Vnitřní předpis stanovující pravidla pro zpracování OÚ v organizaci

Obchodní název:	**Institut vzdělávání SOKRATES, s.r.o.**
Sídlo:	**Na Hradbách 2632/18, Moravská Ostrava, 702 00 Ostrava**
Provozovna:	**Pekařská 407/18, Staré Brno, 602 00 Brno**
IČO:	**25883500**
Statutární zástupce:	**Mgr. Pavel Petr, Ph.D., LL. M.** **Prof. JUDr. Ing. Igor Kotlán, Ph.D.**
Osoba zodpovědná za ochranu osobních údajů:	**Mgr. Pavel Petr, Ph.D., LL. M.**

1. Úvodní ustanovení

Tento předpis stanoví vnitřní pravidla pro technická a organizační opatření k nakládání s osobními údaji fyzických osob (dále jen OÚ) v nadepsané organizaci, aby byla v souladu s platnou legislativou a aby bylo v maximální možné míře (přiměřené účelu zpracování, riziku incidentů, předmětu činnosti organizace a jejím ekonomickým možnostem) zabráněno úniku, ztrátě nebo zneužití osobních údajů.

Protože má organizace počet zaměstnanců nižší než 250, nemusí by podle platné legislativy vést záznamy o činnostech zpracování. Záznamy o činnostech zpracování však vyhotovuje dobrovolně, což vede k lepší orientaci ve zpracování osobních údajů a při výkonu práv subjektu údajů. Záznamy o činnostech jsou pak přílohou této směrnice.

2. Výklad vybraných souvisejících pojmů

Pro účely této směrnice se rozumí:

a) „**osobními údaji**“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

b) „**zpracováním**“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

c) „**pseudonymizací**“ zpracování osobních údajů tak, 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, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

d) „**správcem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;

e) „**zpracovatelem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
f) „**souhlasem**“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

3. Přehled zpracovávaných OÚ a agend zpracování

V organizaci dochází ke zpracovávání níže uvedených základních OÚ:

- audiovizuální záznam,
- skupinové fotografie,
- individuální fotografie,
- jméno a příjmení, titul zobrazené osoby,
- datum, čas a místo pořízení audiovizuálního záznamu nebo fotografie,
- jméno a příjmení, titul,
- rodné příjmení,
- datum narození,
- rodné číslo,
- adresa trvalého pobytu,
- adresa přechodného pobytu,
- korespondenční adresa,
- státní příslušnost,
- místo narození,
- číslo a platnost občanského průkazu,
- číslo a platnost řidičského průkazu,
- rodinný stav,
- nejvyšší dosažené vzdělání,
- telefonní číslo,
- číslo bankovního účtu,
- e-mailová adresa,
- rodná čísla rodinných příslušníků,
- zdravotní pojišťovna,
- dokumentace z pracovně – lékařských prohlídek a posouzení zdravotní způsobilosti zaměstnanců k vykonávané práci,
- informace o probíhajících exekucích zaměstnanců a uchazečů o zaměstnání,
- identifikace přiděleného přístupového prostředku,
- datum a čas využití přiděleného přístupového prostředku,
- pracovní zařazení,
- pracoviště,
- osobní číslo,
- vztah zástupce k subjektu údajů,
- dodavatelem uvedená adresa,
- dodavatelem uvedený obchodní název,
- odběratelem uvedená adresa,
- odběratelem uvedený obchodní název,
- IČO,
- DIČ,
- identifikace soukromého vozidla zaměstnance použitého k pracovní cestě,

- navštívená místa v rámci pracovních cest,
- datum a čas využití komunikačního kanálu,
- obchodní název,
- vztah subjektu údajů ke správci osobních údajů,
- výše pohledávky.

V organizaci dochází ke zpracovávání níže uvedených zvláštních (citlivých) OÚ:

- informace o kategoriích zdravotního postižení
  - OZZ
  - Částečný invalidní důchod (1. a 2. stupeň invalidity)
  - Plný invalidní důchod (3. stupeň invalidity)
- informace o pracovních úrazech zaměstnanců
  - datum a čas úrazu
  - místo úrazu
  - vykonávaná činnost při vzniku úrazu
  - zraněná část těla
  - popis úrazového děje
  - příčina úrazu
- zdravotní omezení s ohledem na typ vykonávané práce
- informace o opatrovnictví z důvodů duševního onemocnění, mentálního postižení, degenerativního onemocnění nebo těžkého tělesného či smyslového postižení

V organizaci dochází ke zpracovávání OÚ v níže uvedených agendách:

1. Kamerový systém,
2. Personalistika,
3. Mzdy,
4. Účetní doklady obsahující osobní údaje,
5. Zálohy dat interních systémů a správa webových stránek,
6. Evidence odběratelů,
7. BOZP,
8. Audiovizuální záznamy a fotografie,
9. Žádosti subjektů údajů.

