



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 finančního řízení a organizačního zajištění jsou:

- účetnictví
- mzdové účetnictví
- účetní administrativa

Jedná se o tyto procesy:

evidence smluv (uživatelů/klientů, s fyzickými osobami – darovací, kupní smlouvy), vedení pošty (příchozí a odchozí faktury, podklady k exekucím zaměstnanců, podklady zaměstnanců k výkonu práce), zpracování příchozí emailové pošty zájemců o služby, příchozí a odchozí pošty klientů/uživatelů, žádost o zřízení přístupu k aplikacím, předávací protokoly, telekomunikační služby (pro zaměstnance, ostatní osoby), proplacení vybraných hrazených činností organizace, pohledávky, dohody o hmotné odpovědnosti, faktury, doklady, ostatní závazky, objednávky, založení nového zaměstnance (do systému, na pojišťovnu, OSSZ), uplatnění slev na daních (např. invalidita), roční zúčtování daně, zpracování a úhrada mzdy, vyúčtování příspěvků ÚP, vyhotovení evidenčního listu důchodového pojištění, pracovní neschopnost zaměstnance, ošetřování člena rodiny, zpracování cestovního příkazu, povolení používání osobního vozidla pro služební cestu, exekuce, zabezpečení budovy pohotovostní služba zabezpečení.

3. Popis kategorií subjektů údajů a kategorií osobních údajů

Subjekty údajů mohou být:

klient, uživatel, zájemce o službu, veřejnost, zaměstnanec, rodinný příslušník, osoba blízká, dítě.

O subjektech údajů jsou v různé míře dle potřeby zpracovávány tyto kategorie osobních údajů: titul, jméno, příjmení, datum a místo narození, adresa (trvalého pobytu), rodné příjmení, rodné číslo, kontaktní údaje (telefon, email), uživatelské jméno, číslo bankovního účtu, sociální situace, údaje o pojištění, důchodu, zdravotním postižení, úvěrech, členských příspěvcích, darech, výši dluhu, výše mzdy, údaj o vyměřovacím základu za předchozí rok, údaj o započitatelném příjmu, dítě (jméno, příjmení, rodné číslo, datum narození), partner (jméno, příjmení, rodné číslo, adresa trvalého pobytu), rodinný příslušník (jméno, příjmení, datum narození adresa trvalého pobytu), majitel vozu (jméno, příjmení, rodné číslo/ datum narození).

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



realizace a sledování příspěvků na provoz a úhradu poskytnutých služeb, poskytnutí služeb, daru, koupě od fyzické osoby, přijetí/odeslání účetního dokladu (faktury), podkladu pro exekuce, podkladů zaměstnanců souvisejících s výkonem práce, přeposlání emailové zprávy na příslušnou službu/činnost organizace, přijetí/odeslání zpráv pro příslušné instituce o práci v činnosti/službách, zřízení přístupu do aplikace, zřízené za účelem žádosti o dotace v oblasti sociálních služeb a SPOD, evidence předaného majetku pro ochranu a vybavení zaměstnanců, zajištění telekomunikačních služeb vybrané společnosti a zprostředkování zajištění telefonních služeb vybrané společnosti, proplácení činností v rámci náhradní rodinné péče při výkonu SPOD, hlídání pohledávek, zajištění svěřených hodnot a věcí, úhrada proběhlé události, závazků organizace, splnění povinného vzdělávání u vybraných zaměstnanců, povinností spojených se správnou úhradou odvodů, přihlášení a odhlášení zaměstnance a úhrada jeho odvodů, snížení daňové povinnosti zaměstnance, vyúčtování zaplacené daně z příjmu zaměstnance za předchozí kalendářní rok, zpracování mzdy zaměstnance, naplnění podmínek smlouvy o vyplácení mzdového příspěvku, vyplácení mzdy a splnění podmínek smlouvy, splnění povinnosti k sociálnímu pojištění, vyplácená dávky nemocenského pojištění, umožnění využívání vlastního automobilu pro služební cesty, zajištění uhrazení pohledávky zaměstnance, zabezpečení budovy, vyplácení oprávněného výdaje činnosti organizace.

Kategorie příjemců, tedy třetích osob mohou být:

kontrolní orgán (dotační, finanční), případný adresát, odesílatel, příslušný exekutor, insolvenční správce, příslušné OSSZ, ČSSZ, OSPOD, příslušný soud, policie, místně příslušná státní správa, příslušné ministerstvo (převážně MPSV), dodavatelská telekomunikační společnost, příslušná zdravotní pojišťovna.

Osobní údaje nejsou předávány do dalších zemí Evropské unie, 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 platného zákona o archivnictví a spisové službě, a konkrétně podle archivačního a skartačního řádu Centra sociálních služeb Ostrava, o.p.s.

6. Obecný popis technických, procesních 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 směrnici 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 uložistům osobních údajů pouze pro oprávněné pracovníky prostřednictvím uzamykatelných skříní, uzamykatelných kancelářů, 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 uložist mezi pracovníky organizace, spolupráce s dodavatelem 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 kancelářů, 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.