INTERNÍ SMĚRNICE

OCHRANA A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

společnosti UNIFRAX s.r.o.

ze dne 24. 5. 2018

(dále jen ***Směrnice)***

I. Úvodní ustanovení

1. Společnost UNIFRAX s.r.o. se sídlem Ruská 311, Dubí - Pozorka, 417 03 Dubí, IČO: 274 53 529, zapsaná v obchodním rejstříku vedeném Krajským soudem v Ústí nad Labem, spisová značka C 24589 (***Společnost***).
2. Společnost je správcem osobních údajů. Směrnice upravuje technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s platnou a účinnou legislativou v oblasti ochrany osobních údajů, zejména nikoliv však výlučně, zákonem č. 110/2019, o ochraně osobních údajů, ve znění pozdějších předpisů a Nařízením 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 - ***GDPR***) (***Předpisy na ochranu osobních údajů***), s cílem zajištění zpracování osobních údajů v souladu s touto legislativou a principy, na kterých je vystavěná.
3. Směrnice je závazná pro všechny zaměstnance Společnosti (***Zaměstnanec***) a osoby, které na základě smluvního vztahu mají Společností povolený přístup k osobním údajům.
4. Veškeré pojmy, pravidla a zásady, které jsou uvedené v této Směrnici, ale nejsou dále podrobněji specifikovány či ty, které nejsou specifikovány, se řídí a jsou vykládány podle a v souvislosti s Předpisy na ochranu osobních údajů.

II. Definice a výklad pojmů

Pro účely této Směrnice se rozumí:

1. ***automatizovaným zpracováním*** zejména:
    1. ukládání informací na nosiče dat;
    2. provádění logických nebo aritmetických operací s těmito daty, zejména jejich změna, výmaz, vyhledávání nebo rozšiřování uskutečňované zcela nebo zčásti pomocí automatizovaných postupů; a
    3. provádění archivace informací jejich uložením na archivační paměťová média a v případě potřeby obnovení informací z archivních médií;
2. ***ICT*** informační a telekomunikační technologie;
3. ***manuálním zpracováním*** jakékoliv zpracování s výjimkou zpracování automatizovaného (např. listinná podoba, kartotéky, spisy);
4. ***oprávněnou osobou***
    1. Zaměstnanec, který v rámci plnění povinností plynoucích mu z pracovní náplně má přístup k osobním údajům a dále je zpracovává; a
    2. osoba, která na základě smluvního vztahu se Společností má povolený přístup k osobním údajům;
5. ***osobním údajem*** jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě (***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;
6. ***příjemcem*** každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje pro potřeby výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci nebo v případech veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů či významného hospodářského a finančního zájmu České republiky nebo Evropské unie;
7. ***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;

8. ***správcem*** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování;
9. ***ÚOOÚ*** znamená Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, PSČ 170 00, Praha 7, webové stránky www.uoou.cz;
10. ***zpracováním*** osobních údajů 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;
11. ***zpracovatelem*** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává (nahlíží do nich, kopíruje je, spravuje, ukládá atd.) osobní údaje pro správce.

III. Úkony před započetím zpracování osobních údajů

1. Před započetím zpracování osobních údajů je povinen:
    1. správce vypracovat záznamy o činnostech zpracování; a
    2. zpracovatel vypracovat záznamy o všech kategoriích činností zpracování prováděných pro správce.
2. Pro každé zpracování osobních údajů musí být stanoven účel (důvody) zpracování. Účely zpracování osobních údajů v jednotlivých agendách vychází ze zvláštních zákonů nebo jsou osobní údaje zpracovávány na základě rozhodnutí správce.
3. Ke každému účelu zpracování musí být přiřazen právní titul; právními tituly pro zpracování jsou:
    1. souhlas subjektu údajů;
    2. plnění smlouvy;
    3. plnění právní povinnosti Společnosti;
    4. zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů;
    5. splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci; a
    6. oprávněný zájem Společnosti.
4. Není-li zpracování osobních údajů nezbytné pro některý z titulů uvedených v bodu 3. výše, zajistí Společnost/zpracovatel před zpracováním osobních údajů souhlas subjektu údajů se zpracováním osobních údajů a tento souhlas v listinné podobě (včetně podmínek, za kterých byl udělen) uchovává po celou dobu zpracování osobních údajů tohoto subjektu.
5. Souhlasy se archivují v osobních složkách (zaměstnanci a uchazeči) na personálním oddělení a BOZP oddělení (návštěvy).

