Preambule

Standard ochrany osobních údajů formuluje základní cíle a zásady při zpracování a ochraně osobních údajů v Domově.
Dokument současně deklaruje vůli vedení Domova informovat zaměstnance o významu ochrany osobních údajů a o jeho podpoře pro zavedení řízeného systému zpracování a ochrany osobních údajů, který je v souladu s GDPR. Dokument vyjadřuje podporu vedení Domova pro zavedení, provozování, hodnocení výkonnosti a neustálé zlepšování tohoto systému.

Hlavní cíle ochrany osobních údajů

1. Zajištění ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů.
2. Zajištění práv a svobod fyzických osob v souvislosti se zpracováním jejich osobních údajů.
3. Udržování trvalého souladu s požadavky GDPR.
4. Udržování souladu s dalšími právními a technickými požadavky stanovenými platnými souvisejícími právními předpisy a technickými normami.
5. Zajistit schopnost předcházet a zvládat nežádoucí události.
6. Prosazení odpovědnosti zaměstnanců při zajišťování ochrany osobních údajů.
7. Neustálé zlepšování vhodnosti, přiměřenosti a účinnosti systému řízení ochrany osobních údajů.

ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Zpracování a ochrana osobních údajů v prostředí Domova se řídí následujícími zásadami GDPR.

1. Zákonnost zpracování osobních údajů

V Domově jsou zpracovávány osobní údaje v oblastech těchto identifikovaných účelů zpracování

1. Výběrová řízení na zaměstnance
2. Pracovněprávní a mzdová agenda
3. Evidence uchazečů o zaměstnání
4. Evidence úrazů zaměstnanců
5. Smlouvy a objednávky služeb
6. Poskytování informací dle zákona o svobodném přístupu k informacím
7. Projekty, žádosti o dotace
8. Vedení účetnictví příspěvkové organizace
9. Ochrana majetku a osob
10. Prezentace příspěvkové organizace
11. Žádosti o poskytování sociální služby
12. Poskytování sociální služby včetně individuálního plánování průběhu služby
13. Poskytování ošetřovatelské péče
14. Zprostředkování zdravotní péče

15. Laboratorní rozbory biologického materiálu
16. Vyúčtování zdravotní péče zdravotním pojišťovnám
17. Sponzoring

K těmto účelům zpracování jsou zpracovány podklady pro záznamy o činnostech zpracování. Všechna zpracování jsou prováděna na základě stanoveného právního základu, který je uveden v příslušném záznamu o činnostech zpracování pro daný účel. Tyto zákonné důvody ke zpracování osobních údajů mohou být pouze

a) plnění právní povinnosti, která se na Domov jako na správce a zpracovatele osobních údajů vztahuje[1],
b) zpracování je nezbytné pro pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů[2], nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů[3],
c) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů[4],
d) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu, kterým je Domov pověřen,
e) zpracování je nezbytné pro účely oprávněných zájmů Domova, či třetí strany (např. Jihomoravského kraje), kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů,
f) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů.

Odpovědnost za udržování aktuálnosti a úplnosti záznamů o činnostech mají příslušní vedoucí zaměstnanci, vždy v součinnosti s ROOÚ, který zodpovídá za jejich evidenci a aktualizaci v součinnosti s příslušným vedoucím zaměstnancem.
Pokyny pro realizaci této zásady jsou podrobněji rozpracovány příloze č. 1 tohoto standardu *„Povinnosti osob při zpracování osobních údajů“.*

2. Omezení účelem

V Domově jsou osobní údaje shromažďovány jen pro předem vymezené, výslovně vyjádřené a legitimní účely.

Pro naplnění zásady jsou uplatňována následující pravidla:

1. Pro každé zpracování je vždy předem stanoven konkrétní a legitimní účel.
2. Právní základ zpracování je vztažen vždy k jednotlivým účelům.
3. Osobní údaje jsou zpracovávány pouze pro daný účel a je zakázáno je využívat pro jiné účely, vyjma situace, kdy k jejich dalšímu využití udělil subjekt údajů souhlas nebo v dalších případech stanovených odst. 4, článek. 6 GDPR.
4. Údaje shromážděné pro různé účely je zakázáno spojovat, jsou evidovány a zpracovávány odděleně, vyjma účelů, jejichž spojení umožňuje zvláštní zákon anebo pro účely archivace ve veřejném zájmu.

