1. Rozsah působnosti

Ustanovení této směrnice jsou závazná pro všechny zaměstnance Domova.

2. Odpovědnost za záměrnou a standardní ochranu osobních údajů

Za záměrnou a standardní ochranu osobních údajů Domova odpovídají vedoucí zaměstnanci v součinnosti s ROÚ.

3. Záměrná ochrana osobních údajů

Záměrná ochrana spočívá v realizaci:

a) návrhu vhodných technických a organizačních opatření stanovených před zahájením vlastního zpracování, ještě v době určování prostředků pro zpracování osobních údajů, ke kterým dává stanovisko ROÚ v součinnosti s příslušnými vedoucími zaměstnanci,

b) zavedení a udržování přiměřených technických a organizačních opatření po celou dobu trvání zpracovatelské operace založených na výsledcích analýzy informačních rizik a s přihlédnutím k různě pravděpodobným a různě závažným rizikům pro práva a svobody subjektů údajů.

4. Standardní ochrana osobních údajů

Standardní ochrana spočívá v dodržení zásady minimalizace s ohledem na zajištění

a) pouze nezbytně nutného rozsahu zpracovávaných osobních údajů pro daný účel zpracování spočívající v
   - aktualizaci záznamů o činnostech zpracování,
   - vyřazení případných „nerelevantních nebo nepřiměřených osobních údajů“[1],
   - systematické kontrolní činnosti,

b) pouze nezbytně nutné doby uchování osobních údajů pro daný účel zpracování, a to jak v listinné, tak i v elektronické podobě, spočívající v
   - aktualizaci záznamů o činnostech zpracování,
   - stanovení lhůt pro uchování osobních údajů vycházející buď ze spisového řádu a jeho lhůt, nebo
   - přiměřenosti vzhledem k účelu zpracování a systematické kontrolní činnosti,

c) dostupnosti osobních údajů pouze pro nezbytně nutný počet osob spočívající v
   - aktualizaci záznamů o činnostech zpracování,
   - stanovením pravidel pro řízení přístupu k osobním údajům,
   - stanovením pravidel pro zveřejňování, sdílení nebo předávání informací,
   - systematické kontrolní činnosti.

5. Porušení zabezpečení osobních údajů

5.1 Oprávněné osoby jsou povinny v případě zjištění porušení zabezpečení osobních údajů nebo nabytí podezření porušení zabezpečení osobních údajů (dále jen „porušení“) neprodleně informovat svého nadřízeného, který následně informuje ROÚ.

[1] Standard kvality sociální služby Ochrana osobních údajů, článek 3, odst. 1.

5.2 ROÚ na základě nahlášení tohoto zjištění v součinnosti s příslušným vedoucím zaměstnancem:

a) vyhodnotí zdroje porušení (interní, externí aj.),
b) vyhodnotí základní informace o porušení a rozhodne o klasifikaci porušení, tj. zda se jedná o bezpečnostní událost[2] nebo bezpečnostní incident[3].

5.3 Pokud je informace vyhodnocena jako bezpečnostní událost, provede pověřenec v rámci dalšího šetření následující kroky:

a) prověří v záznamech o porušení, zda se jedná o nahodilou událost nebo se jedná o událost, která se opakuje,
b) vypracuje návrh na opatření k nápravě, který předá řediteli Domova k posouzení a schválení.

5.4 Pokud je informace vyhodnocena jako bezpečnostní incident, ROÚ přizve další osoby, které jsou kompetentní pro jeho posouzení, a provedou se následující činnosti:

a) pokud je možné, provedou odpovědní zaměstnanci okamžitou nápravu (zastavení provozu, zablokování přístupových oprávnění atd.),
b) identifikace kategorie porušení:
   - porušení důvěrnosti,
   - porušení dostupnosti,
   - porušení integrity,
c) identifikace kategorií osobních údajů, u kterých došlo k porušení,
d) stanovení přibližného počtu dotčených subjektů údajů, dotčených kategorií osobních údajů a dotčených záznamů osobních údajů, u kterých došlo k porušení,
e) identifikace pravděpodobného zdroje úniku, či případného porušení,
f) popis pravděpodobných důsledků dopadů na subjekty údajů,
g) vyhodnocení rizika dopadů na práva a svobody subjektů údajů:
   - bez rizika,
   - s rizikem,
   - s vysokým rizikem.

5.5 Po vyhodnocení rizika ROÚ informuje ředitele Domova, který rozhodne o povinnosti ohlášení nebo oznámení a v případě vyhodnocení

a) rizika – zajistí ROÚ odeslání ohlášení ÚOOÚ, (bez zbytečného odkladu a pokud možno do 72 hodin od zjištění bezpečnostního incidentu),
b) vysokého rizika – zajistí pověřenec odeslání ohlášení ÚOOÚ (bez zbytečného odkladu a pokud možno do 72 hodin od zjištění bezpečnostního incidentu) a oznámení subjektům údajů (bez zbytečného odkladu).

5.6 Dále ROÚ společně s dalšími dotčenými zaměstnanci vypracuje návrh nápravných opatření a příslušní vedoucí zaměstnanci přijmou a neprodleně zrealizují prvotní možná

[2] Událost, která může způsobit narušení bezpečnosti v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.
[3] Událost, která představuje narušení bezpečnosti v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.

nápravná opatření ke snížení dopadů na práva a svobody subjektů údajů nebo k eliminaci příčiny porušení bezpečnosti osobních údajů.

5.7 ROÚ připraví a zpracuje ohlášení v souladu s čl. 33 odst. 3 písm. a) až d) nebo oznámení v souladu s čl. 34 odst. 2 GDPR, vždy podle úrovně vyhodnoceného rizika, které po schválení ředitelem Domova odešle příslušným subjektům (ohlášení ÚOOÚ, oznámení subjektům údajů).

5.8 Pokud není ohlášení ÚOOÚ učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

5.9 ROÚ v součinnosti s příslušnými vedoucími zaměstnanci po odeslání ohlášení provede:

a) další došetřování incidentu na základě návrhů uvedených v ohlášení ÚOOÚ,
b) vypracuje návrh na přijetí dalších nápravných opatření,
c) kontrolu účinnosti přijatých opatření.

5.10 ROÚ společně s dalšími dotčenými zaměstnanci zpracovává dokumentaci týkající se porušení zabezpečení osobních údajů. Dokumentace musí obsahovat

a) veškeré skutečnosti, které se týkají příslušného porušení,
b) dopady porušení,
c) přijatá nápravná opatření.

5.11 Dokumentace o porušení zabezpečení osobních údajů musí ÚOOÚ umožnit ověření souladu s GDPR.