S M Ě R N I C E K O C H R A N Ě O S O B N Í C H Ú D A J Ů dle GDPR

Základní právní normou upravující ochranu osobních údajů v naší organizaci je NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 (**G**eneral **D**ata **P**rotection **R**egulation – dále jen **GDPR, Nařízení)**, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, účinné od 25.5. 2018. Dále je to český adaptační Zákon o zpracování osobních údajů č. 110/19 Sb. a na něj navazující Zákon č. 111/19 Sb., kterým jsou v potřebných ustanoveních novelizovány jiné zákony v českém právním řádu, dotčené tímto novým Zákonem o zpracování osobních údajů, účinným od 24.4.2019. Dalšími právními normami upravujícími ve své příslušné části tuto oblast příp. vztahujícími se k ní je Zákoník práce, Zák. č. 133/00 Sb., o evidenci obyvatel, a další zákonné normy zmíněné v b. 4). Směrnice byla projednána s odborovým orgánem působícím v organizaci.

1) Účel úpravy ochrany osobních údajů při jejich zpracování v organizaci

Účelem vydání této směrnice je aplikace ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů a o volném pohybu těchto údajů, v naší úč. jednotce, tak, aby bylo dosaženo požadované ochrany údajů při jejich zpracování u:

- fyzických osob – zaměstnanců, osob ucházejících se o zaměstnání

- fyzických osob – současných či budoucích klientů

- dalších osob, za něž organizace při své činnosti získává jejich osobní údaje (např. stážistů, praktikantů, klientek vzdělávacího programu NRP atd.)

(dále jen **subjekty údajů,** definované v Zák. č. 110/19 Sb., § 3, jako fyzické osoby, k nimž se osobní údaje vztahují).

Organizace tyto údaje zpracovává, a proto je dle GDPR **zpracovatelem osobních údajů**. Směrnice stanovuje práva a povinnosti zaměstnanců a ostatních fyzických osob při veškerém zpracování osobních údajů. Ke zpracování osobních údajů jí se týkajících je nutný odpovídající právní titul, kterým může být:

a) souhlas této fyzické osoby (**„zpracování na základě souhlasu“**) – zaměstnance (ostatních fyzických osob) (viz GDPR-článek 6 odst. 1 písm. a); článek 4 odst. 11). Údaje, s jejichž zpracováním nebyl udělen souhlas, nelze zpracovávat.
b) Tento souhlas není nutný (viz GDPR-článek 6 odst. 1, písm. c, d, e, f), pokud jsou údaje zpracovávány na základě zvláštního zákona (**„zpracování ze zákona“**, resp. při výkonu veřejné moci), a to v rozsahu údajů uvedených výčtem v příslušném právním předpisu.

   V případě plnění právní povinnosti za údaje, které nejsou uvedeny výčtem v příslušném zákonu, se pak jedná o zpracování na základě souhlasu.

   Dle českého adaptačního Zák. č. 110/19 Sb., § 5, je organizace **oprávněna** zpracovávat tyto osobní údaje bez souhlasu subjektu údajů, pokud je to nezbytné pro

plnění právní povinnosti, která je naší organizaci **uložena** právním předpisem. Nebo jde o úkol prováděný naší organizací ve veřejném zájmu, při výkonu veřejné moci, kterým je naše organizace **pověřena**.

Organizace je pak povinna poskytnout ve vztahu k výše uvedenému oprávněnému zpracování osobních údajů, dle Zák. č. 110/19 Sb., § 8, subjektu údajů informace dle GDPR-článek 13, resp. článek 14 odst. 1, 2, 4. Informace jsou poskytovány formou zveřejnění způsobem umožňujícím dálkový přístup; a to v rozsahu odpovídajícím organizací obvykle prováděnému zpracování osobních údajů nebo jsou osobní údaje nezbytně nutné pro vstoupení fyzické osoby do jednání o smluvním vztahu či plnění uzavřené smlouvy se správcem (**„zpracování na základě uzavřené (obchodní) smlouvy“**), tj. subjekt údajů je smluvní stranou (viz GDPR-článek 6 odst. 1, písm. b)

c) a dále rovněž v situaci, jedná-li se o oprávněně zveřejňované údaje (**„oprávněný zájem“**) v souladu se specifickým zvláštním.

Osobní údaje, které jsou výhradně nutné pro účely zprostředkování zaměstnání, jsou uvedeny v § 23 a § 5, písm. a), bod 1., Zák. o zaměstnanosti č. 435/04 Sb. Osobní údaje se vyskytují v organizaci buď ve formě originálních písemností (či jejich kopií, fotokopií), v elektronické podobě ve formě počítačové databáze.