[1] Např. povinnosti zaměstnavatele podle zákona č. 262/2006 Sb., zákoník práce nebo povinnosti poskytovatelů sociálních služeb podle zákona č. 108/2006 Sb., o sociálních službách.
[2] Např. Smlouva o poskytování sociální služby klientovi, nebo pracovní smlouva zaměstnance.
[3] Např. údaje ze žádosti zájemce o sociální službu.
[4] Např. ošetřovatelská dokumentace klienta nebo dokumentace individuálního plánování průběhu sociální služby.

Odpovědnost za dodržování této zásady mají všichni vedoucí zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.
Odpovědnost za kontrolu této zásady má ROOÚ.
Pokyny pro realizaci této zásady jsou podrobněji rozpracovány v příloze č. 1 tohoto standardu *„Povinnosti osob při zpracování osobních údajů“.*

3. Minimalizace údajů a omezení uložení

V Domově jsou osobní údaje zpracovávané pouze pro stanovený účel a pouze po nezbytně dlouhou dobu.
Pro naplnění této zásady jsou uplatňována následující pravidla

1. Je zakázáno shromažďovat a zpracovávat
   - nepřiměřené osobní údaje (každý zpracovávaný osobní údaj musí být pro daný účel nezbytný),
   - nerelevantní osobní údaje (každý zpracovávaný osobní údaj musí mít odpovídající právní základ).

   Toto pravidlo je u stávajících účelů zpracování zavedeno tím, že v záznamech o činnostech zpracování jsou vyjmenovány kategorie údajů, které jsou verifikovány ROOÚ v součinnosti s odpovědnými vedoucími zaměstnanci.
   U případných budoucích účelů zpracování bude, v souladu s pravidly standardní ochrany, pravidlo uplatňováno stejným způsobem a před zahájením zpracování opět verifikováno ROOÚ.
   Odpovědnost za dodržování této zásady mají všichni vedoucí zaměstnanci a zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.
   Odpovědnost za verifikaci a kontrolu této zásady má ROOÚ.

2. Osobní údaje jsou uchovávány v listinné i elektronické podobě pouze po omezenou dobu, odpovídající účelu zpracování. Po ukončení této doby jsou likvidovány nebo mazány v souladu s pravidly a lhůtami stanovenými ve vnitřním předpisu *„Spisový a skartační řád“*, nebo ve lhůtě stanovené odpovědným vedoucím zaměstnancem, která je uvedena v záznamu o činnostech zpracování.
   Odpovědnost za dodržování této zásady mají u listinné podoby všichni vedoucí zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.
   Odpovědnost za dodržování této zásady u elektronické podoby má správce počítačové sítě Domova.
   Odpovědnost za kontrolu této zásady má ROOÚ.

3. Osobní údaje jsou přístupné jen co nejmenšímu počtu osob.
   Toto pravidlo je zavedeno tím, že jsou určena a zavedena pravidla pro řízení přístupu k osobním údajům v listinné i elektronické podobě a dále pro zveřejňování, sdílení a předávání informací.
   Odpovědnost za dodržování této zásady mají všichni vedoucí zaměstnanci a zaměstnanci.
   Odpovědnost za kontrolu této zásady má ROOÚ.

Pokyny pro realizaci této zásady jsou podrobněji rozpracovány v příloze č. 1 tohoto standardu *„Povinnosti osob při zpracování osobních údajů“.*

4. Přesnost osobních údajů

V Domově jsou zpracovávané pouze přesné osobní údaje. Zásady aktualizace zpracovávaných dat jsou nastaveny způsobem odpovídajícím kritičnosti jejich možných dopadů na subjekty údajů.
Personalistka poučuje každého zaměstnance o povinnosti hlásit případné změny všech jím předaných osobních údajů.
Sociální pracovnice poučuje každého zájemce o sociální službu, klienta Domova, opatrovníka nebo zmocněnce klienta a rodinného příslušníka klienta o povinnosti hlásit případné změny všech jím předaných osobních údajů.
Odpovědnost za stanovení způsobu ověřování přesnosti dat mají všichni vedoucí zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.
Odpovědnost za kontrolu této zásady má ROOÚ.

