

# SMĚRNICE PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

## I.

### Úvodní ustanovení

#### 1. Základní informace

1.1. Tato směrnice upravuje technická a organizační opatření společnosti:

**SERAPA s.r.o.**, IČO: 28381475, se sídlem Mikuláše z Husi 623/7, Nusle (Praha 4), 140 00 Praha, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. C 137535/MSPH (dále „**Společnost**“),

sloužící k zajištění ochrany osobních údajů, a za tímto účelem stanovuje povinnosti zaměstnanců v oblasti ochrany osobních údajů, zásady nezbytné pro zajištění ochrany osobních údajů a správnému nakládání s nimi, jejich zpracování a předávání.

1.2. Tato směrnice pracuje s následujícími pojmy:

- i. „**Osobní údaj**“ - jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě, Společnost doplňuje, že na zákazníky/odběratele Společnosti, kteří jsou právnické osoby, se ochrana GDPR nevztahuje;
- ii. „**Zpracování**“ - jakákoliv manipulace s osobními údaji, ať už prováděné manuálně či prostřednictvím automatizovaných postupů, převážně, ale nejen jejich shromažďování, zaznamenávání, uspořádání, strukturování, ukládání, přizpůsobování, pozměňování, vyhledávání, nahlížení, použití, zpřístupnění třetím osobám, šíření, kopírování, seřazení či jiné organizování, omezení, vymazání nebo zničení;
- iii. „**Subjekt**“ - identifikovaná či identifikovatelná fyzická osoba;
- iv. „**Zpracovatel**“ - fyzická či právnická osoba která zpracovává osobní údaje pro Společnost. Smlouva mezi Společností a Zpracovatelem musí splňovat požadavky stanovené právní úpravou a Zpracovatel je povinen poskytnout jemu svěřeným osobním údajům ochranu alespoň v rozsahu určeném touto směrnicí;
- v. „**Oprávněná osoba**“ nebo „**Odpovědná osoba**“ – Společností určena osoba, která je odpovědná za ochranu osobních údajů ve Společnosti;
- vi. „**Správce**“ – Správcem se rozumí Společnost.

#### 2. Zásady zpracování osobních údajů

2.1. Společnost zpracovává Osobní údaje:

- i. pouze pro určité, výslovně vyjádřené, legitimní důvody, jejichž seznam je veřejně dostupný na webových stránkách Společnosti a přiložen k této směrnici;
- ii. pouze v míře a rozsahu, jaký je nutný k naplnění jasně určeného účelu jejich zpracování, včetně zhodnocení jednotlivých rizik;
- iii. způsobem, který zajistí jejich náležité zabezpečení před neoprávněným či protiprávním zpracováním, jakožto i před náhodnou ztrátou, zničením či poškozením;
- iv. v plné informovanosti jednotlivých Subjektů, transparentně s důrazem na jejich ochranu, včetně stanovení jasně definovaného účelu ke zpracování, který není v rozporu s příslušnou právní úpravou.

2.2. Společnost prostřednictvím Odpovědné osoby zajistí:

- i. přístup k Osobním údajům pouze takovým osobám, které ho potřebují k plnění svých smluvních nebo zákonných povinností a které zachovávají stejnou či vyšší ochranu Osobních údajů než Společnost, zejména svým zaměstnancům či Zpracovatelům, a to pouze v takové míře, jaká je nezbytná pro plnění jejich povinností;

