INTERNÍ SMĚRNICE

OCHRANA A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

VEIDEC s.r.o.

se sídlem Hradecká 565, Polabiny, 530 09 Pardubice, Česká republika

identifikační číslo: 25977580

zapsaná v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, spisová značka C 18401

ze dne 1. května 2018

(***Směrnice***)

1. ÚVODNÍ USTANOVENÍ

(a) Společnost **VEIDEC s.r.o**., se sídlem Hradecká 565, Polabiny, 530 09 Pardubice, Česká republika, IČ: 25977580, zapsaná v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, spisová značka C 18401, (***Společnost***) vykonává podnikatelskou činnost zejména v oblasti nákupu a prodeje chemických výrobků.

(b) V rámci podnikatelské činnosti dochází ke zpracovávání osobních údajů zákazníků, obchodních partnerů či zaměstnanců Společnosti.

(c) Společnost je správcem osobních údajů.

(d) Směrnice pro ochranu osobních údajů 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. 101/2000 Sb., 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) (***Předpisy na ochranu osobních údajů***), s cílem zajištění zpracování osobních údajů v souladu s touto legislativou a principy, na kterých je vystavěná.

(e) Směrnice je závazná pro všechny zaměstnance Společnosti (***Zaměstnanec***) a Oprávněné osoby, jak je tento pojem definován níže.

(f) Zaměstnancem odpovědným za agendu ochrany osobních údajů je paní **Eva Frenclová**, tel: 737 226 801, e-mail: gdpr@veidec.cz, se sídlem kanceláře: Hradecká 565, Polabiny, 530 09 Pardubice.

2. DEFINICE A VÝKLAD POJMŮ

Pro účely této Směrnice se rozumí:

(a) ***automatizovaným zpracováním*** zejména:

(i) ukládání informací na nosiče dat;

(ii) provádění logických nebo aritmetických operací s těmito daty, zejména jejich změna, výmaz, vyhledávání nebo rozšiřování uskutečňované zcela nebo zčásti pomocí automatizovaných postupů;

(iii) provádění archivace informací jejich uložením na archivační paměťová média a v případě potřeby obnovení informací z archivních médií.

(b) ***DPIA*** posouzení vlivu na ochranu osobních údajů (anglicky *Data Protection Impact Assessment*) (jak je tento pojem definován v Předpisech na ochranu osobních údajů).

(c) ***DPO*** pověřenec pro ochranu osobních údajů (anglicky *Data Protection Officer*) (jak je tento pojem definován v Předpisech na ochranu osobních údajů).

(d) ***ICT*** informační a telekomunikační technologie.

(e) ***manuálním zpracováním*** jakékoliv zpracování s výjimkou zpracování automatizovaného (např. listinná podoba, kartotéky, spisy).

(f) ***oprávněnou osobou***

(i) Zaměstnanec, který v rámci plnění povinností plynoucích mu z pracovní náplně má přístup k osobním údajům a dále je zpracovává, a

(ii) osoba, které na základě smluvního vztahu má Společností povolený přístup k osobním údajům.

(g) ***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.

(h) ***osobním údajem zvláštní kategorie*** osobní údaj vypovídající 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.

(i) ***profilováním*** jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, chování, místa, kde se nachází, nebo pohybu.

(j) ***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; v případech veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského a finančního zájmu České republiky nebo Evropské unie.

(k) ***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.

(l) ***správcem*** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování.

(m) ***ÚOOÚ*** znamená Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, PSČ 170 00, Praha 7, webové stránky www.uoou.cz.

(n) ***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.

(o) ***zpracovatelem*** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

(p) Odkazy na jednotné číslo rovněž zahrnují číslo množné a naopak.

3. ÚKONY PŘED ZAPOČETÍM ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

(a) Před započetím zpracování osobních údajů je povinen správce vypracovat záznamy o činnostech zpracování a zpracovatel vypracovat záznamy o všech kategoriích činností zpracování prováděných pro správce, pokud tuto povinnost stanoví Předpisy na ochranu osobních údajů.

(b) Účely (důvody) zpracování osobních údajů v jednotlivých agendách vychází ze zvláštních zákonů, nebo jsou osobní údaje zpracovávány na základě rozhodnutí správce.

