HVOZDY

CENTRUM SOCIÁLNÍCH SLUŽEB HVOZDY, O.P.S.
Masečín 119, 252 07 Štěchovice
IČ: 29128218, tel. 724 110 441
e-mail: info@css-hvozdy.cz
www.css-hvozdy.cz

OCHRANA OSOBNÍCH ÚDAJŮ (GDPR)

vnitřní předpis č. B/05/2023

Část I.
ÚVODNÍ USTANOVENÍ

01. Centrum sociálních služeb Hvozdy, o.p.s. (dále jen „společnost) považuje problematiku ochrany práv a svobod fyzických osob za zásadní a s ohledem na tuto skutečnost přijímá tuto bezpečnostní politiku.
Na základě 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 (dále jen „Obecné nařízení o ochraně osobních údajů“) se společnost zavazuje nakládat s osobními údaji svých zaměstnanců, klientů i třetích stran (uvedené fyzické osoby dále společně jen „subjekty údajů“) v důsledném souladu s tímto nařízením tak, aby nemohla být způsobena subjektům údajů žádná újma (nebo alespoň v maximální možné míře bylo omezeno riziko jejího vzniku) z hlediska zneužití, poškození, krádeže osobních údajů nebo jiného neoprávněného nakládání s nimi, způsobená v souvislosti s poskytováním péče a dalších činností společnosti. Společnost se zavazuje dodržovat základní principy vyplývající z Obecného nařízení o ochraně osobních údajů ve vztahu k nakládání s osobními údaji.
02. Tento vnitřní předpis dále vychází z doporučeného podkladu zpracovaného MPSV - Doporučený postup č. 02/2018, kterým se v rámci metodického a koncepčního vedení MPSV vypracovává Kodex chování ve smyslu č. 40 Obecného nařízení o ochraně osobních údajů - GDPR pro potřeby výkonu sociální politiky vydaného dne 09.04.2018 s účinností od 25.05.2018.
03. V tomto vnitřním předpise je uvedeno následující:
    - Základní pravidla pro nakládání s osobními údaji včetně jejich procesování
    - Informace o základech zpracování osobních údajů, práva subjektu údajů a jejich uplatnění
    - Základní pravidla pro zajištění bezpečného prostředí jak fyzického, tak i kybernetického
04. Přístup k osobním údajům uložených na firemních ICT (informační a komunikační technologie) zařízeních je řízen takovým způsobem, že každý zaměstnanec se může přihlásit do sítě pouze pod svým účtem. Přístup k osobním údajům je umožněn zaměstnancům pouze v takové míře, kterou potřebují k plnění svých pracovních povinností.
05. Společnost se zavazuje pravidelně kontrolovat dodržování stanovených zásad a procesů zaměstnanci. Pravidelné porušování a nedodržování zásad a pravidel stanovených v tomto vnitřním předpise, nebo **hrubé porušení či nedodržení těchto zásad a pravidel**, může být dle intenzity porušení vyhodnoceno jako porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci zvlášť hrubým způsobem nebo jako závažné porušení, jež může vést k ukončení pracovněprávního vztahu příslušného zaměstnance (v případě zaměstnanců v pracovním poměru pak k ukončení tohoto vztahu výpovědí nebo jeho okamžitým zrušením).
06. Společnost se zavazuje zajišťovat, a každý její zaměstnanec je povinen při výkonu práce nebo v souvislosti s ní respektovat, že při zpracovávání osobních údajů budou dodržovány zejména následující podmínky:
    - Zpracování osobních údajů bude probíhat korektním, transparentním a zákonným způsobem
    - Zpracování osobních údajů bude prováděno pouze pro určité, výslovně vyjádřené a legitimní účely
    - Zpracování osobních údajů bude přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu
    - Zpracování osobních údajů bude probíhat jenom po dobu nezbytně nutnou ve vztahu k účelu, po uplynutí této doby budou osobních údajů zlikvidovány
    - Budou přijata taková technická a organizační opatření, aby nemohlo dojít ke zneužití, odcizení či poškození osobních údajů
07. Prevence je zajištěna nastavením systému a procesů, při nichž ke zpracování osobních údajů dochází a proškolení všech zainteresovaných zaměstnanců/zpracovatelů s těmito postupy.
08. Všichni zaměstnanci společnosti, včetně externích dodavatelů služeb, podílející se na zpracování osobních údajů, jsou s tímto vnitřním předpisem seznámeni. Jakmile získá zaměstnanec podezření na bezpečnostní událost nebo incident je dle tohoto předpisu povinen tuto okolnost bezprostředně nahlásit odpovědné osobě (příloha Řízení incidentů).
09. Jakákoliv bezpečnostní událost nebo incident musí být bezprostředně po zjištění prošetřena a příčina incidentu musí být odstraněna, tak, aby nemohlo dojít k dalším škodám. Veškeré relevantní informace týkající se bezpečnostní události nebo incidentu musí být náležitě zdokumentovány.

Část II.
ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZAMĚSTNANCŮ

Zpracování osobních údajů zaměstnanců je plně v kompetenci vedení společnosti a personalisty. Za účelem mzdové agendy jsou osobní údaje zaměstnanců zpracovány mzdovou účetní. Na zpracování osobních údajů zaměstnanců se na základě zákona o nemocenském a zdravotním pojištění nevztahuje podmínka souhlasu se zpracováním osobních údajů.

Čl. 01
Zpracování osobních údajů při přijetí nových zaměstnanců

1.1. Pro účely přijímacího řízení není třeba, aby subjekt osobních údajů udělil informovaný souhlas se zpracováním osobních údajů, neboť zpracování probíhá na základě oprávněných zájmů správce. Subjekt osobních údajů však musí být po poskytnutí osobních údajů informován o rozsahu, právním základu, účelech zpracování a jeho právech v rozsahu dle GDPR.

1.2. Zpracování poskytnutých osobních údajů uchazeče je bez udělení souhlasu možné pouze po dobu trvání přijímacího řízení.

1.3. Poskytnuté osobní údaje je možné uchovávat v nezměněné podobě a v plném rozsahu pouze pokud uchazeč k tomu udělí souhlas, a to například pro účely oslovení při uvolnění relevantní pracovní pozice v budoucnu. Zodpovědnost za toto jednání je na osobě, která přijímací řízení vede.

1.4. Přístup k těmto informacím má pouze ředitelka společnosti a její zástupce. (dále jen vedení společnosti)

Čl. 02
Zákonné **zpracování osobních údajů zaměstnanců**

2.1. Zpracování osobních údajů zaměstnanců je prováděno na základě:
- nezbytnosti zpracování pro plnění pracovní smlouvy
- plnění právních povinnosti správce, vyplývajících zejména ze zákona č.262/2006 Sb., zákoník práce či zákona č. 586/1992 Sb., o daních z příjmů, atp.
- oprávněných zájmů správce
- souhlasu zaměstnanců

2.2. Agenda zpracování je složena z části:

a) Listinné
- Dokumenty tvořící obsah Osobních spisů zaměstnanců. Tyto spisy jsou uloženy a uzamčeny v kanceláři personalisty v uzamykatelné skříni. Přístup k nim má pouze vedení společnosti a personalista.

b) Elektronické
- Data a údaje zaměstnanců vztahující se k jejich personálním, mzdovým, pojistným, sociálním, odvodovým a jiným skutečnostem.
- Elektronicky jsou tyto údaje zpracovány v aplikacích E-quip a Grand, kam mají přístup pouze vybraní zaměstnanci v souladu se svoji autorizací a přístupovými právy. Přesný popis a postupy se nachází v příloze tohoto vnitřního předpisu - **Pravidla užívání informační a komunikační technologie**

2.3. Typ zpracovávaných osobních údajů zaměstnanců:
- příjmení, jméno, titul
- datum a místo narození
- rodné příjmení
- rodné číslo
- adresa trvalého bydliště
- adresa pro korespondenci
- rodinný stav
- státní příslušnost
- telefonní kontakt a e-mail
- kontakt na příbuzné v případě mimořádné situace
- identifikační údaje zdravotní pojišťovny
- ZPS, TZP
- informace a doklady o vzdělání, výcviku, školeních a kvalifikaci
- doklad prokazující školení PO a BOZP
- odborné znalosti a dovednosti
- čísla vedených bankovních účtů (z důvodu převodu mzdy)
- dohoda o hmotné odpovědnosti

- doklad o zdravotní způsobilosti
- evidenční list důchodového pojištění
- mzdový výměr
- předávací protokol
- popis pracovní pozice
- potvrzení o studiu dětí (v případě uplatňování nároku na snížení daně)
- potvrzení o zaměstnání manžela/ky (v případě uplatňování nároku na snížení daně)
- pracovní smlouva, dohoda konaná mimo pracovní poměr (DPP, DPČ)
- prohlášení k dani ze mzdy
- přihláška k nemocenskému pojištění
- zápočtový list (nebo potvrzení ÚP nebo ČSSZ)

2.4. Přístup k osobním údajům zaměstnanců má:
- vedení společnosti
- personalista
- mzdová účetní
- další „určení pracovníci“ - administrátor aplikace/informačního systému používaného pro personálně - mzdovou agendu (z důvodu údržby)

Pokud se jedná o externí spolupracovníky, kteří plní roli zpracovatele, zpracování osobních údajů zaměstnanců probíhá na základě písemné smlouvy a zpracovatel je povinen dodržovat zásady GDPR.
Správce vede evidenci všech zpracovatelů a je za ně zodpovědný. Správce dohlíží a kontroluje, že zpracovatelé zpracovávají osobní údaje v souladu s GDPR, aby byla zajištěna ochrana práv subjektu údajů.

2.5. Zpracování je prováděno za účelem realizace pracovněprávních vztahů, plnění všech právních povinností zaměstnavatele a k zajištění ochrany jeho práv a právem chráněných zájmů. Na toto zpracování se nevztahuje povinnost informovaného souhlasu subjektu údajů.

2.6. Zpracování osobních údajů provádí výhradně personalista a mzdová účetní. Zpracovávané osobní údaje jsou získávány výhradně od příslušných zaměstnanců společnosti.

2.7. Zpracování osobních údajů zaměstnance je prováděno od okamžiku vzniku jeho pracovního poměru a je ukončeno (vyjma archivování vybraných dokumentů v souladu s ustanovením příslušných předpisů a pro oprávněné zájmy zaměstnavatele) bezprostředně po jeho zániku. Údaje o zaměstnancích v digitální formě, jejichž pracovní poměr byl ukončen, jsou následně uloženy v archivu aplikace E-quip a Grand po dobu vyplývající ze zákona.
Písemnosti (doklady) s osobními údaji, jejichž účel pominul, jsou v souladu s ustanovením platných zákonů zlikvidovány.

2.8. Osobní spisy zaměstnanců nesmí být volně přístupné, vždy musí být zpracovány a uloženy tak, aby nedošlo k neoprávněnému přístupu k těmto dokumentům. Zaměstnanci jsou náležitě proškoleni o svých povinnostech. Prostory a skříně s osobními spisy zaměstnanců jsou uzamykatelné. Osobní údaje v elektronické formě jsou přístupné pouze oprávněným osobám na základě přístupových práv.

