CENTRUM SOCIÁLNÍCH SLUŽEB OSTRAVA, o.p.s.
Jahnova 12, 709 00 Ostrava-Mariánské Hory
Telefon: 599 455 121, www.css-ostrava.cz

ZÁZNAM O ČINNOSTECH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V ORGANIZACI CENTRUM SOCIÁLNÍCH SLUŽEB OSTRAVA, O.P.S.

1. Identifikace správce osobních údajů

Správce osobních údajů
Centrum sociálních služeb Ostrava, o.p.s., zastoupena ředitelem Ing. Jiřím Drastíkem
Jahnova 867/12, Ostrava – Mariánské Hory, 709 00
Datová schránka: t744u8y
Telefon: 599 455 121, email: css@css-ostrava.cz.

2. Účel zpracování

Oblasti, ve kterých dochází ke zpracování osobních údajů subjektů, v rámci sociálních služeb a služeb sociálně-právní ochrany dětí organizace, jsou:

- pobytové služby (sociální služby),
- pečovatelská služba (sociální služby),
- poradenství pro občany (sociální služby),
- sociálně aktivizační služby (sociální služby),
- rodinná poradna (sociální služby),
- náhradní rodinná péče (služby SPOD).

Jedná se o tyto procesy:
jednání se zájemcem, evidence zájemců, sociální šetření, smlouva o poskytování služby, individuální plán, dokumentace služby, řešení nouzových a havarijních situací, záznamy stížností neanonymních uživatelů, další vzdělávání, praxe a stáže, dobrovolnictví, evidence docházky, mzdové podklady, evidence darů, pořizování foto, video, audio záznamů (prezentace na webových stránkách, propagačních materiálech, přímá identifikace osob), monitoring pohybu osob v zařízení, součinnost s OSPOD, součinnost se soudy, součinnost s policií, evidence dlužníků, monitoring podpořených osob, pracovní výkaz ESF, komunikace s právními zástupci, uzavření dohody o výkonu pěstounské péče, výkon činnosti doprovázející organizace, uzavření dohody o asistovaných kontaktech, atd.

3. Popis kategorií subjektů údajů a kategorií osobních údajů

Subjekty údajů mohou být:
neanonymní klient/uživatel (výjimkou mohou být činnosti/ služby s možností anonymity klientů), zmocněnec, opatrovník, kontaktní osoba, osoba pečující, osoba blízká (partner, manžel, atd.), biologický rodič, dítě, zaměstnanec, dobrovolník, student, pracovník jiné organizace, veřejnost.

O subjektech údajů jsou v různé míře dle potřeby zpracovávány tyto kategorie osobních údajů: titul, jméno, příjmení, datum a místo narození, adresa (trvalého, přechodného bydliště, doručovací), kontaktní údaje (telefon, email), věk, obec, sociální situace, finanční situace (dluhy, příp. soudní rozhodnutí), rodinná situace, situace bydlení, vztahová situace, vyjádření lékaře o zdravotní způsobilosti, vzdělávací instituce, doporučení OSPOD, kontaktní osoba (jméno, příjmení, kontakt), dítě (jméno, příjmení, datum narození), partner, rodinný příslušník, zmocněnec, opatrovník, osoba pečující (jméno, příjmení, příp. datum narození, adresa, kontakt).

Dále jsou v minimálním rozsahu zpracovávány následující zvláštní kategorie osobních údajů: zdravotní stav, biometrické údaje, příp. sexuální život, sexuální orientace, rasový a etnický

původ, filozofické a náboženské přesvědčení, trestná činnost pouze související s výkonem činnosti/ služby.

4. Popis kategorií příjemců, kterým byly nebo budou osobní údaje zpřístupněny

Účely sběru a zpracování osobních údajů v různé míře a podle potřeby jsou:
řádné poskytování sociální služby a plnění zákona o sociálních službách a zákona o SPOD, plnění standardů kvality sociálních služeb (zde patří např. vypořádání stížností, smlouva o poskytování služby, evidence darů, smlouva o dobrovolnictví, smlouva o praxích, stážích, další vzdělávání pracovníků atd.), řešení nastalé situace podle vnitřních předpisů BOZP a PO, PR organizace, její prezentace donátorům a poděkování dárcům, zpracování a výplata mzdy, zabezpečení dodržování BOZP, oznamovací povinnost (zákon SPOD, občanský soudní řád, trestní zákoník), řádné finanční vypořádání služby (zákon o účetnictví a finanční kontrole).

Kategorie příjemců, tedy třetích osob mohou být:
donátoři (státní - obec, kraj, ministerstvo, nadační), veřejnost, dárci, inspekce kvality, inspekce práce, kontrola BOZP a PO, kontrola OPZ, OSSZ, kontrolní orgány (finanční, příspěvkový, pověřující) dobrovolnická organizace, spolupracující obce (ze smlouvy), příslušný OSPOD, ÚP ČR, soud, orgán, vybraný právní zástupce.

Osobní údaje nejsou předávány do dalších zemí v Evropské unii, mimo ni ani mezinárodním organizacím.

