SMĚRNICE K ZABEZPEČENÍ OCHRANY OSOBNÍCH ÚDAJŮ

1. VŠEOBECNÁ USTANOVENÍ

1.1 ÚVODNÍ USTANOVENÍ

Tato směrnice upravuje technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s NAŘÍZENÍM EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, 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), tzv. GDPR (dále jen „GDPR“) a předpisů souvisících s cílem zajištění správné praxe při přijímání a realizaci opatření k ochraně osobních údajů u osoby: Jsme MILA, z. s., IČ:07543654, se sídlem Wuchterlova 362/11, Praha 6 (dále jen „spolek“ nebo “společnost”).

1.2 ROZSAH PŮSOBNOSTI

a) Touto směrnicí jsou vázáni všichni členové statutárních orgánů spolku, zaměstnanci, pracovníci i další osoby, které přicházejí do styku s osobními údaji ve společnosti, nebo v rámci své práce pro společnost.

b) Tato směrnice platí přiměřeně i pro obchodní společnosti, přicházející do styku s osobními údaji ve společnosti, nebo v rámci své práce pro společnost, případně také pro dceřiné subjekty společnosti, ať již jsou to korporace, či jiné právnické osoby ovládané nebo zřízené společností.

c) Pokud společnost provádí svoji činnost na území jiného státu, je povinna dodržovat i pravidla pro ochranu osobních údajů platná v takovém státu.

1.3 VYMEZENÍ POJMŮ

Pro účely této směrnice se rozumí:

a) **archivace** - uchování informací v listinné, či elektronické podobě;

b) **bezpečnost zpracování osobních údajů** - technická a organizační opatření, zajišťující úroveň zabezpečení odpovídající danému riziku;

c) **biometrické údaje** - osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje, daktyloskopické údaje (otisky prstů), obraz krevního řečiště, biomechanika chůze, obraz sítnice oka, a podobně;

d) **citlivý údaj** – neboli zvláštní kategorie osobních údajů, je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů, genetický údaj subjektu údajů či biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci (proces ověření skutečné identity osoby) subjektu údajů;

e) **genetické údaje** - osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;
f) **likvidace osobních údajů** - fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování;
g) **osobní údaj** - jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, přičemž subjekt údajů se považuje za určený nebo určitelný, jestliže jej lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu, tedy jakékoli údaje, podle kterých je možné přímo, či nepřímo identifikovat konkrétního člověka (zpravidla jméno, příjmení, adresa, rodné číslo, fotografie, apod.);
h) **příjemce** - každý subjekt, kterému jsou osobní údaje zpřístupněny;
i) **pseudonymizace osobních údajů** - proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost;
j) **shromažďování osobních údajů** - systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování;
k) **souhlas subjektu údajů** - svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů;
l) **správce** - každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj (zpracováním osobních údajů může správce pověřit zpracovatele);
m) **subjekt údajů** - fyzická osoba, k níž se osobní údaje vztahují;
n) **uchovávání osobních údajů** - udržování údajů v takové podobě, která je umožňuje dále zpracovávat;
o) **zpracování osobních údajů** - jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, jako je např. shromažďování, ukládání na nosiče, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace osobních údajů;
p) **zpracovate**l - každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona;
q) **zveřejněný osobním údajem** - osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

2. POVINNOSTI OSOB PŘI SPRÁVĚ A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

2.1 VEDENÍ SPOLEČNOSTI

Vedení společnosti v rámci své odpovědnosti za ochranu osobních údajů, samo nebo prostřednictvím pověřených osob:

a) zajišťuje podmínky pro řádnou ochranu osobních údajů, ve smyslu GDPR a ostatních právních předpisů, včetně příslušné legislativy Evropské unie;
b) zajišťuje průběžné vzdělávání zaměstnanců v oblasti ochrany osobních údajů, a to v první řadě formou jejich samostudia, v případě potřeby formou školení, či konzultací;
c) odpovídá za personální zajištění ochrany osobních údajů;
d) zajišťuje zdroje informací ke správné praxi při ochraně osobních údajů, včetně kontaktů na osoby odborně schopné konzultovat předmětnou problematiku, případně na pověřence pro ochranu osobních údajů, pokud je jmenován;
e) zajišťuje kontrolu činnosti při ochraně osobních údajů;
f) zajišťuje realizaci opatření v oblasti ochrany osobních údajů, včetně znalosti povinností osob přicházejících do styku s osobními údaji;
g) v případě potřeby provádí posouzení dopadu činnosti na ochranu osobních údajů,
h) v případě potřeby provádí předběžné konzultace s Úřadem pro ochranu osobních údajů (dále jen „**ÚOOÚ**“);
i) vede záznamy o zpracování osobních údajů;
j) ohlašuje případy narušení bezpečnosti osobních údajů do 72 h od doby, kdy se jako správce o narušení dozví, na ÚOOÚ a pokud je to třeba i dotčeným osobám, o jejichž osobní údaje se jednalo;
k) umožní přenositelnost osobních údajů k jinému správci ve vhodném formátu;
l) v případě potřeby jmenuje pověřence pro ochranu osobních údajů;
m) plní pokyny dozorových orgánů v oblasti ochrany osobních údajů.

2.2 OSTATNÍ OSOBY PŘICHÁZEJÍCÍ DO STYKU S OSOBNÍMI ÚDAJI

Osoby přicházející do styku s osobními údaji jsou povinny:

a) zpracovávat osobní údaje v souladu s GDPR a příslušnými zákony, ostatními právními normami, jakož i dalšími předpisy EU a mezinárodními smlouvami, které se na tuto problematiku při jejich práci vztahují;
b) zachovávat mlčenlivost o osobních údajích a přijatých opatřeních k jejich ochraně, a to i po skončení svého pracovněprávního nebo smluvního vztahu u společnosti;
c) zabránit neoprávněnému čtení, pozměnění, smazání, či znepřístupnění osobních údajů, nevytvářet kopie software nebo listin s osobními údaji pro jinou než pracovní potřebu a nepřipustit takové jednání ani jiným osobám, například tím, že nebude možné z nosičů či úložišť počítačových dat kopírovat na jiné nosiče

větší množství osobních údajů bez toho, že by toto kopírování schválilo a zároveň i technicky umožnilo (např. zadáním hesel) současně dvě nebo více osob;

d) při používání výpočetní techniky používat pouze bezpečný hardware a software, a to bezpečným způsobem a bezodkladně hlásit veškeré nestandardní projevy používané výpočetní techniky příslušným odborníkům;

e) dodržovat zásady bezpečného používání výpočetní techniky zejména používáním vhodných hesel a dbát na jejich ochranu před prozrazením; nenavštěvovat rizikové webové stránky apod., okamžitě hlásit jakékoli důvodné podezření na ohrožení bezpečnosti osobních údajů.

3. SOUHLAS SUBJEKTU ÚDAJŮ

1. V případě, pokud subjekt údajů souhlasí se zpracováním osobních údajů, je společnost povinna na jeho písemnou výzvu vydat potvrzení, zda osobní údaje nadále zpracovává či nikoliv. Subjekt údajů má dále právo získat přístup k osobním údajům včetně účelu jejich zpracování, kategorii zpracovávaných údajů, včetně seznamu osob, které jsou příjemci osobních údajů nebo kterým jsou osobní údaje zpřístupněny včetně předávání osobních údajů do zahraničí.

2. Subjekt údajů může souhlas se zpracováním osobních údajů kdykoliv odvolat. Subjekt údajů má dále právo domáhat se opravy (v případě zpracování nepřesných osobních údajů), domáhat se výmazu osobních údajů, vznést námitku proti zpracování osobních údajů, dále má právo na přenositelnost osobních údajů, na podání stížnosti u dozorového úřadu, právo na omezení zpracování osobních údajů, právo získat opis zpracovávaných osobních údajů.

3. Osobní údaje zpracovávané na základě souhlasu subjektu údajů nebudou zpracovávány na základě automatizovaného rozhodování včetně profilování.