IV. Informační povinnost

1. Při shromažďovaní osobních údajů přímo od subjektu údajů musí být subjekt údajů, k němuž se osobní údaje vztahují, informován o skutečnostech požadovaných Předpisy na ochranu osobních údajů nejpozději v okamžiku získávání jeho osobních údajů.
2. Tuto informační povinnost plní oprávněné osoby shromažďující osobní údaje od subjektů údajů, a to formou okamžitého informování osoby.

V. Informační memorandum – zpracování osobních údajů Zaměstnanců

2. Osobní údaje zaměstnanců v rozsahu stanoveném zvláštními právními předpisy či pro účely výkonu práv a plnění povinností vyplývajících ze zvláštního právního předpisu zaměstnavatel zpracovává pro účely plnění svých povinností stanovených zejména zákoníkem práce a souvisejícími právními předpisy i jinými právními předpisy, zejména v oblasti daní a sociálního zabezpečení.
3. Veškeré písemné dokumenty obsahující osobní údaje zaměstnance, včetně písemného souhlasu, budou založeny do osobní složky daného zaměstnance a uchovávány v

uzamykatelných skříňkách v určených prostorách, případně musí být ochrana Osobních údajů zajištěna jiným způsobem.

4. Pro zajištění správnosti a přesnosti osobních údajů zaměstnanců jsou uvedení zaměstnanci povinni bez zbytečného odkladu oznámit personálnímu oddělení zaměstnavatele jakékoli změny své osobní situace či jakýchkoli údajů zpracovávaných zaměstnavatelem v souvislosti s daným zaměstnancem.
5. Odpovědnost za správu, evidenci, archivaci a výmaz osobních údajů nesou pověření zaměstnanci personálního oddělení. Pověření zaměstnanci jsou oprávněni nahlížet do složky Zaměstnance a zpracovávat jeho osobní údaje pouze v souvislosti s popisem své pracovní činnosti a přidělenými pracovními úkoly. Nahlížet do osobní složky daného zaměstnance jsou oprávněni rovněž vedoucí zaměstnanci, kteří jsou nadřízenými příslušného zaměstnance, a sami daní zaměstnanci.

VI. Zpracování Osobních údajů uchazečů o zaměstnání

1. Před vznikem pracovního poměru či obdobného vztahu mohou osobní údaje uchazečů o zaměstnání shromažďovat a zpracovávat pouze zaměstnanci personálního oddělení a pověření vedoucí zaměstnanci, a to pouze pro účely zjištění, zda je uchazeč vhodný pro práci na příslušné pozici.
2. Osobní údaje uchazečů o zaměstnání jsou obvykle získávány poštou a e-mailem či na osobních schůzkách na základě předložených dokumentů a získaných informací.
3. Osobní údaje poskytnuté uchazeči o zaměstnání, s nimiž nebyl uzavřen pracovní poměr či obdobný vztah, je nutné uchazečům vrátit či bez zbytečného odkladu zlikvidovat.
4. Vybrané osobní údaje lze uchovávat nejdéle po dobu 3 let za účelem kontaktování příslušného uchazeče, pokud by se uvolnila vhodná nová pozice, přičemž takové uchovávání Osobních údajů vyžaduje souhlas uchazeče o zaměstnání.
5. Odpovědnost za správu, evidenci, archivaci a výmaz osobních údajů uchazečů o zaměstnání nesou pověření zaměstnanci personálního oddělení. Pověření zaměstnanci jsou oprávněni nahlížet do složky uchazeče o zaměstnání a zpracovávat jeho osobní údaje pouze v souvislosti s popisem své pracovní činnosti a přidělenými pracovními úkoly.

