Směrnice pro nakládání s osobními údaji

Správce osobních údajů: příspěvková organizace Města Vrchlabí, Regionální turistické informační centrum Krkonoše

1) Úvodní ustanovení

Tyto zásady upravují postup při zpracování a ochraně osobních údajů dle NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
Dalšími právními normami upravujícími ve své příslušné části tuto oblast příp. vztahujícími se k ní je Zákoník práce, Zák. č. 133/00 o evidenci obyvatel a další zákonné normy zmíněné v b. 5). Směrnice byla sestavena na základě doporučení a podkladů firmy Viavis.
Tyto zásady se vztahují na osobní údaje zpracovávané pověřenými osobami **Správce osobních údajů: Regionální turistické informační centrum Krkonoše, dále jen „RTIC“.**

2) Používané pojmy a jejich definice

Osobní údaj, zpracování osobních údajů, správce, zpracovatel a další jsou použity dle definice, či ve smyslu Obecného nařízení o ochraně osobních údajů.
- **správce osobních údajů** – tím, je subjekt určující účel a prostředky zpracování osobních údajů, zpracování provádí a odpovídá za něj
- **osobní údaj** – jím je jakákoliv informace naplňující podmínku vztahu k fyzické osobě – subjektu údajů, jakýkoli údaj týkající se této osoby. Na základě tohoto údaje je subjekt přímo či nepřímo identifikován, určen (např. jméno, příjmení, adresa, datum narození, rodné číslo, telefon, mailová adresa). Osobní údaje jsou zpracovávány v podobě „evidence“ či „datového souboru“
- **zpracovatel osobních údajů** – na základě zmocnění či pověření správcem za něj provádí zpracování osobních údajů (případně na základě zvláštního zákona)
- **zpracování osobních údajů** – jím je jakákoli operace správce či zpracovatele s osobními údaji, zejména shromažďování (získání za účelem jejich uložení pro další zpracování), ukládání na nosiče dat, uchovávání, úprava, vyhledávání, zveřejňování, likvidace
- **subjekt údajů** – jím je osoba, ke které se osobní údaje vztahují. V případě, kdy je vyžadován souhlas subjektu údajů, jde vždy o jednostranný právní úkon tohoto subjektu, jehož obsahem je svolení se zpracováním svých osobních údajů
- **uchovávání, likvidace osobních údajů** – uchováváním údajů se rozumí jejich udržování v podobě umožňující další zpracování. Likvidace pak představuje jejich fyzické zničení (např. skartovačem) či vymazání datových nosičů aj.
- **anonymní údaj** – je takovým údajem, který prošel procesem anonymizace a u něhož nelze zjistit subjekt údajů. V podmínkách organizace jde zejména o uveřejňování neadresných údajů o sumě pohledávek po splatnosti, věková struktura obyvatel v obci v určitých rozpětích (bez uvádění jmen), zápisy z obecních jednání zveřejňovaná tiskem (na úřední desce, elektronické desce, bez uvedení konkrétních osobních údajů) aj.

Pokud se v textu dále uvádí:

- "směrnice", jedná se o tuto směrnici,
- "organizace", jedná se o RTIC,
- „OÚ“, jedná se o osobní údaje
- "zaměstnanci", jedná se o osoby vykonávající závislou práci v základním pracovněprávním vztahu k RTIC (ve smyslu zákoníku práce),
- "Úřad", jedná se o Úřad pro ochranu osobních údajů,
- „počítač“, jedná se o osobní počítač nebo obdobná zařízení (notebook, tablet, smartphone apod.).

