.4. Je-li pro zpracování osobních údajů dítěte (osoby mladší 18 let) nezbytný souhlas subjektu údajů, tento souhlas uděluje zákonný nebo ustanovený zástupce dítěte, a je-li dítě starší 13 let, uděluje jej zároveň i dítě.

4.3. **Korektnost a transparentnost.**

4.3.1. Jakékoliv informace určené subjektům údajů a/nebo veřejnosti jsou úplné a správné, formulované pregnantně, a zároveň stručně a srozumitelně. Tam, kde je to vhodné, použije se vizualizace prostřednictvím piktogramů.

4.4. **Účelové omezení.**

4.4.1. Charita používá a zpracovává osobní údaje zásadně za účelem, pro který byly původně získané.

4.4.2. Pro jiný účel než výše uvedený lze osobní údaje zpracovávat, je-li takový účel slučitelný s původním účelem s ohledem na vazbu mezi účely, okolnosti shromáždění osobních údajů, povahu osobních údajů (zejména zda se nejedná o citlivé údaje), možné důsledky dalšího zpracování pro subjekty údajů a existenci vhodných záruk ochrany osobních údajů. Za neslučitelné se nepovažuje další zpracování pro účely archivace ve veřejném zájmu (např. archivace mzdových listů, daňových dokladů či zdravotnické dokumentace po zákonem stanovenou dobu), pro účely vědeckého či historického výzkumu nebo pro statistické účely.

4.5. **Minimalizace údajů a omezení uložení.**

4.5.1. Charita omezuje zpracování osobních údajů na rozsah nezbytný pro účely zpracování.

4.5.2. Charita neuchovává osobní údaje po dobu delší, než je nezbytné s ohledem na účely zpracování, resp. po kterou je povinna osobní údaje uchovávat. Charita dodržuje povinnosti archivovat stanovené osobní údaje po vymezenou dobu (např. pro účely daňové kontroly, nebo ověření nároků v rámci důchodového nebo nemocenského pojištění atd.).

4.5.3. Osobní údaje lze uchovávat déle, než je nezbytné pro původní účel, vedle archivace ve veřejném zájmu také pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření pro zaručení práv a svobod subjektů údajů.

4.6. **Přesnost.**

4.6.1. Charita zpracovává přesné a v případě potřeby aktualizované osobní údaje. V případě, že je důležité uchovávat vedle aktuálních osobních údajů i osobní údaje původní, např. v rámci zdravotnické dokumentace, Charita uchovává i tzv. historická data.

4.6.2. Zaměstnanci, dobrovolníci a další osoby činné v rámci Charity jsou povinné aktualizovat své osobní údaje, tedy Charitu bez zbytečného odkladu informovat o jakékoliv změně svých osobních údajů.

4.7. **Integrita a důvěrnost.**

4.7.1. Charita zajišťuje náležité zabezpečení osobních údajů, včetně jejich ochrany před neoprávněným či protiprávním zpracováním (únikem) a před náhodnou ztrátou, zničením nebo poškozením, jak je uvedeno dále v této směrnici nebo v prováděcí dokumentaci k ní.

4.8. **Odpovědnost správce.**

4.8.1. Charita coby správce údajů nese odpovědnost za dodržení výše uvedených základních zásad, ale i za celkový soulad zpracování osobních údajů s právní úpravou ochrany osobních údajů. Charita dokládá tento soulad způsoby uvedenými výše v čl. 3 této směrnice.

Článek 5.
TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ; MINIMALIZACE ZPRACOVÁNÍ

5.1. Charita používá vhodná **technická a organizační opatření** přiměřená rozsahu a způsobům zpracování osobních údajů v Charitě a tato opatření reviduje a zavádí nová v případech podstatné změny v oblasti zpracování osobních údajů, jakož i na základě pravidelného posouzení situace zpracování, včetně úrovně zabezpečení osobních údajů, které provádí alespoň jednou ročně. Úplný a konkretizovaný popis všech technických a organizačních opatření u jednotlivé Charity je předmětem její prováděcí dokumentace k této směrnici.

