1 Rozsah působnosti

Ustanovení této směrnice jsou závazná pro všechny zaměstnance Domova.

2. Odpovědnost za zpracování osobních údajů

Ředitel Domova zastupuje správce osobních údajů.

ROOÚ dohlíží na zpracování a ochranu osobních údajů v Domově a kontroluje dodržování zásad zpracování a ochrany osobních údajů stanovených Standardem kvality sociální služby *Ochrana osobních údajů* (dále jen „Standard GDPR“). V době jeho nepřítomnosti plní jeho povinnosti zástupce ředitele.

Vedoucí zaměstnanci odpovídají za zpracování a ochranu osobních údajů v rozsahu své působnosti určené účely zpracování, které jsou uvedeny v celkové evidenci záznamů o činnostech zpracování, která je dostupná na Síti Domova. Dále odpovídají za realizaci a prosazování zásad zpracování a ochrany osobních údajů stanovených Standardem GDPR.

Oprávněné osoby odpovídají za zpracování a ochranu osobních údajů v jimi vykonávaných agendách a činnostech a za dodržování zásad zpracování a ochrany osobních údajů stanovených Standardem ochrany osobních údajů.

3. Správce osobních údajů

Správce osobních údajů je povinen:

3.1. Stanovit oprávněným osobám povinnosti ke zpracování osobních údajů. Těmto povinnostem odpovídají jejich oprávnění přístupu k osobním údajům.

3.2. Stanovit oprávněným osobám postupy při zpracování osobních údajů v jimi zajišťovaných agendách a činnostech a vytvořit jim k tomu podmínky včetně zajištění prostředků pro zpracování osobních údajů.

3.3. Bez zbytečného odkladu, nejpozději ale do 30 dní, zajistit práva subjektů údajů, jejichž osobní údaje jsou v Domově zpracovávány.

3.4. Před zahájením shromažďování osobních údajů poskytnout subjektům údajů informace o zpracování jejich osobních údajů Domovem

3.5. Jiným subjektům předávat osobní údaje pouze v případech, pokud takové předání ukládá nebo umožňuje zvláštní zákon, nebo se souhlasem dotčených osob.

3.6. Stanovit a zajistit realizaci opatření při zabezpečení osobních údajů.

3.7. Ve smlouvách se zpracovateli osobních údajů zakotvit náležitosti v rozsahu požadavků čl. 28 GDPR.

3.8. Zajistit oprávněným osobám podmínky pro ukládání médií s osobními údaji a vyžadovat jejich používání (uzamykatelné úschovné objekty nebo uzamykatelné místnosti s možností vyloučení nekontrolovaného vstupu neoprávněných osob), včetně stanovení pravidel pro ukládání dokumentů uchovávaných po dobu skartační lhůty v archívu. Současně zajistit evidenci těchto médií a stanovit pravidla pro jejich zapůjčování a pořizování kopií. Kopírování médií obsahující zvláštní kategorie osobních údajů je zakázáno, výjimky povoluje ředitel Domova.

3.9. Provádět kontrolní činnost k ochraně osobních údajů a v případě zjištěných nedostatků přijímat opatření k jejich odstranění.

4. Referent pro ochranu osobních údajů (ROOÚ)

ROOÚ je povinen:

4.1. Pro zabezpečení komunikace zajistit:
   a) kontaktní místo pro subjekty údajů, které se na něj mohou obracet ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle GDPR,
   b) kontaktní místo pro ÚOOÚ v záležitostech zpracování, včetně předchozí konzultace podle čl. 36 GDPR a případné vedení konzultací v jakékoli jiné věci,
   c) kontaktní místo pro zpracovatele, jiné správce a dozorové úřady cizích zemí.

4.2. Za účelem komunikace s ROOÚ je zřízena emailová adresa[1]. V rámci trvalého monitoringu souladu s GDPR a dalšími souvisejícími právními předpisy a vnitřními normami upravujícími ochranu osobních údajů:
   a) ověřovat relevantnost vyhodnocení rizik pro práva a svobody subjektů údajů pro prováděné zpracovatelské operace,
   b) ověřovat a případně aktualizovat informace určené subjektům údajů v rozsahu požadavků čl. 13 a čl. 14 GDPR,
   c) v součinnosti s odpovědnými osobami vyhodnocovat účinnost přijatých technických a organizačních opatření a připravovat návrhy nezbytných změnových řízení,
   d) koordinovat výkon práv subjektů údajů a zajišťovat jejich informovanost o průběhu a řešení jejich požadavku na uplatnění práva do stanovené lhůty,
   e) v součinnosti s vedením Domova zajistit:
      1. ohlašování případů porušení zabezpečení osobních údajů ÚOOÚ (bez zbytečného odkladu, a to nejpozději do 72 hodin od zjištění porušení zabezpečení),
      2. oznamování případů porušení zabezpečení osobních údajů subjektům údajů (bez zbytečného odkladu),
   f) vést dokumentaci o všech případech porušení zabezpečení osobních údajů v rozsahu uvedeném v čl. 33 odst. 3 GDPR,
   g) připravovat v součinnosti s vedoucími zaměstnanci návrhy smluv o zpracování osobních údajů, pokud je zpracovatelská operace nebo některá její část zajišťována prostřednictvím zpracovatele,
   h) informovat, radit a vydávat doporučení v oblasti zpracování a ochrany osobních údajů vedoucím zaměstnancům a zaměstnancům,
   i) řídit kontrolní činnost zaměřenou na zpracování a ochranu osobních údajů, v případě zjištění nedostatků informovat příslušného vedoucího zaměstnance a ředitele Domova za účelem sjednání nápravy.