Subjekt údajů je o zpracování svých osobních údajů informován ihned při prvním kontaktu, při němž organizace a subjekt údajů vstupují do právního vztahu (při nástupu zaměstnance do zaměstnání a při navázání dodavatelsko-odběratelských vztahů s obchodními partnery-fyzickými osobami aj.).

Při prvotním zpracování osobních údajů – sběru/získávání – se vždy posuzuje, zda jsou skutečně všechny údaje poskytované subjektem údajů potřebné v organizaci pro jejich další zpracování, tj. zda jimi organizace musí disponovat. Dále se rovněž posuzuje, zda nejsou údaje zpracovávány nad rámec stanovený zákonem. K jednotlivým skupinám (druhům) zpracovávaných osobních údajů se pak přiřazuje časový horizont jejich zpracování/ukončení zpracování, tj. doba zpracování nezbytná pro daný účel).

2) Definice používaných pojmů a povinností z nich pro organizaci vyplývajících

- **správce osobních údajů (pro nás organizace a výkonný ředitel org.)** (viz GDPR-článek 4, odst. 7) – tím, je fyzická nebo právnická osoba, orgán veřejné moci či jiný subjekt určující účel a prostředky zpracování osobních údajů; zpracování provádí a odpovídá za něj

- **osobní údaj** (viz GDPR-článek 4, odst. 1) – jím je jakákoliv informace o identifikované či identifikovatelné fyzické osobě – **„subjektu údajů“**, jakýkoli údaj týkající se této osoby. Na základě tohoto údaje je subjekt přímo či nepřímo ztotožněn, identifikován, určen (např. jméno, příjmení, adresa, datum narození, r.č., identifikační číslo, telefon, emailová adresa). Osobní údaje jsou zpracovávány v neautomatizované podobě jako fyzická „evidence, kartotéka, úřední spis“ či automatizovaným postupem zpracováváním „datového souboru“

- **zpracovatel osobních údajů** (viz GDPR-článek 4, odst. 8) – fyzická nebo právnická osoba, orgán veřejné moci či jiný subjekt, který zpracovává osobní údaje pro správce na základě

smlouvy. Zpracovatel plní stejné nároky na ochranu osobních údajů jako správce; může zpracovávat osobní údaje po technické stránce jen na základě přesných pokynů správce

- **zpracování osobních údajů** (viz GDPR-článek 4, odst. 2) – jím je jakákoli operace správce či zpracovatele s osobními údaji, zejména shromažďování (získání za účelem jejich uložení pro další zpracování), zaznamenání, uspořádání, strukturování, ukládání na nosiče dat, přizpůsobení, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření, či jiné zpřístupnění, seřazení či zkombinování, výmaz nebo zničení. Zpracování musí být vždy účelové

- subjekt údajů (viz GDPR-článek 4, odst. 1, Zák. č. 110/19 Sb., § 3) – jím je identifikovaná či identifikovatelná fyzická osoba, ke které se osobní údaje vztahují

- informovaný souhlas - v případě, kdy je vyžadován souhlas subjektu údajů, je subjektem poskytován pro jeden či více konkrétních účelů (GDPR-článek 6, odst. 1, písm. a). Souhlasem subjektu údajů je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle formou prohlášení či jiným zjevným potvrzením svého svolení ke zpracování osobních údajů (GDPR-článek 4, odst. 11). Souhlas může dle GDPR-článek 8, poskytnout osoba starší 16 let. Českým adaptačním Zák. č. 110/19 Sb., § 7 je tato hranice k udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti (platnost on-line souhlasů) stanovena na 15 let[1].

- právo být zapomenut (právo na výmaz), (viz GDPR-článek 17) – subjekt údajů má právo vymáhat po organizaci výmaz svých údajů (např. zaměstnanec při ukončení pracovního poměru).

- právo vznést námitku (viz GDPR-článek 21) – subjekt údajů má právo v konkrétní situaci kdykoliv vznést námitku proti zpracování svých osobních údajů

- ohlašování případů porušení zabezpečení osobních údajů ÚOOÚ a subjektu údajů (viz GDPR-článek 33, 34) – organizace má povinnost do 72 hodin nahlásit ÚOOÚ porušení zabezpečení osobních údajů. Ve vyjmenovaných případech pak (viz článek 34) oznamuje organizace toto porušení i subjektu údajů; vede záznamy o „událostech“.

V souladu se Zák. č. 110/19 Sb., § 12 a s přihlédnutím k § 11 (chráněný zájem dle § 6, odst. 2), postupuje organizace odlišně oproti výše uvedenému ustanovení GDPR, tj. oznámení provede v omezeném rozsahu nebo jej odloží, pokud je to nezbytné a svým rozsahem přiměřené.

