Dokumentace pro ochranu osobních údajů v souladu s GDPR

Politika ochrany osobních údajů v DS Tovačov

OBSAH

Platnost od: 25. 05. 2018

Aktualizace do: 24. 05. 2020

Počet řízených kopií: 4 (EPÚ, OZÚ, SPA, STRAV)

Elektronická podoba dokumentu: na serveru domova ve složce Vnitřní předpisy

Zpracoval: Mgr. Lenka Olivová

Schválil: Mgr. Lenka Olivová, ředitelka ……
razítko a podpis

Revize interních dokumentů

Evidence procesu přípravy, schválení a revizí směrnice Politika ochrany osobních údajů

vydání č.	platné od	zpracoval	podpis	schválil	podpis
1	25. 05. 2018	Mgr. Lenka Olivová	Olivová, v. r.	Mgr. Lenka Olivová	Olivová, v. r.

Specifikace provedených změn

revize č.	předmět revize	strana	platné od	revidoval (podpis)
1				
2				
3				
4				
5				

Souhrn všech dosud provedených revizí

revize č.	datum revize	zrevidoval	podpis	schválil	podpis
1					
2					
3					
4					
5					

Seznam použitých pojmů a zkratek

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)
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.
Pověřenec pro ochranu osobních údajů	Zaměstnanec příspěvkové organizace ustavený do funkce pověřence pro ochranu osobních údajů.
Správce osobních údajů	Domov pro seniory Tovačov, p.o.
Vedoucí zaměstnanci	Vedoucí zaměstnance stanoví ředitel organizace.
Zaměstnanci	Zaměstnanci příspěvkové organizace. Zaměstnanci vykonávající práci na základě dohod o pracích konaných mimo pracovní poměr.
Záznam o činnosti zpracování	Dokument obsahující údaje dle čl. 30 obecného nařízení, 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.

POZNÁMKA:

Role definované tímto dokumentem předpokládají, že je bude vykonávat i žena. Z důvodu zjednodušení textu jsou použity názvy jednotlivých rolí v mužském rodě. Bude-li danou roli zajišťovat žena, předpokládá se automatické přechylování názvů jednotlivých rolí bez nutnosti úpravy směrnice.

Úvodní ustanovení

1. Dokument Politika ochrany osobních údajů formuluje základní cíle a zásady při zpracování a ochraně osobních údajů v Domově pro seniory Tovačov, příspěvková organizace (dále jen Domov).
2. 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 Nařízením 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 (obecné nařízení o ochraně osobních údajů) – General Data Protection Regulation (dále jen „GDPR“).
3. Dokument vyjadřuje podporu vedení Domova pro zavedení, provozování, hodnocení výkonnosti a neustálé zlepšování tohoto systému.

Hlavní cíle ochrany osobních údajů

Hlavními cíli ochrany osobních údajů jsou:
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 a ochrany osobních údajů

Zpracování a ochrana osobních údajů v Domově se řídí následujícími zásadami GDPR:

1. Zákonnost zpracování osobních údajů

V Domově pro seniory Tovačov jsou zpracovávány osobní údaje zejména za účelem:
a) Výběrová řízení na zaměstnance
b) Pracovněprávní a mzdová agenda
c) Evidence uchazečů o zaměstnání
d) Evidence úrazů
e) Smlouvy a objednávky služeb
f) Poskytování informací dle zákona o svobodném přístupu k informacím
g) Projekty, žádosti o dotace
h) Vedení účetnictví příspěvkové organizace

i) Ochrana majetku a osob
j) Prezentace příspěvkové organizace
k) Žádosti o poskytnutí sociální služby
l) Poskytování sociální služby
m) Poskytování ošetřovatelské péče
n) Zajištění zdravotní péče
o) Vyúčtování zdravotní péče zdravotním pojišťovnám
p) Sponzoring
q) Řešení nároků fyzických osob uplatněných u zdravotnického zařízení / řešení nároků zdravotnického zařízení vůči fyzickým osobám.

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.

Odpovědnost za udržování aktuálnosti a úplnosti záznamů o činnostech mají příslušní vedoucí zaměstnanci, v součinnosti s pověřencem pro ochranu osobních údajů (dále jen pověřenec), který zodpovídá za jejich evidenci a aktualizaci v součinnosti s příslušným vedoucím zaměstnancem. Pokud pověřenec v organizaci jmenován není (organizace v současné době nemá povinnost pověřence jmenovat), plní jeho funkci ředitelka organizace.