VII. Vyřizování žádostí subjektů údajů

1. **Základní zásady vyřizování žádosti**
    1. Společnost přijímá žádosti subjektů údajů v elektronické podobě (zaslané e-mailem) nebo v listinné podobě (zaslané v písemné podobě na adresu sídla Společnosti). V případě, že se subjekt údajů obrátí na Společnost se žádostí ve věci výkonu svých práv v ústní formě telefonicky nebo osobně, příslušný Zaměstnanec subjekt údajů informuje o možnosti zformulovat svoji žádost elektronicky; v případě, že subjekt trvá na vyřízení žádosti telefonicky nebo ústně, žádost bude vyřízena tímto způsobem a evidovaná do informačního systému Společnosti.
    2. Žádosti mohou být Společnosti zaslané i jí určeným zpracovatelem, odpovědnost za vyřízení takových žádostí má však vždy Společnost.
    3. Společnost bude nakládat s přijatou žádostí dle postupu níže v případě, že:
        a. se žádost týká osobních údajů a/nebo jejich zpracování; nebo
        b. v žádosti se uvádí požadavek na výkon práv subjektu údajů dle Předpisů na ochranu osobních údajů; nebo
        c. se v žádostí uvádí, že je spojena s Předpisy na ochranu osobních údajů.

2. **Postup při vyřizování žádosti subjektu údajů**

1. Ověření identity subjektu údajů – aby bylo zajištěno jednání s přímo dotčenou osobou (i v případě, že je žádost podaná zmocněncem subjektu údajů), musí být v rámci vyřizování žádosti subjektů údajů ověřená identita subjektů údajů.
2. Vyjasnění žádosti a jejího předmětu – v případě, že ze žádosti podané subjektem údajů není zřejmé, čeho se subjekt údajů dožaduje, nebo jsou v žádosti obsažené chybné informace, jejichž správné znění je nevyhnutné pro její vyřízení, bude subjekt údajů vyzván k upřesnění své žádosti.
3. Posouzení žádosti – v rámci posuzování žádosti subjektu údajů Společnost vyhodnotí, zda má subjekt údajů právo na výkon práva, kterého se v žádosti dožaduje a zda se na situaci neuplatní výjimka, která by tento výkon znemožňovala
4. Žádost subjektů údajů bude vyřízena následujícím způsobem:
    a. Zamítnutí žádosti – v případě, že subjekt údajů není oprávněn požadovat výkon jeho práva nebo existuje výjimka, kvůli které tento výkon není možný. V odůvodnění zamítavé odpovědi na žádost subjektu údajů musí být uvedeny důvody zamítnutí a informace o možnosti podat stížnost u ÚOOÚ a vyřízení záležitosti soudní cestou; nebo
    b. Vyhovění žádosti – v případě, že subjekt údajů je oprávněn vykonávat svoje právo a neexistuje výjimka, která by vyřízení žádosti bránila.
5. V každém případě musí být subjekt údajů informován o krocích, které byly podniknuty v souvislosti s vyřizováním jeho žádosti, a to do 1 měsíce od jejího podání. V případě větší složitosti záležitosti nebo většího počtu žádosti či námitek podaných subjektem údajů během 1 měsíce, může být lhůta pro vyřízení prodloužena o 2 měsíce, o čem bude subjekt údajů informován, a to včetně důvodů pro tento odklad. Pokud nebude dohodnuto jinak, odpověď bude subjektu údajů podána ve stejné formě, v jaké byla podána jeho žádost.
6. Vyřizování žádosti se činí bezplatně. Jsou-li však žádosti subjektem údajů podané zjevně nedůvodně nebo nepřiměřeně, zejména pokud se opakují, může Společnost účtovat za vyřízení žádosti přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo s učiněním požadovaných úkonů, případně může odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti musí Společnost doložit.

VIII. Specifické postupy ohledně jednotlivých práv subjektů údajů

1. **Právo na přístup**

V obdržené žádosti o uplatnění práva na přístup se identifikuje jeden z následujících předmětů žádosti:

1. potvrzení, jestli jsou nebo nejsou Společností zpracovávané osobní údaje daného subjektu údajů;
2. informace o tom, jak jsou osobní údaje subjektu údajů zpracovávány; nebo
3. přehled veškerých nebo určitých osobních údajů, které jsou o subjektu údajů zpracovávány.

2. **Právo na opravu**

1. Osobní údaje zpracovávané Společností musí být úplné, správné a aktuální. Na základě žádosti subjektu údajů se do všech systémů Společnosti a jí pověřených zpracovatelů či příjemců vloží opravené nebo doplněné údaje, které se budou následně používat při všech dalších zpracováních.
2. Pokud je v žádosti subjektů údajů obsažen také požadavek na omezení zpracování po dobu, než budou osobní údaje subjektu údajů opraveny a takové opatření je nezbytné pro ochranu práv a svobod subjektu údajů, dojde k přerušení zpracování osobních údajů po dobu, kdy probíhá jejich oprava.

