TRIMILL, a.s.

se sídlem Jasenice 2061, 755 01 Vsetín, IČ 25598325

SMĚRNICE

Politika a zásady ochrany osobních údajů

I. Úvodní ustanovení

Směrnice Politika a zásady ochrany osobních údajů formuluje základní cíle a principy při zpracování a ochraně osobních údajů u společnosti TRIMILL, a.s. (dále jen ***„Společnost"*** nebo ***„TRIMILL"***).

Dokument současně deklaruje vůli vedení TRIMILL informovat zaměstnance, zpracovatele, příjemce a třetí strany o významu ochrany osobních údajů a o jeho podpoře pro zavedení řízeného systému zpracování a ochrany osobních údajů, který je v souladu s 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) – General Data Protection Regulation (dále jen „GDPR"). Dokument vyjadřuje podporu vedení TRIMILL pro zavedení, provozování, hodnocení výkonnosti a neustálé zlepšování tohoto systému.

II. Hlavní cíle ochrany osobních údajů

Hlavními cíli ochrany osobních údajů jsou:

1) Zajištění ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů.
2) Zajištění práv fyzických osob v souvislosti se zpracováním jejich osobních údajů.
3) Udržování trvalého souladu s požadavky GDPR.
4) Udržování souladu s dalšími právními a technickými požadavky stanovenými platnými souvisejícími právními předpisy a technickými normami.
5) Zajistit schopnost předcházet a zvládat nežádoucí události.
6) Prosazení odpovědnosti zaměstnanců při zajišťování ochrany osobních údajů.
7) Neustálé zlepšování vhodnosti, přiměřenosti a účinnosti systému řízení ochrany osobních údajů.

III. Principy zpracování a ochrany osobních údajů

Zpracování a ochrana osobních údajů v prostředí Společnosti se řídí následujícími principy GDPR:

1. Zákonnost zpracování osobních údajů

Ve Společnosti jsou zpracovávány osobní údaje zejména za účelem:

1) Služeb, Interních procesů a provozu organizace
    a) smluvní vztahy s dodavateli a odběrateli,
    b) pracovně právní a mzdová agenda,
    c) ochrana majetku.

K těmto účelům zpracování jsou zpracovány záznamy o činnostech zpracování, které jsou uvedeny v příloze č. 1 tohoto dokumentu.

Všechna zpracování jsou prováděna na základě stanoveného právního základu, který je uveden v příslušném záznamu o činnostech zpracování pro daný účel.

Odpovědnost za udržování aktuálnosti a úplnosti záznamů o činnostech mají příslušní vedoucí zaměstnanci.

Pokyny pro realizaci tohoto principu jsou podrobněji rozpracovány ve Směrnici „Povinnosti osob při zpracování osobních údajů".

2. Omezení účelem

Ve Společnosti jsou osobní údaje shromažďovány jen pro předem vymezené, výslovně vyjádřené a legitimní účely.

Pro naplnění principu jsou uplatňována následující pravidla:

1) Pro každé zpracování je vždy předem stanoven konkrétní a legitimní účel.
2) Právní důvod zpracování je vztažen vždy k jednotlivým účelům.
3) Údaje jsou zpracovávány pouze pro daný účel a je zakázáno je využívat pro jiné účely.
4) Údaje shromážděné pro různé účely je zakázáno spojovat, jsou evidovány a zpracovávány odděleně, vyjma účelů, jejichž spojení umožňuje zvláštní zákon anebo pro účely archivace ve veřejném zájmu.

Odpovědnost za dodržování tohoto principu mají všichni vedoucí zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.

Pokyny pro realizaci tohoto principu jsou podrobněji rozpracovány ve Směrnici „Povinnosti osob při zpracování osobních údajů".

3. Minimalizace údajů a omezení uložení

Ve Společnosti jsou osobní údaje zpracovávané pouze pro stanovený účel a pouze po nezbytně dlouhou dobu.

Pro naplnění principu jsou uplatňována následující pravidla:

1) Je zakázáno shromažďovat a zpracovávat:
    - nepřiměřené osobní údaje,
    - nerelevantní osobní údaje,

- osobní údaje, které nejsou nezbytné.

Toto pravidlo je u stávajících účelů zpracování zavedeno tím, že v záznamech o činnostech zpracování jsou vyjmenovány základní typy a kategorie údajů.

U případných budoucích účelů zpracování bude, v souladu s pravidly standardní ochrany, pravidlo uplatňováno stejným způsobem.

Odpovědnost za dodržování tohoto principu mají všichni vedoucí zaměstnanci a zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.

2) Osobní údaje jsou uchovávány v listinné i elektronické podobě pouze po omezenou dobu, odpovídající účelu zpracování. Po ukončení této doby jsou likvidovány nebo mazány v souladu s pravidly a lhůtami stanovenými v obecně závazných právních předpisech.

   Odpovědnost za dodržování tohoto principu mají u listinné podoby všichni vedoucí zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.

   Odpovědnost za dodržování tohoto principu u elektronické podoby má zaměstnanec nebo osoba (fyzická osoba podnikající nebo právnická osoba na základě uzavřeného smluvního vztahu), odpovídající za správu a provoz informačních technologií.

3) Osobní údaje jsou přístupné jen co nejmenšímu počtu osob.

   Toto pravidlo je zavedeno tím, že jsou určena a zavedena pravidla pro řízení přístupu k osobním údajům v listinné i elektronické podobě a dále pro zveřejňování, sdílení a předávání informací.

   Odpovědnost za dodržování tohoto principu mají všichni vedoucí zaměstnanci a zaměstnanci.