Pokyny pro realizaci této zásady jsou podrobněji rozpracovány ve vnitřním předpisu SM GDPR 03Povinnosti 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 této zásady jsou uplatňována následující pravidla:
1) Pro každé zpracování je vždy předem stanoven konkrétní a legitimní účel.
1) Právní základ zpracování je vztažen vždy k jednotlivým účelům.
2) 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 čl. 6, odst. 4 GDPR.
3) 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.

Odpovědnost za dodržování této zásady mají všichni vedoucí zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.

Odpovědnost za kontrolu této zásady má pověřenec pro ochranu osobních údajů, v případě, že není jmenován, ředitelka organizace.

Pokyny pro realizaci této zásady jsou podrobněji rozpracovány ve vnitřním předpisu SM GDPR 03 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 pověřencem / ředitelkou 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 pověřencem / ředitelkou.

   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 pověřenec / ředitelka.

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 Ř 06 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 zaměstnanec nebo osoba (fyzická osoba podnikající nebo právnická osoba na základě uzavřeného smluvního vztahu), odpovídající za správu a provoz informačních technologií.

   Odpovědnost za kontrolu této zásady má pověřenec pro ochranu osobních údajů.

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 pověřenec pro ochranu osobních údajů.

   Pokyny pro realizaci této zásady jsou podrobněji rozpracovány ve vnitřním předpisu SM GDPR 03 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.

Zaměstnanec odpovědný za přípravu a uzavření pracovní smlouvy poučuje každého zaměstnance 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 pověřenec / ředitelka.

5. Korektnost a transparentnost při zpracování osobních údajů

Při zpracování osobních údajů jsou subjekty údajů transparentně informovány těmito způsoby:

- základní informace na webových stránkách Domova *www.dstovacov.cz*, 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 objektu 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 pověřenec / ředitelka ve spolupráci s příslušnými vedoucími zaměstnanci, do jejichž působnosti příslušný požadavek na uplatnění práva spadá.

Za výkon práv subjektů údajů v Domově jsou odpovědní:

- pověřenec pro ochranu osobních údajů / ředitelka,
- vedoucí zaměstnanci.

Pokyny pro realizaci této zásady jsou podrobněji rozpracovány ve vnitřním předpisu SM GDPR 03 Povinnosti osob při zpracování osobních údajů, a směrnici SM GDPR 04 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 aktiva, 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 přiměřená 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 osoba (fyzická osoba podnikající nebo právnická osoba na základě uzavřeného smluvního vztahu), odpovídající za správu a provoz informačních a komunikačních technologií a příslušní vedoucí zaměstnanci.

Za kontrolu dodržování stanovených technických a organizačních opatření odpovídá pověřenec / ředitelka 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 následujících vnitřních předpisech a dokumentech:

- ✓ Směrnice „Povinnosti osob při zpracování osobních údajů“,
- ✓ Směrnice „Záznamy o činnostech zpracování“,
- ✓ Směrnice „Výkon práv subjektu údajů“,
- ✓ Směrnice „Záměrná a standardní ochrana osobních údajů“,
- ✓ Směrnice „Bezpečnost ICT“,
- ✓ Směrnice „Ochrana osobních údajů v kamerovém systému“,
- ✓ Směrnice „Metodika analýzy rizik GDPR“,
- ✓ Směrnice „Řízení rizik“,
- ✓ Směrnice „Provoz kamerového systému v DS Tovačov“.

7. Odpovědnost správce osobních údajů

Správcem osobních údajů je *příspěvková organizace* Domov pro seniory Tovačov. Správce je povinen zajistit soulad s GDPR a tento soulad prokazuje:

1) zpracováním Politiky 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 Politiky ochrany osobních údajů do vnitřních předpisů a dokumentů uvedených v bodě 6,
4) jmenováním pověřence pro ochranu osobních údajů a stanovením jeho působnosti a odpovědnosti, pokud se tato povinnost Domova týká (bude týkat),
5) zajištěním zásad záměrné a standardní ochrany osobních údajů, realizované:
   - návrhem vhodných technických a organizačních opatření záměrné ochrany stanovených příslušnými vedoucími zaměstnanci a pověřencem pro ochranu osobních údajů, 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.