- ii. Subjektům, jejichž Osobní údaje zpracovává, jednotlivá jejich práva a jejich výkon, zejména poskytnutí informace o zpracování Osobních údajů Společností;
  - iii. přehled všech Zpracovatelů, kterým Osobní údaje poskytuje, daný přehled je k dispozici rovněž k nahlédnutí u Odpovědné osoby, v pravidelně aktualizované podobě.
- 2.3. Společnost zpracovává osobní údaje ve svém sídle a provozovně.
- 2.4. Společnost Osobní údaje nepředává neoprávněným zpracovatelům, třetím stranám, u kterých neexistuje právní titul pro legitimní zpracování Společností zpracovávaných osobních údajů, či mimo území členských států Evropské unie.
- 3. Základní povinnosti zaměstnanců Společnosti při zpracování Osobních údajů**
- 3.1. Zaměstnanci Společnosti jsou povinni dodržovat pravidla a postupy stanovené touto směrnicí, a to zejména:
- i. zpracovávat Osobní údaje pouze v míře nutné k plnění jejich pracovních povinností, či dle pokynu nadřízeného zaměstnance;
  - ii. zachovávat mlčenlivost o všech Osobních údajích;
  - iii. Osobní údaje nijak nešířit, nekopírovat, nevynášet z pracoviště ani jinak nezneužívat a dále rovněž nezpřístupnit jakkoliv Osobní údaje nepovolaným třetím osobám;
  - iv. dbát na přesnost zpracovávaných Osobních údajů a jejich zabezpečení;
  - v. využívat Osobní údaje pouze v souladu s platnými právními předpisy;
  - vi. neprodleně oznámit Společnosti, resp. odpovědné osobě, jakékoliv narušení ochrany Společností zpracovávaných Osobních údajů, jakmile takové narušení nastane, nebo jakmile se o něm dozví;
  - vii. poskytnout veškerou potřebnou součinnost pro zajištění ochrany Osobních údajů, informovat odpovědnou osobu určenou spravovat agendu ochrany Osobních údajů o skutečnostech, které zjistili a které mohou ohrozit ochranu Osobních údajů a v případě potřeby provést neodkladná opatření v zájmu zamezení neoprávněného nakládání s Osobními údaji;
  - viii. absolvovat pravidelná školení v oblasti ochrany Osobních údajů pořádané Společností.
- 3.2. Společnost určila Odpovědnou osobu pro ochranu Osobních údajů ve Společnosti. Oprávněná osoba odpovídá za dodržování a vymáhání pravidel pro ochranu Osobních údajů stanovených touto směrnicí, za aktualizaci této směrnice v případě, že dojde ke změně rozsahu zpracovávaných Osobních údajů, ke změně pravidel a zásad ochrany Osobních údajů nebo ke změně příslušné legislativy. Konkrétní osoba vykonávající agendu Odpovědné osoby je uvedena v sídle Společnosti a provozovně.

## II.

### Kategorizace osobních údajů

#### 4. Základní vymezení

- 4.1. Společnost dle provedené analýzy zpracování Osobních údajů vyhodnotila a zpracovala jednotlivé účely pro zpracovávání Osobních údajů. Jednotlivé konkrétní účely, jakož jejich název, jejich konkrétní vymezení, podrobný popis, určení Subjektů, důvod zpracování, podkladů pro prokázání zpracovávání daných Osobních údajů, včetně konkrétních Osobních údajů a lhůt pro jejich uchování jsou přehledně zpracovány v příloze k této směrnicí s označením „*Tabulka účelů*“.
- 4.2. Účely jsou vždy kategorizovány dle následujících základních skupin:

- i. „zaměstnanci“ – v této skupině byly identifikovány účely, které vycházejí z pracovněprávního vztahu či s ním bezprostředně souvisejí, Osobní údaje jsou zpracovávány zejména z důvodů plnění povinností z pracovních smluv, v rámci plnění zákonných povinností (z příslušných právních předpisů upravujících daňové povinnosti zaměstnanců, jejich sociální a zdravotní pojištění), a z důvodu oprávněného zájmu např. ochrany Společnosti;
- ii. „uchazeči o zaměstnání“ – Osobní údaje uchazečů o zaměstnání jsou zpracovávány na základě oprávněného zájmu nebo jejich výslovného souhlasu, a to za účelem rozhodnutí o (ne)přijetí zájemce o zaměstnání do pracovněprávního poměru, ev. jeho evidence v případě budoucího zájmu Společnosti;
- iii. „dodavatelé“ – v této skupině jsou především Osobní údaje týkající se dodavatelů externích služeb, popř. účetních, právních či daňových poradců, tyto Osobní údaje jsou zpracovávány především z důvodů plnění povinností ze smlouvy s dodavatelem a z důvodů plnění zákonných povinností (z příslušných právních předpisů upravujících daňové povinnosti Společnosti);
- iv. „odběratelé“ – do této skupiny spadají především zákazníci, případně další odběratelé Společnosti, hlavním důvodem zpracování Osobních údajů v této skupině je plnění povinností ze smlouvy, případně oprávněný zájem Společnosti;
- v. „věrnostní program“ – ten zahrnuje zvláštní služby poskytované Společností zákazníkům na základě jimi vyplněné přihlášky do věrnostního programu, a tedy Osobní údaje, které zákazník za tímto účelem poskytne;
- vi. „marketing“
  - a. Odběratelský – tato skupina obsahuje Osobní údaje získané od odběratelů a potenciálních odběratelů Společnosti, a to za účelem propagace Společnosti a jejich produktů prostřednictvím elektronických, tištěných i telefonních marketingových kampaní, důvodem zpracování jsou souhlasy se zpracováním Osobních údajů pro účely marketingu Společnosti od Subjektů, ale i oprávněný zájem jedná-li se o stávající zákazníky,
  - b. Zaměstnanecký – do této skupiny patří Osobní údaje zaměstnanců Společnosti, včetně znázornění jejich podoby v podobě fotografie či videa, které byly získány pro účely propagace Společnosti a jejich produktů prostřednictvím elektronických, případně tištěných, propagačních materiálů, důvodem zpracování jsou souhlasy se zpracováním Osobních údajů pro účely propagace Společnosti od jejich zaměstnanců.
- vii. „cookies“ – samostatnou skupinu tvoří Osobní údaje získané od návštěvníků webových stránek Společnosti v podobě takzvaných cookies souborů, tyto údaje slouží především k personalizaci a zjednodušení používání webových stránek konkrétním uživatelem (dříve vyplněné údaje, automatické přihlášení apod.), důvodem jejich zpracování je souhlas Subjektu; cookies se dělí na funkční (zprostředkovávající základní funkčnost stránky), analytické (umožňující sběrem anonymních statistik Společnosti lépe pochopit své (potenciální) odběratele a stránky tak neustále vylepšovat) a marketingové (shromažďující informace pro lepší přizpůsobení reklamy zájmům odběratelů),
- viii. „archivace dat“ – tato skupina obsahuje Osobní údaje, které je Společnost povinna archivovat na základě zákonných povinností vyplývajících z konkrétních právních předpisů,
- ix. „vymáhání nároků“ – do této skupiny spadají Osobní údaje Subjektů, za kterými má Společnost pohledávku či proti nimž může Společnost v budoucnu uplatnit nárok (zejm. na základě zákona, smluv, protiprávních jednání), důvodem zpracování je oprávněný zájem Společnosti,
- x. „vyřizování žádostí“ – kdy jsou na základě oprávněného nároku zpracovávány Osobní údaje za účelem vedení evidence žádostí subjektů údajů a jejich vyřizování

zejména prostřednictvím e-mailové komunikace či formuláře na webových stránkách Společnosti.

## **5. Změny účelů**

- 5.1. Oprávněná osoba může zavedené účely, jejich popis a jiné doplňující informace o zpracování Osobních údajů jednostranně měnit či upravovat a definovat nové účely.
- 5.2. V případě změny či úpravy dosavadního účelu je Oprávněná osoba povinna nejpozději do pěti (5) dnů od zavedení příslušné změny informovat Subjekt, jehož údaje zpracovává a všechny zaměstnance. Je-li změna zásadní a podléhá-li dané zpracování souhlasu se zpracováním Osobních údajů, nelze Osobní údaje zpracovávat, a to až do doby případného udělení nového souhlasu či souhlasu se změnou od příslušného Subjektu.
- 5.3. Při definování nového účelu je Oprávněná osoba bez zbytečného odkladu, nejpozději však do pěti (5) dnů od příslušného stanovení nového účelu, povinna uvědomit o tomto všechny zaměstnance, případně jednotlivé Subjekty vyplývá-li taková změna z právních předpisů.
- 5.4. Oprávněná osoba je povinna udržovat seznam účelů zpracování osobních údajů v aktuální podobě tak, aby co nejlépe odpovídal stavu zpracovávání Osobních údajů ve Společnosti.