4. TECHNICKÁ OPATŘENÍ K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

4.1 UCHOVÁVÁNÍ DAT

Písemnosti a jiné hmotné nosiče dat, které obsahují osobní údaje, je možné uchovávat pouze v uzamykatelných místnostech a pokud možno i uzamykatelných skříních. Mimo uzamykatelné místnosti lze mít písemnosti a jiné hmotné nosiče dat, které obsahují osobní údaje, uloženy např. na chodbách, jen za podmínky, že se jedná o chodby, kam nemají volný přístup jiné osoby než zaměstnanci společnosti a tyto skříně jsou trvale uzamčeny vhodnými zámky a jsou konstruovány tak, aby je nebylo možné snadno vypáčit, či jinak do nich

snadno vniknout násilím. Podrobnější pokyny k uzamykání místností a skříní, jakož i k přidělování, ukládání a výrobě klíčů vydávají jednatelé společnosti.

4.2 ELEKTRONICKÉ DATOVÉ SOUBORY

Elektronické datové soubory obsahující osobní údaje je možné uchovávat v paměti počítače pouze:

a) je-li přístup k takovýmto souborům chráněn doménovým jménem, které umožní zpětně zjistit, kdo měl k osobním údajům přístup a komu byly osobní údaje případně předány a heslem, které musí mít nejméně 6 znaků, z nichž alespoň jeden musí mít podobu čísla nebo znaku (přiměřené heslo);

b) je-li přístup k užívání počítače, v jehož paměti jsou tyto soubory umístěny, chráněn přiměřeným heslem (softwarovým či hardwarovým) nebo vhodným zámkem;

c) tak, že veškerá data musí být pravidelně zálohována a zálohová média musí být v přiměřených intervalech měněna, přičemž musí být zabráněno neoprávněnému přístupu k datovým nosičům;

d) tak, aby příslušné osoby měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby.

e) Podrobné pokyny k ochraně datových souborů (včetně hardware, které využívají) a k přidělování, ukládání a tvorbě domén, hesel a dalších ochranných prvků, obsahuje chráněná doložka k této směrnici, k níž mají přístup jen pověřené osoby uvedené v chráněné doložce.

4.3 LISTINNÉ NOSIČE DAT, CITLIVÉ OSOBNÍ ÚDAJE, KAMEROVÉ A AUDIO ZÁZNAMY

a) Osobní údaje, které nejsou v elektronické podobě, musí být chráněny v uzamykatelných místnostech, případně i uzamykatelných skříních, od nichž mají klíče jen pověřené osoby, které je nesmí zpřístupnit žádným nepovolaným osobám. Tam, kde se pracuje s citlivými údaji, musí být citlivé osobní údaje zabezpečeny zvlášť důkladně a musí být minimalizován okruh osob, které k nim mohou mít přístup).

b) Veškeré listiny a jednorázově použitelné datové nosiče i jiné jednorázově použitelné materiály obsahující osobní údaje, musí být poté, co skončí důvody pro uchovávání osobních údajů, které se na nich nalézají, zničeny, či jinak zlikvidovány, pod dohledem osoby určené společností. Pokud likvidaci listin, datových nosičů, či jiných materiálů obsahujících osobní údaje, provádí pracovník (zaměstnanec, či externí pracovník) společnosti, musí být u takové činnosti přítomny nejméně dvě osoby, které nejsou vzájemně osobami blízkými. Při likvidaci většího množství písemností a jiných hmotných nosičů dat, které obsahují osobní údaje, se sepisuje likvidační protokol, ve kterém se uvede datum, místo likvidace a její způsob; stejně se postupuje při likvidaci listin, datových nosičů, či jiných materiálů obsahujících

citlivé osobní údaje. Likvidace osobních údajů na opakovatelně použitelných nosičích se provádí tak, aby je nebylo možno ani zpětně obnovit (nosiče není třeba ničit), přičemž i v tomto případě musí být likvidaci přítomny nejméně dvě osoby, které nejsou vzájemně osobami blízkými. V případě likvidace listin, datových nosičů, či jiných materiálů obsahujících osobní údaje externí společností musí být prováděna alespoň občasná namátková kontrola zástupcem společnosti nebo jinou pověřenou osobou.

