



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 projektové a obchodní činnosti organizace, jsou:

- projekty (zadavateli mohou být EU, MPSV, Moravskoslezský kraj, MAS, atd.)
- komerční činnost (sociální akademie, aj.)

Jedná se o tyto procesy:

jednání se zájemcem o vstup do projektu, oslovování potenciálních klientů, zařazení klientů do projektu, přihlašování účastníků akce (se souhlasem, pro odběratele akce, akreditovaných akcí), přihlašování dětí, podpora klientů v rámci jednotlivých programů projektu, monitoring podpořených osob, zvláštní pracovní výkaz, dokumentace střediska/ projektu, pořizování foto, video a audio záznamů (prezentace na webových stránkách, propagačních materiálech, přímá identifikace osob), dobrovolnictví, evidence docházky a mzdové podklady, řešení nouzových a havarijních situací, záznamy stížností neanonymních stěžovatelů, dluhové poradenství, kopie DPP pracovníků.

3. Popis kategorií subjektů údajů a kategorií osobních údajů

Subjekty údajů mohou být:

uživatel, klient, osoba blízká (partner, manžel, atd.), dítě, zaměstnanec, dobrovolník, 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), věk, kontaktní údaje (telefon, email), údaje ke zvláštním požadavkům (strava, ubytování), informace k péči, číslo bankovního účtu, pracovní pozice, pracovní zaměření, sociální situace (sociální a zdravotní znevýhodnění, sociální dávky), zaměstnání (kvalifikace, evidence na ÚP, trestní bezúhonnost, dovednosti, praxe), bydlení (vedení domácnosti), finanční situace (příjmy a výdaje, dluhy a jejich zpracování), partner (jméno, příjmení, datum narození), děti (jméno, příjmení, věk).

Dále jsou v minimálním rozsahu zpracovávány následující zvláštní kategorie osobních údajů: zdravotní stav (zdravotní omezení) a biometrické údaje.

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

Účely sběru a zpracování osobních údajů v různé míře a podle potřeby jsou:

vykazování indikátorů projektu, prokazování výdajů projektu, zpracování ukazatelů a výstupů, prokazování uznatelnosti finančních nákladů a plnění podmínek projektu, PR organizace, prezentace donátorů, obchodní nabídky, zpracování a výplata mzdy, vypořádání stížností dle vnitřních pravidel a podle zákona, řešení daných situací dle vnitřních předpisů organizace,



BOZP a PO, zajištění podmínek pracovníků na pracovišti, doplnění personálních a finančních kapacit (dobrovolnictví), organizační a kvalitní zajištění vybrané akce, finanční vypořádání, kontrolní činnosti střediska, umožnění opakované účasti na akcích, řešení dluhů klientů.

Kategorie příjemců, tedy třetích osob mohou být:

kontrolní orgán (dotační, finanční, akreditační, BOZP a PO, OPZ, OSSZ, odběratel akce, Krajský soud, insolvenční správce), inspekce práce, inspekce kvality, dobrovolnická organizace, dárci, sponzoři, donátoři (státní, nadační).

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, technických a organizačních 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 uložitím 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.