5. Korektnost a transparentnost při zpracování osobních údajů

Při zpracování osobních údajů v působnosti Domova jsou subjekty údajů transparentně informovány těmito způsoby:

- základní informace na webových stránkách Domova, dostupná všem subjektům údajů dálkovým přístupem,
- doplňující informace o zpracování osobních údajů poskytované k jednotlivým účelům zpracování před zahájením shromažďování osobních údajů,
- písemná informace o zpracování osobních údajů pro účely pracovněprávní agendy poskytovaná novým zaměstnancům,
- informace zaměstnancům o dohledu nad užíváním informačních a komunikačních technologií na pracovišti,
- informace zaměstnancům o monitoringu docházky,
- informace o monitoringu objektů a prostor kamerovými systémy.

V Domově jsou stanoveny postupy pro výkon práv subjektu údajů. Těmito právy se rozumí:

- právo na přístup k osobním údajům,
- právo na opravu nepřesných osobních údajů,
- právo na výmaz (být zapomenut),
- právo na omezení zpracování,
- právo na přenositelnost,
- právo vznést námitku proti zpracování osobních údajů,
- právo nebýt předmětem automatizovaného individuálního rozhodování.

Výkon práv subjektů údajů v Domově koordinuje ROOÚ ve spolupráci s příslušnými vedoucími zaměstnanci, do jejichž působnosti příslušný požadavek na uplatnění práva spadá.

Za výkon práv subjektů údajů v domově jsou odpovědní:

- ROOÚ,
- vedoucí zaměstnanci.

Pokyny pro realizaci této zásady jsou podrobněji rozpracovány v přílohách tohoto standardu č. 1 *„Povinnosti osob při zpracování osobních údajů“* a č. 2 *„Výkon práv subjektu údajů“*.

6. Důvěrnost, integrita a dostupnost osobních údajů

V Domově jsou za účelem ochrany osobních údajů přijata vhodná technická a organizační opatření odpovídající kontextu a účelům zpracování osobních údajů.
Veškerá technická a organizační opatření jsou přijata na základě provedené analýzy informačních rizik. Analýza rizik byla provedena na základě:

a) posouzení hrozeb působících na aktivity, v rámci kterých jsou zpracovávány osobní údaje,
b) posouzení hrozeb pro práva a svobody subjektů údajů.

Na základě závěrů z provedené analýzy rizik byla implementována organizační a technická opatření pro zajištění odpovídající úrovně ochrany zpracovávaných osobních údajů.
Pro provedení analýzy rizik byla stanovena metodika hodnocení rizik, která vychází z požadavků vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). V rámci provedené analýzy rizik byly současně zohledněny hrozby, které představují zejména možnost náhodného nebo protiprávního zničení, ztráty, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů nebo neoprávněný přístup k nim.
Za stanovení a aktuálnost technických a organizačních opatření vyplývajících z analýzy rizik odpovídá zaměstnanec nebo správce počítačové sítě Domova a příslušní vedoucí zaměstnanci.
Za kontrolu dodržování stanovených technických a organizačních opatření odpovídá ROOÚ v součinnosti s vedoucími zaměstnanci.
Pokyny pro realizaci této zásady, včetně stanovení odpovídajících technických a organizačních opatření pro oblast fyzické, personální, administrativní a počítačové bezpečnosti, jsou podrobněji rozpracovány v přílohách tohoto standardu.

7. Odpovědnost správce osobních údajů

Správcem osobních údajů je Domov.