4.3. Při dohledu nad zpracovatelskými operacemi:
   a) vést celkovou evidenci záznamů o činnostech zpracování podle čl. 30 GDPR a provádět její aktualizaci na návrh vedoucích zaměstnanců,

[1] dszastavka.burianek@seznam.cz

b) monitorovat a případně aktualizovat požadavky na zabezpečení osobních údajů,
c) v součinnosti s příslušnými vedoucími zaměstnanci průběžně ověřovat, zda jsou stávající technická a organizační opatření dostatečná, případně předložit řediteli Domova návrh k úpravě existujících opatření.

4.4. Při vzniku potřeby nové zpracovatelské operace, nebo změny již existující, zejména se zřetelem na zpracování zvláštních kategorií osobních údajů, vyjádřit své stanovisko k návrhu nové nebo změně zpracovatelské operace ve smyslu:

a) dodržení zásad zpracování osobních údajů a zvláštních kategorií osobních údajů uvedených v čl. 5 – čl. 11 GDPR, s cílem zejména analyzovat a prověřovat právní soulad zpracovatelských činností, zejména:
   - dodržení zásad zpracování osobních údajů dle čl. 5 GDPR,
   - definici právního základu pro zpracování dle čl. 6 GDPR,
   - v případě, že právním základem zpracování je souhlas subjektu údajů se zpracováním, stanovit podmínky jeho vyjádření, prokazatelnosti a postupů v případě jeho odvolání dle čl. 7 GDPR,
   - v případě, že budou zpracovávány zvláštní kategorie osobních údajů, zajistit jejich zpracování v souladu s čl. 9 GDPR, tj. zejména:
     ~ deklarovat zákonnost zpracování,
     ~ stanovit právní základ zpracování,
     ~ v případě, že se bude jednat o zpracování těchto údajů na základě uděleného výslovného souhlasu, v případě vyhodnocení nezbytnosti tohoto zpracování vydat písemný souhlas k tomuto zpracování.

b) vyhodnocení rizik pro práva a svobody subjektů údajů:
   - v případě, že riziko bude vyhodnoceno jako vysoké, posoudit právní základ nového zpracování a vyjádřit se ke skutečnosti, zda provést či neprovést posouzení vlivu na ochranu osobních údajů,
   - v případě kladného vyjádření zajistit provedení posouzení vlivu zamýšlené zpracovatelské operace na ochranu osobních údajů a případně zahájit konzultační činnost s ÚOOÚ,
   - o stanovisku ÚOOÚ neprodleně informovat ředitele Domova,

c) přijetí opatření na zabezpečení osobních údajů, přičemž bude vycházet z posouzení rizika zpracování pro práva a svobody subjektů údajů. Bude vyhodnocena vhodnost nasazení opatření dle článku čl. 32 GDPR k:
   - případnému šifrování osobních údajů,
   - zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování osobních údajů,
   - obnovitelnosti a zajištění dostupnosti osobních údajů,
   - testování, posuzování a hodnocení účinnosti zavedených bezpečnostních opatření.
   - v případě záměru zpracovávat osobní údaje k jinému účelu, než byly shromážděny, a subjekt údajů neposkytl souhlas pro jejich další využití, provést posouzení slučitelnosti obou účelů a zdokumentované stanovisko s doporučením dalšího postupu předat odpovědnému vedoucímu zaměstnanci a řediteli Domova.

4.5. Při zániku zpracovatelské operace, nebo jakékoli její části, vyjádřit své stanovisko k návrhu zániku zpracovatelské operace ve smyslu:
   a) doby uchování osobních údajů za účelem archivace, pokud není určena platným Spisovým a skartačním řádem,
   b) kategoriemi osobních údajů, které budou pro případnou archivaci ve veřejném zájmu uchovány,
   c) způsobu likvidace zbývajících osobních údajů v elektronické i listinné podobě.