c) Tzv. citlivé osobní údaje musí být uchovávány, jen pokud je to nezbytné k plnění zákonných povinností a musí být chráněny zvláště pečlivě před přístupem třetím osobám. Přesnější pokyny k ochraně citlivých osobních údajů, mohou být podrobněji upraveny v jiných interních dokumentech společnosti. Tam, kde není zřejmé, že se citlivé osobní údaje shromažďují na základě zákona, musí být získány i kvalifikované souhlasy se zpracováním těchto citlivých osobních údajů od příslušných subjektů údajů, nebo jejich zákonných zástupců.
d) Veškeré kamerové, či audio záznamy, musí být pořizovány jen v souladu s příslušnými právními předpisy, veškeré kamery a ukládání záznamů z těchto kamer, musí být posouzeny z hlediska jejich dopadu na ochranu osobních údajů. Záznamy z těchto kamer musí být kódovány a ve formě tzv. černé skříňky musí být uloženy mimo dosah nepovolaných osob. Pokud není důvodná potřeba delšího uchování, např. jako důkaz pro pozdější právní úkony, musí být kamerové záznamy mazány nejpozději ve lhůtách přiměřených účelu jejich ukládání. Tam, kde jsou kamery umístěny i z důvodu bezpečnosti a ochrany zdraví při práci, včetně využití pro náhradu škody zaměstnanci, se považuje **lhůta pro vymazání kamerových záznamů** za přiměřenou, pokud jsou kamerové záznamy vymazány nejpozději **do 21 dnů od jejich pořízení**, a to vzhledem ke lhůtám, ve kterých jsou zaměstnanci povinni hlásit zaměstnavateli vznik škody podle zákoníku práce.
e) Žádné kamerové, či audio záznamy, nesmí být pořizovány tam, kde by mohly urážet lidskou důstojnost nebo zvyšovat nebezpečí úrazu či vzniku škody.
f) O umístění kamer nebo pořizování audiozáznamů musí být všechny osoby řádně informovány informačními tabulkami, či jiným vhodným způsobem, včetně informace, kde mohou získat o takových záznamech podrobnější informace.
g) Podrobné pokyny k technickým a organizačním opatřením na ochranu kamerových záznamů před ztrátou, zničením nebo zneužitím, mohou být upraveny v chráněné doložce k této směrnici, k níž budou mít přístup jen pověřené osoby uvedené v takové chráněné doložce.

5. POSOUZENÍ DOPADU ČINNOSTI NA OCHRANU OSOBNÍCH ÚDAJŮ

1. Pokud je pravděpodobné, že určitý druh zpracování osobních údajů ve společnosti, nebo u jejího zpracovatele, zejména při využití nových (počítačových) technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, vypracuje společnost posouzení dopadu své činnosti na ochranu osobních údajů. Posouzení dopadu činnosti na ochranu osobních údajů musí obsahovat systematický popis zamýšleného zpracování, posouzení rizik, provedení testu proporcionality a podobně. V posouzení dopadu činnosti na ochranu osobních údajů musí být také jasně definována přijatá bezpečností opatření a záruky k ochraně osobních údajů.

2. Společnosti nesmí provádět systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad. Zejména jsou povinni zkoumat, zda nejsou podle výpočetní techniky, zvláště pak v případě využití umělé inteligence, zaměstnanci, zákazníci, či jiné osoby, tříděny do určitých skupin a v důsledku takového roztřídění do skupin zda pak nejsou bez konečného rozhodnutí člověka určována jejich práva, či povinnosti (např. rozhodování o změně pracovního zařazení, o výši mzdy, či benefitů, o skončení pracovního poměru a podobně).

3. Společnost nesmí provádět rozsáhlé zpracování zvláštních kategorií údajů (citlivých údajů, včetně biometrických), nebo rozsáhlé systematické monitorování veřejně přístupných prostorů, např. kamerovými systémy.