V souladu se Zák. č. 110/19 Sb., § 10, nemusí naše organizace provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením tehdy, pokud je mu tato povinnost zpracování osobních údajů stanovena zákonem („zpracování ze zákona“).

- **povinnosti, preventivní a proaktivní přístup správce, zpracovatele ve vztahu k vymahatelnosti práv subjektů údajů, pod hrozbou vysokých pokut** (viz GDPR-článek 12, 24, 83) – aby si organizace aktivně a v plném rozsahu plnila všechny své výše uvedené povinnosti, musí postupovat aktivně; v opačném případě bude sankcionována dle článku 83 *(likvidační pokuta)*. Je dodržován princip vyžadovaný GDPR. Dále je dodržován „princip

rizikovosti“, kdy na základě rostoucí rizikovosti zpracování osobních údajů jsou stupňovány i povinnosti naší organizace

- anonymní údaj – je takovým údajem, který prošel procesem **anonymizace** a u něhož nelze zjistit subjekt údajů. Zásady ochrany osobních údajů se tedy nevztahují na anonymní informace, tj. informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným. GDPR se tedy netýká zpracování těchto anonymních informací, včetně zpracování pro statistické nebo výzkumné účely (viz GDPR-recitál 26)

- pseudonymizace - osobní údaje, na něž byla uplatněna pseudonymizace a jež by mohly být přiřazeny fyzické osobě na základě dodatečných informací, by měly být považovány za informace o identifikovatelné fyzické osobě (viz GDPR-recitál 26); podléhají tedy ochraně osobních údajů dle GDPR. Přičemž pseudonymizací se rozumí takové zpracování osobních údajů, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření. A to tak, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě (viz GDPR-článek 4, odst. 5). Pseudonymizace je tedy spolu se šifrováním součástí záměrné a standardní ochrany osobních údajů.

- výjimka z povinnosti posuzování slučitelnosti účelů - v případě, že dle Zák. č. 110/19 Sb., § 6 naše organizace-správce zajišťuje „chráněný zájem“, pak není povinna posuzovat před zpracováním osobních údajů k jinému účelu, než ke kterému byly shromážděny, slučitelnost těchto účelů. Přičemž přezkoumávání slučitelnosti účelů původního a následného zpracování je v běžných případech dle GDPR-článek 6 odst. 4 a článek 5 odst. 1b) vyžadováno.

3) Zpracování zvláštních kategorií osobních údajů dle GDPR-článek 9, tj. citlivé osobní údaje

Citlivým osobním údajem/citlivým údajem (dle GDPR-článek 9; recitál 10, recitál 51-56, 75, Zák. č. 110/19 Sb., § 66 odst.6), jehož zpracování je zakázáno, jsou údaje vypovídající o rasovém, etnickém původu, politických názorech, členství v odborech, náboženském vyznání, filozofickém přesvědčení, odsouzení za trestný čin, údaje týkající se rozsudků v trestních věcech a trestných činů nebo souvisejících bezpečnostních opatření, údaje o zdravotním stavu, sex. životě a orientaci, biometrické a genetické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby.

Výjimku ze zákazu zpracování citlivých osobních údajů (dle článku 9) představují zejména tyto případy: subjekt údajů udělil výslovný souhlas se zpracováním těchto citlivých osobních údajů; zpracování je nezbytné pro účely plnění povinností naší organizace v oblasti pracovněprávní, sociálního zabezpečení; zpracování je nezbytné pro účely spisové služby, archivaci ve veřejném zájmu, či pro statistické účely.

4) Oblasti nakládání s osobními údaji v organizaci, způsob jejich zpracování

K zpracování osobních údajů dochází v organizaci našimi vlastními zaměstnanci – výkonný ředitel, vedoucí soc. služby, sociální pracovnice, poradci. Organizace zpracovává pouze přesné a pravdivé osobní údaje, které za tím účelem průběžně (v případě změn) ověřuje. Právo (a zároveň povinnost) přijít do styku a nakládat s osobními údaji je zde uvedeným zaměstnancům stanoveno v pracovní náplni, v rámci jejich pracovních úkolů určených přímo výkonným ředitelem.

Na základě podepsané „dohody o mlčenlivosti" jsou zaměstnanci přicházející při plnění svých pracovních úkolů do styku s osobními údaji povinni se vyhýbat jakémukoliv jednání, které by mohlo být považováno za neoprávněné zveřejňování osobních údajů, a to jak na pracovišti, tak i mimo něj. Osobní údaje jsou předávány pouze tam, kde je to nezbytné pro plnění pracovních povinností (tzn. např. vůči nadřízenému, spolupracovníkovi, předání osobních údajů externímu smluvnímu zpracovateli - účetní, oprávněným externím uživatelům – zdravotní pojišťovna, ÚSSZ, FÚ, ČSÚ, Úřad práce ...).