## **III.**

### **„Cesta Osobních údajů ve Společnosti“ – činnosti zpracovávání**

## **6. Získání osobních údajů**

- 6.1. Osobní údaje Společnost získává následujícími způsoby:
  - i. osobním kontaktem se Subjektem;
  - ii. elektronicky – e-mailem, prostřednictvím webového formuláře Společnosti či sociální sítě Facebook;
  - iii. telefonicky;
  - iv. v listinné podobě – korespondenčně či předáním listinných podkladů.

## **7. Prvotní uložení Osobních údajů a kontrola oprávněnosti zpracování Osobních údajů Společností**

- 7.1. Při získání Osobního údaje provádí oprávněná osoba nebo jí pověřený zaměstnanec kontrolu, zda je Společnost oprávněna dle jednotlivých účelů zpracovávat dané Osobní údaje. Tato kontrola spočívá v prověření zda:
  - i. je Společnost oprávněna zpracovávat Osobní údaje poskytnuté Subjektem k danému účelu;
  - ii. jsou Osobní údaje poskytovány k tomu oprávněnou osobou (tj. především Subjektem či zákonným zástupcem Subjektu);
  - iii. je možno oprávněnost zpracování Osobních údajů Společností prokázat a zda jsou veškeré potřebné podklady pro daný účel zpracování od Subjektu poskytnuty.
- 7.2. V případě, že je na základě proběhlé kontroly zpracování Osobního údaje v souladu s nastavenými postupy a mírou ochrany Osobních údajů ve Společnosti dle této směrnice a Informačního memoranda, provede zaměstnanec prvotní uložení, a to:
  - i. v případě Osobních údajů získaných elektronickou cestou uloží dané Osobní údaje do interního systému, neproběhlo-li již uložení automaticky dle propojení systému s příslušným webovým formulářem;
  - ii. v případě poskytnutí Osobních údajů v listinné podobě či osobním kontaktem nebo telefonicky uloží zaměstnanec tyto údaje do interního systému ručně a poskytnuté listinné podklady či hmotné nosiče Osobních údajů (případně listinné kopie v případě, že je hmotný nosič navrácen Subjektu) uloží na zabezpečené místo,

tj. do uzamykatelné skříně v sídle či provozovně Společnosti, která je k tomu určena (dále „**Úschovna**“).

7.3. Společnost pro uchování a správu Osobních údajů v elektronické podobě používá Wordpress, který má minimálně následující parametry:

- i. obsahuje klasifikaci jednotlivých Osobních údajů, a to alespoň dle kategorií:
  - a. účelu zpracování Osobních údajů (tj. marketing, aj.);
  - b. typů osobních údajů (tj. jméno, příjmení, telefonní číslo, či e-mail aj.);
  - c. právního titulu zpracování (tj. na základě souhlasu se zpracováním osobních údajů, či na základě plnění ze smlouvy aj.);
  - d. podkladů pro zpracování (tj. jaký podklad je nutné uchovávat, aby pro případ kontroly bylo doložitelné, že Osobní údaj Společnost zpracovává v souladu s GDPR), případně dalších.
- ii. umožňuje třídění Osobních údajů tak, aby např. jeden Zpracovatel měl přístup pouze k omezenému okruhu Osobních údajů, nikoliv ke všem Osobním údajům;
- iii. umožňuje zřízení přístupového účtu do systému pro každou individuální osobu, na základě zabezpečeného přístupu (např. heslo) tak, aby do interního systému nemohla nahlédnout, či se přihlásit jakákoliv neoprávněná osoba;
- iv. umožňuje nastavení oprávnění u jednotlivých osobních účtů tak, aby pouze jedna osoba měla přístup ke všem osobním údajům a další osoby měly přístup pouze k určitým skupinám / souhrnům Osobních údajů, a to v nezbytném rozsahu (např. ke svým podřízeným);
- v. umožňuje vyhledávat osobní údaje dle osoby a tyto následně (i) měnit, (ii) mazat, (iii) archivovat, (iv) označit jako „převedené na jiného správce osobních údajů“.
- vi. umožňuje nastavení povinné změny přístupových údajů, zejména hesla přístupových účtů, v pravidelném období;
- vii. v případě změny, úpravy či zásahu do Osobních údajů umožňuje zjistit, která osoba tuto změnu provedla, či dané Osobní údaje z interního systému zkopírovala či do nich nahlédla;
- viii. umožňuje omezení možnosti kopírování dat, či jejich exportování ze systému (a to i pouze pro jednu osobu / přístupový účet).