Správce je povinen zajistit soulad s GDPR a tento soulad prokazuje:

1. Zpracováním Standardu ochrany osobních údajů, stanovující
   - cíle ochrany osobních údajů,
   - zásadami zpracování a ochrany osobních údajů,
   - odpovědnosti za realizaci zásad,
   - odpovědnost za kontrolu.
2. Zpracováním záznamů o činnostech zpracování.
3. Rozpracováním Standardu ochrany osobních údajů do příloh uvedených v bodě 8.
4. Jmenováním ROOÚ a stanovením jeho působnosti a odpovědnosti,
5. Zajištěním zásad záměrné a standardní ochrany osobních údajů, realizované:
   - návrhem vhodných technických a organizačních opatření záměrné ochrany stanovených příslušnými vedoucími zaměstnanci a ROOÚ, před zahájením vlastního zpracování, ještě v době určování prostředků pro zpracování osobních údajů.

- zavedením a udržováním záměrné a standardní ochrany přiměřenými technickými a organizačními opatřeními založenými na výsledcích analýzy rizik.

6. Dodržováním všech zásad GDPR ve vztahu ke zpracovatelům a dalším správcům.

8. Struktura standardu kvality sociální služby Ochrana osobních údajů

Přílohy

1. Povinnosti osob při zpracování osobních údajů
2. Výkon práv subjektu údajů
3. Záměrná a standardní ochrana osobních údajů
4. Bezpečnost ICT
5. Ochrana osobních údajů v kamerovém systému
6. Analýza osobních údajů zpracovávaných Domovem

Metodiky

1. Metodika analýzy rizik GDPR

Formuláře

1. Záznamový list k žádosti subjektu údajů podle článku 15 – 22 GDPR
2. Záznamy o činnostech zpracování osobních údajů

Seznam použitých pojmů a zkratek

Active Directory	Je řešení adresářových služeb pro správu síťových prostředků. Active Directory využívají administrátoři počítačových sítí pro různé účely. Nastavují za jeho pomoci pravidla a politiku sítě, instalují programy na veliké množství PC stanic zároveň či řeší kritické situace v síti.
Administrátor	Osoba pověřená správou jednoho, nebo více ICT zařízení, která je schválena ředitelem organizace a má nejvyšší úroveň oprávnění pro ICT zařízení ve své správě.
Administrátorský účet	Uživatelský učet, jenž má nevyšší možná oprávnění v rámci daného operačního systému nebo aplikace.
Aplikace	Programové vybavení výpočetní techniky organizace (např. MS Word).
Autentizace	Je proces ověření proklamované identity subjektu.
Bezpečnost informací	Je zajištění následujících atributů chráněných informací: důvěrnosti (ochrana před neoprávněným čtením), integrity (ochrana před neoprávněnými úpravami nebo zničením) a dostupnosti (zajištění adekvátního přístupu a ochrana před jeho neoprávněným zamezením).
Cloud	Externí internetové datové uložiště (např. One Drive, Google drive, Dropbox apod.).
Fyzická bezpečnost	Fyzická bezpečnost znamená používání fyzických a technických ochranných opatření k zamezení neoprávněného přístupu k majetku a informacím organizace.
Garant aplikace	Zaměstnanec odpovědný za konkrétní aplikaci. Garant aplikace je odborný zaměstnanec se znalostí dané aplikace a rozhoduje o požadavcích na přístup k dané aplikaci.
GDPR	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů – General Data Protection Regulation).
Hardware	Označuje veškeré fyzicky existující technické vybavení výpočetní techniky či síťových prostředků.
Operační systém	Základní programové vybavení počítače (tj. software), který je zaveden do paměti počítače při jeho startu a zůstává v činnosti až do jeho vypnutí (např. MS Windows 10).
Důvěrnost	Zajištění, že informace (data) jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
Dostupnost a odolnost	Zajištění, že osobní údaje jsou pro oprávněné uživatele přístupné v okamžiku jejich potřeby. Jedná se o zničení dat, nebo úmyslné blokování či zahlcení technických prostředků, prostřednictvím