3) Účel úpravy

Účelem vydání nové směrnice je aplikace NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679. o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů u:

a) fyzických osob – zaměstnanců, osob ucházejících se o zaměstnání

b) fyzických osob – současných či budoucích obchodních partnerů

c) dalších osob, za něž organizace při své činnosti získává jejich osobní údaje (účastníci výherních soutěží pořádaných organizací aj.). Směrnice stanovuje práva a povinnosti zaměstnanců a ost. fyzických osob při veškerém zpracování (shromažďování, evidenci) osobních údajů, a to jak při ručním, tak automatizovaném zpracování. Ke zpracování osobních údajů jí se týkajících je nutný souhlas této fyzické osoby – zaměstnance (ostatních fyz. osob). Tento souhlas není nutný, pokud jsou údaje zpracovávány na základě zvláštního zákona, nebo jsou nezbytně nutné pro vstoupení fyzické osoby do jednání o smluvním vztahu či plnění uzavřené smlouvy se správcem a dále rovněž v situaci, jedná-li se o oprávněně zveřejňované údaje v souladu se zvláštním zákonem. Osobní údaje, které jsou výhradně nutné pro účely zprostředkování zaměstnání, jsou uvedeny v § 23 a § 5 a)1. Zák. o zaměstnanosti. Osobní údaje se vyskytují v organizaci buď ve formě originálních písemností (či jejich kopií), v elektronické podobě ve formě počítačové databáze a na archivních a záložných médiích (CD, FD,externí disk, ..).

4) Zvláštní kategorie osobních údajů

Pověřené osoby mohou zpracovávat zvláštní kategorie osobních údajů („citlivé osobní údaje“), tedy osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby jen, pokud subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, nebo je splněn, některý z dalších případů uvedených v odst. 2, čl. 9 Obecného nařízení o ochraně osobních údajů.

Citlivé údaje, kdy je vyžadován písemný souhlas zaměstnance, jsou zpracovávány v organizaci v těchto případech:

a) Údaje o trestní bezúhonnosti (vyžadovány u zaměstnanců s hmotnou zodpovědností)
b) Podrobné údaje o zdravotním stavu, zdravotní testy, vše nad rámec běžné vstupní zdravotní prohlídky

U přijatého zaměstnance se údaje stávají součástí jeho osobního spisu, nepřijatým uchazečům jsou poštou vráceny do 14 dnů po ukončení přijímacího řízení“. Dotazník a případné další dokumenty jsou podepsány zaměstnancem.

c) Pro provádění srážek ze mzdy a poukazování odborových příspěvků zaměstnanců - členů odborů disponuje organizace – správce údaji o případném členství svých určitých zaměstnanců v dané konkrétní odborové organizaci a má pro tento případ písemný souhlas zaměstnance s prováděnou srážkou. Organizace údaj o odborovém členství dále nezpracovává, proto se na něj nevztahuje oznamovací povinnost. Údaj je navíc částečně anonymizován, neboť v dohodě o srážkách ze mzdy je uvedeno číslo účtu a částka, bez další podrobnější identifikace protistrany.

5) Pověřené osoby

Pověřenými osobami, které jsou oprávněny zpracovávat osobní údaje, jsou:

- zaměstnanci vykonávající vedoucí pozici RTIC,
- zaměstnanci provádějící zpracování osobních údajů na základě pověření,
- zaměstnanci, kteří zabezpečují informační systémy pro zpracování osobních údajů,

  osoby, které k tomu mají oprávnění na základě uzavřené smlouvy (např. zpracování mezd, účetnictví). Ve smlouvě je definován rozsah, účel, doba platnosti smlouvy, zodpovědné osoby, technické a organizační zabezpečení ochrany os. údajů, a to jak při vzájemném předávání těchto údajů, tak při jejich zpracování u dodavatele této služby – zpracovatele.

Pověřené osoby jsou povinny v rámci plnění svých povinností vyplývajících z jejich vztahu k RTIC plnit i opatření k ochraně osobních údajů stanovená zákonem, tímto a dalšími vnitřními předpisy RTIC, zejména:

1. Zachovávat mlčenlivost o osobních údajích a přijatých technickoorganizačních opatřeních k jejich ochraně, o nichž se v souvislosti se svým zaměstnáním dozvěděly, a to i po skončení svého pracovního poměru,
2. zpracovávat osobní údaje za podmínek a v rozsahu jim stanoveném (např. v souladu s platnými přístupy do systémů pro automatizované zpracování OÚ),
3. osobní údaje shromažďovat a dále zpracovávat v rozsahu:
    a. stanoveném zvláštními zákony, resp.
    b. nezbytně nutném k naplnění stanového účelu, není-li rozsah zpracovávaných osobních údajů stanoven pro konkrétní účel zvláštním zákonem.
4. Při shromažďování osobních údajů od subjektů údajů:
    a. vyžadovat jejich souhlas se zpracováním osobních údajů (není-li zpracování osobních údajů dáno zvláštním zákonem),
    b. informovat a poučit je o jejich právech v souladu se zákonem,
    c. shromažďovat osobní údaje pouze otevřeně, tj. neshromažďovat osobní údaje skrytě nebo pod záminkou jiného účelu.
5. Při zpracování osobních údajů:
    a. zpracovávat pouze přesné osobní údaje s ohledem na účel zpracování; v případě zjištění, že zpracovávané osobní údaje nejsou přesné, zpracování zablokovat do doby jejich opravy nebo doplnění,
    b. zpracovávat osobní údaje pouze k účelům, k nimž byly shromážděny (k jinému účelu pouze v případě, že fyzická osoba, ke které se osobní údaje vztahují, dala k tomu předem souhlas),
    c. nesdružovat osobní údaje získané k rozdílným účelům,
    d. uchovávat osobní údaje pouze po dobu, která je nezbytně nutná k účelu zpracování,
    e. ukládat nosiče obsahující osobní údaje, a to v listinné i elektronické podobě, na určená místa. Při práci s nosiči postupovat tak, aby jiná osoba nemohla zneužít tyto nosiče jako zdroj informace (dle zásad „čistého stolu“ a „prázdné obrazovky“).
6. Nepořizovat kopie nosičů s osobními údaji či osobních údajů samých pro jinou než pracovní potřebu a ani to umožňovat jiným; s takovými kopiemi nakládat stejně jako s originálem.
7. Neumožnit zpracování osobních údajů jiné osobě, která není pro konkrétní účel zpracování pověřenou osobou.
8. Osobní údaje v listinné i elektronické formě, předávat nebo poskytovat:
    a. pouze pověřeným a oprávněným osobám,
    b. stanoví-li tak zvláštní zákon nebo v souladu s platnou smlouvou,
    c. pouze předepsaným způsobem.
9. V případě zjištění porušení bezpečnostních opatření k zajištění ochrany osobních údajů informovat bez zbytečného odkladu vedoucího zaměstnance.

6) Vedoucí zaměstnanec (ředitel/zástupce ředitele RTIC)

1. Zajišťuje popis a jeho aktualizaci zpracování osobních údajů na formuláři, jehož vzor je uveden v příloze B této směrnice, nejméně 1x ročně,

2. zajišťuje aktuálnost evidence zpracování osobních údajů,
3. pověřuje zaměstnance organizace zpracováním osobních údajů a stanoví jeho podmínky a rozsah, a to písemně (vzor pověření je v příloze A),
4. vede evidenci pověření zpracováním osobních údajů,
5. zajišťuje kontrolu plnění povinností vyplývajících z ustanovení z této směrnice v mezích své působnosti,
6. zabezpečuje získání souhlasu subjektu údajů, není-li, zpracování možné bez tohoto souhlasu,
7. zabezpečuje splnění povinností ve vztahu ke zpracovatelům OÚ,
8. zabezpečuje likvidaci písemností a záznamových médií,
9. zabezpečuje podmínky pro řádné plnění povinností uložených touto směrnicí.

7) Bezpečnost informací

a) Zabezpečení písemností a záznamových médií obsahujících osobní údaje

Písemnosti a digitální záznamová média, které obsahují osobní údaje, musí být zabezpečeny v uzamčených skříních, popř. na jiných místech, kde je možno zajistit jejich ochranu.
To platí i pro kopie písemností obsahující osobní údaje.
Za plnění povinností stanovených ve výše uvedených odstavcích tohoto článku jsou odpovědny pověřené osoby, ředitel, účetní.

b) Zabezpečení dat obsahujících osobní údaje v osobních počítačích

Data obsahující osobní údaje, která jsou uložena v osobních počítačích, musí být zabezpečena před volným přístupem neoprávněných osob, před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů.
Za plnění povinností stanovených v prvním odstavci tohoto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění, ředitel, účetní. Spolupracují při tom se Správcem IT.

c) Likvidace písemností, záznamových médií a dat obsahujících osobní údaje

Za likvidaci písemností a záznamových médií v rámci příslušné organizační jednotky v oblasti personální zodpovídá ředitel, za likvidaci v oblasti mzdové zodpovídá účetní. Za likvidaci dat v rámci informačních systémů pro zpracování osobních údajů zodpovídá Správce IT. Likvidace písemností je v souladu se Směrnicí k archivaci.