5.2. Charita odpovídá za vhodnost, přiměřenost a účinnost a také aktuální stav svého systému technických a bezpečnostních opatření; v případě, že správu budov a objektů, v nichž Charita působí, vykonává jiná organizační součást CHČR, tato odpovídá Charitě za zabezpečení ostrahy předmětných budov a objektů.

5.3. Charita **minimalizuje** činnosti zpracování osobních údajů na nezbytný rozsah a zpracování provádí po dobu nezbytnou pro účely zpracování, příp. po dobu, po kterou je povinna osobní údaje uchovávat. Charita zavádí za účelem minimalizace zpracování alespoň následující vhodná opatření:

5.3.1. při obdržení osobních údajů (ústně nebo v dokumentu) tyto třídí a neukládá či začerňuje údaje, které jsou nepotřebné;

5.3.2. pravidelně prochází spisy klientů, spisy zaměstnanců a jiné evidence osobních údajů a nepotřebné osobní údaje, které již neslouží svému účelu nebo které není povinna uchovávat, vymazává a skartuje;

5.3.3. při převodu již neaktivních spisů do archivace třídí osobní údaje v nich obsažené a začerňuje či skartuje nepotřebné údaje;

5.3.4. řídí se svým archivačním a skartačním řádem, který zohledňuje zákonem stanovené doby archivace (např. pro účetní záznamy, daňové doklady, zdravotnickou dokumentaci).

5.4. Charita zpracovává mj. osobní údaje **uchazečů o zaměstnání**. U úspěšných uchazečů se předložené životopisy a další dokumenty stávají součástí osobního spisu zaměstnance. U neúspěšných uchazečů o zaměstnání Charita uchovává životopisy maximálně po dobu dvou let pro účely případného pozdějšího oslovení zájemce; poté Charita případně uchovává informaci o tom, která konkrétní osoba se u ní ucházela o zaměstnání a jaký byl výsledek výběrového řízení (a důvod výsledku).

5.5. Provozuje-li Charita **kamerový systém**, zajistí smazávání pořízených záznamů nejpozději po 7 dnech a v případě příležitostně navštěvovaných prostor po 14 dnech od vzniku jednotlivého záznamu. Záznam kamerového systému může být výjimečně uchován i déle, tj. po nezbytnou dobu, zachycuje-li důležitou skutečnost (např. vstup neoprávněné osoby do objektu Charity, krádež atd.) a je-li jej nadále potřeba pro účely vyšetřování trestného činu či přestupku či pro vedení soudního řízení apod.

5.6. Zpracovává-li Charita biometrické údaje (např. otisky prstů, snímky obličejů) za účelem identifikace subjektů údajů (typicky zaměstnanců), zejména pro účely systému přístupu do objektů / prostor Charity, podrobí takovéto zpracování posouzení vlivu na ochranu osobních údajů (DPIA) ve smyslu čl. 10 této směrnice a poté jej konzultuje s Úřadem pro ochranu osobních údajů. Za zpracování biometrických údajů ze strany Charity se nepovažuje nákup a používání koncových uživatelských zařízení (např. mobilní telefony, notebooky) nabízejících možnost přihlašování přes otisky prstů či jiné biometrické údaje, pokud jsou tyto biometrické údaje bezpečně uloženy v koncových zařízeních a Charita k nim nemá přístup a dále je nezpracovává; Charita však nakupuje předmětná zařízení pouze od ověřených výrobců, kteří poskytují dostatečné záruky ochrany biometrických údajů.

Článek 6.
INFORMOVÁNÍ SUBJEKTŮ ÚDAJŮ

6.1. Charita srozumitelně informuje subjekty údajů o zpracování jejich osobních údajů v rozsahu své informační povinnosti minimálně do té míry, v jaké subjekty údajů vyžadovanými informacemi nedisponují. **Obsahem informační povinnosti** je zejména údaj o tom, které kategorie osobních údajů, za jakým účelem a na základě jakého právního titulu jsou zpracovávány, kdo je správcem a případně pověřencem pro ochranu osobních údajů, jaké subjekty nebo kategorie subjektů mohou být příjemci osobních údajů a o případném úmyslu předat osobní údaje do třetí země nebo mezinárodní organizaci (s odkazem na vhodné záruky ochrany). Je-li to s ohledem na požadavek transparentnosti nezbytné a vhodné, je součástí poučení mj. informace o právech subjektů údajů a o době uložení osobních údajů.