	kterých mají být tyto osobní údaje přístupné v požadovaném čase.
Integrita	Vyjadřuje, jak je důležité, aby informace nebyla neoprávněně změněna.
Likvidace osobních údajů	Fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.
Oprávněná osoba	Oprávněnými osobami se pro účely této směrnice rozumí: a) zaměstnanci Domova, kteří v rámci plnění povinností plynoucích jim z jejich pracovních náplní mají přístup k osobním údajům a dále je zpracovávají, b) osoby vykonávající práci na základě dohod o pracích konaných mimo pracovní poměr, pokud z uzavřené dohody vyplývá, že pro plnění předmětu dohody mají mít přístup k osobním údajům a dále je zpracovávat.
Organizační celek	Sekce, oddělení, pracoviště.
Osobní údaj	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.
Počítačová síť organizace	Síťové prostředky a výpočetní technika ve správě a/nebo v majetku organizace, které realizují spojení a výměnu informací.
Provozní deník	Písemný dokument nebo elektronický soubor, který obsahuje všechny činnosti, které při správě počítačové sítě provádí správce ICT.
Přístupový údaj	Sada informací potřebných pro přihlášení do operačního systému nebo aplikace. V základní podobě jsou tvořeny uživatelským jménem a heslem.
Racková skříň	Standardizovaný systém umožňující přehlednou montáž a propojování různých elektrických a elektronických zařízení spolu s vyústěním kabelových rozvodů, zajišťující základní fyzickou bezpečnost.
Referent pro ochranu osobních údajů	Zaměstnanec Domova, ustanovený do funkce referenta pro ochranu osobních údajů (Dále jen „ROOÚ“).
Režimová opatření	Ucelený soubor opatření, pokynů, příkazů, zákazů a omezení představující soupis instrukcí pro vstup, odchod, pohyb v objektu a přístup k informacím organizace.
Síťové prostředky	Technická zařízení používaná k zajištění provozu, správy a bezpečnosti sítě organizace. Jedná se zejména o Routery, servery, switche, firewall apod.

SLA – Service Level Agreement	Je dohoda o úrovni poskytovaných služeb. SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi. SLA definuje rozsah, úroveň a kvalitu služby.
Správce ICT	Osoba odpovědná za provozování a správu počítačové sítě a prostředků ICT organizace. Disponuje administrátorskými účty k operačním systémům a některým aplikacím.
Souhlas	Svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.
Správce osobních údajů	Domov pro seniory Zastávka, příspěvková organizace (dále jen „Domov“).
Subjekt údajů	Fyzická osoba, k níž se osobní údaje vztahují.
Účel zpracování	Účel, pro který jsou osobní údaje zpracovávány (obvykle agenda nebo činnost).
Uživatel	Zaměstnanec využívající výpočetní techniku organizace
Uživatelské jméno	Je jednoznačný identifikátor uživatele v systému. Jedná se o unikátní jméno zpravidla složené z písmen (případně i číslic).
Uživatelský účet	Jednoznačná identifikace uživatele v rámci operačního systému nebo aplikace. Uživatelský účet umožňuje plnou práci, ale bez možnosti instalovat aplikace do výpočetní techniky nebo měnit nastavení operačního systému nebo aplikace. Uživatelský účet se standardně skládá z uživatelského jména a hesla.
VPN	Virtuální privátní síť (zkratka VPN, anglicky Virtual Private Network) je v informatice prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě.
Výpočetní technika	Soubor počítačů, notebooků, tabletů nebo smartphonů organizace. Obecně všech zařízení, která disponují vlastním operačním systémem.
Vedení příspěvkové organizace	Ředitel, zástupce ředitele, vedoucí sekcí.
Vedoucí zaměstnanci	Zaměstnanci uvedení v článku 8 Organizačního řádu Domova.
Zaměstnanci	Zaměstnanci Domova.
Zásada „prázdného stolu“	Každý zaměstnanec je povinen udržovat na svém pracovním stole a ve svém okolí pořádek tak, aby volně přístupné byly pouze informace, se kterými aktuálně pracuje, a aby veškeré důležité informace byly bezpečně uloženy.
Záznam o činnosti zpracování	Dokument obsahující údaje dle čl. 30 GDPR, který vedou pro jednotlivé účely zpracování v rozsahu své působnosti vedoucí zaměstnanci a v celkové evidenci také pověřenec pro ochranu

	osobních údajů.
Zpracování osobních údajů	Jakákoliv operace nebo soubor operací s osobními údaji, nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.
Zpracovatel	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
Zpracovatelská operace	Proces, v rámci kterého se zpracovávají osobní údaje.
Zvláštní kategorie údajů	Osobní 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.