(c) Ke každému účelu zpracování musí být přiřazen právní titul, právními tituly pro zpracování jsou:

(i) souhlas subjektu údajů;

(ii) plnění smlouvy, které stranou je subjekt údajů;

(iii) plnění právní povinnosti Společnosti;

(iv) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů;

(v) splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci; a

(vi) oprávněný zájem Společnosti.

(d) Není-li zpracování osobních údajů nezbytné (i) pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů, (ii) pro splnění právní povinnosti, která se na Společnost vztahuje, (iii) zpracování není nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, (iv) zpracování není nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým by Společnost byla pověřena, (v) zpracování není nezbytné pro účely oprávněných zájmů Společnosti či třetí strany, zajistí Společnost/zpracovatel před zpracováním osobních údajů souhlas subjektu údajů se zpracováním osobních údajů a tento souhlas (včetně podmínek, za kterých byl udělen) uchovává po celou dobu zpracování osobních údajů tohoto subjektu.

(e) Za souhlas se zpracováním osobních údajů je považováno poskytnutí těchto údajů subjekty osobních údajů:

(i) v listinné podobě s uvedením vlastnoručního podpisu včetně údaje o čase podpisu;

(ii) v elektronické podobě s např. připojením elektronického podpisu, se zaškrtnutím příslušného políčka se souhlasem v elektronickém formuláři atd.

(f) Udělený souhlas musí být prokazatelný po celou dobu zpracování, včetně všech podmínek, ze kterých je zřetelné k čemu a v jakém znění byl souhlas udělen. V případě, že subjekt údajů souhlas neposkytne, nelze jeho osobní údaje zpracovávat.

Pokud je pravděpodobné, že určitý druh zpracování osobních údajů ve Společnosti bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede Společnost před zpracováním ***DPIA***. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení. V každém takovém případě Společnost požádá o předchozí konzultaci s ÚOOÚ.

4. INFORMAČNÍ POVINNOST

(a) Při shromažďovaní osobních údajů přímo od subjektu údajů musí být subjekt osobních údajů, k němuž se osobní údaje vztahují, informován nejpozději v okamžiku získávání jeho osobních údajů o:

(i) totožnosti a kontaktních údajích Společnosti a její případného zástupce;

(ii) kontaktních údajích zaměstnance odpovědného za agendu ochrany osobních údajů, případně DPO Společnosti;

(iii) účelech zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;

(iv) oprávněných zájmech Společnosti nebo třetí strany v případě, že je zpracování založeno na tomto právním důvodu zpracování;

(v) případných příjemcích nebo kategoriích příjemců osobních údajů;

(vi) případném úmyslu Společnosti předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Evropské komise o odpovídající ochraně nebo, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny;

(vii) době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

(viii) existenci práva požadovat od Společnosti přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

(ix) pokud je zpracování založeno na souhlasu subjektu údajů, existenci práva kdykoli odvolat tento souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;

(x) existenci práva podat stížnost u ÚOOÚ;

(xi) skutečnosti, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů; a

(xii) skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování a informacích týkajících se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

(b) Při shromažďovaní osobních údajů jiným způsobem než od subjektu údajů, musí být subjekt osobních údajů, k němuž se osobní údaje vztahují, informován nejpozději v okamžiku získávání jeho osobních údajů o skutečnostech v odstavcích (i), (ii), (iii), (v), (vi) písmene (a) tohoto článku a kategoriích dotčených osobních údajů.

Informační povinnost dle tohoto článku plní oprávněné osoby shromažďující osobní údaje od subjektů údajů, a to formou Informačního memoranda Společnosti.

5. VYŘIZOVÁNÍ ŽÁDOSTÍ SUBJEKTŮ ÚDAJŮ

(a) **Základní zásady vyřizování žádosti**

(i) Společnost přijímá žádosti subjektů údajů v elektronické podobě (zaslané e-mailem nebo vložené do webového formuláře Společnosti) 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.

(ii) Žádosti mohou být Společnosti zaslané i jí určeným zpracovatelem, odpovědnost za vyřízení takových žádostí má však vždy Společnost.