6.2. Obsah a forma informace pro subjekt údajů je přizpůsobena kategorii adresátů a jejich

průměrným rozumovým schopnostem.

6.3. Charita plní informační povinnost:

6.3.1. ve vztahu ke klientům a příjemcům služeb a pomoci individuálně před započetím poskytování služeb a pomoci, nebo jakmile je to vhodné;

6.3.2. ve vztahu k zaměstnancům a dobrovolníkům individuálně při uzavírání smlouvy nebo dohody; a

6.3.3. ve vztahu k dalším kategoriím subjektů údajů zejména obecně zveřejněním příslušné informace na webových stránkách Charity.

Je-li od subjektu údajů získáván souhlas se zpracováním osobních údajů, je informace o zpracování osobních údajů připojena k textu souhlasu, není-li takový postup nevhodný.

6.4. Charita zajistí **doložitelnost** splnění informační povinnosti (např. odkazem na webové stránky, potvrzením od subjektu údajů) a obsahu poskytnuté informace.

Článek 7.
DALŠÍ PRÁVA SUBJEKTŮ ÚDAJŮ A USNADŇOVÁNÍ JEJICH VÝKONU

7.1. Charita usnadňuje subjektům údajů výkon jejich dále uvedených práv. Subjekty údajů se můžou se svými žádostmi na uplatnění jednotlivých práv **obracet** osobně či písemně, včetně emailem, **na danou Charitu**; Charita přístupným způsobem zveřejňuje kontaktní údaje pro adresování těchto žádostí. Pracovníci jednotlivé Charity pomůžou v případě nesnází subjektům údajů jejich žádost formulovat, případně ji společně se subjektem údajů sepíší. Každá žádost subjektu údajů je řádně evidována Charitou, které byla adresována. Tato Charita posoudí a vyřídí žádost subjektu údajů a zároveň informuje subjekt údajů o způsobu vyřízení jeho žádosti do 30 kalendářních dní od podání žádosti; je-li rozhodnutí o způsobu vyřízení žádosti skutkově či právně složité, Charita se může obrátit pro stanovisko na svou nadřízenou složku (arci/diecézní Charitu resp. sekretariát CHČR či pověřence ČBK), příp. na Úřad pro ochranu osobních údajů, přičemž lhůta pro posouzení a vyřízení žádosti a informování subjektu údajů může být v tomto případě přiměřeně prodloužena, maximálně však o dalších 60 kalendářních dní.

7.2. Jakékoliv informace nebo úkony v oblasti práv subjektů údajů Charita poskytuje a činí bezplatně, ledaže je žádost subjektu údajů zjevně nedůvodná nebo nepřiměřená. V takovém případě může Charita uložit přiměřený poplatek zohledňující administrativní náklady, nebo může žádosti nevyhovět.

7.3. Charita bere na vědomí, že každému subjektu údajů náleží následující práva:

7.3.1. právo na **přístup** k osobním údajům dle čl. 15 GDPR, tedy na informaci, zda jsou jeho osobní údaje zpracovávány, a na informace o tomto zpracování (o kategoriích zpracovávaných osobních údajů, účelech zpracování, příjemcích atd.);

7.3.2. právo na **opravu** nepřesných či doplnění neúplných osobních údajů dle čl. 16 GDPR – tím však není dotčeno právo Charity ponechat si tzv. historická, tj. neaktuální

data v nezbytném rozsahu (např. pro účely daňových kontrol nebo kontrol v oblasti sociálního pojištění);

7.3.3. právo na **výmaz** (likvidaci) osobních údajů ve stanovených případech dle čl. 17 GDPR, např. z důvodu, že osobní údaje již nejsou potřebné pro účely zpracování, nebo subjekt údajů odvolá souhlas se zpracováním a neexistuje další právní titul, nebo zpracování je v rozporu s právní úpravou či výmaz je nezbytný ke splnění zákonné povinnosti – Charita nemusí žádosti subjektu údajů vyhovět, je-li naplněna některá z výjimek, např. je-li další zpracování nezbytné pro splnění zákonné povinnosti, splnění úkolu prováděného ve veřejném zájmu nebo uplatňování právních nároků;