4.6. Rozvíjet znalosti a metodicky vést vzdělávání zaměstnanců zpracovávajících osobní údaje z problematiky ochrany osobních údajů.

4.7. Poskytovat poradenství a informace vedení Domova vedoucím zaměstnancům a oprávněným osobám, a to zejména
   a) formou ad hoc poradenství na vyžádání,
   b) formou trvalého monitoringu informací z dostupných zdrojů (stanoviska ÚOOÚ a evropských orgánů, judikáty, rozhodovací praxe atd.), jejich následného vyhodnocení a předání návrhů ředitele Domova pro případné zlepšení či aktualizaci,
   c) formou ad hoc konzultací s ÚOOÚ.

5. Vedoucí zaměstnanci

Vedoucí zaměstnanci jsou povinni:

5.1. V součinnosti s ROOÚ:
   a) vést a aktualizovat záznamy o činnostech zpracování v rozsahu své působnosti,
   b) před zahájením shromažďování osobních údajů zajistit informovanost subjektů údajů,
   c) vést evidenci souhlasů subjektů údajů v rámci příslušného záznamu o činnosti zpracování,
   d) hodnotit efektivitu a účinnost přijatých organizačních a technických opatření,
   e) zajistit v součinnosti s ROOÚ výkon práv subjektů údajů,
   f) v případě, že některá zpracovatelská operace nebo její část je zajišťována zpracovatelem a zmocnění ke zpracování nevyplývá z právního předpisu, vyjadřovat se ke smlouvám o zpracování osobních údajů.

5.2. Neprodleně oznamovat ROOÚ:
   a) vznik nové zpracovatelské operace, změny nebo zánik již existující zpracovatelské operace nebo jakékoli její části,
   b) změnu v příslušném právním předpise, který je buď právním základem pro zpracování osobních údajů ve zpracovatelské operaci, nebo je jím zpracovatelská operace regulována,
   c) porušení nebo podezření na porušení zabezpečení osobních údajů u jimi řízeného organizačního celku.

5.3. V případě doručení žádosti na uplatnění výkonu některého práva subjektu údajů, předat tuto žádost ROOÚ.

5.4. Stanovit podřízeným zaměstnancům postupy při zpracování osobních údajů v jimi zajišťovaných agendách a činnostech a vytvořit jim k tomu podmínky včetně zajištění prostředků pro zpracování osobních údajů.

5.5. Seznámit podřízené zaměstnance s jejich konkrétními povinnostmi při zpracování a ochraně osobních údajů v r rámci činností vykonávaných v souladu s pracovní náplní.

5.6. Zajistit podřízeným zaměstnancům podmínky pro uchovávání nosičů osobních údajů v uzamykatelných úschovných objektech nebo v uzamčených místnostech s vyloučeným nekontrolovaným vstupem neoprávněných osob.

5.7. Zajišťovat přidělení uživatelských oprávnění do aplikací a datových zdrojů pro své podřízené, a to v rozsahu nezbytně nutném pro splnění jejich pracovních povinností vyplývajících z pracovních náplní.

5.8. Zajistit, aby dokumenty, jejichž původcem je jejich útvar a které jsou zveřejňovány nebo zpřístupňovány např. dálkovým způsobem, obsahovaly pouze takové osobní údaje, které vyžaduje nebo umožňuje zvláštní zákon, dle kterého ke zveřejnění dochází.

5.9. Zajistit účast zaměstnanců v rámci jejich průběžného vzdělávání na kurzech zaměřených k problematice zpracování a ochrany osobních údajů.

5.10. Při zpracování osobních údajů plnit povinnosti oprávněné osoby dle kapitoly 2.4 této přílohy Standardu ochrany osobních údajů.

5.11. Kontrolovat dodržování stanovených technických a organizačních opatření k zajištění ochrany osobních údajů.

6. Oprávněné osoby

Oprávněné osoby jsou při zpracování osobních údajů a pro zajištění jejich ochrany povinny:

6.1. Zachovávat mlčenlivost o osobních údajích a o přijatých opatřeních k jejich ochraně, o nichž se v souvislosti se svým zaměstnáním nebo plněním smlouvy dozvěděly, a to i po skončení svého pracovního poměru v Domově nebo platnosti smlouvy.

6.2. Zpracovávat osobní údaje za podmínek a v rozsahu jim stanoveném v souladu s platnými přístupy do informačních systémů a SW aplikací.

6.3. Osobní údaje shromažďovat pouze pro určité, výslovně vyjádřené a legitimní účely v rozsahu
   a) stanoveném zvláštními zákony, resp.
   b) pouze relevantním a nezbytně nutném, není-li rozsah zpracovávaných osobních údajů stanoven pro konkrétní účel (agendu nebo činnost) zvláštním zákonem.