(iii) 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 Právních předpisů v oblasti ochrany osobních údajů; nebo

(C) se v žádostí uvádí, že je spojena s Právními předpisy v oblasti ochrany osobních údajů.

(b) **Postup při vyřizování žádosti subjektu údajů**

(i) Ověření identity subjektu údajů – aby bylo zajištěno jednání s konkrétní dotčenou osobou, a to nejen v případě, že je žádost podaná zmocněncem subjektu údajů;

(ii) Vyjasnění žádosti a jejího předmětu – v případě, že ze žádosti není zřejmé, čeho se subjekt údajů dožaduje, nebo jsou v žádosti obsažené chybné informace, jejichž správné znění je však nevyhnutné pro její vyřízení, subjekt údajů bude vyzván k její upřesnění;

(iii) Posouzení žádosti – zda má subjekt údajů právo na výkon daného práva a zda neexistuje výjimka, která by tento výkon znemožňovala;

(iv) Vyřízení žádosti:

(A) Zamítnutí žádosti – subjekt údajů není oprávněn vykonat požadované právo nebo existuje výjimka, kvůli které tento výkon není možný. V odůvodnění zamítavé

odpovědi na žádost musí být uvedeny důvody zamítnutí a informace o možnosti podat stížnost u ÚOOÚ a vyřízení záležitosti soudní cestou; nebo

(B) Vyhovění žádosti – subjekt údajů je oprávněn vykonávat svoje právo a neexistuje výjimka, která by mu v tom bránila.

(c) Subjekt údajů musí být informován o krocích, které byly podniknuty v souvislosti s vyřizováním jeho žádosti 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, včetně důvodů pro tento odklad. Odpověď bude subjektu údajů podána ve stejné formě, v jaké byla podána jeho žádost, pokud nebude dohodnuto jinak.

(d) 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 odmítnou žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti musí být Společnost schopna doložit.

(e) **Specifické postupy ohledně jednotlivých práv subjektů údajů**

(i) **Právo na přístup**

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

(A) potvrzení, jestli jsou nebo nejsou Společností zpracovávané osobní údaje daného subjektu údajů;

(B) informace o tom, jak jsou osobní údaje subjektu údajů zpracovávány; nebo

(C) přehled veškerých nebo určitých osobních údajů, které jsou o subjektu údajů zpracovávány.

(B) Toto právo je nepodmíněné a nejsou zde žádné výjimky, takže se žádosti musí vyhovět, přičemž se musí brát ohled na práva a svobody třetích osob, které by mohly být dotčeny poskytnutím vyžádaného přehledu. V případě dotazů či nejasností prosím kontaktujte zaměstnance odpovědného za agendu ochrany osobních údajů, případně DPO.

(ii) **Právo na opravu**

(A) 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 a ty budou použity při všech dalších zpracováních.

(B) Pokud je v žádosti subjektů údajů obsažen také požadavek na omezení zpracování po dobu, než bude korekce údajů a takové opatření je nezbytné pro ochranu práv a svobod subjektu údajů, dojde k přerušení zpracování osobních údajů po dobu, kdy

probíhá jejich korekce. V případě dotazů či nejasností prosím kontaktujte zaměstnance odpovědného za agendu ochrany osobních údajů, případně DPO.

(iii) **Právo na výmaz (právo být zapomenut)**

(A) Subjekt údajů je oprávněn požadovat výmaz jen za určitých podmínek, a to když:

(A) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány;

(B) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;

(C) subjekt údajů vznese námitku proti zpracování a neexistují žádné převažující oprávněné důvody Společnosti pro zpracování;

(D) osobní údaje byly zpracovány protiprávně;

(E) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Evropské unie nebo České republiky; nebo

(F) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti.

(B) Každá žádost musí být individuálně posouzena, zda jsou podmínky 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 zaměstnance odpovědného za agendu ochrany osobních údajů, případně DPO.

(C) V případě, že Společnosti vyhodnotí, že požadované údaje lze vymazat, uvědomí o této skutečnosti i všechny ostatní zpracovatelé a zajistí, aby ani tito již předmětné osobní údaje nezpracovávali.