2.9. Pokud by chtěl správce osobních údajů zpracovávat osobní údaje zaměstnanců za jinými účely, než jsou uvedeny výše, je povinen o tom subjekt údajů informovat a v případě, že takové zpracování nebude mít jiný zákonný důvod, opatřit si jejich informovaný souhlas. Takovou situací může být například umístění fotografie zaměstnance na webových stránkách zaměstnavatele.

2.10. Povinností zaměstnavatele je vydat zaměstnanci při měsíčním vyúčtování mzdy nebo platu dle § 142 odst. 5 zákoníku práce výplatní pásku. Vzhledem k tomu, že uvedený doklad obsahuje osobní údaje, je zaměstnavatel povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Proto k výše uvedené skutečnosti se výplatní pásky vydávají elektronicky prostřednictvím e-mailové korespondence v zaheslované příloze ve formátu pdf, s tím, že každý pracovník má svoje unikátní heslo.

Část III.
ZPRACO**VÁNÍ OSOBNÍCH ÚDAJŮ KLIENTŮ**

01. Zpracování osobních údajů klientů začíná zasláním Žádosti o přijetí do služby. Informace o žadatelích jsou ve společnosti uloženy v listinné podobě u sociálního pracovníka. Listinné osobní složky jsou umístěny v uzamykatelné skříni v kanceláři sociálního pracovníka.

02. Ve společnosti dochází ke zpracování osobních údajů klientů na základě plnění smlouvy za účelem poskytování sociálních služeb. Rozsah poskytovaných služeb a stejně tak zpracování osobních údajů klientů je předmětem Smlouvy o poskytování sociální služby. Nedílnou součástí smlouvy je i informovaný souhlas subjektu údajů, kde klient může udělit

nebo zamítnout souhlas se zpracováním svých údajů, pro něž nemá správce jiný právní základ. Příkladem takového zpracování je např. umístění fotografií z různých akcí společnosti.

03. Součástí smlouvy je také informace, komu mohou být sdělovány osobní a citlivé údaje o klientovi. Společnost se těmito pravidly musí striktně řídit.

04. Osobní údaje klientů jsou zpracovány v:

    a) **Listinné formě**
        - Osobní složka každého klienta je umístěna v uzamykatelné skříni v kanceláři sociálního pracovníka.

    b) **Elektronické formě**
        - Elektronická aplikace informační systém E-quip, která obsahuje veškeré nezbytné osobní údaje klientů. Přístup do této aplikace je umožněn pouze zaměstnancům pod svým uživatelským účtem a heslem na základě jednotlivých přístupových práv.

05. Při zpracování zvláštních kategorií osobních údajů klientů je třeba zvýšené opatrnosti, neboť zdravotnická dokumentace nutná k přijetí subjektu obsahuje natolik citlivé informace, že jejich zneužití by mohlo znamenat pro subjekt osobních údajů značné omezení osobních práv a svobod.

06. Typ zpracovávaných osobních údajů klientů:
    - příjmení, jméno
    - datum a místo narození, rodné číslo
    - adresa trvalého bydliště, korespondenční adresa
    - telefonický kontakt
    - údaje o zdravotní pojišťovně
    - kopie OP, průkazu ZTP, ZTP/P
    - státní příslušnost
    - údaje o svéprávnosti
    - dietologické údaje
    - informace o příspěvku na péči
    - výše důchodu
    - údaje o schopnosti zvládat životní potřeby
    - údaje vedené v souladu s právními předpisy ve zdravotnické dokumentaci

07. Přístup k osobním údajům klientů v odlišném rozsahu má:
    - Vedení společnosti
    - Sociální pracovník
    - Pracovník v sociálních službách
    - Odborný pracovník (např. psycholog)
    - Hospodářsko - administrativní pracovník
    - Studenti, dobrovolníci a všichni další externisté nemají k žádným osobním údajům klientů přístup, ledaže je to nezbytně nutné pro realizaci jejich činnosti. V takovém případě musejí podepsat dohodu o mlčenlivosti.

    Správce (vedení společnosti) vede evidenci všech externistů a zpracovatelů a je za ně zodpovědný. Správce dohlíží a kontroluje, že zpracovatelé zpracovávají osobní údaje v souladu s GDPR aby byla zajištěna ochrana práv subjektu údajů.

08. Zpracování osobních údajů klientů provádí pouze personál společnosti k tomu určený, externí pracovníci na základě smlouvy a ve velmi omezené míře studenti a dobrovolníci, každý zaměstnanec i externista je vázán povinností mlčenlivosti a je prokazatelně seznámen s interními směrnicemi týkající se zpracování osobních údajů. Zpracování se provádí pouze v prostorech k tomu určených.

09. Zpracovávané osobní údaje jsou získávány od příslušných subjektů údajů, pokud subjekt údajů není schopen tyto informace poskytnout, tak od zákonných zástupců, či jiné k tomu oprávněné osoby.

10. Informace k délce zpracování jsou uvedeny v kapitole Archivace, skartace a likvidace dokumentace s obsahem osobních údajů. Písemnosti (doklady) s osobními údaji, jejichž účel pominul, jsou v souladu s ustanovením platných zákonů zlikvidovány.

11. Dokumentace s obsahem osobních údajů (listinná i elektronická) nesmí být volně dostupná. Dokumentace musí být vždy zpracována a uložena tak, aby nedošlo k neoprávněnému přístupu k těmto dokumentům. Prostory a skříně s těmito dokumenty jsou uzamykatelné a přístup k nim má pouze pověřený personál. Elektronická dokumentace je přístupná pouze oprávněným osobám na základě přístupových práv.

12. Pokud chce správce zpracovávat i další údaje, na které se uvedené zákonné důvody zpracování nevztahují, musí správce před tímto zpracováním získat podepsaný (výslovný) informovaný souhlas. Příkladem takového zpracování je umístění fotografií klientů na webových stránkách za účelem propagace správce.

Všechna zpracování musí být uvedena v Registru osobních údajů (příloha tohoto dokumentu), kde správce uvede účel, rozsah, zákonnost, technická opatření, způsob zpracování, přístupy k těmto údajům a další podrobnosti týkající se daného zpracování osobních údajů.

Část IV.
ZPRACOVÁNÍ OSTATNÍCH KATEGORIÍ OSOBNÍCH ÚDAJŮ

01. Ve společnosti jsou kromě osobních údajů zaměstnanců a klientů zpracovávány i jiné kategorie osobních údajů, avšak v podstatně menším měřítku. Patří sem osobní údaje studentů, brigádníků, dobrovolníků, dárců, rodinných příslušníků a jiných kontaktních osob klientů.
02. Podrobný výčet kategorií, včetně definování právních základů, účelů a způsobů zpracování je předmětem dokumentu Registr osobních údajů a jejich zpracování.

Část V.
INFORMOVANÝ SOUHLAS

01. Zpracovávat osobní údaje může správce na základě:
    a) Souhlasu subjektu údajů
    b) Nezbytnosti zpracování pro plnění či uzavření smlouvy
    c) Nezbytnosti zpracování pro plnění právní povinnosti
    d) Nezbytné ochrany životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
    e) Oprávněných zájmů správce
    f) Veřejného zájmu či výkonu veřejné moci nebo na základě životně důležitého zájmu
02. Získání informovaného souhlasu - zásady udělení souhlasu:
    - správce musí být vždy schopen doložit, že subjekt udělil souhlas s daným zpracováním jeho osobních údajů
    - udělení souhlasu musí být jasně identifikovatelné pro konkrétní účel
    - udělení souhlasu musí být jazykově srozumitelné
    - subjekt údajů má právo svůj souhlas kdykoliv odvolat; toto odvolání musí být zdokumentované; tímto odvoláním není dotčena zákonnost zpracování před jeho odvoláním. Odvolání musí být stejně jednoduché jako udělení souhlasu.
    - Souhlas musí být konkrétní, svobodný, informovaný a jednoznačný
    - Za určitých okolností uděluje za nesvéprávné osoby souhlas se zpracováním jejich údajů jejich zákonný zástupce.
03. Správce k získání informovaného souhlasu využívá některý z příslušných dokumentů (Informování a souhlas pro klienty, Informování a souhlas pro zaměstnance apod.). Podepsaný souhlas je uložen v osobním spise zaměstnance či v osobním spise klienta.
04. Správce osobních údajů je povinen subjekt údajů informovat o všech zpracováních s tím, že poskytuje subjektu údajů, od kterého osobní údaje získal informace o:
    - Totožnosti a kontaktních údajích správce/ popř. pověřence
    - Účelu zpracování
    - Právním základu pro zpracování
    - Případných oprávněných zájmech správce
    - Případných příjemcích osobních údajů
    - Době, po kterou budou osobní údaje uloženy
    - Právu požádat o přístup ke svým osobní údaje
    - Právu na opravu, výmaz, omezení zpracování nebo vznést námitku proti zpracování
    - Právu na přenositelnost osobní údaje
    - Právu podat stížnost dozorovému úřadu

Část VI.
PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ

01. Předání osobních údajů třetím stranám (např. pojišťovna, finanční úřad) probíhá pouze v rozsahu nezbytném pro plnění zákonných povinností správce. (např. Osobní údaje klientů jsou na základě právní povinnosti předávány Úřadu práce za účelem stanovení příspěvku na péči nebo osobní údaje klientů jsou dále předávány soudu v rámci dědického řízení).
02. Předání osobních údajů na jiném základě, než na základě plnění právní povinnosti správce, může proběhnout pouze na základě souhlasu subjektu údajů.

Část VII.
KAMEROVÝ SYSTÉM

Ve společnosti nejsou v současné době umístěny žádné kamery se záznamem ani žádné kamery snímající prostory společnosti. Pokud by kamery se záznamem byly instalovány, budou pro jejich používání platit přesně vymezená pravidla.

Část VIII.
LISTINNÁ DOKUMENTACE

Listinná dokumentace je specifickým datovým nosičem, protože u ní nelze zajistit ochranu přístupovým heslem ani zašifrováním. Pro listinnou dokumentaci tedy nelze nastavit technická opatření. O to důležitější je dodržovat organizační a fyzická opatření. Zejména:

- Pravidlo prázdného stolu
- Uzamykání prostor
- Ukládání dokumentů s obsahem osobních údajů v uzamykatelných skříních
- Nenechávat nikde volně ležet dokumenty s obsahem chráněných informací bez dozoru
- Chránit dokumenty před poškozením apod.

Část IX.
INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE

Informační a komunikační technologie (ICT) má definována závazná pravidla pro všechny uživatele ICT přicházející do kontaktu s osobními údaji v samostatném dokumentu s názvem Pravidla užívání ICT, který je přílohou k tomuto vnitřnímu předpisu. Při práci v počítačové síti je dodržování bezpečnostních zásad zvláště důležité, protože provozní nekázeň jednoho uživatele může ohrozit práci ostatních uživatelů počítačové sítě, anebo vážně narušit společné databáze a zejména ohrozit bezpečnost chráněných dat a informací.