3. **Právo na výmaz (právo být zapomenut)**
    1. Subjekt údajů je oprávněn v souladu s čl. 17 GDPR požadovat výmaz svých osobních dat jen za určitých podmínek.
    2. Každá žádost musí být individuálně posouzena, zda jsou podmínky pro výmaz splněny a zda se neuplatní žádné výjimky, na základě, kterých musí být určité osobní údaje i přes žádost o výmaz zpracovávány (např. k plnění zákonné povinnosti) V případě dotazů či nejasností prosím kontaktujte ředitele Společnosti.
    3. V případě, že Společnost vyhodnotí, že požadované údaje lze vymazat, uvědomí o této skutečnosti i všechny ostatní zpracovatele či příjemce a zajistí, aby ani tito již předmětné osobní údaje nezpracovávali.

4. **Právo na omezení zpracování**
    1. Omezení zpracování je dočasné opatření, o které může být subjektem údajů žádáno v případě:
        a. že zpracování je protiprávní, subjekt údajů odmítá výmaz a žádá místo toho omezení použití svých osobních dat;
        b. že Společnost již osobní údaje již nepotřebuje pro své účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu svých právních nároků;
        c. že subjekt popírá přesnost svých osobních údajů, a to na dobu potřebnou k tomu, aby Společnost ověřila přesnost osobních údajů, např. během vyřizování žádosti o opravu nebo námitky subjektu údajů proti zpracování; a
        d. jako ochranu proti vymazání osobních údajů, ke kterému by jinak došlo (např. subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody Společnosti převažují nad důvody subjektů údajů).
    2. Za některých podmínek můžou být osobní údaje, jejichž zpracování je omezeno, zpracovány pro určité účely, např.: ochrana právních zájmů nebo zpracování se souhlasem subjektu. V případě dotazů či nejasností prosím kontaktujte ředitele Společnosti.

5. **Právo vznést námitku proti zpracování**
    1. Prvním krokem ke zpracování námitky proti zpracování je zjištění, zda existují závažné oprávněné důvody Společnosti pro zpracování těchto osobních dat, které převažují nad zájmy nebo právy a svobodami subjektu údajů nebo pro určení, výkon či obhajobu právních nároků Společnosti. Pokud takové důvody neexistují, Společnost již nemůže osobní údaje subjektu dat zpracovávat.
    2. Právo vznést námitku proti zpracování pro účely přímého marketingu je nepodmíněné a námitce se musí vždy vyhovět. V této souvislosti není podstatné, na jakém právním důvodu se toto zpracování zakládá.
    3. Každá žádost musí být individuálně posouzena, zda jsou podmínky práva vznést námitku splněny a zda se neuplatní žádné výjimky. V případě dotazů či nejasností prosím kontaktujte ředitele Společnosti.
    4. Po vyhovění žádosti nesmí být osobní údaje používány pro dané účely (oprávněný zájem) a budou v souladu s principem minimalizace vymazány. Pokud jsou dané osobní údaje zpracovávány pro jiné účely, toto zpracování může probíhat i nadále.

6. **Právo na přenositelnost**
    1. Právo na přenositelnost může subjekt údajů uplatnit v případě, že je zpracování založeno na souhlasu subjektu údajů nebo probíhá za účelem uzavření a plnění smlouvy nebo v případě, že je zpracování prováděno automatizovaně.

2. Osobní údaje (poskytnuty Společnosti subjektem údajů nebo které byly vytvořeny na základě požadavků subjektu údajů) budou poskytnuty ve strojově čitelném formátu (např. XML).
3. Subjekt údajů může rovněž požádat o předání těchto osobních údajů jinému správci (je-li to technicky proveditelné), a to bez souhlasu Společnosti.
4. Přenos osobních údajů se uskuteční v takové formě, která minimalizuje bezpečnostní rizika (např. za využití šifrování).

7. **Oznámení ohledně výmazu, opravy nebo omezení zpracování**
V případě vyhovění výkonu výše uvedených práv, musí být zpracovatelé a jiní příjemci osobních údajů informováni o jakémkoliv výmazu, opravě nebo omezení zpracování. Zároveň musí být jasně instruováni k podniknutí kroků k danému výmazu, opravě nebo omezení zpracování.