6.4. Při shromažďování osobních údajů poskytovat subjektům údajů informace o zpracování jejich údajů v rozsahu čl. 13 a čl. 14 GDPR.

6.5. Při shromažďování osobních údajů od subjektů údajů vyžadovat jejich souhlas se zpracováním pouze v případě, že nebyl nalezen jiný zákonný důvod pro zpracování těchto osobních údajů, kterým je:
   a) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
   b) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,

c) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
d) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
e) zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

6.6 Pokud jsou shromažďovány osobní údaje na základě uděleného souhlasu od subjektu údajů, musí být tento poučen i o možnosti tento souhlas kdykoli odvolat. Současně musí být subjekt údajů poučen o možných následcích jeho odvolání.

6.7 Je zakázáno shromažďovat zvláštní kategorie osobních údajů. Výjimku tvoří případy uvedené v čl. 9 odst. 2 GDPR., a to

a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů,
b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany,
c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
d) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
e) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků,
f) zpracování je nezbytné z důvodu významného veřejného zájmu,
g) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče,
h) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví,
i) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely,

při současném zachování podmínky určené čl. 9 odst. 3 GDPR, tj. zpracování je prováděné pracovníkem vázaným služebním tajemstvím nebo se na něj vztahuje povinnost mlčenlivosti a zpracování je nezbytné pro poskytování zdravotní a sociální péče.

6.8. V případě, že je shromažďována některá ze zvláštních kategorií osobních údajů na základě čl. 9 odst. 2 písm. a), tedy na základě výslovného souhlasu subjektu osobních údajů, musí být záměr shromažďovat tento typ údajů vždy písemně odsouhlasen ROOÚ.

6.9. Při zpracování osobních údajů:

a) zpracovávat pouze přesné údaje s ohledem na účel zpracování; v případě zjištění, že zpracovávané údaje nejsou přesné, osobní údaje opravit nebo vymazat,
b) zpracovávat osobní údaje pouze k účelům, k nimž byly shromážděny; k jinému účelu, pouze v případě, že subjekt údajů dal k tomu předem souhlas,

c) neumožnit zpracování osobních údajů jiné osobě, která není pro konkrétní účel zpracování těchto údajů k tomu oprávněna (v souladu s popisem pracovní náplně – činnosti nebo povinnostmi plynoucími ze smlouvy).

6.10. Dokumenty, obsahující osobní údaje, předávat a poskytovat způsoby stanovenými platným Spisovým a skartačním řádem:
a) v rámci Domova pouze příslušným oprávněným zaměstnancům,
b) mimo Domov pouze v případech plynoucích z působnosti Domova, stanoví-li tak zvláštní zákon, v souladu s platnou smlouvou o zpracování osobních údajů nebo se souhlasem subjektů údajů.

6.11. Média, obsahující osobní údaje (listinné i elektronické), ukládat způsobem zamezujícím neoprávněnému či nahodilému přístupu k těmto osobním údajům (uzamykatelné úschovné objekty). Při práci s médii postupovat tak, aby jiná osoba nemohla zneužít tyto nosiče jako zdroj informace (dle zásady „prázdného stolu“).

6.12. Nepořizovat kopie médií s osobními údaji či osobních údajů samých pro jinou než pracovní potřebu a ani to umožňovat jiným; s takovými kopiemi nakládat stejně jako s originálem. Pořizování kopií médií obsahujícími zvláštní kategorie osobních údajů je zakázáno, výjimky povoluje ředitel Domova.

6.13. Vytištěné dokumenty, obsahující osobní údaje, neprodleně po vytištění odebírat z tiskáren, kopírek nebo faxů.

6.14. Soubory, obsahující osobní údaje, adresované mimo Domov, zasílat pouze chráněné (prostřednictvím datových schránek, nebo prostřednictvím elektronické pošty minimálně v archivním souboru (např. ve formátu „zip“, „rar“ atd.) opatřeného heslem, přičemž heslo zaslat adresátovi jiným komunikačním kanálem, např. prostřednictvím SMS).

6.15. Dokumenty, obsahující zvláštní kategorie osobních údajů, zasílat pouze prostřednictvím datové schránky nebo poštou.

6.16. Osobní údaje zpracovávat a ukládat na přenosných zařízeních (např. notebooky, flash a externí disky atd.) pouze za podmínky, že je zajištěna jejich ochrana šifrováním disku tohoto zařízení.

6.17. Dodržovat další, v této příloze neuvedené, zásady fyzické, personální a administrativní bezpečnosti a bezpečnosti informačních a komunikačních technologií, stanovené dalšími platnými vnitřními předpisy Domova

6.18. V případě zjištění porušení zabezpečení osobních údajů (nebo nabytí podezření) neprodleně informovat svého nadřízeného.