Část X.
ŘÍZENÍ INCIDENTŮ

Základní principy procesu řízení bezpečnostních incidentů vychází z normy ISO/IEC 27001. Řízení incidentů je detailně popsáno v příloze tohoto vnitřního předpisu s názvem **Popis řízení incidentů**. Tento dokument definuje rozsah činností zahrnutých do pojmů řízení bezpečnostních incidentů ve specifických podmínkách Centra sociálních služeb Hvozdy, o.p.s. a stanovuje hlavní zásady při jejich zvládání v souladu s požadavky Obecného nařízení o ochraně osobních údajů.

Část XI.
SEZNÁMENÍ ZAMĚSTNANCŮ S VNITŘNÍM PŘEDPISEM

01. Každý nový zaměstnanec společnosti (stejně tak každá jiná osoba přistupující k osobním údajům) je při nástupu do zaměstnání seznámen s tímto vnitřním předpisem. Při podpisu pracovní smlouvy každý zaměstnanec, případně i externí spolupracovník na kontraktorské bázi, podepíše dohodu o mlčenlivosti. Tím se oproti svému podpisu zavazuje, že nijakým způsobem neposkytne žádné z osobních údajů zaměstnanců, klientů nebo smluvních stran, se kterými se v rámci výkonu své pracovní/smluvní činnosti setkal, dalším osobám nebo organizacím.
02. Porušení mlčenlivosti může mít za následek rozvázání pracovního poměru pro hrubé porušení pracovních povinností a vzniku škody na straně zaměstnavatele, za kterou je zaměstnanec odpovědný podle dotčených ustanovení zákoníku práce. Porušení povinnosti mlčenlivosti, jenž by mohlo vést i ke zneužití osobních údajů, může být rovněž předmětem veřejnoprávních sankcí v rámci správního, případně trestního řízení.
03. Zaměstnanec při nástupu do zaměstnání obdrží seznam interní dokumentace, se kterou je povinen se seznámit. Seznámení probíhá formou samostudia, při nejasnostech se zaměstnanec obrací na svého nadřízeného, který mu danou problematiku vysvětlí.
04. Své seznámení s daným vnitřním předpisem společnosti potvrzuje zaměstnanec datem a podpisem v dokumentu Seznámení s vnitřním předpisem. Tato seznámení s vnitřními předpisy jsou uloženy ve složkách jednotlivých vnitřních předpisů v kanceláři hospodářsko-administrativního úseku. Zodpovědnost za jejich vedení má hospodářsko-administrativní pracovník.
05. Stávající zaměstnanci jsou informováni o změnách v interních směrnicích a s každou novou verzí musí být také seznámeni.
    Seznámení s vnitřním předpisem může probíhat formou samostudia nebo hromadně. Seznámení s vnitřním předpisem musí být opět zdokumentováno na formuláři, kde zaměstnanec svým podpisem stvrzuje, že byl náležitě seznámen. Záznamy jsou opět uloženy ve složkách jednotlivých vnitřních předpisů v kanceláři hospodářsko-administrativního úseku. Zodpovědnost za jejich vedení má hospodářsko-administrativní pracovník.

Část XII.
ARCHIVACE, SKARTACE A LIKVIDACE DOKUMENTŮ A ZÁZNAMŮ OBSAHUJÍCÍ OSOBNÍ ÚDAJE

01. Obecné povinnosti pro archivaci jsou předmětem několika zákonů, zejména pak:
    - Zákon č. 499/2004 Sb Zákon o archivnictví a spisové službě
    - Zákon č. 563/1991 Sb. Zákon o účetnictví
    - Zákon č. 235/2004 Sb. Zákon o dani z přidané hodnoty
    - Zákon č. 582/1991 Sb. Zákon o organizaci a provádění sociálního zabezpečení
    - Zákon č. 108/2006 Sb. Zákon o sociálních službách
02. Zákoník práce neukládá zaměstnavateli povinnost uchovávat veškeré dokumenty týkající se zaměstnanců (zaměstnavatel je však oprávněn vést osobní spis zaměstnance).
03. Zaměstnavatel se zavazuje tuto dokumentaci (včetně elektronické) zlikvidovat do 5 let po ukončení pracovního poměru. Konkrétní lhůta pro zničení relevantní dokumentace musí být určena, s ohledem na konkrétní dokumenty a konkrétní postavení zaměstnance.
04. Zákon o organizaci a provádění sociálního zabezpečení ukládá povinnost uchovávat:
    - Evidenční listy 3 roky
    - Záznamy o pojistném a sociálním zabezpečení a příspěvku na státní politiku zaměstnanosti 6 let
    - Mzdové listy a účetní záznamy pro účely důchodového pojištění (např. doklady o trvání pracovního poměru, lékařské prohlídky, záznamy o úrazech a nemocech, evidenci docházky aj. po dobu 30 let.
05. Archivace dokumentace klientů sociálních služeb se řídí zákonem č. 108/2006 Sb. Zákonem o sociálních službách, vyhlášky MPSV č. 505/2006 Sb (Standardy kvality, SQ č. 6), který uvádí, že „Poskytovatel má stanovenou dobu pro uchování dokumentace o osobě po ukončení poskytování sociální služby“.
    Doba pro uchování klientské dokumentace je ve společnosti Centrum sociálních služeb Hvozdy, o.p.s. stanovena na délku 5 let.
06. Tyto dokumenty musí být archivovány po tuto dobu. Správce osobních údajů, tedy zaměstnavatel, musí zajistit, že dokumentace bude uložena tak, aby nemohlo dojít k poškození, zničení nebo zneužití těchto dokumentů.
07. Společnost archivuje dokumentaci ve svém archivu s omezeným přístupem pouze pro vedení společnosti, mzdovou účetní a hospodářsko-administrativního pracovníka. Případný převoz archivovaných dokumentů je řádně zdokumentován.
08. Po skončení účelu pro zpracování daných dokumentů má zaměstnavatel povinnost tyto dokumenty prokazatelně zlikvidovat.

Část XIII.
ZÁVĚREČNÁ USTANOVENÍ

01. Všichni zaměstnanci společnosti jsou povinni řídit se tímto vnitřním předpisem.
02. V případě nutnosti či potřeby mohou zaměstnanci společnosti do tohoto vnitřního předpisu kdykoliv nahlédnout v kanceláři hospodářsko - administrativního úseku.
03. Veškeré změny a doplňky tohoto vnitřního předpisu vydává ředitelka společnosti.
04. Tento vnitřní předpis **nabývá účinnosti** dnem 01.01.2023.

Ve Hvozdech dne 01.12.2022

Romana Hromádková
ředitelka společnosti

PŘÍLOHY
- Pravidla užívání informační a komunikační technologie
- Řízení incidentů
- Informace o zpracování osobních údajů, Souhlas se zpracováním osobních údajů (klient)
- Informace o zpracování osobních údajů, Souhlas se zpracováním osobních údajů (zaměstnanec)
- Souhlas se zpracováním osobních údajů pro kontaktní osoby
- Prohlášení o mlčenlivosti

PRAVIDLA UŽÍVÁNÍ
INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE

příloha k vnitřnímu předpisu č. B/05/2023 GDPR

V této části nazvané Informační a komunikační technologie (ICT) jsou definována závazná pravidla pro všechny uživatele ICT přicházející do kontaktu s osobními údaji. Při práci v počítačové síti je dodržování bezpečnostních zásad zvláště důležité, protože provozní nekázeň jednoho uživatele může ohrozit práci ostatních uživatelů počítačové sítě, anebo vážně narušit společné databáze a zejména ohrozit bezpečnost chráněných dat a informací.

Popis sítě a aplikací ICT

01. Společnost Centrum sociálních služeb Hvozdy, o.p.s. (dále jen společnost) zpracovává osobní údaje svých zaměstnanců, klientů a dalších zainteresovaných stran v několika softwarových aplikacích.

02. Seznam softwarových aplikací

E-QUIP

- jedná se o internetový databázový informační systém, kde se uchovávají a zpracovávají osobní údaje zaměstnanců a klientů společnosti
- tento systém se nachází v internetovém prostoru a osobní údaje jsou ukládány a zálohovány v souladu s GDPR, podrobněji popsáno ve Smlouvě o poskytnutí systému E-quip se společností, která systém zpravuje
- do tohoto systému mají přístup tyto osoby:
  - vedení společnosti
  - účetní, mzdová účetní
  - dotační a grantový manažer
  - hospodářsko-administrativní pracovník
  - vedoucí služeb
  - sociální pracovnice
  - pracovníci v sociálních službách
  - administrátor systému
- přístup a přihlášení do systému je zajištěn samostatnými a unikátními uživatelskými účty, hesly a přístupovými právy

GRAND - komplexní ekonomický systém

- jedná se o počítačovou aplikaci, kde se uchovávají a zpracovávají osobní údaje zaměstnanců v souvislosti se mzdovou agendou společnosti
- tato aplikace je nainstalovaná v notebooku účetní společnosti a osobní údaje jsou ukládány a zálohovány v souladu s GDPR.
- do tohoto systému mají přístup tyto osoby:
  - vedení společnosti
  - účetní, mzdová účetní
  - administrátor systému
- přístup a přihlášení do systému je zajištěn samostatným a unikátním heslem

Uživatel ICT

01. Každý uživatel ICT musí dodržovat určená pravidla společnosti.

02. Uživatelem ICT je každý zaměstnanec společnosti přicházející do styku s ICT a jeho daty, nezávisle na tom, zda má právo data modifikovat, vkládat, kopírovat, mazat nebo jenom nahlížet.
Pro oblast bezpečnosti informací obecně platí, že všichni zaměstnanci (uživatelé) mají **odpovědnost** za:
- svěřené prostředky ICT, které v rámci své pracovní činnosti používají
- obsah dat, která ukládají, mění nebo jinak využívá v rámci svých oprávnění
- zálohování lokálních dat souvisejících s výkonem pracovních povinností
- aktuálnost lokální antivirové ochrany na přiděleném PC
- veškeré činnosti provedené v ICT pod jeho účtem

03. Každý uživatel musí zejména:

- seznámit se s politikou bezpečnosti informací a dalšími vnitřními předpisy souvisejícími s bezpečností zpracovávaných osobních údajů
- seznámit se s pravidly používání prostředků ICT
- znát své povinnosti směřující k ochraně dat a informací v používaných prostředcích a zařízeních ICT
- ICT obsluhovat podle manuálů a provedeného zaškolení, vyvarovat se náhodných nebo chybných postupů
- užívat přidělené zařízení a prostředky ICT pouze v rozsahu nutném pro plnění pracovních povinností a svěřených úkolů a jen v rozsahu přidělených přístupových práv
- pracovat s prostředky a zařízením tak, aby je nepoškodil, zejména mechanicky
- pro práci se do ICT **přihlašovat vždy** jen pod svým **uživatelským účtem**
- informace zpracovávat pouze v souladu s přidělenými uživatelskými přístupovými právy
- chránit na používaném počítači zpracovávané chráněné informace heslem, které nesmí sdělovat žádné jiné osobě
- pořizovat nebo modifikovat data v ICT pouze v souladu se skutečností a v rozsahu svého oprávnění
- důsledně dodržovat pravidla antivirové prevence, nechat automaticky kontrolovat na přítomnost virů všechny přijaté soubory, a to včetně souborů na výměnných médiích, stažených z internetu nebo připojených k e-mailu před jejich použitím, otevřením nebo zkopírováním do ICT
- mít svůj lokální PC uživatelsky nastaven tak, aby při opuštění svého pracoviště (i dočasném) na něm žádná osoba nemohla pracovat bez řádného přihlášení (dodržovat „pravidlo čisté obrazovky“)
- zachovávat mlčenlivost o obsahu, způsobu zpracování a způsobu zajištění bezpečnosti chráněných informací vyskytujících se v ICT
- počínat si tak, aby chráněná data a informace nemohly být odposlechnuty, odpozorovány, nebo vyčteny ze zpracovávaných dokumentů a obrazovek neoprávněnými osobami
- zjištění každého bezpečnostního incidentu nebo slabiny v ICT bez zbytečného prodlení hlásit odpovědné osobě
- dodržovat licenční politiku používaného softwaru a respektovat autorskoprávní ochranu dat
- důsledně zálohovat, popřípadě archivovat, veškerá data, pokud nejsou uživateli uložena na centrálních zálohovacích prostředcích
- poskytovat potřebnou součinnost administrátorům ICT v případě plánované údržby počítačových prostředků, při poruchách, závadách nebo při jiných obdobných činnostech