8) Informační povinnost

Dle nařízení je organizaci dána povinnost informovat subjekt údajů (zaměstnance, obchodního partnera – fyzickou osobu) o tom, že jsou údaje o něm správcem shromažďovány, zpracovávány, v jakém rozsahu a pro jaký účel, kdo bude údaje zpracovávat a komu mohou být zpřístupněny. Dále je subjekt informován o svém právu přístupu ke svým osobním údajům a možnosti jejich opravy, příp. podání vysvětlení ze strany správce. V zákonem stanovených případech je subjekt údajů o výše uvedených skutečnostech informován při prvním kontaktu, při němž správce a subjekt údajů vstupují do právního vztahu (při nástupu zaměstnance do zaměstnání a při navázání dodavatelskoodběratelských vztahů s obchodními partnery – fyzickými osobami).

9) Oznamovací povinnost

Režim nařízení EP o ochraně osobních údajů fyzických osob se na organizaci vztahuje z toho titulu, že je zpracovatelem osobních údajů (správcem) za své zaměstnance a dále v dalších případech. Povinnost registrovat se na Úřadu pro ochranu osobních údajů, ale z tohoto titulu nemá, neboť zpracování osobních údajů provádí pouze ze své povinnosti vyplývající ze zvláštních zákonů. Pokud tedy organizace provádí zpracování osobních údajů na základě zvláštních zákonů (zejména Zák. práce, zák. o soc. zabezpečení, zák. o zdr. pojištění, zák. o zaměstnanosti, zák. o služebním poměru...) a pro plnění povinností stanovených těmito zvláštními zákony, pak oznamovací povinnost nevzniká. Pokud jsou nad rámec splnění výše uvedeného účelu shromažďovány některé nadbytečné údaje, jde o porušení zákona. Oznamovací povinnost (povinnost registrovat se) má organizace v případě, že zpracovává osobní údaje nad rámec daný těmito zákony, např. paušálně vyžaduje výpis z rejstříku trestů od všech

zaměstnanců (narozdíl od pokladní, kde je to považováno za nutnost), dále pořádá reklamní soutěže se zpracováním dat účastníků, jmenovitě zveřejňuje seznam dlužníků organizace apod. Smyslem oznamovací povinnosti je zajistit výkon dozoru ze strany ÚOOÚ.

10) Způsob zpracování osobních údajů v organizaci

a) Osobní údaje zaměstnanců (vč. uchazečů)

Účelem shromažďování a zpracování osobních údajů zaměstnanců tedy je plnění zákonných povinností organizace plynoucích z pracovněprávních, daňových, bezpečnostních, hygienických předpisů a dále povinností plynoucích ze vztahů vůči OSSZ a zdravotním pojišťovnám, z předpisů o zaměstnanosti. Zpracování osobních údajů se dále provádí z hlediska interních potřeb organizace, jimiž je zejména výběr, zvyšování kvalifikace zaměstnanců, přeřazování na jiné funkce, program péče o zaměstnance a jejich rodinné příslušníky, vč. finanční pomoci. Další selektivní úkoly pro správce vyplývají z uzavření kolektivní smlouvy s odbory. U uchazečů o zaměstnání jde o výběr vhodných osob pro obsazení konkrétních volných pracovních míst.

Údaje jsou získávány přímo od dotčených zaměstnanců a to písemně (občanské průkazy – kontrola a opis dat, potvrzení o zaměstnání od předchozího zaměstnavatele, pracovní posudky, dotazníky, žádosti, životopisy, žádosti o přijetí, zdravotní prohlídky, doklady o dosaženém vzdělání a praxi, výpisy z rejstříku trestů, písemná potvrzení o absolvování speciálních školení, kurzů), nebo ústně (nahlašování změn, doplnění údajů při rozšíření požadavků plynoucích ze zvláštních zákonů). Ústní údaje jsou pověřeným zaměstnancem podchyceny a převedeny do písemné podoby.