6. KONZULTACE S ÚŘADEM PRO OCHRANU OSOBNÍCH ÚDAJŮ

Vzhledem k tomu, že v rámci posouzení dopadu činnosti společnosti na ochranu osobních údajů nebylo zjištěno, že by určitý druh zpracování osobních údajů ve společnosti, nebo u jejího zpracovatele, zejména při využití nových (počítačových) technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování osobních údajů, mohl mít za následek vysoké riziko pro práva a svobody fyzických osob, v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika, společnosti bude sledovat, zda nedošlo ke změně těchto poměrů ve společnosti. Pokud by v souvislosti se změnami zpracování osobních údajů ve společnosti došlo k situaci, že by vzniklo vysoké riziko pro práva a svobody fyzických osob a nebylo by známo, jaká přijmout opatření ke zmírnění

tohoto rizika, společnost zajistí, aby byla provedena předchozí konzultace řešení takového stavu s Úřadem pro ochranu osobních údajů.

7. POVINNOST VÉST ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. Společnost je povinna zajistit, aby byly o veškerém zpracování osobních údajů vedeny záznamy, na základě kterých bude možné kdykoli doložit, kdo byl jejich správcem (jméno, příjmení a kontaktní údaje), případně kdo vystupoval jako pověřenec pro ochranu osobních údajů, účely zpracování osobních údajů, popis kategorií subjektů údajů a kategorií osobních údajů, kategorie příjemců, včetně příjemců ve třetích zemích nebo mezinárodních organizacích, informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, doložení vhodných záruk ochrany osobních údajů, plánované lhůty pro výmaz jednotlivých kategorií osobních údajů (podle skartačních předpisů), obecný popis technických a organizačních bezpečnostních opatření.

2. Vedení záznamů o zpracování osobních údajů je možné provádět jak v elektronické tak i papírové podobě. Záruky ochrany osobních údajů vyplývají z této směrnice, ve které je i obecný popis technických a organizačních bezpečnostních opatření).

3. Pokud si společnost nechává zpracovávat osobní údaje od jiné osoby, je povinností společnosti zajistit, aby byly osobní údaje zpracovávány na základě řádně uzavřené smlouvy o zpracování osobních údajů.

8. POVINNOST OHLAŠOVAT PŘÍPADY NARUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

1. Veškeré případy narušení bezpečnosti osobních údajů budou nahlášeny Úřadu pro ochranu osobních údajů do 72 h od doby, kdy se jako společnost správce o takovém narušení dozví. Při tom jsou povinni zajistit, aby bylo řádně rozlišeno, zda se jedná skutečně o narušení bezpečnosti osobních údajů, či zda je riziko pro ochranu osobních údajů v takovém případě bezvýznamné.

2. Pokud hrozí bezprostřední riziko pro práva subjektů údajů, společnost zajistí, aby tyto osoby byly také přiměřeným způsobem informovány o rizicích spojených s předmětným narušením bezpečnosti osobních údajů a byly jim poskytnuty i vhodné informace, jak případné hrozící škodě zabránit, nebo ji alespoň minimalizovat).

3. Pokud došlo k narušení bezpečnosti osobních údajů, je třeba předtím než bude taková skutečnost nahlášena Úřadu pro ochranu osobních údajů, řádně zanalyzovat situaci, vyhodnotit míru rizika pro společnost i subjekty, připravit a spustit nápravná opatření a připravit plán oznámení dotčeným osobám. Teprve pak je vhodné oznámit Úřadu pro ochranu osobních údajů, co se událo, včetně informace co již bylo provedeno k minimalizaci škod a jaké kroky budou provedeny do budoucna.

4. Dojde-li k narušení bezpečnosti osobních údajů je nutno nejprve odstranit zdroj porušení ochrany osobních údajů, poté musí být provedena informace dle předchozích odstavců tohoto článku.

5. Je-li jmenován ve společnosti pověřenec pro ochranu osobních údajů, veškeré kroky týkající se reakce na narušení ochrany osobních údajů, musí být konzultovány s tímto pověřencem pro ochranu osobních údajů a tam kde je to možné, prováděny jeho prostřednictvím.