04. Uživatel nesmí zejména:

- záměrně poškozovat prostředky ICT a v nich uložená data
- měnit nastavení prostředků ICT týkající se bezpečnosti nebo nastavení zásadně ovlivňující jejich funkčnost
- využívat nedovoleným způsobem data systému, systémy a sítě nebo neoprávněně zkoušet, zkoumat či testovat zranitelnost systému nebo sítí
- porušovat bezpečnostní opatření a ověřovací procedury ICT
- poskytovat jiným uživatelům jakékoliv klíče, dekodéry či jiné technické prostředky sloužící k zajištění ochrany ICT
- umožnit práci jiné osobě pod svým uživatelským účtem
- zprostředkovávat služby počítačové sítě jiným osobám
- používat neznámá a neidentifikovatelná přenosná média
- provádět jakékoliv technické zásahy do hardwarového vybavení, včetně snímání krytů a porušení plomb, jakožto i změny v konfiguraci hardwaru
- provádět samostatné instalace neodsouhlaseného softwaru (SW) a hardwaru (HW)
- provádět změny v konfiguraci PC
- přemísťovat prostředky a zařízení ICT, rozpojovat kabely a provádět technické úpravy
- využívat ICT pro komerční účely
- přistupovat do sítě nebo k datovým zdrojům v rozporu s přidělenými přístupovými právy a pokoušet se získat neoprávněný přístup k informacím
- kopírovat a distribuovat části nebo celky nainstalovaného operačního systému, aplikací a jiných programů v používaném ICT
- hrát v pracovní době počítačové hry
- komunikovat pomocí internetu mimo rámec svých pracovních povinností (chaty, hlasová a video komunikace)
- ukládat nezpracovávané chráněné informace a data mimo stanovená úložiště (v adresářích a složkách lokálních PC)
- ponechávat dokumenty s obsahem důvěrných informací volně dostupné
- činit jakékoliv pokusy o omezení bezpečnostního nastavení svěřených prostředků a zařízení ICT, zejména činit pokusy o získání cizích či privilegovaných přístupových práv, k získání fyzického nebo logického přístupu k chráněným informacím a datům, k nimž není autorizován
- zneužívat nedbalosti jiného uživatele (např. opomenuté odhlášení) k tomu, aby v ICT pracoval pod cizí identitou

- přinášet na pracoviště bez povolení svého nadřízeného jakékoliv vlastní zařízení nebo prostředky pro zpracování informací, pracovat s nimi, ani se s nimi bez povolení připojovat odkudkoli do interní sítě
- umožnit připojení zařízení třetích stran do interní počítačové sítě bez souhlasu odpovědné osoby
- podávat jakékoliv informace o zjištěných slabinách a nedostatcích, bezpečnostních událostech nebo bezpečnostních incidentech, včetně přijatých opatřeních neoprávněným osobám

Administrátor ICT

01. Administrátor ICT je zásadním a výkonným uživatelem ICT zajišťujícím správu ICT s nejvyšší odpovědností za jeho provoz a spolehlivé fungování. Pro používání ICT pro něj platí v zásadě stejná pravidla jako pro ostatní uživatele.

Administrátor ICT:

- zajišťuje bezpečný provoz ICT
- řeší provozní závady ICT
- zajišťuje antivirovou ochranu
- je zodpovědný za důvěrnost, integritu a dostupnost zpracovávaných dat, jejich zálohování a archivaci
- provádí bezpečnou instalaci a spolehlivé fungování systémového a aplikačního programového vybavení
- odpovídá za licenční ujednání instalovaného SW a případné registrace
- nastavuje bezpečnostní charakteristiky operačního systému a aplikačního SW
- provádí případné zálohování souborů a dat
- odpovídá za bezpečnou obnovu dat uložených v ICT v případě jeho havárie dle plánu obnovy
- provádí bezpečnou a spolehlivou likvidaci počítačových médií
- zajišťuje bezpečné napojení na jiné ICT
- zajišťuje aktuální správu uživatelů ICT, vytváří uživatelské účty, přiděluje uživatelské jméno (ID) a počáteční heslo (vede přehled přidělení přístupových práv uživatelů včetně správy hesel)
- dohlíží na dodržování bezpečnostních opatření uživateli ICT
- užívá své správcovské identity pouze pro práci, vyžadující privilegovaný přístup, pro běžnou práci pak užívá své uživatelské identity
- kontroluje dodržování fyzické bezpečnosti ke klíčovým prostorům ICT
- kontroluje trvalé dodržování schválené konfigurace HW i SW
- spolupodílí se na řešení bezpečnostních incidentů
- zajišťuje nebo provádí školení uživatelů v oblasti bezpečnosti ICT
- kontroluje dodržování bezpečnostních předpisů a pokynů pro ICT
- plní další úkoly v oblasti ICT stanovené mu vedením společnosti

Rozsah ICT **a řízení přístupu**

01. ICT společnosti je tvořen aplikačními a souborovými servery, poštovními servery, internetovými routery/firewally, pracovními stanicemi (PC a notebooky uživatelů), operačním a aplikačním programovým vybavením, zpracovávanými daty, přenosnými médii - nosiči informací (CD, DVD, flash disky, externí disky, atd.)
02. Cílem přístupové politiky je jasně definovat, kdo a kam má přístupová práva a jaká má oprávnění (nahlížení, modifikace, ukládání, mazání). Tato práva nastavuje vedení společnosti. Za technické nastavení zodpovídá administrátor ICT.
03. Přístup do sítě začíná nástupem zaměstnance do pracovního poměru a je zrušen po jeho ukončení.
04. Přístup do sítě je umožněn na základě přihlašovacího jména a hesla. Toto heslo musí uživatel držet v tajnosti a nesmí jej svěřit dalším osobám. Heslo je uloženo u administrátora ICT.

E-mailová korespondence

01. Pro používání elektronické pošty (e-mailu), která nějakým způsobem souvisí s činností společnosti či přímo používání služebního e-mailu, platí stejná bezpečnostní a etická pravidla jako pro používání běžné listinné pošty. Navíc platí ještě následující pravidla a zásady:

Uživateli je zakázáno:

- rozesílat spam, řetězové dopisy a hoaxy (poplašné zprávy) v jakékoliv formě a podobě
- používat e-mail pro šíření a výměnu komerčních informací
- předávat e-mailem informace vulgárního nebo sexuálně expresivního charakteru či jiné nepracovní informace
- používat síť pro politickou, náboženskou a rasovou agitaci a k šíření materiálů, které jsou v rozporu s právními předpisy
- obtěžování ostatních uživatelů hromadnými zprávami a zprávami, které svým charakterem nesouvisí přímo s pracovním zařazením a povinnostmi

- používat vulgárních a silně emotivních výrazů při komunikaci otevřené dalším účastníkům (elektronické diskusní skupiny, atd.)
- zneužívat e-mail k reklamním a jiným účelům, sloužícím k získání osobního prospěchu
- využívat elektronických prostředků (především elektronické pošty) k obtěžování nebo zastrašování jiných uživatelů (spadá sem i rozesílání řetězových dopisů či dopisů na náhodně vybrané adresy v síti)
- používat e-mail a vůbec prostředky a zařízení ICT k činnostem namířeným proti jakékoliv další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím počítačové sítě
- zasílat jakékoliv osobní či citlivé údaje v nezašifrované podobě.

02. V případě využívání e-mailu k zasílání dokumentů či informací, které obsahují osobní a citlivé údaje, např. vyúčtování placené sociální služby, jsou tyto informace chráněny heslem.

03. Vyúčtování placené sociální služby je ve většině případu zasíláno klientům či jejich zástupcům prostřednictvím e-mailové korespondence. Jelikož se jedná o dokument obsahující osobní a citlivé údaje, je toto vyúčtování chráněno unikátním heslem, které zná pouze osoba odpovědná za vyúčtování a klient či jeho zástupce.

Používání internetu

01. Dodavatelem internetových služeb je společnost LAM Plus, s.r.o. - areál CSS Hvozdy, o.p.s. a O2 Czech Republic - pracoviště Štěchovice. Pro používání internetu platí následující zásady:

Uživatel nesmí:
- měnit parametry elektronické komunikace, měnit nastavení parametrů internetového prohlížeče, ani nastavení a úrovně zabezpečení elektronické pošty
- prostřednictvím internetu šířit nelegální SW, popřípadě jej z internetu vědomě stahovat a používat
- na pracovišti využívat služeb internetu k soukromým komerčním záležitostem (za účelem zisku)
- na ICT přes internet stahovat, instalovat a spouštět jakýkoliv SW bez souhlasu administrátora ICT
- využívat internet ke hraní on-line her, stahovat a sledovat videoklipy, filmy a podobné multimediální soubory včetně sledování streamovaného (on-line vysílaného) audia a videa;
- komunikovat přes internet s jinými osobami mimo rámec svých pracovních povinností, jedná se zejména o používání chatů a audio a video rozhovorů v reálném čase;
- prohlížet stránky a stahovat materiály s nežádoucím obsahem, zejména erotické, pornografické, sexuální a vulgární; propagující nenávist, politickou, náboženskou a rasovou agitaci; související s poškozováním autorských práv (cracky, warez apod.).

02. Při podezření na opakované porušování uvedených pravidel může být na pokyn vedení společnosti činnost na internetu zkontrolována / zmonitorována administrátorem ICT. Opakované porušování podmínek provozu internetu může být důvodem k dočasnému odebrání přístupu a následnému disciplinárnímu řízení.