7.3.4. právo na **omezení zpracování** osobních údajů ve stanovených případech dle čl. 18 GDPR, tj. aby osobní údaje byly pouze uchovávány a nebyly jinak zpracovávány z důvodu, že subjekt údajů namítá nepřesnost údajů, nebo zpracování je v rozporu s právní úpravou, nebo Charita nepotřebuje osobní údaje, ale subjekt údajů je požaduje pro uplatnění právních nároků, či subjekt údajů vznesl námitku proti zpracování (dokud nebude ověřeno, zda oprávněné důvody Charity na zpracování převažují nad právy subjektu údajů) – Charita je oprávněna osobní údaje navzdory omezení zpracovávat se souhlasem subjektu údajů, pro uplatnění právních nároků, z důvodu ochrany práv jiné osoby či z důvodu důležitého veřejného zájmu;

7.3.5. právo na **přenositelnost** osobních údajů dle čl. 20 GDPR, tj. na získání svých osobních údajů ve strukturovaném, běžně používaném a strojově čitelném formátu, nebo na jejich předání jinému správci údajů – toto právo se týká osobních údajů, které Charitě poskytl subjekt údajů a které Charita zpracovává automatizovaně na základě souhlasu subjektu údajů nebo pro účely plnění smlouvy;

7.3.6. právo vznést **námitku** proti zpracování dle čl. 21 GDPR – v případě zpracování osobních údajů z titulu oprávněných zájmů Charity nebo z titulu plnění úkolu prováděného ve veřejném zájmu nebo výkonu veřejné moci, kterým je Charita pověřena – Charita osobní údaje dále nezpracovává, dokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy či právy subjektu údajů;

7.3.7. právo nebýt předmětem automatizovaného individuálního rozhodování s právními nebo obdobnými účinky dle čl. 22 GDPR – tj. právo nebýt předmětem rozhodnutí s uvedenými účinky bez účasti lidského faktoru, až na vymezené případy.

7.4. Subjekt údajů má dále právo **podat stížnost** u dozorového úřadu, tj. v rámci České republiky u Úřadu pro ochranu osobních údajů ČR, aniž jsou dotčeny jiné prostředky ochrany, domnívá-li se, že zpracování jeho osobních údajů je v rozporu s právní úpravou. Subjekt údajů má také právo **kdykoliv odvolat souhlas** se zpracováním osobních údajů, aniž je dotčena zákonnost dřívějšího zpracování osobních údajů.

7.5. Veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s GDPR oznamuje příslušná Charita všem subjektům, jimž byly dotčené osobní údaje zpřístupněny, ledaže se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí.

7.6. Zaměstnanci Charity odpovědní za zpracování žádostí subjektů údajů o výkon jejich práv jsou povinni podrobně se seznámit s úpravou práv subjektů údajů, včetně podmínek pro jejich uplatnění.

Článek 8.
VEDENÍ ZÁZNAMŮ O ČINNOSTECH ZPRACOVÁNÍ

8.1. Charita vede písemné záznamy o činnostech zpracování, v papírové nebo elektronické podobě, v rozsahu informací vyžadovaných právní úpravou; vzor záznamů o činnostech zpracování tvoří přílohu č. 1 této směrnice.

8.2. Záznamy o činnostech zpracování předloží Charita dozorovému úřadu na požádání.

8.3. Charita v prováděcí dokumentaci určí jednoho nebo několik zaměstnanců odpovědných za vedení a aktualizaci záznamů o činnostech zpracování.

Článek 9.
OHLAŠOVÁNÍ A OZNAMOVÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

9.1. Bezpečnostními incidenty se pro účely této směrnice rozumí tzv. porušení zabezpečení osobních údajů, tedy případy porušení zabezpečení, které vedou k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění osobních údajů, jakými jsou kupříkladu hackerský útok, úmyslné i nedbalostní poskytnutí osobních údajů jednotlivým zaměstnancem neoprávněné třetí osobě, ztráta dešifrovacího klíče či zničení evidence osobních údajů v důsledku povodně, požáru atd.