Organizace pro zajištění potřebného pracovního kontaktu na své zaměstnance uveřejňuje na svých webových stránkách a v dalších informačních materiálech na základě informovaného souhlasu zaměstnance tyto jejich údaje: příjmení, jméno, titul, funkční zařazení. Jsou tedy zveřejňovány pouze takové osobní údaje zaměstnance týkající se výhradně jeho pracovních aktivit a nedotýkající se jeho soukromého života.

a) Osobní údaje zaměstnanců (vč. uchazečů)

Účelem zpracování osobních údajů zaměstnanců je tedy plnění zákonných povinností organizace plynoucích z pracovněprávních (např. uzavření pracovní smlouvy, evidence pracovní doby), daňových, bezpečnostních a dále povinností plynoucích ze vztahů vůči ÚSSZ a zdravotním pojišťovnám, z předpisů o zaměstnanosti **(„zpracování ze zákona"**).

Zpracování osobních údajů se dále provádí z hlediska interních potřeb organizace, jimiž je zejména výběr, zvyšování kvalifikace zaměstnanců, přeřazování na jiné funkce, monitoring zaměstnanců na pracovišti.

Údaje jsou získávány přímo od dotčených zaměstnanců a to písemně (občanské průkazy – kontrola a opis dat, potvrzení o zaměstnání od předchozího zaměstnavatele, dotazníky, životopisy, žádosti o přijetí, doklady o dosaženém vzdělání a praxi, výpisy z rejstříku trestů (pouze u zaměstnanců s hmotnou odpovědností), písemná potvrzení o absolvování spec. školení, kurzů.

Veškeré osobní údaje zaměstnanců v **listinné - papírové podobě** jsou shromažďovány v osobním spisu zaměstnanců (v uzamčené kanceláři s omezeným přístupem). Nikdy nejsou ponechávány bez dozoru a mají k nim omezený přístup – na vyžádání tito zaměstnanci: (výkonný ředitel, vedoucí služby, soc. pracovnice a poradci). Údaje **v elektronické podobě** se nacházejí na počítači u mzdové účetní.

5) Povinnosti dotčených zaměstnanců a dalších osob

Touto směrnicí jsou povinni se řídit v rámci svých pracovních povinností všichni zaměstnanci organizace a rovněž tak další osoby, které jsou k organizaci v obdobném právním

vztahu (zaměstnanci na dohody, vedoucí zaměstnanci). V případě, že je nakládání s osobními údaji přeneseno na základě písemné smlouvy ke zpracovateli mimo organizaci (např. zpracování mezd, účetnictví), je tento zpracovatel rovněž povinen se řídit GDPR, adaptačním zákonem č. 110/19 Sb. a touto směrnicí. Ve smlouvě se zpracovatelem je definován rozsah, účel, doba platnosti smlouvy, zodpovědné osoby – zpracovatele. Za organizaci je kontaktní osobou p. Vejsadová a za zpracovatele – p. Zemanová.

6) Ochrana osobních údajů a její ukončení

Dle výše uvedených ustanovení je ochrana osobních údajů zabezpečena: u osobních údajů ve fyzické podobě formou jejich uzamčení oprávněnou osobou – sociální pracovnice organizace – uzamykatelná kartotéka, výkonný ředitel organizace - uzamykání kanceláře a skříní obsahujících data – spisy, složky, osobní karty aj.) a obdobně u archivovaných nosičů dat. U údajů v elektronické podobě formou přístupových hesel k jednotlivým počítačovým složkám. U údajů předávaných ústně formou jasně vymezených kompetencí a pracovních povinností určených v pracovní náplni zodpovědných osob a podvázaných „dohodami o mlčenlivosti“. Za nastavení a udržování tohoto ochranného režimu v organizaci zodpovídá výkonný ředitel organizace.

Organizace - je povinna provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje shromažďovány, anebo pokud o tuto likvidaci požádá zaměstnanec (právo na výmaz). Výjimkou jsou ale údaje, které organizace zpracovává na základě zvláštního zákona („zpracování ze zákona“). Za likvidaci, skartaci zde uložených dokumentů po projití povinné skartační lhůty dle spisového a skartačního plánu (pokud dokument nebyl vybrán k archivaci).

7) Součinnost s kontrolními orgány

Zaměstnancům organizace – pokud se dopustí přestupku proti zákonu a poruší zákaz zveřejnění osobních údajů („smlouvu o mlčenlivosti v oblasti osobních údajů“), pak v trestněprávní rovině hrozí odnětí svobody až na 8 let (trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací; neoprávněné nakládání s osobními údaji).

Dne 11.4.2024 výkonný ředitel organizace