7.4. Správcem interního systému je ředitel obchodu, který zajišťuje údržbu interního systému a aktualizaci jeho zabezpečení, jakož i zřizování a rušení přístupových účtů k systému dle pokynů oprávněné osoby.

## **8. Zpracovávání osobních údajů Společností**

8.1. Společnost po prvotním uložení Osobních údajů zpracovává Osobní údaje pouze k předem definovaným účelům.

8.2. Dokumenty zachycující Osobní údaje v listinné podobě či na jiném hmotném nosiči zejména:

- i. pracovní smlouvy se zaměstnanci včetně dodatků;
- ii. smlouvy o spolupráci s dodavateli včetně dodatků;
- iii. smlouvy o zpracování osobních údajů;
- iv. smlouvy s externími účetní, daňovým či jiným poradcem;
- v. smlouvy o poskytování služeb odběratelům;
- vi. ostatní smlouvy;
- vii. listinné souhlasy se zpracováním Osobních údajů;
- viii. daňové doklady obsahující Osobní údaje;
- ix. záznamy o úrazu;

- x. karta zaměstnance;
- xi. záznam o existenci exekuce/insolvence zaměstnance;

jsou po prvotním uložení Osobních údajů a kontrole uschovány **v uzamčené skříni** v prostorách Společnosti (dále „**Úschovna**“). Klíče od této úschovny má k dispozici pouze Oprávněná osoba. Jakákoliv manipulace s těmito dokumenty musí probíhat za přítomnosti Oprávněné osoby nebo jí pověřenou osobou, dané dokumenty není možno kopírovat, měnit, ničit ani vynášet mimo prostory Společnosti. Tyto dokumenty nesmí být nikdy ponechány mimo Úschovnu bez dohledu Oprávněné osoby, nebo osoby jí pověřené. S těmito dokumenty je možno manipulovat pouze s ohledem na naplnění předem určených účelů zpracovávání osobních údajů, a to zejména pro plnění smluvních povinností, či zákonných povinností Společnosti, či prokázání skutečností před příslušnými orgány veřejné moci. Po odpadnutí důvodu jejich uschování a uplynutí archivační lhůty zajistí Oprávněná osoba skartaci. Důvody, včetně lhůt aj. jsou uvedeny v příloze k této směrnici.

Za ochranu Osobních údajů uvedených v listinné podobě a jejich zneprůstřednění, tj. zajištění uzamčené skříni, odpovídá Oprávněná osoba.

8.3. Osobní údaje získané pomocí elektronických prostředků, zejména elektronická korespondence (e-mail, vyplněné formuláře z webových stránek Společnosti) jsou:

- i. automatizovaným procesem evidovány v informačním systému Společnosti, nebo
- ii. manuálním způsobem zaneseny Oprávněnou osobou nebo jí pověřenou osobou z e-mailového serveru Společnosti do informačního systému či k tomu určené evidence, včetně případného uložení e-mailové komunikace dokládající způsob získání Osobního údaje;

kdy zabezpečení informačního systému Společnosti a e-mailového serveru Společnosti sestává z individuálních přístupových účtů v informačním systému Společnosti, každý takový účet se svým vlastním přístupovým heslem, jehož změna bude Společností vyžadována nejméně jednou za šest (6) měsíců.

