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 oblasti řízení lidských zdrojů a produktového řízení jsou:

- personalistika
- řízení činností
- administrativa řízení

Jedná se o tyto procesy:
uzavření pracovního poměru (žádost o zaměstnání, osobní dotazník a jeho příloha, mzdový výměr a dohoda o vyplácení mzdy, pracovní profil, pracovní smlouva, příp. dohoda o pracovní činnosti, o provedení práce), nástup do zaměstnání (školení BOZP, nástupní list, lékařská prohlídka a lékařský posudek, informace o právech a povinnostech zaměstnance), změna sjednaných pracovních podmínek, jmenování/pověření vedoucího pracovníka, databáze zaměstnanců, registrace sociálních služeb (dokládání odborné způsobilosti pracovníků), pověření SPOD (dokládání odborné způsobilosti pracovníků), odborné praxe, stáže a dobrovolnictví, dohoda o používání motorového vozidla a doklad o zaučení, hodnocení zaměstnanců, ukončení pracovního vztahu, žádost o dotace, vyúčtování dotace a pověření k realizaci projektů, propagace služeb a činnosti organizace, evidence (darů, stížností, nouzových a havarijních situací), finanční plán organizace, přehledy rozpočtů, cílů, personálu služeb, příp. navazující procesy produktového a finančního řízení.

3. Popis kategorií subjektů údajů a kategorií osobních údajů

Subjekty údajů mohou být:
zaměstnanci, zájemci o zaměstnání, dobrovolníci, studenti, pracovníci jiné organizace, veřejnost, sponzoři, soukromí dárci, uživatelé/klienti.

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), stát, rodné číslo, kontaktní údaje (telefon, email), číslo bankovního účtu, nejvyšší dosažené vzdělání, kvalifikace, trestní bezúhonnost, zdravotní pojišťovna, srážky ze mzdy, důchod, peněžní ústav, výše mzdy, číslo občanského průkazu, atd.

Dále jsou v minimálním rozsahu zpracovávány následující zvláštní kategorie osobních údajů:
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:

ucházení se o pracovní pozici, uzavření a plnění pracovního vztahu, vyplácení mzdy, zadání náplně práce, zaučení se na pracovní místo, seznámení se s vnitřními předpisy, zajištění a dodržování BOZP a PO, vstupní lékařská prohlídka, prokázání zdravotní způsobilosti k výkonu práce, změna pracovní smlouvy, jmenování do funkce, hodnocení zaměstnance za uplynulý rok, ukončení pracovního poměru, ucelený přehled o zaměstnancích organizace, hlášení změn v rámci výkonu SPOD, registrace personálního zajištění sociálních služeb, práce s dobrovolníky, podpora kvalifikované sociální práce, naplňování standardů kvality, řádné zpracování stížností, podklad pro zpracování finančního plánu a vedení středisek, finanční řízení, zpracování žádosti o dotaci, rozúčtování mezd, sledování dodržování povinných parametrů krajské sítě sociálních služeb.

Kategorie příjemců, tedy třetích osob mohou být:
kontrolní orgán (dotační, finanční, akreditační, BOZP a PO), inspekce kvality, inspekce práce, vybraný lékař, registrační orgán Moravskoslezského kraje, pověřený orgán SPOD, donátoři, dárci, veřejnost.

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, případně v období třiceti až čtyřiceti pěti let, konkrétně pak 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 vymezena 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.