4. Zásady a forma zpracování OÚ

Aspekty zpracování OÚ v organizaci s ohledem na minimalizaci zásahu do soukromí fyzických osob:

- data jsou zpracovávána jen k účelově vymezeným důvodům a organizačními a technickými prostředky je zamezeno jejich použití k jiným účelům;
- jsou zpracovávány jen osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu zpracování;
- jsou zpracovávány jen osobní údaje přesné z hlediska účelu zpracování a je zajištěna jejich aktualizace;
- osobní údaje jsou uchovávány pouze po nezbytnou dobu s ohledem na účel zpracování;
- osobní údaje jsou zpracovávány transparentně a je zabezpečena informační povinnost a dodržování práv subjektů údajů.

V organizaci jsou OÚ zpracovávány výhradně na základě platné legislativy nebo na základě souhlasu subjektů údajů. Formy důvodů zpracování osobních údajů jsou:

- právní povinnost,
- plnění smlouvy,
- oprávněný zájem správce,
- souhlas fyzické osoby (subjektu údajů), resp. jejího opatrovníka nebo zmocněnce.

Formy uchovávání OÚ jsou:

- OÚ v listinné podobě,
- OÚ v elektronické podobě.

5. Ochrana OÚ v organizaci

Fyzická ochrana OÚ v organizaci je zajištěna bezpečnostními dveřmi s bezpečností vložkou, přístup do těchto prostor mají jen oprávněné osoby mající klíč.

Prostory organizace jsou chráněny kamerovým systémem, vzhledem k tomu, že organizace je v nájmu, zpracování záznamů (OÚ) z kamerového systému provádí nájemce, se kterým se sepsána smlouva.

Osobní údaje v listinné podobě jsou uloženy ve skříních, přístup k nim mají jen oprávněné osoby. Skartace listinných OÚ probíhá v souladu se zákonnými archivačními lhůtami, případně jsou lhůty stanoveny v individuálních souhlasech, blíže viz vnitřní dokument Archivační lhůty.

Osobní údaje v elektronické podobě jsou uloženy v lokálním počítači v sídle společnosti. Přístup k těmto datům mají oprávněné osoby, jejichž přístup je zabezpečen heslem k uživatelskému účtu. Záloha dat je prováděna min. 1x měsíčně, a to formou záloh na externím datovém úložišti, které uloženo v prostorách organizace. Výmaz dat probíhá stejně jako u listinných OÚ, a to v souladu se zákonnými archivačními lhůtami, případně jsou lhůty stanoveny v individuálních souhlasech, blíže viz vnitřní dokument Archivační lhůty.

6. Proces zpracování OÚ

OÚ jsou v organizaci zpracovávány výhradně oprávněnými osobami z řad vlastních zaměstnanců nebo oprávněnými subjekty (externí zpracovatelé osobních údajů). U vlastních zaměstnanců je ochrana osobních údajů zajištěna vnitřními předpisy organizace a také písemným závazkem povinné mlčenlivosti. U externích zpracovatelů osobních údajů je ochrana osobních údajů zajištěna zodpovědným výběrem těchto subjektů (subjekty „GDPR compliant“) a písemným závazkem zpracovatele k ochraně zpracovávaných OÚ ve smlouvě o poskytování takových služeb či dodatku ke smlouvě. Ochrana OÚ u jejich příjemců je dána většinou právní povinností, případně zajištěna odpovídající smlouvou.

Před zahájením každého nového zpracování OÚ provádí organizace vždy základní analýzu rizik zpracování těchto údajů s ohledem na práva subjektů údajů a posuzuje, zda stávající zavedená pravidla ochrany OÚ v organizaci jsou dostatečná k eliminaci hrozících rizik a nové zpracování osobních údajů zahájí jen v případě, že nastavená pravidla vyhovují. Pokud organizace zjistí, že aktuálně nastavená pravidla nestačí, provede podrobnější analýzu a rozšíří organizační a technická opatření tak, aby zabezpečení bylo adekvátní pravděpodobným rizikům, a teprve pak nové zpracování OÚ zahájí.