Veškeré osobní údaje zaměstnanců v papírové podobě jsou shromažďovány v osobním spisu zaměstnanců v personálním útvaru (uložené v uzamčené skříni). Údaje v elektronické podobě se nacházejí na počítači u účetní a u ředitele. Data jsou archivovány v jeho kanceláři v zajištěném počítači a na CD v uzavřené skříni (po uplynutí 12 měsíců jsou nosiče správcem sítě fyzicky zničeny). Fyzicky jsou elektronická data umístěna na samostatném serveru (v samostatném adresáři), přístup k nim je možný pouze pro oprávněné osoby za pomoci přístupového hesla. Oprávněnou osobou za údaje zaměstnanců je účetní a ředitel/zástupce ředitele.

b) Osobní údaje fyzických osob v rámci dodavatelskoodběratelských vztahů

Účelem shromažďování údajů v této oblasti je výběr vhodných obchodních partnerů pro uzavření obchodních smluv k zajištění plnění úkolů organizace. Údaje jsou získávány formou odpovědí na inzeráty správce, prostřednictvím výběrových řízení na dodavatele, předkládáním nabídek odběratelům, jsou to rovněž údaje z veřejných databází, z tisku a dalších zdrojů. Samotnými doklady obsahujícími osobní údaje pak jsou živnostenské listy, nabídky, návrhy smluv, obchodní smlouvy, výpisy z rejstříku a dalších evidencí.

Obdobně jako u zaměstnanců jsou osobní údaje chráněny v oblasti dodavatelskoodběratelských vztahů, kdy k údajům v elektronické podobě je přístup prostřednictvím hesla oprávněné osoby, údaje v papírové podobě (smlouvy s obchodními partnery – fyzickými osobami) jsou v uzavřených skříních s omezeným přístupem.

Veškeré elektronické údaje jsou před napadením zvenčí chráněny firewallem, antivirovou ochranou a jsou vytvářeny bezpečnostní kopie.

Ke styku s osobními údaji dochází rovněž při rozdělování došlé pošty a rovněž při nakládání s osobními údaji v elektronické podobě správcem počítačové sítě. Všechny tyto osoby jsou rovněž vázány mlčenlivostí a jsou povinny při plnění svých povinností zabránit jakémukoli úniku osobních údajů, s kterými přicházejí do styku.

11) Závěrečná ustanovení

a) Kontrola dodržování ustanovení směrnice

Vedoucí zaměstnanec RTIC zajistí kontrolu plnění povinností vyplývajících z ustanovení Směrnice pro nakládání s osobními údaji v mezích své působnosti.

Vedoucí zaměstnanec RTIC zajistí, aby byli s dokumentem Směrnice pro nakládání s osobními údaji seznámeni všichni zaměstnanci RTIC.

b) Součinnost s kontrolními orgány

Zaměstnanci organizace – pokud poruší „smlouvu o mlčenlivosti v oblasti osobních údajů“, mohou být pokutováni dle zákona až do výše Kč 100 000,-. Organizaci pak může být udělena pokuta za porušení jejích povinností až Kč 10 mil. Pro ochranu svých zákonných práv se naopak zaměstnanci mohou obracet přímo na ÚOOÚ s žádostí o zajištění nápravy, pokud organizace sdělila neoprávněně jinému jeho osobní údaje.

c) Revize směrnice

Revize Směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky.

Za zpracování, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá ředitel/zástupce ředitele – vedoucí zaměstnanec organizace.

d) Účinnost směrnice

Dokument Směrnice pro nakládání s osobními údaji nabývá účinnosti a platnosti dnem vydání.

Dne 21. 5. 2018

Zpracovala: Karla Svatá, DiS. zástupce ředitele RTIC Krkonoše

Revize směrnice, dne 9. 8. 2024

…….

Bc. Klára Hančová

ředitelka RTIC Krkonoše