8. **Pravidla řízení přístupu k osobním údajům**

1. Řízení přístupu k prostředkům ICT je prováděno za uplatnění následujících principů vztahujících se jak na Zaměstnance, tak na externí subjekty jako obchodní partnery a dodavatele, např. zajišťující služby pro Společnost na základě smluvního vztahu:
    a. princip minimálního oprávnění, tzn. přidělení pouze takových oprávnění, která jsou nezbytná k plnění jeho pracovních/smluvních povinností;
    b. princip periodického přezkoumávání přístupových oprávnění;
    c. princip revize a změny přístupových oprávnění při změně pracovní pozice či pracovní náplně Zaměstnance či změně smluvního vztahu s externími subjekty; a
    d. princip odebrání všech přístupových oprávnění při ukončení pracovního/smluvního vztahu.
2. Pravidla řízení přístupu se uplatňují pro uživatele, administrátory, privilegované účty s rozšířenými přístupovými oprávněními, externí subjekty, kterým má být umožněn přístup do informačního systému Společnosti.
3. Každý uživatel, aplikace, systém nebo externí subjekt má přidělen jednoznačný identifikátor. Pro tvorbu identifikátorů jsou stanovena jednotná pravidla v rámci Společnosti.
4. Uživatel podá svoji žádost o přidělení přístupových práv stanoveným a formálním způsobem k rukám externího správce sítě.
5. Okamžité zablokování přístupových oprávnění při zjištění porušení pravidel autorizace.
6. Uživatelé jsou odpovědni za autentizační informace (hesla) a jsou povinni zajistit jim řádnou ochranu.

9. **Zabezpečení přístupu heslem**
Systém správy hesel ve Společnosti má za cíl zajištění kvality hesla a zajištění zabezpečení přístupu do informačního systému Společnosti dle potřeb Společnosti. Systém správy hesel zajistí mimo jiné požadavky vynucení pravidelné změny hesla uživateli a stanovení parametrů hesel (např. doba platnosti nebo existence stanovených znaků).

10. **Pravidla používání prostředků ICT**

1. Zaměstnanci pracujícímu s ICT prostředky, které mu byly svěřené Společností, je mohou využívat pouze k výkonu svých pracovních povinností.
2. Zaměstnanci mají povinnost chránit svěřené ICT prostředky před ztrátou, poškozením, zničením či zcizením. Zaměstnanci jsou zejména povinni uzamykat místnosti s ICT technologií při nepřítomnosti a přiměřeným způsobem chránit přidělené mobilní ICT prostředky.
3. V případě, že Zaměstnanec ICT prostředek nemá pod přímou kontrolou (např. při opuštění kanceláře), musí používat základní ochranné prostředky, tj. např. software „uzamykání“ ICT prostředku nebo jeho vypínání.

4. Pro bezpečný vzdálený přístup do ICT prostředí Společnosti je administrátorem ICT prostředků technologicky zajištěna bezpečná cesta se šifrovanou komunikací.

IX. Bezpečnostní události a incidenty

1. Základní pravidla řízení bezpečnostních incidentů

Řízení bezpečnostních incidentů a událostí ve Společnosti zahrnuje následující pravidla:

1. Pro oznamování událostí a incidentů, je ve Společnosti určen Zaměstnanec na pozici Ekonomický ředitel, který přijímá oznámení o bezpečnostních událostech a incidentech. Kontaktní informace příslušného Zaměstnance a osob, které ho zastupují v případě jeho nepřítomnosti nebo informace o nedostupnosti jsou uveřejněny na webové stránce Společnosti.
2. Všechny bezpečnostní incidenty jsou následně vyhodnoceny s cílem určit příčinu výskytu incidentu a přijmout nápravné opatření.
3. Postup a opatření ke zvládání bezpečnostního incidentu jsou průběžně dokumentována. Veškeré dokumentované informace k bezpečnostnímu incidentu jsou Společností uchovávány.