5. Plánovaná lhůta pro výmaz kategorií údajů

Výmaz vybraných osobních údajů bude zajištěn v souladu s platnou legislativou.
Správce plánuje zajistit výmaz údajů v období od pěti do deseti let a to podle zákona o archivnictví a spisové službě, konkrétně podle archivačního a skartačního řádu Centra sociálních služeb Ostrava, o.p.s.

6. Obecný popis procesních, organizačních a technických opatření

Procesní opatření
Procesní opatření organizace představují doporučené postupy řešení situací, vznikajících v souvislosti se zpracováním osobních údajů. V rámci interní směrnice ke zpracování osobních údajů má organizace vymezeny konkrétní postupy pro řešení následujících situací – postupy při uplatňování práv subjektů, řešení bezpečnostních incidentů a postup pravidelné aktualizace zásadních dokumentů ke zpracování osobních údajů v organizaci. Zároveň s tím jsou v dalších interních dokumentech organizace vymezeny obecná pravidla zacházení s osobními údaji v případě jejich zpracovávání v rámci vybraných činností a procesů, např. v rámci směrnic, metodických postupů, standardů kvality, atd.

Organizační opatření
Organizační opatření spočívají ve fyzickém výkonu zabezpečení osobních údajů, v rozdělení kompetencí pro oblast zabezpečení ochrany osobních údajů v organizaci, v rozdělení kompetencí a přístupů jednotlivých pracovníků k vybraným osobním údajům při jejich zpracování a jejich pravidelná kontrola a revize. Mezi základní organizační opatření konkrétně patří:

- Vymezení pracovních kompetencí pro danou pracovní pozici, seznámení pracovníka s jeho konkrétními povinnostmi při zpracování osobních údajů subjektů vzhledem k vykonávané činnosti, seznámení zaměstnance s vnitřní směrnicí k dodržování nařízení GDPR, veřejným závazkem, atd.

- Zabezpečení zpracování osobních údajů prostřednictvím povinnosti zachovávat mlčenlivost o zpracovávaných osobních údajích a přijatých opatřeních k jejich ochraně, o nichž se v souvislosti se svým zaměstnáním nebo plněním smlouvy pracovníci dozvěděli a to i po skončení svého pracovního poměru.
- Omezování přístupů k fyzickým uložištím osobních údajů pouze pro oprávněné pracovníky prostřednictvím uzamykatelných skříní, uzamykatelných kanceláří, a zabezpečení budov klíčem, elektronickým alarmem, elektronickým vrátným a u vybraných středisek čipovými kartami a kamerovým systémem.
- Dodržování politiky čistého stolu, tj. že osobní údaje jsou vždy při odchodu pracovníka z kanceláře/střediska zabezpečeny proti zneužití (osobní údaje v písemné podobě uzamčeny, osobní údaje v elektronické podobě chráněny politikou hesel).
- Vymezení správce a odpovědných osob za dodržování zásad zpracování osobních údajů podle nařízení GDPR.

Technická opatření

Technická opatření spočívají v samotném zabezpečení osobních údajů. Organizace zabezpečuje osobní údaje, zpracovávané v písemné i elektronické podobě, následujícími způsoby:

- Přidělení odpovědnosti za správu a administraci elektronických zařízení a systémů vybranému pracovníkovi - administrátorovi IT, který má spolu s ředitelem přístup do systémů, programů a aplikací k tomu určených.
- Politikou hesel, tj. zabezpečení PC, notebooků, mobilních telefonů, datové schránky, elektronických systémů a alarmů budov prostřednictvím přístupových hesel. Přístupy a hesla jsou přidělována pouze oprávněným pracovníkům v rámci výkonu vybrané pracovní pozice administrátorem, svá hesla si zaměstnanci navzájem nesdělují. Veškerá přístupová hesla a uživatelská jména jsou uložena v aplikaci, která je chráněna prostřednictvím hlavního hesla, které má u sebe pro potřeby monitoringu činnosti pracovníků uložen v zalepené obálce ředitel organizace.
- Správa a monitorování elektronických zařízení (PC, notebooků) prostřednictvím pozice administrátora IT, který má práva správce u těchto zařízení, a elektronického programu, který je schopen monitorovat a kontrolovat činnost v rámci zařízení, tedy i využívání externích datových nosičů a sledovat s jakými typy dat se pracuje. Administrátor vede evidenci externích nosičů v rámci vybraného systému.
- Mezi další technická opatření patří zabezpečení wi-fi sítě, serveru, používání antivirových programů, firewallu, práce se zašifrovanými soubory při práci s osobními údaji, nevyužívání emailové komunikace k zasílání osobních údajů až na specifické situace, kdy dochází k zašifrování zasílaných souborů, využívání sdílených uložišť mezi pracovníky organizace, spolupráce s dodavateli systémů, programů a aplikací, které se zavazují k dodržování nařízení GDPR a zajištění možnosti omezení přístupu k vybraným osobním údajům subjektu nebo jejich výmazu.
- Písemná dokumentace je zabezpečena samotným výkonem zaměstnanců, popsaným v organizačních opatřeních v rámci uzamykatelných skříní, uzamykatelných kanceláří, a zabezpečení budov klíčem, elektronickým alarmem, elektronickým vrátným a u vybraných středisek čipovými kartami a kamerovým systémem. Zároveň vedením k politice čistého stolu, popsáno výše.