Vlastnická práva

01. V rámci dodržování vlastnických práv platí následující pravidla:
- všechny prvky ICT sítě jsou vlastnictvím společnosti, případně k nim vlastní či vykonává práva užívání; nepřípustnost krádeže a poškození se pak vztahuje na elektronickou podobu dat a informací stejně jako na vlastní fyzické prostředky
- uživatelé nesmí jakýmkoliv způsobem dále šířit (a to ani bezúplatně) jakýkoliv software, který je součástí sítě; software se může používat a šířit pouze v souladu s licenčními podmínkami pro daný software

02. **Uživatelům je proto dále zakázáno:**
- neautorizované kopírování SW i jeho částí nebo dat
- neautorizovaná modifikace SW nebo dat
- vědomě využívat nelegální SW a data, případně takovýto SW či data nabízet jiným
- používat počítačovou síť k získání neautorizovaného přístupu k chráněným informacím a k jejich neveřejným zdrojům
- vytvářet nebo pozměňovat data s cílem mást nebo jinak ovlivňovat kontrolu oprávněnosti použití počítačových programů

Antivirová ochrana

01. Na všech PC stanicích je nainstalován antivirový program Avast, Eset nebo Windows Defender.

02. Program zabezpečuje nejenom ochranu proti virům, ale i proti trojským koňům, červům a dalším druhům škodlivého SW. Program vytváří na každém počítači po spuštění rezidentní štít, který kontroluje všechny používané soubory a brání vniknutí a šíření škodlivých programů do počítače.

03. Program kontroluje soubory na lokálních discích počítače a výměnných médiích, data přijímaná ze sítě a zprávy elektronické pošty včetně jejich příloh.

04. V rámci antivirové bezpečnosti jsou uživatelé povinni dodržovat následující základní pravidla antivirové prevence:
- neukončovat běh antivirového programu ani žádné jeho části (rezidentní štít)
- nepřerušovat aktualizaci antivirového prostředku a řídit se pokyny antivirového programu, především pokynu pro opětovné spuštění (restart) počítače
- neukončovat časově spuštěné testování
- používat jen legální a odsouhlasený SW
- nespouštět SW s nejasným či neznámým původem
- neotevírat a nespouštět podezřelé soubory s neznámým původem, podezřelé přílohy e-mailů
- nepoužívat počítač podezřelý z infikování virem do jeho odborného prověření administrátorem ICT
- nechat automaticky kontrolovat na přítomnost virů všechny přijaté soubory, a to včetně souborů na výměnných médiích, stažených z internetu nebo připojených k e-mailu před jejich použitím, otevřením nebo zkopírováním do ICT
- neprodleně oznamovat odpovědné osobě (vedení společnosti, administrátor ICT) případné závady nebo podezření na zavirování stanice nebo aplikace

05. Administrátor ICT průběžně / při servisní činnosti kontroluje nastavení a aktuálnost antivirového programu. V rámci prováděných opatření při podezření na aktivity škodlivého SW má administrátor ICT právo na:
- odstavení pracovní stanice PC
- odpojení internetové připojení
- vyžadování součinnosti uživatele po nezbytně nutnou dobu
- omezení nebo přerušení provozu počítačové sítě
- vypnutí serveru

Instalace aplikací

01. Instalaci a odinstalování jakéhokoliv SW provádí výhradě administrátor ICT.

02. Ve výjimečných případech mohou po předchozí domluvě provádět instalaci i poučení a proškolení uživatelé. V této souvislosti je administrátorem ICT periodicky prováděna kontrola nainstalovaného SW na lokálních stanicích PC uživatelů.

03. Cílem je zajistit užívání počítačových programů výlučně oprávněnými uživateli na základě licenčních smluv a zajistit důsledný soulad užívání počítačových programů s platnými právními předpisy a příslušnými licenčními ujednáními a respektovat zákonná práva nositelů autorských a průmyslových práv k jednotlivým softwarovým produktům.

04. Uživatelé jsou povinni instalovat automaticky nabízené bezpečnostní aktualizace operačního systému a dalšího software v PC, případně nebránit jejich automatické instalaci.

Manipulace s **přenosnými počítačovými medii**

01. Uživatel je povinen veškerá přenosná počítačová média uchovávat takovým způsobem, aby k nim nebyl umožněn fyzický přístup neoprávněných osob. V době jeho nepřítomnosti na pracovišti se média nesmí nacházet v mechanikách a portech počítačů, ležet volně přístupná na pracovních stolech, monitorech, parapetech, skříních apod.

02. Média, obsahující chráněné informace, musí být ukládána vždy do uzamykatelných úschovných objektů.

03. Všechna média musí být uchovávána a musí být s nimi manipulováno takovým způsobem, aby se zabránilo jejich zničení nebo poškození na nich zaznamenaných dat. Jedná se zejména o mechanické poškození, znečištění prachem a jinými nečistotami a pevnými částicemi, poškození teplem (intenzivní přímý sluneční svit, zdroje tepla v kancelářích), poškození elektromagnetickým polem apod.

04. Při přenášení a přepravě musí být média uložena v přepravním obalu a takovým způsobem, aby se omezila možnost jejich poškození a odcizení.

05. Citlivé osobní údaje na přenášených a přepravovaných médiích musí být zabezpečena proti neoprávněnému přístupu zašifrováním. Média s obsahem citlivých osobních údajů se předávají vždy a pouze oproti podpisu s uvedením data a identifikačními údaji přebírající osoby.

06. **Bezpečné mazání médií**
Uživatel, jenž vyžaduje spolehlivé a bezpečné vymazání přepisovatelného média, je povinen tuto činnost řešit cestou administrátora ICT.

07. Likvidace médií
Nepotřebná média nebo nepřepisovatelná média určená k likvidaci jsou uživatelé povinní odevzdat k likvidaci osobně administrátoru ICT. Ten provádí jejich bezpečné a spolehlivé zničení stanoveným způsobem.

08. Notebooky

Notebook je uživateli předán na základě předávacího protokolu. Pro používání pracovních notebooku platí následující pravidla:

- v rámci plnění pracovních úkolů smí zaměstnanci používat pouze notebooky přidělené zaměstnavatelem, pokud se se zaměstnavatelem nedohodnou jinak
- Notebook smí používat pouze ten uživatel, který je seznámen se způsobem jeho obsluhy a při používání se těmito pokyny musí řídit
- notebooky mohou být uživateli používány výhradně k činnosti přímo spojené s plněním pracovních úkolů nebo v jejich souvislosti (pokud se zaměstnanec/uživatel se zaměstnavatelem nedohodnou jinak)
- instalace a používání jakéhokoliv jiného softwaru, než byl instalován při předání zařízení uživateli, je zakázáno a porušení může vést k odebrání notebooku, za případné škody je zodpovědný uživatel

Uživatel je dále povinen:

- dodržovat předepsané pokyny údržby notebooku
- účinně chránit notebook před neautorizovaným přístupem a před jeho zcizením
- při používání notebooku dodržovat „pravidlo omezené komunikace“ a zejména dbát na to, aby nemohlo dojít k neoprávněnému nakládání s chráněnými informacemi zpracovávanými a uloženými v tomto zřízení
- mít v notebooku chráněné informace účinně zabezpečeny tak, aby při neautorizovaném přístupu cizí osobou nemohlo dojít k jejich vyzrazení, aniž by musely být vynaloženy nepřiměřené prostředky a úsilí k jejich získání
- při jakékoliv závadě nebo poruše HW a SW notebooku tento stav bez prodlení oznámit svému přímému nadřízenému a administrátoru ICT a řídit se jimi vydanými pokyny, uživatel má zakázáno závadu sám odstraňovat

Uživateli je zakázáno:

- mít v notebooku uloženy v nezašifrované podobě jakékoliv chráněné informace
- nechávat bez dozoru notebook v zaparkovaném automobilu, v hotelu, ubytovně, na nezabezpečeném pracovišti, ve společenských, zdravotních, servisních, klientských apod. prostorech
- přenechávat notebook k používání neautorizovaným a cizím osobám včetně rodinných příslušníků

09. Mobilní telefony

- zaměstnanci jsou povinni při uskutečňování telefonních hovorů dodržovat „pravidlo omezené komunikace“ a sdělovat pouze nezbytné informace
- zaměstnanci berou na vědomí, že charakter provozu mobilních telefonů umožňuje jejich relativně přesnou lokalizaci a že v podstatě všechny uskutečněné hovory a přenosy informací mohou být dlouhodobě a efektivně monitorovány
- zaměstnanci nesmějí v mobilních telefonech uchovávat v nešifrované podobě přístupová hesla a další chráněné informace, aby při ztrátě nebo odcizení mobilního telefonu tato nemohla být přístupná neautorizovaným osobám

10. Telefony - pevná linka

- zaměstnanci používají telefony výhradně k hovorům v souvislosti s výkonem pracovní činnosti
- vedení soukromých telefonátů je povoleno pouze se svolením přímého nadřízeného
- přestože by telefonní hovory měly být věcné, stručné a srozumitelné, musí při nich zaměstnanci zachovávat zásady společenského chování, být korektní a mít na paměti, že i jimi uskutečňované hovory jsou součástí kultury organizace a mají vliv na image společnosti
- zaměstnanci jsou při uskutečňování telefonních hovorů povinni dodržovat „pravidlo omezené komunikace“ a sdělovat pouze nezbytné informace
- zaměstnanci mají kromě běžné obsluhy zakázáno zasahovat do přístrojů, a telefonních rozvodů
- zaměstnanci jsou povinni při jakékoliv závadě nebo poruše telefonu a telefonního spojení tento stav bez prodlení oznámit svému přímému nadřízenému a nesmějí poruchu nebo závadu sami odstraňovat

Pravidla pro **přemisťování a vynášení HW, SW a informací**

01. **Nepřenosná zařízení**

- Manipulace s nepřenosnými PC stanicemi je zakázána. S takovým zařízením je možné manipulovat pouze po předchozím svolení nadřízeného a za pomocí administrátora.
- V případě poruchy zařízení zajišťuje převoz vadné techniky nutné k opravě administrátor ICT. Za manipulaci s uloženými chráněnými daty v průběhu přepravy a servisního zásahu odpovídá opět administrátor.

02. **Data na datových nosičích**

- Média obsahující chráněné informace je zakázáno bez povolení nadřízeného vynášet nebo odesílat mimo objekt společnosti. Zaměstnanec, který datový nosič přenáší, je plně odpovědný za obsah nosiče a jeho zabezpečení.
- Pokud to užívané zařízení dovolí, musí uživatel zajistit paměťové médium proti ztrátě a poškození vhodným obalem a způsobem transportu.

- Z hlediska bezpečnosti chráněných dat je uživatel povinen v rámci dané aplikace nebo zařízení, k němuž je datový nosič používán, data zajistit přístupovým heslem nebo zajistit jejich uložení v zašifrované podobě.

Provozní a bezpečnostní incidenty

01. Každý zaměstnanec, který detekuje podezření na bezpečnostní událost nebo incident, nebo zjistí jiné slabé místo zabezpečení je povinen tuto skutečnost nahlásit svému přímému nadřízenému.
02. Uživatel ICT nesmí za žádných okolností podezřelé slabiny prověřovat.
03. Každý zaměstnanec je povinen při detekci a identifikaci selhání SW a HW vybavení dodržovat následující zásady:
    - zaznamenat příznaky problému a jakékoliv zprávy objevující se na obrazovce monitoru
    - přestat používat pracovní stanici PC nebo jiné zařízení pro zpracování informací, a pokud je to možné, izolovat jej od dalšího provozu
    - ihned provést oznámení stanoveným způsobem
    - zamezit přístup osob neautorizovaných k řešení incidentu k prostředkům a zařízení
    - vyjmout z PC veškerá výměnná média, vhodným způsobem je označit a předat administrátorovi ICT
    - nepřenášet žádné přenosné nosiče informací používané před a po zaznamenání selhání programového vybavení, do jiných stanic PC
    - neprovádět žádné pokusy o odstranění podezřelého programového vybavení ani žádné jiné opravy prostředků a zařízení ICT
    - zaměstnanec nesmí podávat jakékoliv informace o zjištěných slabinách a nedostatcích, bezpečnostních událostech nebo bezpečnostních incidentech neoprávněným osobám
04. Uživatelé jsou informováni a jsou si vědomi, že při zjištění zavinění bezpečnostní události nebo incidentu z jejich strany v důsledku nedodržení ustanovení směrnic s nimi může být zahájeno standardní disciplinární řízení se všemi vyplývajícími důsledky.