2. Postup zvládání bezpečnostních incidentů

1. Postup při řešení bezpečnostního incidentu zahrnuje následující činnosti:
   a. oznámení incidentu např. e-mailem, telefonicky, ústně prostřednictvím kontaktů Zaměstnance pověřeného příjmem těchto oznámení;
   b. pověřený Zaměstnanec Společnosti provede prvotní posouzení a prověření incidentu, jeho kategorizaci, posouzení incidentu a jeho dopadů, stanoví míru závažnosti incidentu;
   c. pověřený Zaměstnanec navrhne přijetí příslušného opatření a Společnost tato opatření ke zmírnění či eliminaci dopadů incidentu dle odhadnuté závažnosti incidentu přijme. Společnost dle svých aktuálních možností rozhodne o přijetí okamžitých protiopatření k eliminaci podobných incidentů a zabránění šíření jejich dopadů;
   d. pověřený Zaměstnanec Společnosti provede analýzu a vyhodnocení příčin vzniku incidentu, posouzení slabého místa zabezpečení osobních údajů ve Společnosti a návrh opatření ke zlepšení;
   e. projednání události na celopodnikové úrovni a odsouhlasení navržených protiopatření a opatření ke zlepšení, dále se projednají případná preventivní opatření; a
   f. pověřený Zaměstnanec Společnosti monitoruje realizaci protiopatření a vyhodnocuje jejich účinnost.

2. Při kategorizaci bezpečnostních incidentů se zohlední:
   a. důležitost dotčených osobních údajů;
   b. dopady na poskytované služby Společnosti;
   c. předpokládané škody a jiné dopady na práva a povinnosti subjektů údajů.

3. Pro potřeby zvládání bezpečnostních incidentů se incidenty dělí do následujících kategorií:

Kategorie	Bezpečnostní incident

Kategorie 1 **(Méně závažný bezpečnostní incident)**	Dochází k méně významnému narušení bezpečnosti osobních údajů. Musí být zamezeno další šíření bezpečnostního incidentu.
Kategorie 2 **(Závažný bezpečnostní incident)**	Je narušena bezpečnost osobních údajů. Jeho řešení vyžaduje neprodlený zásah k zamezení dalšímu šíření bezpečnostního incidentu.
Kategorie 3 **(Velmi závažný bezpečnostní incident)**	Je významně narušena bezpečnost osobních údajů. Řešení vyžaduje neprodlený zásah obsluhy, všemi dostupnými prostředky musí být zabráněno dalšímu šíření bezpečnostního incidentu.

3. **Oznamování případů porušení zabezpečení osobních údajů**

1. Druh, způsob a lhůty podávání oznámení závisí na tom, do které kategorie bezpečnostní incident/událost spadá:
   a. Kategorie 1: žádné oznámení není nutné;
   b. Kategorie 2: v případě porušení zabezpečení osobních údajů je Společnost povinna oznámit bez zbytečného odkladu, a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, toto porušení ÚOOÚ, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob; nebo
   c. Kategorie 3: Společnost musí oznámit porušení zabezpečení osobních údajů bez zbytečného odkladu subjektu údajů.
1. Oznámení o porušení zabezpečení osobních údajů musí být vyhotoveno v souladu s čl. 33 a 34 GDPR.
2. V případě, že k porušení zabezpečení osobních údajů dojde u zpracovatele, , ohlásí je zpracovatel bez zbytečného odkladu správci ihned jakmile takové porušení zjistí.
3. Oznámení subjektu údajů dle tohoto článku se nevyžaduje, je-li splněna kterákoli z těchto podmínek:
   a. Společnost zavedla náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
   b. Společnost přijala následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;
   c. vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

X. **Likvidace osobních údajů**

1. Likvidaci osobních údajů provádí pověření pracovníci (HR Manager, Mzdové oddělení, BOZP Manager, pracovník Spisovny a archivace dle Skartačního plánu).
2. Zpracování osobních údajů je ukončeno a osobní údaje budou neprodleně zlikvidovány:
   a. jakmile pomine účel, pro který byly osobní údaje zpracovávány;

b. na základě žádosti subjektu údajů v případě, že již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
b. pokud subjekt údajů odvolal svůj souhlas se zpracováním;
c. pokud subjekt údajů vznesl námitku proti zpracování osobních údajů, které se jej týkají;
d. zpracování jeho osobních údajů je v rozporu s Předpisy na ochranu osobních údajů z jiných důvodů.