(iv) **Právo na omezení zpracování**

(A) Omezení zpracování je dočasné opatření, o které může být subjektem údajů žádáno v případě:

(A) že zpracování je protiprávní, subjekt dat odmítá výmaz a žádá místo něho omezení;

(B) aby se aplikovalo během vyřizování žádosti o opravu nebo námitky subjektu údajů proti zpracování (subjekt dat popírá přesnost údajů); a

(C) jako ochrana proti vymazání osobních údajů, ke kterému by jinak došlo (např. subjekt vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody Společnosti převažují nad důvody subjektů dat).

(B) Za některých podmínek můžou být osobní údaje, kterých zpracování je omezeno, zpracovány pro určité účely, např.: ochrana právních zájmů nebo zpracování se

souhlasem subjektu. V případě dotazů či nejasností prosím kontaktujte zaměstnance odpovědného za agendu ochrany osobních údajů, případně DPO.

(v) **Právo vznést námitku**

(A) Prvním krokem ke zpracování námitky je zjištění, zda je podávána proti zpracování osobních údajů týkající se Společnosti, resp. zda pro marketingové účely, oprávněné zájmy Společnosti nebo zda jde o zpracování ve veřejném zájmu nebo pro vědecké či statistické účely týkající se jedinečné situace subjektu údajů.

(B) Právo vznést námitku proti zpracování pro účely přímého marketingu je nepodmíněné a námitce musí vždy vyhovět, přičemž není podstatné, na jakém právním důvodu se toto zpracování zakládá.

(C) Každá žádost musí být individuálně posouzena, zda jsou podmínky splněny a zda se neuplatní žádné výjimky. V případě dotazů či nejasností prosím kontaktujte zaměstnance odpovědného za agendu ochrany osobních údajů, případně DPO.

(D) Po vyhovění žádosti nesmí být osobní údaje používány pro dané účely (marketing, oprávněný zájem, statistika, výzkum) a budou v souladu s principem minimalizace vymazány. Pokud jsou dané osobní údaje zpracovávány pro jiné účely, toto zpracování může probíhat i nadále.

(vi) **Právo na přenositelnost**

(A) Právo na přenositelnost může subjekt údajů uplatnit v případě, že je zpracování založeno na právním důvodu uděleného souhlasu a pro účely uzavření a plnění smlouvy a zároveň když je zpracování prováděno automatizovaně. Výjimkou je zpracování nezbytné ve veřejném zájmu nebo při výkonu veřejné moci.

(B) Osobní údaje (poskytnuty Společnosti subjektem údajů nebo které byly vytvořeny na základě požadavků subjektu údajů) budou poskytnuty ve strojově čitelném formátu (např. XML).

(C) Subjekt údajů může rovněž požádat o předání těchto osobních údajů jinému správci, a to bez souhlasu Společnosti.

(D) Přenos osobních údajů se uskuteční v takové formě, která minimalizuje bezpečnostní rizika (např. za využití šifrování).

(E) Pokud byly vyžádané osobní údaje předány subjektu údajů, oznámení subjektu údajů se podá jen v případě, že došlo k omezením v důsledku např. dopadu na práva třetích subjektů.

(f) **Oznámení subjektům 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.

6. HLAVNÍ BEZPEČNOSTNÍ RIZIKA

(a) Mezi hlavní bezpečnostní rizika, které hrozí při zpracování osobních údajů v rámci Společnosti patří zejména:

(i) zničení nebo zneužití technických prostředků;

(ii) přístup neoprávněných osob k osobním údajům;

(iii) zneužití záznamů ohledně osobních údajů oprávněnými osobami;

(iv) živelní událost.

7. POSOUZENÍ RIZIK BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

(a) V rámci Společnosti je definován proces posuzování rizik bezpečnosti osobních údajů. V rámci tohoto procesu je stanovená metodika hodnocení rizik, tj. postupy a kritéria pro posuzování rizik a vyhodnocení identifikovaných rizik.

(b) Posouzení rizik se provádí periodicky, s maximální periodou dva roky, nebo v případě takových situací, které mají nebo mohou mít vliv na bezpečnost osobních údajů.