Pokyny pro realizaci tohoto principu jsou podrobněji rozpracovány ve Směrnici „Povinnosti osob při zpracování osobních údajů“.

4. Přesnost osobních údajů

Ve Společnosti jsou zpracovávané pouze přesné osobní údaje. Principy aktualizace zpracovávaných dat jsou nastaveny způsobem odpovídajícím kritičnosti jejich možných dopadů na subjekty údajů.

Zaměstnanec odpovědný za přípravu a uzavření pracovní smlouvy poučuje každého zaměstnance o povinnosti hlásit případné změny všech jím předaných osobních údajů.

Odpovědnost za stanovení způsobu ověřování přesnosti dat mají všichni vedoucí zaměstnanci, v jejichž působnosti a agendách se osobní údaje zpracovávají.

5. Korektnost a transparentnost při zpracování osobních údajů

Při zpracování osobních údajů v působnosti TRIMILL jsou subjekty údajů transparentně informovány těmito způsoby:

- základní informace na webových stránkách společnosti TRIMILL www.trimill.cz, dostupná všem subjektům údajů,
- doplňující písemná informace o zpracování osobních údajů poskytované k jednotlivým agendám vyžadujícím souhlas se zpracováním osobních údajů a dále k vybraným agendám,
- písemná informace o zpracování osobních údajů pro účely pracovněprávní agendy poskytovaná novým zaměstnancům,
- informace o monitoringu objektů či prostor kamerovými systémy,
- informace v dalších vnitřních předpisech.

Ve Společnosti jsou stanoveny postupy pro výkon práv subjektu údajů. Těmito právy se rozumí:

- právo na přístup k osobním údajům,
- právo na opravu nepřesných osobních údajů,
- právo na výmaz (být zapomenut),
- právo na omezení zpracování,
- právo na přenositelnost,
- právo vznést námitku proti zpracování osobních údajů,
- právo nebýt předmětem automatizovaného individuálního rozhodování.

Výkon práv subjektů údajů v TRIMILL řídí příslušní vedoucí zaměstnanci, do jejichž působnosti příslušný požadavek na uplatnění práva spadá.

Postupy pro realizaci tohoto principu jsou podrobněji rozpracovány v Pokynech

- „Povinnosti osob při zpracování osobních údajů“,
- „Výkon práv subjektu údajů“.

6. Důvěrnost, integrita a dostupnost osobních údajů

Ve Společnosti jsou přijata vhodná technická a organizační opatření odpovídající kontextu a účelům zpracování osobních údajů.

Veškerá technická a organizační opatření jsou přijata na základě provedené analýzy informačních rizik. Analýza rizik byla provedena na základě:

a) posouzení hrozeb působících na zařízení, systému a další aktiva, v rámci kterých jsou zpracovávány osobní údaje,

b) posouzení hrozeb pro práva a svobody subjektů údajů.

Na základě závěrů z provedené analýzy rizik byla implementována přiměřená organizační a technická opatření pro zajištění odpovídající úrovně ochrany zpracovávaných osobních údajů.

Pro provedení analýzy rizik byla stanovena metodika hodnocení rizik, která vychází z požadavků vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických

bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). V rámci provedené analýzy rizik byly současně zohledněny hrozby, které představují zejména možnost náhodného nebo protiprávního zničení, ztráty, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů nebo neoprávněný přístup k nim.

Za stanovení a aktuálnost technických a organizačních opatření vyplývajících z analýzy rizik odpovídá zaměstnanec nebo osoba (fyzická osoba podnikající nebo právnická osoba na základě uzavřeného smluvního vztahu), odpovídající za správu a provoz informačních a komunikačních technologií a příslušní vedoucí zaměstnanci.

Pokyny pro realizaci tohoto principu, včetně stanovení odpovídajících technických a organizačních opatření pro oblast fyzické, personální, administrativní a počítačové bezpečnosti, jsou podrobněji rozpracovány v následujících Pokynech ředitele společnosti a dokumentech:

- Pokyn „Povinnosti osob při zpracování osobních údajů“
- Pokyn „Výkon práv subjektu údajů“,
- Pokyn „Ochrana osobních údajů“,
- Pokyn „Bezpečnost ICT“,
- Pokyn „Ochrana osobních údajů v kamerovém systému“,
- Metodika analýzy rizik GDPR,
    - Seznam hrozeb a opatření,
    - Plán zvládání rizik,
- Nástroj pro hodnocení rizik GDPR.

7. Odpovědnost správce osobních údajů

Správcem osobních údajů je Společnost.

Správce je povinen zajistit soulad s GDPR a tento soulad prokazuje:

1) zpracováním Politiky a zásad ochrany osobních údajů, stanovující:
    - cíle ochrany osobních údajů,
    - principy zpracování a ochrany osobních údajů,
    - odpovědnosti za realizaci principů,
    - odpovědnost za kontrolu.
2) zpracováním záznamů o činnostech zpracování,
3) rozpracováním Politiky a zásad ochrany osobních údajů do Směrnic a dokumentů uvedených v bodě 6,
4) zajištěním principů záměrné a standardní ochrany osobních údajů, realizované:

- návrhem vhodných technických a organizačních opatření záměrné ochrany stanovených před zahájením vlastního zpracování, ještě v době určování prostředků pro zpracování osobních údajů,
- zavedením a udržováním záměrné a standardní ochrany přiměřenými technickými a organizačními opatřeními založenými na výsledcích analýzy rizik.

5) dodržováním všech zásad GDPR ve vztahu ke zpracovatelům a dalším správcům.