9. PŘENOSITELNOST OSOBNÍCH ÚDAJŮ

1. O veškerém zpracování osobních údajů jsou vedeny záznamy, na základě kterých bude možné kdykoli doložit, kdo byl jejich správcem (jméno, příjmení a kontaktní údaje), případně kdo vystupoval jako pověřenec pro ochranu osobních údajů, účely zpracování osobních údajů, popis kategorií subjektů údajů a kategorií osobních údajů, kategorie příjemců, včetně příjemců ve třetích zemích nebo mezinárodních organizacích, informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, doložení vhodných záruk ochrany osobních údajů, plánované lhůty pro výmaz jednotlivých kategorií osobních údajů (podle skartačních předpisů), obecný popis technických a organizačních bezpečnostních opatření.

2. Při přenosu osobních údajů konkrétní osoby k jinému správci nebude nepříznivě dotčena práva a svobody jiných osob, nebo práva duševního vlastnictví).

3. Na přenositelnost osobních údajů musí být subjekt údajů výslovně upozorněn a toto právo musí být uvedeno zřetelně a odděleně od jakýchkoli jiných informací již v okamžiku první komunikace se subjektem údajů, tedy s osobami, jejichž osobní údaje mají být zpracovávány.

10. VÝMAZ OSOBNÍCH ÚDAJŮ A PRÁVO NA ZAPOMENUTÍ

1. Společnost zajistí, aby byly bez zbytečného odkladu vymazány veškeré osobní údaje, pokud:
   a) Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány.
   b) Subjekt údajů odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování.
   c) Osobní údaje byly zpracovány protiprávně.
   d) Pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí v souvislosti s nabídkou služeb informační společnosti.

2. Společnost provede přiměřené kroky, včetně technických opatření k vymazání veškerých osobních údajů, včetně záloh a automatických obnov IT systémů.

11. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

1. V případě, že jsou k tomu splněny podmínky, je povinností společnosti jmenovat pověřence pro ochranu osobních údajů.

2. Pokud by byl jmenován pověřenec pro ochranu osobních údajů, ať již proto, že společnost naplňuje podmínky pro jeho povinné jmenování, nebo proto, že jej společnost jmenovala dobrovolně, bude se činnost pověřence pro ochranu osobních údajů řídit samostatnou speciální směrnicí.

3. Pokud není pověřenec pro ochranu osobních údajů jmenován, vždy musí nejvyšší vedení společnosti zajistit, aby měla společnost osobu, která je zodpovědná za plnění povinností v oblasti ochrany osobních údajů.

12. PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

1. Pokud je nezbytné předávat osobní údaje do zahraničí, je povinností společnosti zajistit, aby byly takové osobní údaje předávány jen vhodným a spolehlivým obchodním partnerům, aby bylo před předáním osobních údajů do zahraničí řádně prozkoumáno právního prostředí v zemi smluvního partnera, včetně ověření, zda existují mezinárodní smlouvy se zemí obchodního partnera na ochranu osobních údajů.

2. Při předávání osobních údajů do zahraničí musí být vždy na takové předání uzavřena příslušná smlouvy s obchodním partnerem, která bude řešit i ochranu osobních údajů, včetně sankcí za její porušení).

13. ZÁVĚREČNÁ USTANOVENÍ

1. Jednotlivá opatření podle této směrnice mohou být podrobněji rozpracována ve specializovaných směrnicích, pokynech, nebo jiných relevantních dokumentech společnosti. Otázky neupravené touto směrnicí se řídí obecně závaznými právními předpisy, a to jako českými, tak předpisy Evropské unie, včetně doporučení.

2. Společnost je povinna řádně a včas komunikovat s Úřadem pro ochranu osobních údajů, a zajistit, aby byl o komunikaci s Úřadem pro ochranu osobních údajů vždy řádně a včas informován výbor spolku.

3. Tato směrnice nabývá účinnosti dnem 1. května 2022.

4. Jakékoliv změny či doplnění této směrnice schvaluje předsedkyně výboru.