ŘÍZENÍ INCIDENTŮ

příloha k vnitřnímu předpisu č. B/05/2023 GDPR

01. Základní principy procesu řízení bezpečnostních incidentů vychází z normy ISO/IEC 27001. Tento dokument definuje rozsah činností zahrnutých do pojmů řízení bezpečnostních incidentů ve specifických podmínkách Centra sociálních služeb Hvozdy, o.p.s. (dále jen společnost) a stanovuje hlavní zásady při jejich zvládání v souladu s požadavky Obecného nařízení o ochraně osobních údajů.

02. Cílem tohoto dokumentu je vymezení kompetencí konkrétních funkcí a rolí, stanovení postupů, činností a definování klíčových procesů pro řízení vzniklých a podchycených bezpečnostních incidentů včetně analyzování jejich příčin za účelem jejich efektivního předcházení a eliminace.

03. Pojmy v rámci řízení incidentů:

Bezpečnost informací
Zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

Bezpečnostní incident
Nechtěná nebo neočekávaná bezpečnostní událost, u které existuje nezanedbatelná pravděpodobnost ohrožení bezpečnosti chráněných informací.

Bezpečnostní událost
Identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření; může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací.

Data
Informace zpracované pomocí výpočetní techniky a uložené na záznamovém médiu.

Chráněná aktiva
Všechno, co má pro společnost hodnotu (aktiva: informační, programová, personální, služby, opatření aj.).

Informace
Poznatek týkající se jakýchkoliv objektů a osob, např. faktů, činností, událostí, věcí, výzkumu, vývoje, testování, procesů nebo myšlenek, včetně pojmů, který mají v daném kontextu specifický význam.

Osobní údaje
Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); 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.

Citlivé údaje
Tedy osobní údaje, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod, zasluhující zvláštní ochranu, jelikož by při jejich zpracování mohla vzniknout závažná rizika pro základní práva a svobody dotčených osob. Jedná se zejména o údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

04. V případě porušení zabezpečení osobních údajů je tato skutečnost zaznamenána do Záznamu o porušení **zabezpečení osobních údajů** a do **Registru incidentů**.

05. Není-li porušení zabezpečení osobních údajů řešeno náležitě a včas, může to fyzickým nebo i právnickým osobám způsobit hmotnou či nehmotnou újmu, jako je ztráta kontroly nad jejich osobními údaji nebo omezení jejich práv, diskriminace, krádež nebo zneužití identity, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti, ztráta důvěrnosti osobních údajů chráněných služebním tajemstvím nebo jakékoliv jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob. S ohledem na tuto skutečnost vydává společnost tuto vnitřní směrnici, se kterou se povinně seznámí všichni zaměstnanci a budou se jí řídit.

BEZPEČNOSTNÍ INCIDENTY

01. Do této kategorie jsou zahrnuty incidenty a události, jež přímo či nepřímo souvisí s ohrožením nebo narušením bezpečnosti chráněných informačních aktiv, zejména tedy osobních či citlivých údajů fyzických osob (**Registr chráněných aktiv** a **Registr osobních údajů a jejich zpracování**).

    Jedná se zejména o:

    - projev počítačového viru nebo jiného programu, který ohrožuje bezpečnost chráněných informací
    - ztrátu telefonu s firemním emailem
    - stahování neschváleného software na firemní počítač
    - stahování firemní pošty na nezabezpečené elektronické zařízení (např. tablet, soukromý počítač)
    - ukládání firemních dat na nezabezpečené externí uložiště (soukromé flash disky apod.)
    - neoprávněný vstup na pracoviště nebo podezření na něj
    - neoprávněný přístup k chráněným informacím uloženým v kartotéce
    - neoprávněné nakládání s osobními údaji zaměstnancem společnosti
    - zpracování osobních údajů nad rámec informovaného souhlasu
    - nezákonné zpracování osobních údajů

02. Pro vyjasnění tohoto procesu lze za bezpečnostní událost a bezpečnostní incident považovat jakékoliv narušení bezpečnostních pravidel a opatření, které vede nebo by mohlo vést k jakékoliv škodě nebo ohrožení zpracovávaných osobních údajů.

03. Naplňováním ustanovení tohoto dokumentu všemi zaměstnanci a zainteresovanými stranami je zajištěn jednotný způsob řízení bezpečnostních situací a bezpečnostních incidentů tak, jak je vyžadováno evropským nařízením GDPR.

SPRÁVA INCIDENTŮ

01. Obecným cílem řízení bezpečnostních událostí a incidentů je minimalizovat škody způsobené bezpečnostními incidenty a selháními, sledovat je a učit se z nich.

02. Za správu incidentů ve společnosti odpovídá určená odpovědná osoba, která musí být o všech incidentech bezprostředně informována písemnou formou.

03. Mechanismus řízení incidentů obsahuje činnosti spojené s bezprostřední detekcí hrozícího nebo již uplatněného incidentu, se způsobem jeho ohlášení a zdokumentování, s možnostmi jeho eliminace vzhledem ke způsobu zajištění ochrany chráněných informací.

HLÁŠENÍ INCIDENTŮ

01. Bezpečnostní události nebo incidenty mohou být zjištěny v průběhu běžné provozní činnosti, ale i při monitorování, prováděných kontrolách a interních auditech.

02. S postupy hlášení bezpečnostních incidentů jsou seznámení všichni zaměstnanci společnosti a třetí strany, jež mají přístup k osobním údajům zaměstnanců nebo klientů.

03. Za seznámení smluvních nebo třetích stran se způsobem hlášení bezpečnostních incidentů je zodpovědný ten zaměstnanec společnosti, jež smluvní vztah oficiálně uzavřel nebo uzavírá.

04. Následující tabulka obsahuje důležité kontakty pro hlášení bezpečnostních incidentů.

Funkce	Jméno	Telefon	Mail
Správce osobních údajů	Romana Hromádková	724 110 441	hromadkova@css-hvozdy.cz
Odpovědná osoba	Jakub Čanda	731 417 229	canda@css-hvozdy.cz
Úřad pro ochranu osobních údajů	Pplk. Sochora 27, 170 00 Praha 7, www.uoou.cz		

05. Zaměstnanec, který bezpečnostní událost/incident zjistil, ihned ohlásí tuto skutečnost **odpovědné osobě** písemnou formou. Odpovědná osoba, bezprostředně poté, co získá dostatečné informace o výši rizika na dotčené subjekty osobních údajů, dále hlásí porušení zabezpečení osobních údajů Správci osobních údajů (dále jen správci), který nahlásí incident na ÚOOÚ (Úřad pro ochranu osobních údajů) popřípadě SOÚ (subjekt osobních údajů).

06. Po domluvě musí být stanoven řešitel, aby bylo zajištěno, že incident bude dále ověřen a vyřešen.

07. Úkoly, činnosti a postupy řízení incidentů jsou stanoveny v následující posloupnosti:
- včasná identifikace (detekce)
- zamezení případné eskalaci působení
- předání informace (oznámení) o události nebo incidentu ÚOOÚ
- oznámení incidentu dotčenému subjektu osobních údajů
- záznam (dokumentování) o události nebo incidentu
- odstranění nebo eliminace přímého důsledku incidentu
- opatření k nápravě a minimalizace následků
- shromáždění důkazů, rozbor (přezkoumání) příčin
- ponaučení se - návrh a přijetí preventivních opatření - zamezujících vznik stejných událostí nebo incidentů
- případné disciplinární řízení

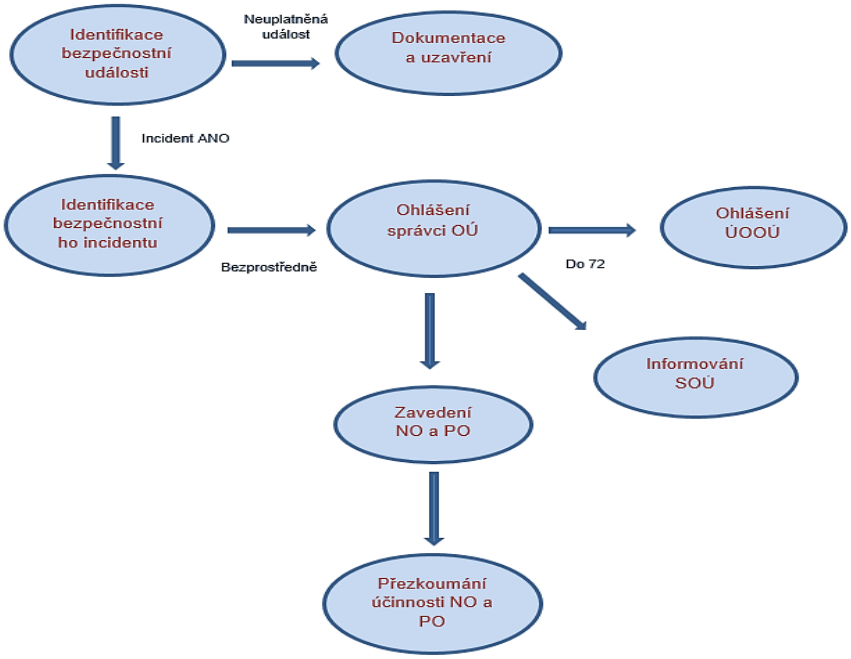
08. **Hlášení porušení zabezpečení osobních údajů** na ÚOOÚ

a) Jakmile se správce osobních údajů o porušení zabezpečení osobních údajů dozví, měl by je bez zbytečného odkladu, a je-li to možné, do 72 hodin poté, co se o něm dozvěděl, ohlásit příslušnému dozorovému úřadu.
b) Hlášení dozorovému úřadu podává správce telefonicky či mailem prostřednictvím formuláře Hlášení o porušení **zabezpečení osobních údajů** pro ÚOOÚ.
c) Není-li toto ohlášení možné učinit do 72 hodin, měly by být spolu s ním uvedeny důvody zpoždění a informace mohou být poskytnuty postupně bez zbytečného dalšího prodlení.
d) Bezpečnostní incident nemusí být ohlášen ÚOOÚ pouze v případě, že může správce osobních údajů v souladu se zásadou odpovědnosti doložit, že je nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob.