8. OŠETŘENÍ RIZIK BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

(a) V rámci Společnosti je definován proces k ošetření rizik bezpečnosti osobních údajů, v rámci, kterého je prováděn výběr vhodných variant na ošetření identifikovaných rizik s ohledem na výsledky posouzení rizik.

(b) S ohledem na identifikovaná rizika bezpečnosti osobních údajů je:

(i) proveden výběr vhodných opatření k ošetření identifikovaných rizik,

(ii) vytvořen plán pro implementaci navrhovaných opatření k eliminaci nebo snížení identifikovaných rizik bezpečnosti osobních údajů.

9. PRAVIDLA ŘÍZENÍ PŘÍSTUPU K OSOBNÍM ÚDAJŮM

(a) Řízení přístupu k prostředkům ICT je prováděno za uplatnění následujících principů, které se uplatňují jak pro Zaměstnance, tak pro externí subjekty jako obchodní partnery a dodavatele, např. zajišťující služby pro Společnost na základě smluvního vztahu:

(i) princip minimálního oprávnění, tzn. přidělení pouze takových oprávnění, která jsou nezbytná k plnění jeho pracovních/smluvních povinností;

(ii) princip periodického přezkoumávání přístupových oprávnění;

(iii) princip revize a změny přístupových oprávnění při změně pracovní pozice či pracovní náplně Zaměstnance či změně smluvního vztahu s jinými subjekty; a

(iv) princip odebrání všech přístupových oprávnění při ukončení pracovního/smluvního vztahu.

(b) 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.

(c) Každý uživatel, aplikace, systém nebo externí subjekt má přidělen jednoznačný identifikátor. Pro tvorbu identifikátorů jsou stanovena jednotná pravidla v rámci Společnosti.

(d) Uživatel podá svoji žádost o přidělení přístupových práv stanoveným formálním způsobem k rukám osoby odpovědné za správu IT Společnosti.

(e) Okamžité zablokování přístupových oprávnění při zjištění porušení pravidel autorizace.

(f) Uživatelé jsou odpovědni za autentizační informace (hesla) a jsou povinni zajistit jim řádnou ochranu.

10. ŘÍZENÍ ROZŠÍŘENÝCH OPRÁVNĚNÍ

(a) V rámci přidělování rozšířených přístupových oprávnění je uplatňován princip minimální potřeby pro danou provozní roli. Rozšířená oprávnění jsou řízena a přidělována dle stanoveného formálního procesu autorizace.

(b) Rozšířená práva by měla být přiřazena k identifikátoru uživatele odlišného od identifikátoru používaného pro běžné činnosti ve Společnosti. Je veden přehled o identifikátorech (účtech), kterým byla udělena rozšířená přístupová oprávnění.

(c) Kompetence uživatelů s rozšířenými přístupovými právy (např. administrátoři) musí být pravidelně přezkoumávány s cílem ověření, zda jsou v souladu s jejich povinnostmi. Přezkoumání se provádí nejméně 1x za rok.

11. ZABEZPEČENÍ PŘÍSTUPU HESLEM

Systém správy hesel ve Společnosti má za cíl zajištění kvality hesla a způsobů jeho implementace při autentizaci uživatele dle potřeb Společnosti pro zajištění zabezpečení přístupu do informačního systému Společnosti. Systém správy hesel zabezpečí mimo jiné požadavky vynucení pravidelné změny hesla uživateli a stanovení parametrů hesel (např. doba platnosti nebo existence stanovených znaků).

12. PRAVIDLA POUŽÍVÁNÍ PROSTŘEDKŮ ICT

(a) Zaměstnanci pracující ICT prostředky, které mu byly svěřené Společností, je mohou využívat pouze k výkonu svých pracovních povinností.

(b) Zaměstnanci mají povinnost chránit svěřené ICT prostředky před ztrátou, poškozením, zničením či zcizením. Zejména jsou povinni uzamykat místnosti s ICT technologií při nepřítomnosti a přiměřeným způsobem chránit přidělené mobilní ICT prostředky.

(c) 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.