9.2. Charita **ohlásí bezpečnostní incident Úřadu pro ochranu osobních údajů**, příp. jinému příslušnému dozorovému úřadu, bez zbytečného odkladu, nejpozději však do 72 hodin poté, co se o bezpečnostním incidentu dozvěděla. Není-li tato lhůta dodržena, v rámci ohlášení jsou uvedeny důvody pro nedodržení lhůty. Jinak ohlášení obsahuje informace v rozsahu dle čl. 33 GDPR; vzor ohlášení tvoří přílohu č. 2 této směrnice. Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

9.3. Ohlašovány **nemusí** být **drobné bezpečnostní incidenty**, tedy takové, které ve svém důsledku pravděpodobně nepředstavují riziko pro práva subjektů údajů (např. únik šifrovaných nebo pseudonymizovaných osobních údajů).

9.4. Pokud bezpečnostní incident **pravděpodobně** představuje **vysoké riziko** pro práva subjektů údajů, Charita **oznámí** bezpečnostní incident bez zbytečného odkladu **dotčeným subjektům údajů**, a to srozumitelně za použití jasných a jednoduchých jazykových prostředků. Oznámení obsahuje informace v rozsahu dle čl. 34 GDPR; vzor oznámení tvoří přílohu č. 3 této směrnice. Vysoké riziko pro práva subjektů údajů je pravděpodobné zejména v případech, kdy subjekty údajů v důsledku bezpečnostního incidentu mohou i potenciálně dojít k jakékoliv újmě z hlediska psychiky, cti, pověsti či majetku (např. uniknou-li citlivé či zneužitelné údaje, nebo jsou-li zničeny důležité osobní údaje bez zálohy).

9.5. **Oznámení** o bezpečnostním incidentu dotčeným subjektům údajů **se nevyžaduje**, pokud

ohledně dotčených subjektů údajů Charita zavedla preventivní nebo následná opatření, která zajistí, že vysoké riziko se pravděpodobně neprojeví (např. šifrování nebo znehodnocení uniklých osobních údajů). Vyžaduje-li oznámení bezpečnostního incidentu nepřiměřené úsilí, subjekty údajů jsou informovány veřejným oznámením nebo podobným opatřením.

9.6. Charita **dokumentuje** všechny případy bezpečnostních incidentů bez ohledu na to, zda bezpečnostní incident musí být ohlášen dozorovému úřadu nebo oznámen dotčeným subjektům údajů. Dokumentace obsahuje popis bezpečnostního incidentu, jeho účinky a přijatá nápravná opatření, a je vedena tak, aby umožnila dozorovému úřadu ověřit soulad postupu s právní úpravou.

9.7. Charita v prováděcí dokumentaci určí jednoho nebo několik odpovědných zaměstnanců, kteří posuzují povahu a okolnosti bezpečnostního incidentu a rozhodují o tom, zda Charita jednotlivý bezpečnostní incident ohlásí dozorovému úřadu a/nebo oznámí dotčeným subjektům údajů.

Článek 10.
POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ (DPIA)

10.1. V případě, že se Charita domnívá, že některá její stávající nebo budoucí činnost zpracování osobních údajů, zejména při využití nových technologií, má/bude mít **pravděpodobně** s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek **vysoké riziko** pro práva subjektů údajů (např. využití cloudových služeb, monitorování webových aktivit zaměstnanců apod.), provede před zpracováním, resp. před účinností GDPR, **posouzení vlivu** dotčeného zpracování **na ochranu osobních údajů**, tzv. DPIA. V rámci tohoto posouzení Charita zhodnotí nezbytnost a přiměřenost zpracování osobních údajů, jeho možná rizika a plánová opatření k řešení těchto rizik. Výsledkem posouzení je písemný dokument, který je součástí dokumentace vedené k prokázání souladu s GDPR.

10.2. Charita provádí DPIA zejména v případě, že rozsáhle zpracovává citlivé údaje nebo rozsáhle a systematicky monitoruje veřejně přístupné prostory či spadá-li některá její činnost zpracování do seznamu druhů zpracování podléhajících požadavku DPIA, který sestaví Úřad pro ochranu osobních údajů nebo jiný dozorový úřad členského státu Evropské unie.