09. H**lášení porušení zabezpečení osobních údajů subjektům osobních údajů**

a) Správce je povinen porušení zabezpečení osobních údajů oznámit subjektu údajů bez zbytečného prodlení, pokud je pravděpodobné, že toto porušení bude mít za následek vysoké riziko pro práva a svobody fyzické osoby, aby mohl učinit nezbytná opatření. V oznámení by měla být popsána povaha daného případu porušení zabezpečení osobních údajů a obsažena doporučení pro dotčenou fyzickou osobu, jak případné nežádoucí účinky zmírnit. Tato oznámení by měla být subjektům údajů učiněna, jakmile je to proveditelné, v úzké spolupráci s dozorovým úřadem a v souladu s pokyny tohoto úřadu nebo jiných příslušných orgánů.
b) Informovat dotčený SOÚ je nutné co nejdříve, nejprve je však nutné přijmout vhodná opatření s cílem zabránit tomu, aby porušení zabezpečení osobních údajů pokračovalo nebo aby docházelo k podobným případům porušení.
c) Správce informuje dotčené SOÚ telefonicky či písemně.
d) Správce není povinen dotčený SOÚ informovat v případě že:
- Zavedl taková technická a organizační opatření, která činí OÚ nesrozumitelnými
- Správce přijal taková opatření, že vysoké riziko pro práva a svobody SOÚ už nehrozí
- By to vyžadovalo nepřiměřené úsilí. V tomto případě o porušení zabezpečení OÚ informuje např. veřejný orgán.

10. Cyklus incidentu zobrazuje následující schéma:



EVIDENCE INCIDENTŮ

01. Bezpečnostní incident je zaznamenán a zdokumentován ve formuláři **Záznam o porušení zabezpečení** osobních **údajů**, a to včetně veškerých důkazů a záznamů týkajících se daného incidentu. Tento formulář vyplní řešitel incidentu komunikující s ÚOOÚ a s dotčenými SOÚ.

02. Všechny incidenty jsou souhrnně vedeny v tabulce **Registr incidentů**.

03. V případě řešení incidentů, vyžadujících koordinaci a spolupráci externích odborníků musí o tomto existovat záznamy. Za vedení evidence bezpečnostních incidentů odpovídá správce osobních údajů, popřípadě jiná správcem pověřená osoba.

PREVENTIVNÍ A NÁPRAVNÁ OPATŘENÍ

01. Správce je povinen s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření tak, aby zajistil dostatečnou úroveň zabezpečení odpovídající danému riziku, tzn.:
    - Pseudonymizace a šifrování OÚ
    - Schopnost zajistit neustálou důvěrnost, integritu a dostupnost a odolnost systémů a služeb zpracování
    - Schopnost obnovit dostupnost a přístup k OÚ
    - Zavést a udržovat proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření.

02. Preventivní (PO) i nápravná (NO) opatření jsou aplikována na základě zjištění/nálezů interních/externích auditů, pravidelného přezkoumání a hodnocení opatření při zpracování osobních údajů nebo jako reakce na již vzniklý incident.

03. Jak nápravná, tak preventivní opatření se přijímají s cílem řešit podstatu problému vzniku neshod nebo možných neshod (a z nich vyplývajících ztrát).

04. Dle výše rizika plynoucího z daného zpracování rozhodne správce osobních údajů o potřebě stanovení nápravných a preventivních opatření.

05. **Nápravné opatření**

    Při rozhodování se zvažují následující okolnosti:
    - pravděpodobnost, že se neshoda bude opakovat, nebudou-li odstraněny její příčiny a nebude-li do budoucna zabráněno opakování vzniku těchto příčin
    - složitost (pracnost) případného opatření k nápravě
    - úměrnost přijatého opatření k nápravě vůči důsledkům zjištěných problémů
    - náklady na případné provedení opatření k nápravě
    - způsob ovlivnění spokojenosti zákazníka přijatým opatřením k nápravě
    - zda je vedle opatření k nápravě třeba přijmout také preventivní opatření

06. **Preventivní opatření**

    Pro stanovení preventivního opatření se využívají:
    - právní požadavky
    - informace o incidentech
    - analýza rizik, příčina rizika a možné následky
    - výstupy z pravidelného ročního přezkoumání bezpečnosti zpracování osobních údajů
    - ponaučení získaná na základě minulých zkušeností
    - údaje z procesů, které poskytují včasná varování o blížících se stavech mimo stanovené meze;
    - údaje o již přijatých opatřeních k nápravě.

    Při rozhodování se zvažují následující okolnosti:
    - pravděpodobnost, že se vyskytne neshoda
    - potřeba preventivního opatření (preventivní opatření musí být úměrné následkům možných problémů)
    - složitost (pracnost) případného preventivního opatření
    - náklady na případné provedení preventivního opatření

07. Odpovědná osoba vede o realizaci nápravných a preventivních opatření podrobné záznamy.

08. Správce zhodnotí na základě porovnání předchozího a nového stavu, zda NO/PO byla dostatečná nebo zda bude nutno zavést dodatečná opatření. Přijatá NO/PO jsou dále vyhodnocována v rámci přezkoumání systému řízení bezpečnosti informací. Výstupem tohoto procesu je vypořádaný incident a minimalizace rizika vzniku a následků dalšího bezpečnostního incidentu.

09. Pro případy právních řízení a sporů v souvislosti s porušením zabezpečení osobních údajů je třeba shromažďovat veškeré důkazy související s uplatněnými incidenty. Pro shromažďování důkazů v souvislosti s řešením bezpečnostních incidentů jsou stanoveny následující základní zásady a postupy:
    - za důkazy mohou být považovány veškeré auditní záznamy přímo i nepřímo související s posuzovaným bezpečnostním incidentem (např. údaje v logových záznamech, zápisy v provozní dokumentaci organizace, kopie modifikovaných souborů; záznamy o používání neautorizovaného a nepovoleného SW; záznamy o používání neautorizovaného a neodsouhlaseného HW, zadržený nepovolený SW a HW apod.)
    - veškeré potenciální důkazy musí být chráněny před zničením, modifikací, likvidací nebo případným zneužitím
    - za uchovávání potenciálních důkazů odpovídá správce osobních údajů
    - veškeré předávání nebo poskytování potenciálních důkazů musí být prokazatelně evidenčně dokumentováno
    - při uchovávání listinných dokumentů - důkazů je pořizován záznam o tom kdo jej nalezl, kde byl nalezen, kdy byl nalezen, kdo dosvědčí jeho nález
    - pro uchovávání informací na počítačových médiích platí:
        - pro zajištění dostupnosti jsou pořízeny kopie nebo obrazy všech výměnných médií, informací na pevných discích nebo v paměti počítače
        - jsou uchovány logy o všech činnostech v průběhu kopírování
        - proces musí být svědecky doložitelný
        - jedna kopie (nejlépe originál) musí být uschován na bezpečném místě
        - pro jakékoliv forenzní zkoumání se poskytují zásadně kopie důkazů (vždy záznam o tom, kdy a kde byla kopie vytvořena, kdo kopírování prováděl a jaké nástroje a programy byly pro vytvoření kopií použity).

10. Důkazy v případném soudním řízení by měly být předem konzultovány s ÚOOÚ.

INFORMACE O ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ

klienta sociálních služeb

Jméno a příjmení klienta:

Datum narození klienta:

Bydliště klienta:

Zástupce klienta (opatrovník):

Klient Centra sociálních služeb Hvozdy, o.p.s., se sídlem Masečín 119, 252 07 Štěchovice, IČ: 29128218 (dále jen „poskytovatel“), nebo jeho zástupce, podpisem tohoto dokumentu bere na vědomí, že při poskytování sociálních služeb dle Smlouvy o poskytnutí sociální služby jsou zpracovávány jeho níže uvedené osobní údaje v rozsahu nutném pro splnění smluvních a zákonných povinností zařízení sociálních služeb, a to po dobu vyplývající z právních předpisů, případně po dobu trvání smlouvy:

- *jméno, příjmení, datum narození, rodné číslo, adresa bydliště, korespondenční adresa, telefonický kontakt, zdravotní pojišťovna, číslo občanského průkazu, státní příslušnost, údaje o svéprávnosti, dietologické údaje, stupeň příspěvku na péči, výše důchodu, údaje o schopnosti zvládat základní životní potřeby, údaje vedené v souladu s právními předpisy ve zdravotnické dokumentaci*

Povinnost poskytnout osobní údaje

Klient, nebo jeho zástupce, je srozuměn s tím, že pokud by se zpracováním osobních údajů ve výše uvedeném rozsahu nesouhlasil, zařízení sociálních služeb by mu nemohlo požadovanou sociální službu poskytnout. Poskytnutí výše uvedených údajů je tedy smluvním požadavkem.

Zpracování na základě oprávněných zájmů

Klient, nebo jeho zástupce, dále bere na vědomí, že poskytovatel sociálních služeb zpracovává na základě svých oprávněných zájmů další osobní údaje klienta (dosažené vzdělání, rodinný stav, státní příslušnost, poslední zaměstnání, místo narození, dřívější bydliště), a to za účelem individualizace péče a zlepšování poskytovaných služeb. Poskytnutí těchto údajů není povinné.

Příjemci osobních údajů jsou pouze subjekty, u nichž předání vyplývá přímo ze zákona, tedy zejména zdravotní pojišťovna, úřad práce apod.

Práva klienta související se zpracováním

- Klient má právo žádat o informace o kategoriích zpracovávaných osobních údajů, účelu, době a povaze zpracování a o příjemcích osobních údajů;
- Klient má právo požádat o poskytnutí kopie zpracovávaných osobních údajů;
- Klient má právo požádat při naplnění podmínek stanovených relevantními právními předpisy, aby osobní údaje byly opraveny, doplněny nebo vymazány, případně jejich zpracování omezeno;
- Klient má právo vznést námitku proti zpracovávání osobních údajů a právo podat stížnost u dozorového úřadu;
- Klient má právo být informován o případech porušení zabezpečení osobních údajů a to tehdy, pokud je pravděpodobné, že daný případ porušení bude mít za následek vysoké riziko pro jeho práva a svobody.

Prohlášení klienta nebo jeho zástupce

Poté, co jsem měl možnost klást doplňující otázky a zeptat se na vše, co pokládám za podstatné, a moje dotazy mi byly uspokojivě zodpovězeny, prohlašuji, že jsem informacím a vysvětlením plně porozuměl a považuji poučení mé osoby za dostatečné.

V případě, že tento dokument podepisuji v zastoupení klienta, prohlašuji, že s jeho obsahem a důsledky pro práva a povinnosti dotčených subjektů byl přiměřeným způsobem, tedy jasně, srozumitelně a za použití jednoduchých jazykových prostředků, seznámen i samotný klient.

Ve Hvozdech dne .....

podpis klienta (zástupce)

SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

týkající se pořizování fotografií a videozáznamů

Jméno a příjmení klienta:

Datum narození klienta:

Bydliště klienta:

Zástupce klienta (opatrovník):

Klient, nebo jeho zástupce, tímto dobrovolně uděluje svůj kdykoliv odvolatelný souhlas se zpracováním osobních údajů Centrem sociálních služeb Hvozdy, o.p.s., se sídlem Masečín 119, 252 07 Štěchovice, IČ: 29128218, a to v následujícím rozsahu a pro uvedené účely:

ANO / NE souhlasím s pořizováním mých fotografií

ANO / NE souhlasím s pořizováním mých **videozáznamů**

pro interní účely a běžný, každodenní chod zařízení sociálních služeb (výukové účely, rozvoj sociálních dovedností, pořádání různých tematických akcí apod.) a dále za účelem prezentace a propagace poskytovatele, a to zejména formou zveřejnění těchto záznamů na internetových stránkách poskytovatele.