Rozsah Osobních údajů dostupných skrze každý účet bude odpovídat osobním údajům, které daný uživatel, tj. Oprávněná osoba, jí pověřená osoba, zpracovatel nezbytně potřebují pro plnění svých pracovních či smluvních povinností.

Odpovědná osoba má výhradní přístup ke všem Osobním údajům v informačním systému a je odpovědná za jejich ochranu.

8.4. Osobní údaje předané Společnosti prostřednictvím telefonického hovoru jsou evidovány příslušným zaměstnancem nebo zpracovatelem a jsou manuálně vloženy do informačního systému.

8.5. Součástí evidence získaných osobních údajů Subjektů určených ke zpracování, ať už z jakéhokoli titulu, je zanesení informace o metodě získání, a případný odkaz na důkazní materiál ve smyslu dokumentu legitimizujícího zpracování daných osobních údajů Společností, konkrétně se jedná o písemný formulář s udělením souhlasu, smlouvu se Společností, elektronický formulář o poskytnutí souhlasu, informace o získání osobních údajů prostřednictvím telefonického hovoru, příslušný e-mail aj.

## 9. Zpracovávání Osobních údajů zpracovateli

9.1. Společnost spolupracuje s externími subjekty, které mají omezený přístup ke konkrétní sadě Osobních údajů. Oprávněná osoba nebo jí pověřená osoba je povinna zkontrolovat, případně uzavřít, smlouvu o zpracování osobních údajů.

9.2. Postup před poskytnutím Osobního údaje: Poskytuje-li Společnost Osobní údaje třetím osobám za účelem zpracování, je jakýkoliv zaměstnanec či Oprávněná osoba povinna zajistit, aby před poskytnutím Osobního údaje bylo:

- i. ověřeno, zda taková třetí osoba má pravidla pro nakládání s Osobními údaji a má nastavenou stejnou či vyšší ochranu Osobních údajů než ve Společnosti;

- ii. prokazatelně doloženo, že zpracovatel je seznámen s pravidly a postupy dle této směrnice a nastavenou ochranu Osobních údajů ve Společnosti minimálně v rozsahu Informačního memoranda;
- iii. smluvně zakotveno na základě smlouvy o zpracování mezi Společností a Zpracovatelem, že Zpracovatel bude dodržovat pod hrozbou smluvní pokuty povinnosti plynoucí mu z právních předpisů o ochraně Osobních údajů, jakož i postupy Společnosti, včetně poskytnutí součinnosti při případné kontrole ze strany dozorových orgánů (Úřad pro ochranu osobních údajů) a povinnosti poskytnout veškeré podklady pro prokázání dodržování jednotlivých postupů na ochranu Osobních údajů;

nejsou-li splněny výše uvedené základní podmínky, Společnost neposkytne zpracovateli žádný osobní údaj a zaměstnanec je tedy povinen tuto skutečnost sdělit Oprávněné osobě.

Oprávněná osoba následně zjistí příčiny nesplnění výše uvedených podmínek a zhodnotí míru rizika ve vztahu k citlivosti Osobního údaje a Subjektu a ve vztahu k oprávněnému zájmu Společnosti na předání takového Osobního údaje Zpracovateli. Je-li riziko minimální, tj. zejména nemůže dojít k zneužití Osobních údajů, tyto jsou zpracovávány ve velmi malém rozsahu, provede oprávněná osoba o tomto zhodnocení záznam a může Osobní údaje zpracovateli poskytnout, v opačném případě je povinna předání Osobních údajů třetí osobě odmítnout.