Pokud organizace na základě provedené podrobnější analýzy a posouzení provedených opatření zjistí, že ani při vynaložení odpovídajícího rozšířeného úsilí nemůže riziko neoprávněného nebo protiprávního přístupu vyloučit (vysoké reziduální riziko), bude

konzultovat vhodný způsob zabezpečení a ochrany s Úřadem na ochranu osobních údajů (dále v textu jen ÚOOÚ) = tzv. předchozí konzultace. Teprve po zavedení dozorovým úřadem doporučených opatření zahájí zpracování osobních údajů.

Předávání OÚ třetím stranám se realizuje:

- v České republice,
- do zemí EU a EHP,
- do ostatních zemí.

Incidenty zabezpečení OÚ hlásí **správce** dozorovému úřadu ÚOOÚ bez zbytečného odkladu (pokud možno nejpozději do 72 hodin od okamžiku, kdy se o události dozvěděl), ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Jakmile **zpracovatel** zjistí porušení zabezpečení OÚ, ohlásí je bez zbytečného odkladu správci.

Ohlášení incidentu dozorovému úřadu musí obsahovat:

a) popis povahy daného případu porušení zabezpečení OÚ včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů OÚ;
b) jméno a kontaktní údaje osoby zodpovědné za ochranu OÚ nebo jiného kontaktního místa, které může poskytnout bližší informace;
c) popis pravděpodobných důsledků porušení zabezpečení OÚ;
d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení OÚ, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Správce dokumentuje veškeré případy porušení zabezpečení OÚ, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

Pokud je pravděpodobné, že určitý případ porušení zabezpečení OÚ bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu i **subjektu / subjektům údajů**.

7. Postup pro poskytování informací o zpracování OÚ subjektům údajů v rámci informační povinnosti správce

Pokyny subjektům údajů, které se týkají poskytování informací o zpracování OÚ, jsou organizací zveřejňovány a v případě potřeby aktualizovány prostřednictvím vlastních webových stránek nebo prostřednictvím vývěsní desky v objektu sídla organizace, případně prostřednictvím obojího.

Druhy podání jsou:

- žádost o informace o zpracovávaných OÚ,
- žádost o opravu zpracovávaných OÚ,
- žádost o výmaz zpracovávaných OÚ,
- žádost o předání zpracovávaných OÚ třetí straně,
- námitka proti zpracovávání OÚ.

Forma podání žádosti je buď osobní, nebo písemná (poštou, případně elektronicky). Adresou pro doručení podání je sídlo společnosti, provozovna, případně kontaktní emailová adresa.

Protože jde o OÚ, je nutné vždy ověřit totožnost žadatele. Způsob ověření totožnosti se liší v závislosti na formě podání žádostí:

a) při osobním podání je žadatel ověřen podle platného dokladu totožnosti:
   - občan České republiky prokazuje svou totožnost občanským průkazem,
   - občan členské země Evropské unie prokazuje svou totožnost občanským průkazem vydaným danou členskou zemí nebo cestovním pasem,
   - občan jiné země prokazuje svou totožnost cestovním pasem,

b) při písemném podání doručeném poštou musí být podpis žadatele na žádosti úředně ověřen,

c) při podání prostřednictvím elektronické pošty musí být dokument podepsán kvalifikovaným elektronickým podpisem.

Termín pro poskytnutí odpovědi na žádost je 1 měsíce ode dne podání žádosti, v případě složitějších případů je správce oprávněn rozhodnout o prodloužení lhůty až na 3 měsíce ode dne podání žádosti, v takovém případě pak o prodloužení lhůty informuje žadatele, a to do 1 měsíce ode dne podání žádosti.

U každého podání je individuálně posuzováno, zda se vzhledem k předchozím žádostem v daném případě nejedná o nedůvodné, nepřiměřené nebo šikanózní podání. V případě, že je vyhodnoceno podání jako nedůvodné, nepřiměřené, nebo šikanózní, může být individuálně rozhodnuto o zpoplatnění poskytnutí informace o zpracovávaných OÚ ve výši částky odpovídající administrativním nákladům na zpracování a předání nebo odeslání odpovědi, případně o odmítnutí poskytnout informace o zpracovávaných OÚ.

8. Závěrečné ustanovení

Tento vnitřní předpis bude průběžně revidován, doplňován a aktualizován na základě novelizace dotčené legislativy a dalších skutečností majících vliv na jeho obsah.

Tento vnitřní předpis byl schválen statutárním orgánem organizace. Nabývá účinnosti dne 25. května 2018.

V OSTRAVĚ, dne 24. 05. 2018

Institut vzdělávání
SOKRATES, s.r.o.
Na Hradbách 18, 702 00 Ostrava
IČ 25883500

razítko organizace, podpis statutárního zástupce