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

13. BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY

(a) **Základní pravidla řízení bezpečnostních incidentů**

Řízení bezpečnostních incidentů a událostí v Společnosti zahrnuje následující pravidla:

(A) Pro oznamování událostí a incidentů, je ve Společnosti určen zaměstnanec odpovědný za agendu ochrany osobních údajů, případně DPO, který přijímá oznámení o bezpečnostních událostech a incidentech. Kontaktní informace příslušného zaměstnance odpovědného za agendu ochrany osobních údajů, případně DPO, jsou uveřejněny na webové stránce Společnosti.

(B) Všechny bezpečnostní incidenty jsou následně vyhodnoceny s cílem určit příčinu výskytu incidentu a přijmout nápravné opatření.

(C) Postup a opatření ke zvládání bezpečnostního incidentu jsou průběžně dokumentována, veškeré dokumentované informace k bezpečnostnímu incidentu jsou Společností uchovávány.

(b) **Postup zvládání bezpečnostních incidentů**

Postup při řešení bezpečnostního incidentu zahrnuje následující činnosti:

(A) oznámení incidentu např. e-mailem, telefonicky, ústně prostřednictvím kontaktů zaměstnance odpovědného za agendu ochrany osobních údajů, případně DPO;

(B) zaměstnanec odpovědný za agendu ochrany osobních údajů, případně DPO, provede prvotní posouzení a prověření incidentu, jeho kategorizaci, posouzení incidentu a jeho dopadů, stanoví míru závažnosti incidentu;

(C) zaměstnanec odpovědný za agendu ochrany osobních údajů, případně DPO, navrhne přijetí a Společnost přijme opatření ke zmírnění či eliminaci dopadů incidentu dle odhadnuté závažnosti incidentu a dle aktuálních možností Společnosti

rozhodne o přijetí okamžitých protiopatření k eliminaci incidentu a zabránění šíření jeho dopadů;

(D) zaměstnanec odpovědný za agendu ochrany osobních údajů, případně DPO, 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) zaměstnanec odpovědný za agendu ochrany osobních údajů, případně DPO, monitoruje realizaci protiopatření a vyhodnocuje jejich účinnost.

(a) Při kategorizaci bezpečnostních incidentů se zohlední:

(A) důležitost dotčených osobních údajů,

(B) dopady na poskytované služby Společností,

(C) předpokládané škody a jiné dopady na práva a povinnosti subjektů údajů.

(b) 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.

(c) **Oznamování případů porušení zabezpečení osobních údajů**

(i) 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.

(ii) Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

(iii) 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.

14. LIKVIDACE OSOBNÍCH ÚDAJŮ

(a) Zpracování osobních údajů je ukončeno a osobní údaje budou neprodleně zlikvidovány:

(i) jakmile pomine účel, pro který byly osobní údaje zpracovávány,

(ii) na základě žádosti subjektu údajů v případě, že

(A) 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 Právními předpisy na ochranu osobních údajů z jiných důvodů.

(iii) po uplynutí doby, na kterou byly osobní údaje uchovávány dle pravidel uvedených v příslušných právních předpisech a/nebo následujících vodítek:

Osobní údaje (potenciálních) zákazníků	
Původ osobních údajů	**Požadovaná/maximální doba uchovávání**
Ze smlouvy	10 let od konce obchodního vztahu
Z marketingových aktivit	3 roky od získání těchto osobních údajů

Osobní údaje (potenciálních) obchodních partnerů	
Původ osobních údajů	**Požadovaná/maximální doba uchovávání**
Ze smlouvy	10 let od konce obchodního vztahu
Z marketingových aktivit	3 roky od získání těchto osobních údajů

Osobní údaje (potenciálních) zaměstnanců	
Původ osobních údajů	**Požadovaná/maximální doba uchovávání**
Z přijímacího procesu	1 měsíc od získání těchto osobních údajů
Z pracovní smlouvy	3 roky od konce pracovního vztahu
Evidenční listy	3 kalendářní roky po roce, kterého se týkají
Záznamy ohledně poživatele starobního nebo invalidního důchodu	10 let následujících po roce, kterého se záznamy týkají
Mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění	30 let následujících po roce, kterého se záznamy týkají