- 9.3. Kontrola Zpracovatele: Oprávněná osoba je povinna jedenkrát za rok, či vícekrát (i) dle potřeby, (ii) v případě zpracování většího množství Osobních údajů či citlivých Osobních údajů nebo (iii) rovněž v případě podezření o nedodržování pravidel na ochranu Osobních údajů zpracovatelem, provést kontrolu zpracování Osobních údajů u zpracovatele, jakož i si vyžádat od Zpracovatele doložení, že dané postupy jsou z jeho strany dodržovány. Nesplňuje-li Zpracovatel ochranu Osobních údajů minimálně na stejné úrovni jako Společnost, je Společnost povinna ho vyzvat k nápravě, nestane-li se tak, Odpovědná osoba vypoví příslušnou smlouvu, zajistí znepřístupnění jakýchkoliv Osobních údajů a písemně zašle Zpracovateli žádost o výmaz veškerých jemu poskytnutých Osobních údajů.
- 9.4. Účel: Společnost spolupracuje s externí účetní, daňovými a jinými poradci, kdy těmto nedochází k předání či jinému zpřístupnění Osobních údajů s výjimkou nezbytných údajů o zaměstnancích Společnosti za účelem plnění zákonem stanovených povinností nebo Osobních údajů jiných Subjektů v rámci zpracování příslušných smluvních či předmluvních povinností.
- 9.5. Seznam všech Zpracovatelů způsobilých zpracovávat osobní údaje je dostupný k nahlédnutí u Oprávněné osoby, včetně rozsahu, v jakém mají k osobním údajům přístup, dále uveden v záznamu o zpracování osobních údajů.

## **10. Zabezpečení Osobních údajů a výkon práv subjektů**

- 10.1. Oprávněná osoba zajistí, že:
  - i. uzamykatelná skříň (Úschovna) bude plně pod jejím dohledem, kdy v době její nepřítomnosti bude vždy uzamčena;
  - ii. informační systém bude splňovat minimální požadavky uvedené v této směrnici.
- 10.2. Oprávněná osoba je povinna do tří (3) pracovních dnů po obdržení požadavku na uplatnění práva Subjektu Osobních údajů takový požadavek:
  - i. je-li úplný a oprávněný vyřídit, zejména v případě žádosti o poskytnutí informací týkající se rozsahu zpracovávaných osobních údajů nebo v případě žádosti o výmaz Osobních údajů z databází Společnosti;
  - ii. je-li úplný ale neoprávněný, informovat žadatele, že danému požadavku nebude vyhověno, včetně uvedení důvodu (např. není možné ověřit totožnost žadatele, dané informace nejsou zpracovávány, a tedy nelze je vymazat aj.);
  - iii. je-li neúplný, informovat žadatele, že daný požadavek je neúplný a nelze mu vyhovět, včetně informace o úplnosti požadavku.

- 10.3. Další práva Subjektů ve vztahu k jejich osobním údajům, které Společnost zpracovává, jsou k nalezení v Informačním memorandu, dostupném na webových stránkách Společnosti, u věrnostního programu v sekci po přihlášení.

## **11. Uchovávání, skartace, obecná skartační lhůta**

- 11.1. Osobní údaje jsou uchovávány v listinné podobě v Úschovně nebo v informačním systému Společnosti.
- 11.2. Osobní údaje obsažené v jakékoli formě, zpracovávané na základě uděleného souhlasu, budou uchovávány po dobu maximálně 5 let, po jejímž uplynutí dojde k vymazání všech elektronických dokumentů z informačního systému a e-mailového serveru Společnosti, a zničení všech písemných dokumentů, ve kterých jsou osobní údaje obsaženy, není-li v příloze této směrnice uvedeno jinak.
- 11.3. Obecná lhůta pro skartaci či výmaz Osobních údajů činí 10 let, s výjimkou takových lhůt, které jsou vyžadovány příslušnými právními předpisy.
- 11.4. Po uplynutí doby oprávněného uchovávání Osobních údajů na základě Subjektem poskytnutého souhlasu, smluvního plnění nebo lhůty určené závazným právním předpisem, provede Společnost jejich výmaz.