3. Po uplynutí doby, na kterou byly osobní údaje uchovávány dle pravidel uvedených v příslušných právních předpisech a/nebo následujících vodítek:

Osobní údaje (potenciálních) obchodních partnerů
Původ osobních údajů
Ze smlouvy – 3 roky po skončení smluvního vztahu
Osobní údaje (potenciálních) zaměstnanců
Původ osobních údajů
Z příjímacího procesu – maximálně po dobu zkušební doby přijatého kandidáta (3 měsíce) nebo na základě souhlasu 2 roky od jeho udělení
Z pracovní smlouvy – 3 roky po skončení smluvního vztahu
Evidenční listy – 5 let
Záznamy ohledně poživatele starobního nebo invalidního důchodu – 10 let
Mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění – 30 let
Osobní údaje z různých dokumentů
Původ osobních údajů
Účetní záznamy – 5 let
Daňové doklady – 10 let

XI. Předání osobních údajů do jiných zemí předávají do jiných zemí

1. V případě předání osobních údajů do členských států Evropského hospodářského prostoru není potřeba realizovat žádná dodatečná opatření. Předávání osobních údajů do třetích zemí může být založeno na základě mezinárodní smlouvy, příp. na základě rozhodnutí orgánů Evropské unie, aktuální podmínky pro takové předávání, které jsou dodržovány, jsou uvedeny na webových stránkách ÚOOÚ.[1]
2. Z hlediska předávání dat do třetích zemí společnost Unifrax s.r.o. předává data mateřské společnosti Unifrax se sídlem v USA a to na měsíční bázi. Jedná se o přehledy obsahující jména zaměstnanců, jejich mzdové údaje, datum nástupu a případného ukončení pracovního poměru.

XII. Smluvně zajištěný zpracovatel

3. Zpracovatelé jsou osoby pověřené zpracováváním osobních údajů v souladu s podmínkami zakotvenými ve smlouvě o zpracování se Společností. Tato smlouva má vždy písemnou formu.

XIII. Povinnosti zaměstnance odpovědného za agendu ochrany osobních údajů

1. Zaměstnanec odpovědný za agendu ochrany osobních údajů je Zaměstnanec na pozici – HR Manager.

   V rámci své odpovědnosti za ochranu osobních údajů tento Zaměstnanec zajišťuje informovanost oprávněných osob o problematice ochrany osobních údajů se zaměřením na:

   a. změny v Předpisech o ochraně osobních údajů, příp. dalších právních předpisů s dopadem do problematiky zpracování osobních údajů;
   b. zevšeobecnění poznatků z kontrolní činnosti ÚOOÚ;
   c. nové skutečnosti promítající se do systému ochrany osobních údajů (např. organizační, personální změny, update software);
   d. zahrnutí problematiky ochrany osobních údajů do plánu vzdělávání Zaměstnanců Společnosti,
   e. provedení aktualizace této Směrnice při výrazných změnách Předpisů na ochranu osobních údajů; a
   f. realizace neodkladných opatření v oblasti zabezpečení ochrany osobních údajů.

XIV. Kamerové systémy

1. Ve výrobních a skladovacích prostorech Společnosti na adrese sídla Společnosti jsou instalovány kamerové systémy se záznamovým zařízením. Účelem instalace těchto kamerových systémů je ochrana majetku, bezpečnosti a dalších chráněných zájmů Společnosti, jejich Zaměstnanců i dalších osob, nacházejících se v budově Společnosti. O tomto zpracování je taktéž vyhotoven Záznam o zpracování. Subjekty údajů jsou o kamerovém systému informováni formou piktogramu.
2. Snímané záběry jsou uchovávány v záznamových zařízeních po dobu nejvýše 30 dnů. Po této době jsou zaznamenaná data automaticky přemazána novým zápisem.
3. Kamerové systémy nejsou napojeny na žádnou databázi operující s osobními údaji. Záznamy z kamerových systémů budou využívány pouze v souladu s účelem jejich instalace, a to v případě vnitřního šetření identifikovaného incidentu, nebo budou předány na vyžádání orgánů činných v trestním řízení jako důkazní materiál vyšetřování.

[1] https://www.uoou.cz/predavani-osobnich-udaju-do-zahranici/ds-1633/p1=1633&rd=1000

XV. **Závěrečná ustanovení**

Tato Směrnice nabývá účinnosti dne 24. 5. 2018.