10.3. Pokud nelze vysoké riziko zpracování dle výsledků provedeného DPIA dostatečně eliminovat vhodnými opatřeními, Charita **konzultuje** předmětnou činnost zpracování s Úřadem pro ochranu osobních údajů.

10.4. Charita v prováděcí dokumentaci určí zaměstnance, kteří pravidelně posuzují pravděpodobnost vysokého rizika zpracování pro práva subjektů údajů a rozhodují o tom, zda Charita provede DPIA, a kteří na základě DPIA rozhodují, zda Charita bude činnost zpracování konzultovat s dozorovým úřadem.

Článek 11.
POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ (DPO)

11.1. V případě, že Charita nebo některé Charity společně ustanovují pověřence pro ochranu osobních údajů (dále také jako „pověřenec“), jmenují do této funkce osobu s potřebnými znalostmi a praxí v oblasti ochrany osobních údajů. **Pověřencem může být jmenován** zaměstnanec Charity nebo externí poskytovatel služeb, Charita však zajistí, aby u pověřence nedocházelo ke střetu zájmů z důvodu jeho pracovního zařazení nebo výkonu další činnosti u Charity. S externím poskytovatelem služeb pověřence Charita uzavírá smlouvu o výkonu funkce pověřence.

11.2. Za účelem zajištění **nezávislosti** výkonu jeho funkce pověřenec nedostává ohledně výkonu funkce a jeho způsobu žádné pokyny – tím není dotčena možnost Charity zadávat pověřenci úkoly v oblasti jeho působnosti – a není za výkon své funkce sankcionován. Pověřenec má **přímý přístup** k vedení Charity a také k sekretariátu CHCŘ, aby se na vedení Charity/CHCŘ mohl kdykoli obrátit v záležitostech ochrany osobních údajů.

11.3. Charita zajistí, že pověřenec je náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů, že má přístup k osobním údajům a operacím zpracování, a poskytne mu zdroje nezbytné k plnění jeho funkce a k udržování jeho odborných znalostí.

11.4. Je-li pověřenec jmenován, Charita zveřejní jeho **kontaktní údaje** a zároveň je sdělí Úřadu pro ochranu osobních údajů.

11.5. V případě, že Charita nejmenuje pověřence, jelikož dle jejího posouzení k tomu není povinna, písemně sepíše toto **posouzení** tak, aby byla schopna prokázat, že byly řádně zohledněny relevantní faktory, a založí toto posouzení do dokumentace vedené k prokázání souladu s GDPR.

Článek 12.
ZÁVĚREČNÁ USTANOVENÍ

12.1. Nedílnou součástí tohoto vnitřního předpisu jsou následující přílohy:

Příloha č. 1 – Vzor záznamů o činnostech zpracování (dle čl. 30 GDPR)

Příloha č. 2 – Vzor ohlášení bezpečnostního incidentu dozorovému úřadu (dle čl. 33 GDPR)

Příloha č. 3 – Vzor oznámení bezpečnostního incidentu subjektům údajů (dle čl. 34 GDPR)

12.2. Tento vnitřní předpis nabývá účinnosti dnem 25. 5. 2018.

Mgr. et Mgr. Lukáš Curylo

ředitel CHČR

PŘÍLOHA č. 1 – Vzor záznamů o činnostech zpracování (dle čl. 30 GDPR)

Záznamy o činnostech zpracování dle čl. 30 nařízení GDPR	
Název zpracování	
Popis zpracování osobních údajů	
Datum vzniku zpracování	
Datum poslední aktualizace záznamů	

Kontaktní údaje	Jméno/Název	Adresa (ulice, město, PSČ)	Tel./Fax	Email/Jiné
Správce				
Pověřenec pro ochranu osobních údajů (DPO)				
Zástupce správce				
Společný správce 1				
Společný správce 2				

Účel zpracování osobních údajů	Účel zpracování osobních údajů
Hlavní účel zpracování osobních údajů	
Účel zpracování 1	
Účel zpracování 2	
Účel zpracování 3	

Kategorie subjektů údajů	Popis kategorií subjektů údajů
Kategorie 1	
Kategorie 2	
Kategorie 3	