## **IV.**

### **Osobní spis zaměstnance**

## **12. Obsah osobního spisu zaměstnance**

- 12.1. Osobní spis zaměstnance obsahuje všechny dokumenty týkající se Zaměstnance, které vzniknou či mohou vzniknout v průběhu trvání pracovněprávního vztahu. Jedná se zejména o následující dokumenty:
- Dotazník uchazeče o zaměstnání,
  - Pracovní smlouva, dohoda o provedení práce nebo dohoda o provedení pracovní činnosti,
  - Mzdový výměr,
  - Pracovní náplň a její změny,
  - Doklad o seznámení zaměstnance s vnitřními předpisy a pracovním řádem,
  - Doklady o absolvovaných školeních,
  - Evidence pracovní doby v rozsahu,
  - Evidence nepřítomnosti v práci,
  - Evidence pracovní neschopnosti,
  - Evidence čerpání dovolené,
  - Evidence přestávek v práci a bezpečnostních přestávek podle zvláštních právních předpisů,
  - Dohoda o rozvázání pracovního poměru,
  - Výpověď z pracovního poměru,
  - Okamžité zrušení pracovního poměru,
  - Zrušení pracovního poměru ve zkušební době,
  - a veškeré další dokumenty, které vzniknou v souvislosti s výkonem práce Zaměstnance po dobu trvání pracovněprávního vztahu.
- 12.2. Osobní spis zaměstnance je zpracováván, uchováván, archivován a skartován v souladu s touto Směrnicí, a to zejména s články č. 8 – 11 této směrnice.



## V.

### Rizika

#### 13. Eliminace rizik zpracování Osobních údajů

13.1. Všichni Zaměstnanci a Zpracovatelé mají povinnost absolvovat Společností organizované školení zaměřené na ochranu Osobních údajů a jejich zpracování, a to pravidelně, alespoň jednou ročně. U nových Zaměstnanců a Zpracovatelů pak proběhne speciální školení v zacházení s osobními údaji při vzniku příslušného vztahu se Společností.

Školení a jeho rozsah zajistí Oprávněná osoba.

13.2. Alespoň jednou ročně Oprávněná osoba zajistí zátěžový test elektronických ochranných opatření, tedy zabezpečení informačního systému, e-mailového serveru a webových stránek Společnosti. Tento zátěžový test spočívá zejména ve vyzkoušení:

- i. zajištění uzamčení Úschovny;
- ii. přihlášení do informačního systému náhodnými přihlašovacími údaji;
- iii. přihlášení do informačního systému přístupovými údaji s omezeným přístupem a kontrolou, že taková osoba má přístup pouze k předpokládaným Osobním údajům;
- iv. zkouška propojení webových formulářů, včetně prokliků na webových stránkách Společnosti;
- v. další kroky, dle technických možností informačního systému.

13.3. Společnost provedla zhodnocení rizik ve vztahu k osobním údajům a dospěla k závěru, že v souladu s GDPR není třeba jmenovat zvláštního tzv. compliance officera ke správě nakládání s Osobními údaji.

#### 14. Úřad pro ochranu osobních údajů – hlášení rizik

14.1. V případě, že dojde k porušení zabezpečení Osobních údajů, tj. porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných Osobních údajů, je Oprávněná osoba povinna bez zbytečného odkladu uvědomit příslušný dozorující úřad (Úřad pro ochranu osobních údajů), a to nejpozději do 72h poté, co se Společnost o porušení zabezpečení dozvěděla ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

14.2. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

14.3. Ohlášení porušení zabezpečení Osobních údajů musí obsahovat alespoň:

- i. popis povahy daného případu porušení zabezpečení Osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených Subjektů a přibližného množství dotčených záznamů Osobních údajů;
- ii. jméno a kontaktní údaje Oprávněné osoby, příp. pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
- iii. popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
- iv. popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

## VI.

### Závěr

#### 15. Závěrečná ustanovení

15.1. Tato směrnice je závazná od 16/06/2024.

15.2. Společnost má právo kdykoliv tuto směrnici měnit či doplňovat.

*Příloha:*

- ***Přehled účelů***
- ***Přehled zpracovatelů***
- ***Informační memorandum***
- ***Vzor souhlasu se zpracováním osobních údajů***