Osobní údaje z různých dokumentů	
Původ osobních údajů	**Požadovaná/maximální doba uchovávání**
Účetní záznamy	5 let (účetní závěrky a výroční zprávy 10 let)
Daňové doklady	10 let od konce zdaňovacího období, ve kterém se plnění uskutečnilo

15. PŘEDÁNÍ OSOBNÍCH ÚDAJŮ DO JINÝCH ZEMÍ

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]

16. SMLUVNĚ ZAJIŠTĚNÝ ZPRACOVATEL

(a) Zpracovatelé jsou osoby pověřené zpracováváním osobních údajů v souladu s podmínkami zakotvenými ve smlouvě o zpracování se Společností. Tato smlouva má vždy písemnou formu. Ve smlouvě musí být minimálně uvedeno jaký je předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva Společnosti jako správce. Dále se zpracovatel v této smlouvě zaváže k/ke:

(A) zpracovávání osobních údajů pouze na základě doložených pokynů Společnosti,

(B) zajištění, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

(C) přijetí vhodných opatření k zajištění bezpečnosti osobních údajů;

(D) dodržení smluvených/zákonných podmínek pro případné zapojení dalšího zpracovatele;

(E) zohledňování povahy zpracování, tj. že bude Společnosti nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné,

(F) součinnost pro splnění povinnosti Společnosti reagovat na žádosti o výkon práv subjektu údajů;

(G) pomoci Společnosti při zajišťování souladu s jejími povinnostmi podle Předpisů v oblasti ochrany osobních údajů, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;

(H) k tomu, že osobní údaje buď vymaže, nebo je vrátí Společnosti po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Evropské unie nebo České republiky nepožaduje uložení daných osobních údajů; a

(I) poskytnutí veškerých informací Společnosti potřebných k doložení skutečnosti, že byly splněny povinnosti stanovené v tomto článku, a umožnění auditů, včetně inspekcí, prováděných Společností nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.

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

17. ZPRACOVÁNÍ ZVLÁŠTNÍCH KATEGORIÍ OSOBNÍCH ÚDAJŮ

(a) Před zpracováním zvláštních kategorií osobních údajů musí být subjekt údajů informován a poučen v rozsahu informační povinnosti dle této Směrnice. Zvláštní kategorie osobních údajů mohou být zpracovány pouze s výslovným souhlasem subjektu údajů, kterého se týkají. Za výslovný souhlas lze považovat pouze takové právní jednání, kterým dotčená fyzická osoba výslovně svoluje ke zpracování svých osobních údajů zvláštních kategorií. Nedá-li tato fyzická osoba výslovný souhlas s jejich zpracováním, nelze její osobní údaje zvláštních kategorií zpracovávat.

(b) Poskytnuté osobní údaje zvláštních kategorií jsou pokládány za důvěrné informace a v rámci jejich dalšího zpracování se s nimi mohou seznamovat pouze oprávněné osoby, které tyto údaje potřebují pro plnění svých pracovních povinností.

(c) Specifické podmínky, za nichž je možné zpracovávat citlivé údaje bez souhlasu, resp. s dodatečným souhlasem, jsou uvedeny v Předpisech o ochraně osobních údajů.

18. POVINNOSTI ZAMĚSTNANCE ODPOVĚDNÉHO ZA AGENDU OCHRANY OSOBNÍCH ÚDAJŮ

(a) Zaměstnanec odpovědný za agendu ochrany osobních údajů v rámci své odpovědnosti za ochranu osobních údajů 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 Právních předpisů v oblasti ochrany osobních údajů;

(F) realizace neodkladných opatření v oblasti zabezpečení ochrany osobních údajů.

19. KAMEROVÉ SYSTÉMY

(a) Ve vnějších a vnitřních prostorech budovy a skladu 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 viditelného označení monitorovaného prostoru.

(b) Snímané záběry jsou uchovávány v záznamových zařízeních po dobu nejvýše 30 dnů. Po této době jsou zaznamenaná data automaticky přemazána novým zápisem.

(c) Kamerové systémy nejsou napojeny na žádnou databázi operující s osobními údaji. Záznamy z kamerových systémů budou využity 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.

20. ZÁVĚREČNÁ USTANOVENÍ

Tato Směrnice nabývá účinnosti dne 1. května 2018.