Jsem srozuměn s tím, že i pokud souhlas neudělím, bude mi sociální služba bez dalšího poskytnuta a uvedené osobní údaje v takovém případě nebudou poskytovatelem sociálních služeb jakkoliv zpracovávány.
Byl jsem informován o tom, že ke zpracování na základě tohoto souhlasu bude docházet po dobu 5 let od ukončení poskytování sociální služby.

Práva klienta

Dále jsem byl(a) informován(a) o tom, že má práva a další skutečnosti uvedené v dokumentu INFORMACE O ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ, který jsem obdržel(a) před udělením tohoto souhlasu, se vztahují i na zpracování prováděné na základě tohoto souhlasu.

Prohlášení klienta nebo jeho zástupce

Tento můj souhlas zůstává v plném rozsahu v platnosti a účinnosti po dobu trvání poskytování sociální služby. Jsem si vědom toho, že udělení tohoto souhlasu je dobrovolné a mohu ho s účinky do budoucna kdykoliv odvolat.

Ve Hvozdech dne .....

podpis klienta (zástupce)

INFORMACE O ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ

Jméno a příjmení zaměstnance:
Datum narození zaměstnance:
Bydliště zaměstnance:

Zaměstnanec Centra sociálních služeb Hvozdy, o.p.s., se sídlem Masečín 119, 252 07 Štěchovice, IČ: 29128218, (dále jen společnost) podpisem tohoto dokumentu bere na vědomí, že zaměstnavatel zpracovává jeho níže uvedené osobní údaje v rozsahu nutném pro splnění smluvních a zákonných povinností zaměstnavatele, a to po dobu vyplývající z právních předpisů, případně po dobu trvání pracovní smlouvy.

- *jméno, příjmení, akademické tituly, datum narození, rodné číslo, adresa bydliště, telefonický kontakt, emailová adresa, bankovní spojení, údaje o rodinných příslušnících dle daňových předpisů, informace o vzdělání, odborné praxi a pracovních zkušenostech*

ZPRACOVÁNÍ NA ZÁKLADĚ OPRÁVNĚNÝCH ZÁJMŮ

Zaměstnanec dále bere na vědomí, že zaměstnavatel zpracovává na základě svých oprávněných zájmů níže uvedené osobní údaje zaměstnanců, a to tak, že je zveřejňuje po dobu trvání pracovní smlouvy na svých stránkách: www.css-hvozdy.cz. Oprávněnými zájmy zaměstnavatele v této souvislosti je jeho zájem na usnadnění komunikace zaměstnavatele s veřejností a prezentace navenek.

- *jméno, příjmení, akademické tituly, pracovní pozice, e-mailovou adresu a telefonní kontakt zřízený zaměstnavatelem*

POVINNOST POSKYTNOUT OSOBNÍ ÚDAJE

Zaměstnanec je srozuměn s tím, že pokud by se zpracováním osobních údajů ve výše uvedeném rozsahu nesouhlasil, zaměstnavatel by ho nemohl do pracovního poměru přijmout. Poskytnutí výše uvedených údajů je tedy smluvním požadavkem zaměstnavatele.
Příjemci osobních údajů jsou pouze subjekty, u nichž předání vyplývá přímo ze zákona, tedy zejména finanční úřad, správa sociálního zabezpečení a zdravotní pojišťovna.

SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Zaměstnanec tímto dobrovolně uděluje svůj kdykoliv odvolatelný souhlas se zpracováním osobních údajů Centru sociálních služeb Hvozdy, o.p.s., se sídlem Masečín 119, 252 07 Štěchovice, IČ: 29128218, a to v následujícím rozsahu a pro uvedené účely*:*

ANO / NE souhlasím s pořizováním mých fotografií

ANO / NE souhlasím s pořizováním mých **videozáznamů**

pro interní účely a běžný, každodenní chod zařízení sociálních služeb (výukové účely, rozvoj sociálních dovedností, pořádání různých tematických akcí apod.) a dále za účelem prezentace a propagace poskytovatele, a to zejména formou zveřejnění těchto záznamů na internetových stránkách zaměstnavatele. Jsem srozuměn/a s tím, že **neudělení souhlasu není překážkou** vzniku či trvání mého pracovního vztahu se zaměstnavatelem a pokud souhlas neudělím, nebudou uvedené osobní údaje zaměstnavatelem jakkoliv zpracovávány.

PRÁVA ZAMĚSTNANCE SOUVISEJÍCÍ SE ZPRACOVÁNÍM

- Zaměstnanec má právo žádat o informace o kategoriích zpracovávaných osobních údajů, účelu, době a povaze zpracování a o příjemcích osobních údajů;
- Zaměstnanec má právo požádat o poskytnutí kopie zpracovávaných osobních údajů;
- Zaměstnanec má právo požádat při naplnění podmínek stanovených relevantními právními předpisy, aby osobní údaje byly opraveny, doplněny nebo vymazány, případně jejich zpracování omezeno;
- Zaměstnanec má právo vznést námitku proti zpracovávání osobních údajů a právo podat stížnost u dozorového úřadu;
- Zaměstnanec má právo být informován o případech porušení zabezpečení osobních údajů a to tehdy, pokud je pravděpodobné, že daný případ porušení bude mít za následek vysoké riziko pro jeho práva a svobody.

Bližší informace o zpracování osobních byly sděleny zaměstnanci při podpisu tohoto dokumentu a jsou dostupné u příslušného pracovníka/pracovnice personálního oddělení.

PROHLÁŠENÍ ZAMĚSTNANCE

Poté, co jsem měl možnost klást doplňující otázky a zeptat se na vše, co pokládám za podstatné, a moje dotazy mi byly uspokojivě zodpovězeny, prohlašuji, že jsem informacím a vysvětlením plně porozuměl a považuji poučení mé osoby za dostatečné.

Ve Hvozdech dne ..... Podpis

PROHLÁŠENÍ O POVINNOSTI ZACHOVÁVAT MLČENLIVOST

Já, níže podepsaný(á), tímto prohlašuji, že jsem byl(a) dnešního dne poučen(a) Centrem sociálních služeb Hvozdy, o.p.s, se sídlem Masečín 119, 252 07 Štěchovice, IČ: 29128218 (dále jen „poskytovatelem“), o mé povinnosti zachovávat

p o v i n n o s t m l č e n l i v o s t i

vyplývající z ustanovení § 100 zákona č. 108/2006 Sb. o sociálních službách, podle kterého jsou zaměstnanci poskytovatelů sociálních služeb, dobrovolníci a další fyzické osoby povinny zachovávat mlčenlivost o údajích týkajících se osob, kterým jsou poskytovány sociální služby nebo příspěvek, které se při své činnosti dozvědí. Tato povinnost trvá i po skončení pracovního nebo jiného vztahu.

Nad rámec výše uvedeného se tímto rovněž

z a v a z u j i z a c h o v á v a t m l č e l i v o s t

o všech dalších skutečnostech, o kterých se dozvím při vykonávání činnosti pro poskytovatele, zejména o obsahu veškerých interních směrnic a dalších dokumentů týkajících se bezpečnostních opatření přijatých poskytovatelem a o obsahu pracovních nebo jiných smluv, na základě kterých jsou činnosti pro poskytovatele vykonávány, včetně informací o mých právech a povinnostech a o výši případné mzdy, platu nebo odměn.

Beru na vědomí, že porušení povinnosti mlčenlivosti, představuje závažné porušení povinnosti vyplývající z právních předpisů vztahujících se k mnou vykonávané činnosti a může vést mimo jiné k okamžitému zrušení pracovního poměru nebo ukončení jakékoliv jiné formy spolupráce.

Jsem si vědom(a) toho, že za účelem zajištění bezpečnosti a integrity veškerých informací, na které se vztahuje i moje povinnost zachovávat mlčenlivost, byla poskytovatelem přijata řada interních opatření, se kterými jsem byl(a) seznámen(na) a kterými jsem povinen(na) se řídit.

Byl(a) jsem informován(a) o tom, že porušení mé povinnosti zachovávat mlčenlivost může vzhledem k citlivosti zpracovávaných osobních údajů klientů, zaměstnanců a dalších informací vést ke vzniku značných škod na straně poskytovatele, za které budu odpovídat dle ustanovení zákoníku práce, případně ustanovení občanského zákoníku. Porušením povinnost mlčenlivosti může dojít rovněž ke spáchání trestného činu neoprávněného nakládání s osobními údaji.

Prohlášení jsem porozuměl(a), beru jej na vědomí a zavazuji se svou výše uvedenou povinnost mlčenlivosti a další povinnosti a omezení ve všech případech dodržovat.

Ve Hvozdech dne .....

Jméno a příjmení Podpis

SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

pro kontaktní osoby

Jméno a příjmení kontaktní osoby:

Datum narození kontaktní osoby:

Bydliště kontaktní osoby:

Jméno a příjmení klienta:

Kontaktní osoba tímto dobrovolně uděluje svůj kdykoliv odvolatelný souhlas se zpracováním osobních údajů Centrem sociálních služeb Hvozdy, o.p.s., se sídlem Masečín 119, 252 07 Štěchovice, IČ: 29128218, a to v následujícím rozsahu a pro uvedené účely*:*

Souhlasím s evidováním a používáním mých osobních údajů (jméno, příjmení, emailová adresa, telefonní číslo, korespondenční adresa) za účelem kontaktování mé osoby a zasílání informací a pozvánek, to vše výhradně v souvislosti s poskytováním sociální služby uvedenému klientovi.

Jsem srozuměn/a s tím, že neudělení souhlasu není překážkou poskytování péče uvedenému klientovi, pokud souhlas neudělím, nebudou uvedené osobní údaje jakkoliv zpracovávány. Ke zpracování na základě tohoto souhlasu bude docházet po dobu trvání Smlouvy o poskytování sociální služby klientovi.

Práva související se zpracováním

- právo žádat o informace o kategoriích zpracovávaných osobních údajů, účelu, době a povaze zpracování a o příjemcích osobních údajů;
- právo požádat o poskytnutí kopie zpracovávaných osobních údajů;
- právo požádat při naplnění podmínek stanovených relevantními právními předpisy, aby osobní údaje byly opraveny, doplněny nebo vymazány, případně jejich zpracování omezeno;
- právo vznést námitku proti zpracovávání osobních údajů a právo podat stížnost u dozorového úřadu;
- právo být informován o případech porušení zabezpečení osobních údajů a to tehdy, pokud je pravděpodobné, že daný případ porušení bude mít za následek vysoké riziko pro práva a svobody kontaktní osoby.

Prohlášení kontaktní osoby

Tento můj souhlas zůstává v plném rozsahu v platnosti a účinnosti po dobu trvání smlouvy o poskytování služby sociální péče klientovi. Jsem si vědom toho, že udělení tohoto souhlasu je dobrovolné a mohu ho s účinky do budoucna kdykoliv odvolat.

Ve Hvozdech dne .....

podpis kontaktní osoby