Kategorie osobních údajů	Popis kategorií osobních údajů
Kategorie 1	
Kategorie 2	

Kategorie 3	

Bezpečnost	**Bezpečnost zpracování osobních údajů (popis jednotlivých technických a organizačních opatření)**
Technická opatření	*[vyplňuje se, pokud je to možné]*
Organizační opatření	*[vyplňuje se, pokud je to možné]*
Poznámky	*[vyplňuje se, pokud je to možné]*

Plánované lhůty pro výmaz jednotlivých kategorií údajů	**Plánovaná lhůta pro výmaz**
Kategorie 1	*[vyplňuje se, pokud je to možné]*
Kategorie 2	*[vyplňuje se, pokud je to možné]*
Kategorie 3	*[vyplňuje se, pokud je to možné]*

Příjemci osobních údajů	**Popis příjemců**
Příjemce 1	
Příjemce 2	
Příjemce 3	
Příjemce 4	

Přenos OÚ mimo EU/EHP (3. země či mezinárodní organizace)	**Příjemce**	**Země**	**Typ záruk**	**Poznámka**
Subjekt 1				
Subjekt 2				
Subjekt 3				

PŘÍLOHA č. 2 – Vzor ohlášení bezpečnostního incidentu dozorovému úřadu (dle čl. 33 GDPR)

Ohlášení případu porušení zabezpečení osobních údajů (bezpečnostního incidentu)				
Kontaktní údaje	**Jméno/Název**	**Adresa (ulice, město, PSČ)**	**Tel./Fax**	**Email/Jiné**
Pověřenec pro ochranu osobních údajů				
Jiné kontaktní místo				

Povaha a rozsah incidentu	**Popis incidentu**
Popis případu	
Kategorie dotčených subjektů údajů	*[vyplňuje se, pokud je to možné]*
Přibližný počet dotčených subjektů údajů	*[vyplňuje se, pokud je to možné]*
Kategorie dotčených (záznamů) osobních údajů	*[vyplňuje se, pokud je to možné]*
Přibližné množství dotčených (záznamů) OÚ	*[vyplňuje se, pokud je to možné]*

Pravděpodobné důsledky incidentu	**Popis pravděpodobných důsledků**
Důsledek 1	
Důsledek 2	
Důsledek 3	

Navržená/přijatá opatření k řešení incidentu	**Popis opatření k řešení incidentu, včetně opatření ke zmírnění nepříznivých dopadů**
Opatření 1	
Opatření 2	
Opatření 3	

Odůvodnění zmeškání lhůty pro ohlášení (72 hodin od zjištění incidentu)	**Popis důvodů zpoždění ohlášení**
Důvod 1	
Důvod 2	

<u>Poznámka</u>: výše přiložený formulář ohlášení lze využít také pro účely vedení dokumentace o veškerých bezpečnostních incidentech (viz čl. 33 odst. 5 GDPR).

PŘÍLOHA č. 3 – Vzor oznámení bezpečnostního incidentu subjektům údajů (dle čl. 34 GDPR)

Poznámka: informace o bezpečnostním incidentu adresovaná dotčeným subjektům údajů musí být formulována co nejsrozumitelněji, pomocí jasných a jednoduchých jazykových prostředků. Vzor možného informačního sdělení zde:

Vážená paní / vážený pane,

s politováním Vás musíme informovat, že dne *[datum]* došlo v naší organizaci *[název]* k bezpečnostnímu incidentu, v rámci kterého *[popis incidentu a jeho povahy]*.

Z informací dostupných k dnešnímu dni lze předpokládat, že v důsledku incidentu pravděpodobně *[popis pravděpodobných důsledků incidentu, zejména pro subjekty údajů a jejich osobní údaje]*.

K vyřešení daného incidentu a ke zmírnění možných negativních dopadů na Vaši osobu a Vaše osobní údaje jsme navrhli a přijali několik opatření. *[popis navržených / přijatých opatření]*

Pro více informací se můžete obrátit na našeho pověřence pro ochranu osobních údajů *[jméno/název]* / se na nás můžete obrátit na tel. čísle *[tel. číslo]* nebo na emailové adrese *[email]*.

S úctou,

[název organizace]
[jméno, příjmení zástupce]
[pozice/funkce]